CENAA

Information Warfare as a Geopolitical Tool

CENAA.ORG

CENAA

CENTRE
FOR EUROPEAN AND NORTH
ATLANTIC AFFAIRS

Tomáš Čižik

AUTHOR: Tomáš Čižik
RELEASED: April, 2017

Tomáš Čižik, Director, Centre for European and North Atlantic Affairs (CENAA)
e-mail: cizik@cenaa.org

Introduction

Since Russian annexation of Crimea, in March 2014, international community experiences massive use of information warfare in international affairs. In last 3 years, informational warfare became one of the most challenging issues not only for Europe and European Union, but also for the United States. Information warfare can be considered now as a very powerful tool, by which political integrity of states and alliances can be influenced. It is used by not only state actors (national states), but also non-state actors, such as ISIS to achieve various goals. The main goal of this article is to show, how easily and non-visibly can information warfare influence development in international affairs.

Information Warfare – A Short Definition

For better understanding of information warfare and its power, it is crucial to define, what information warfare is and why it is so powerful and dangerous tool in international affairs. Information warfare is a subpart of hybrid warfare. Hybrid warfare according to Frank Hoffman is "the combination of the multiple types of warfare used simultaneously to flexibly fit the political goals in particular circumstances (Hoffman, 2007, 27). He continues with statement that most important is it's asymmetric and flexible nature. Hybrid warfare is composed of 4 main parts: information warfare, psychological operation, use of special forces and cyber operation. For the purpose of this article, only the information warfare will be described into details. The definition of information warfare varies.

According to Nichiporuk (1999, 188) information warfare is the process of "protecting one's own sources of battlefield information, and at the same time, seeking to deny, degrade, corrupt, or destroy the enemy's source of battlefield information". Information warfare is composed of "six pre-existing subareas", which are: "operational security, electronic warfare (EW), psychological operations (PSYOPs), deception, physical attack on information processes, and information attack on informational processes". This definition can be considered as incomplete, because it defines information warfare mainly from military point of view and missing the crucial definition of information warfare conducted nowadays by state and non-state actors. Author's definition does not cover the manipulation of information on internet, social networks, media or propaganda itself, which creates a huge part of today's information warfare. We have to differentiate between cold war propaganda and propaganda of recent days. "In Soviet times the concept of truth was important. Even when they were lying they took care to prove what they were doing was 'the truth'. Now no one even tries providing the 'truth'. You can just say anything. Create realities" (Pomerantsev, n.d.).

ISSN 1339-7168

So nowadays, information warfare is conducted mainly in social area, where the main target are civilians and their capability to differentiate between correct information and information that is intended to confuse them. There is clear shift from strictly military use of information warfare during Soviet times to influence adversary from outside to information warfare aimed to civilians to influence adversary from inside. Information warfare became very dangerous tool in international affairs, which can fulfil one's own political and military goals without need to send army into foreign country or without any significant investments into hard power military capabilities. Moreover, information warfare is not limited by boundaries, it can reach foreign state easily via internet or social networks.

Information warfare can be used on domestic and also on international level. On domestic level, it is used to justify state actions in eyes of citizens, or manipulate their minds that certain actions of other states are unjustified and tend to harm interests of their own country. On international level, information warfare is used, as was described above, to create realities, to undermine trust of citizens into their political elites and democratic institutions, to undermine trust of states to each other, to create chaos and to invoke fear among citizens (Čižik, 2016).

The main tool of information warfare is information and "can be used in several ways, such as manipulation, i.e. provision of erroneous information to the enemy with an aim to confound or to affect the decision-making, [and] to use information to one's advantage is to induce fear and thus dissuade the enemy from action. This example refers to classic deterrence, characteristic of the Cold War period".

Moreover "[i]nformation war does not use information in just one fashion; there is always a combination of several ways it gets employed with the aim of achieving the best possible effect. What's more, the advent of the Internet has opened new opportunities of virtually unlimited manipulation with information: commonly referred to as propaganda" (Čižik, 2015).

Globalization and information era allowed information warfare to gain new dimension. States, coalitions and alliances became more interconnected and interdependent and therefore it is easier to influence more than one state at the time. One's state action will influence the decision-making and actions taken of other state and vice versa. Coalitions and alliances are even more interconnected and interdependent than independent states. Based on most recent development in the international relations it seems that democracy is more vulnerable to information warfare than other forms of government. According to Thomas Rid (n.d.), professor of security studies at King's College London: "[i]t's political engineering, social engineering on a strategic level". This "social engineering" is provided by social media and it is difficult to counter it. Main reason is that social media platforms are struggling with verification of information sources "without limiting freedom of speech" (Ismail, 2016). As author further states "democracy has been undercut by social media in the past and it can have an immense influence on the democratic process".

There can be found very recent examples (Brexit, US presidential elections) on how information warfare, propaganda and manipulation with information can influence people's voting. Both, Brexit and US presidential elections were accompanied by massive social media campaigns. Both campaigns contained factual inaccuracies, distortions and myths that clearly influenced the outcome of both events. For example, in Brexit case, the "inaccurate statement of Boris Johnson […] that the UK sends Brussels £350m a week" can be considered as incorrect information that was massively spread via social media and one of the reasons why UK citizens voted for "leave" (Lythgoe and Dixon, 2016).

As can be seen above, information warfare and carefully prepared information campaigns are powerful weapon by which can be successfully influenced whole nations. In following part, the main aim will be given to Russian information warfare and Russian attempts to influence decision-making of European leaders and possibly (in long-term perspective) dissolve EU and NATO.

Russian Information Warfare and Propaganda as a Geopolitical Tool

In 2007, it became clear that Russia is interested in regaining its status of "great power" and its behavior became more and more aggressive throughout following years. It started at Munich Security Conference in 2007, where Vladimir Putin said that "Russia should play and increasingly active role in world affairs" (The Washington Post, 2007), it follows by "the suspension of the implementation of the Treaty on Conventional Armed Forces in Europe in 2007, Russian "peacekeeping mission" in Abkhazia followed by the Russian intervention to Abkhazia and South Ossetia in 2008, large military exercises on Russia's western borders near Georgia and Ukraine, or multiple incursions against the air sovereignty of many NATO member states, which continues to this day at high rates" (Čižik, 2016). According to SIPRI (n.d.) Russian military budget rose from 3,3 % of GDP in 2008 to 4,5 % in 2014, in number it means increase from 56,2 billion dollars to 84,5 billion dollars. Higher expenditures into military were accompanied also by military reform, which took place in 2008 after the Russia-Georgian war. Military reform was "launched to address technological and organizational weaknesses of the Russian military" (Beznosiuk, 2016). All these measures resulted on annexation of Crimean Peninsula in March 2014.

According to Darczewska (2014) "[t]he Crimean operation has served as an occasion for Russia to demonstrate to the entire world the capabilities and the potential of information warfare. Its goal is to use difficult to detect methods to subordinate the elites and societies in other countries by making use of various kinds of secret and overt channels (secret services, diplomacy, and the media), psychological impact, and ideological and political sabotage".

As author further argues the annexation of Crimea showed the essence of information warfare – the ability of resistance was diminished or was completely missing, mainly due to psychological and informational treatment (intoxication) that Russian-speaking citizens underwent.

Since 2014, there are visible massive investments of the Russian Federation in media. A case in point, the budget for the RT agency (formerly Russia Today) in the period 2007-2015 was approximately 120 million USD, reaching its height over 2013-2014 with 400 million USD. Sputnik News in conjunction with Ria Novosti have a combined operating budget of 200 million USD per year, not to mention the local media involved in the spreading of propaganda (DELFI 2015). Without any doubts, Russia's investments into development of tools of information warfare are not coincidence. In Russian Military doctrine from December 2014 is information treated as cheap and universal weapon, which is easily accessible and permeated all states borders without restrictions. As one of the main internal military risks for Russian Federation, which is mentioned in Military Doctrine (2014) are "subversive information activities against the population, especially young citizens of the State, aimed at undermining historical, spiritual ad patriotic traditions related to the defense of the Motherland". Previous statements show that Russia is aware of the effectiveness of the information warfare and the impacts it can have on civilians on domestic and international level. In addition, in December 2016, President Putin signed the new Russian information security doctrine, which outlines the "Russian government's perception of threats to its national interest and security in the information sphere and priorities for countering those threats" (Coalson, 2016). As author further argues "among the threats indentified in the document are the expansion of the use of 'information-psychological influences' by foreign intelligence services 'aimed at the destabilization' of various regions of the world, including Russia". Russia itself acknowledges the power of information warfare and it is also using information warfare to its own benefit.

Information warfare has a long tradition in Russia. "It is derived directly from *spetspropaganda* (special propaganda) theory, which was first taught as a separate subject in 1942 at the Military Institute of Foreign Languages. In 2000, this institute was reorganized and renamed to the Military Information and Foreign Languages Department of the Military University of the Ministry of Defence of the Russian Federation and it is aimed on training specialists in "organizing foreign information and military communication, information analysis and monitoring and development of military information" (Darczewska, 2014).

The reform of this institution was directly influenced by the creation of the Information Security Doctrine of the Russian Federation from 2000. This reform can be considered as a cornerstone of the today's Russian information warfare. "Russia's modern information warfare adapts Soviet reflexive control to the contemporary geopolitical context" (Snegovaya, 2015). Thomas (2004) defines this "reflexive control" as a "means of conveying to a partner or an opponent specially prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action".

Taking all facts into consideration, Russian information warfare and propaganda has clear geopolitical context. It is carefully prepared by experts and tailor-made for each state not only in close neighborhood of Russia, such as Ukraine and Georgia, but also for NATO and EU member states. “The information and network struggle (more frequently, the information-psychological struggle), including its extreme forms, such as information-psychological warfare and netwars, are means the state [Russia] uses to achieve its goals in international, regional and domestic politics and also to gain a geopolitical advantage” (Darczewska, 2014). Geopolitical context of Russian information warfare lies in the Cold War heritage and rivalry of ideologies. As General Philip Breedlove stated at the NATO Wales Summit “Russia…is waging the most amazing information blitzkrieg we have ever seen in the history of information warfare” (Pomerantsev, 2014). Pomerantsev further states that “[t]he new Russia doesn’t just deal in the petty disinformation, forgeries, lies, leaks, and cyber-sabotage usually associated with information warfare. It reinvents reality, creating mass hallucinations that then translate into political action”. Most recent researches show that Russian propaganda is very popular among young people (but not only young people) mainly in Central Europe. According to latest report prepared by Globsec Policy Institute (2016) “support for a pro-Russian (Eastern) orientation is marginal, just above 12% [...], the pro-West camp is relatively weak, with only 23% of support”. In Czech Republic, 30% of citizens prefer pro-western orientation and only 4% an eastward orientation. In Hungary, 32% of citizens prefer pro-western orientation and only 6% an eastward orientation. Support for NATO membership is also decreasing in comparison with the year of their accession to NATO. Currently, 30% of Slovaks, 44% of Czechs and 47% of Hungarian citizens think that NATO is a good thing, while support for NATO accession was following (Hungary 85%, Czech Republic 57% both in 1998 and Slovakia 51% in 2004) (IVO 2005, EU Commission Archives 2004, Dvorský 2007). However, Russian involvement into European affairs does not end in the Central and Eastern Europe. It is no secret the Putin openly supports politicians such as Marine Le Penn, Victor Orbán or Miloš Zeman, who are known by their friendly relations with Russia and open anti-EU and anti-NATO policy. In addition, these negative trends of declining NATO and EU support in combination with internal state problems (such as corruption, bad educational system, poor judicial system, etc.) are exploited by extreme right-wing parties, pro-Russian politicians and so-called “alternative media” to regularly organize protests against NATO and EU and to acquire even more support and people’s votes in elections.

Conclusion

From long-term perspective, information warfare and propaganda has the power to influence whole states and alliances without direct military involvement, so it can be considered as a powerful tool of geopolitics. Currently it is massively used by Russian Federation to influence decision-making on the European level and in the same time, it is using elements of hybrid warfare to challenge NATO. Many EU and NATO member states started fighting with Russian propaganda extremely late and without any doubts some of them were deeply hit by it. In March 2015, European Council set up the East StratCom Task Force. Its main goal is to cooperate with EU institutions and member states in addressing Russian propaganda and disinformation campaigns. However, budget of this counter-propaganda cell is very limited in comparison with Russian investment into their press agencies and media, its work is very significant. According to Eriksson (2016) budget of the East StratCom Task Force could reach €1 million. Russia is able to use democracy against democracies and the freedom of information to inject disinformation into various target groups under the label of freedom of speech. Information warfare blurs the border between peace and war and between fact and fiction. People feel betrayed by the West, by the EU and it seems that first generation that doubts democracy as a viable political system arises in Europe. It is important to develop inner resilience of EU citizens against disinformation campaigns, conspiracy theories and hoaxes. It can be done by supporting critical thinking of young people, higher investments into education, supporting investigative journalism, and proper and open communication of state institutions.

References

Beznosiuk, Maksym. 2016. "Russia's military reform: Adopting to the realities of modern warfare". October 13*. New Eastern Europe.* Available at: http://www.neweasterneurope.eu/articles-and-commentary/2153-russia-s-military-reform-adapting-to-the-realities-of-modern-warfare. Accessed January 29, 2017.

Čižik, Tomáš. 2015. "Implications for Security and Defence Cooperation of the Nordic-Baltic Region Following the Annexation of Crimea by Russian Federation"*.* In Róbert Ondrejcsák and Grygoryi Perepelytsia (eds.). *Ukraine, Central Europe and the Future of European Security*. Bratislava: Centre for European and North Atlantic Affairs. pp. 66-87.

Čižik, Tomáš. 2015. "Informačná vojna – nová bezpečnostná hrozba pre Európu". *Zahraničná politika.* Available at: http://zahranicnapolitika.dennikn.sk/informacna-vojna-nova-bezpecnostna-hrozba-pre-europu/.

Čižik, Tomáš. 2016. "Russian Information Warfare – Security Threat not only for Visegrad Countries". *Nemzeti Érdek (National Interest Journal), Volume 17*. Századvég Alapitvány (in Hugarian).

Čižik, Tomáš. 2016a. "Information Warfare – Europe's New Security Threat". *CENAA Policy Papers, Volume 5.* Centre for European and North Atlantic Affairs. Available at: http://cenaa.org/en/new-policy-paper-information-warfare-europes-new-security-threat/.

Coalson, Robert. 2016. "New Kremlin Information-Security Doctrine Calls For 'Managing' Internet in Russia". December 6. *Radio Free Europe – Radio Liberty.* Available at: http://www.rferl.org/a/russia-informaiton-security-internet-freedome-concerns/28159130.html. Accessed January 30, 2017.

Darczewska, Jolanta. 2014. "The Anatomy of Russian Information Warfare: The Crimean Operation, A Case Study. *Centre for Eastern Studies (OSW).* Available at: https://www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_information_warfare.pdf. Accessed January 30, 2017.

DELFI. 2015. "Kremlin's millions: How Russia funds NGOs in Baltics (3)". Available at: http://en.delfi.lt/nordic-baltic/kremlins-millions-how-russia-funds-ngos-in-baltics.d?id=68908408. Accessed September 4, 2016.

Dvorský, Daniil. 2007. "Komparace zahraniční politiky České republiky a Slovenské republiky v kontextu vstupu do NATO". *Masarykova Univerzita.*

Eriksson, Aleksandra. 2016. “EU myth-busters set for budget upgrade”. October 25. *EU Observer.* Available at: https://euobserver.com/institutional/135589. Accessed February 1, 2017.

Globsec Policy Institute. 2016. “Russia’s Information War in Central Europe: New Trends and Counter-Measures”. Available at: http://www.cepolicy.org/sites/cepolicy.org/files/attachments/russias_information_war_in_central_europe.pdf. Accessed October 24, 2016.

Hoffman, Frank. 2007. “Conflict in 21st century: a rise of hybrid wars”. *Potomac institute for political studies*. Available at: http://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf. Accessed November 21, 2016.

Inštitút pre verejné otázky (IVO). 2004. “Na Slovensku má EU výrazně vyšší podporu než NATO. Podpora EU a NATO je v České republice vyrovnaná”. Available at: http://www.ivo.sk/buxus/docs/vyskum/subor/produkt_4159.pdf [Accessed 24 October, 2016]

Ismail, Nick. (2016). “Cyber security: information warfare challenges the essence of democracy”. *Information Age.* November 25. Available at: http://www.information-age.com/cyber-security-information-warfare-challenges-essence-democracy-123463369/. Accessed January 29, 2017.

Lelich, Milan. 2014. “Victims of Russian Propaganda”. July 2015. *New Eastern Europe*, Available at: http://www.neweasterneurope.eu/interviews/1278-victims-of-russian-propaganda. Accessed January 30, 2017.

Lythoe, Luke and Dixon, Hugo. 2016. “EU-bashing stories are misleading voters – here are eight of the most toxic tales”. *The Guardian.* May 19. Available at: https://www.theguardian.com/commentisfree/2016/may/19/inaccurate-pro-brexit-infacts-investigation-media-reports-eu-referendum. Accessed January 29, 2017.

Nichiporuk, Brian. 1999. “U.S: Military opportunities: Information-warfare concepts of operation” in Zalmay K., White J.O., and Marshall A W., eds. *Strategic Appraisal: The Changing Role on Information Warfare.* Santa Monica: RAND Corporation. Available at: https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1314/MR1314.ch6.pdf.

Pomerantsev, Peter. n.d. “Russia and the Menace of Unreality.” *The Atlantic Global.* September 9. Available at: http://www.theatlantic.com/international/archive/2014/09/russia-putin-revolutionizing-information-warfare/379880/. Accessed December 19, 2016.

Rid, Thomas. n.d. “Russia’s information warfare – strategic ‘social engineering’. *Democracy Digest.* January 9. Available at: http://www.demdigest.net/social-engineering-strategic-level/. Accessed January 29, 2017.

SIPRI. n.d. “SIPRI Military Expenditure Database”. *Stockholm International Peace Research Institute*. Available at: http://www.sipri.org/research/armaments/milex/milex_database/milex_database. Accessed July 20, 2015.

Snegovaya, Maria. 2015. “Putin’s Information Warfare in Ukraine: Soviet Origins of Russia’s Hybrid Warfare”. *Institute for the Study of War (ISW)*. Available at: http://understandingwar.org/sites/default/files/Russian%20Report%201%20Putin's%20Information%20Warfare%20in%20Ukraine-%20Soviet%20Origins%20of%20Russias%20Hybrid%20Warfare.pdf. Accessed January 30, 2017.

The Washington Post. 2007. “Putin’s Prepared Remarks at 43rd Munich Conference on Security Policy.” February 12. Available at: http://www.washingtonpost.com/wp-dyn/content/article/2007/02/12/AR2007021200555.html. Accessed July 20, 2015.

Theatrum Belli. 2015. “The Military Doctrine of the Russian Federation”. Available at: http://www.theatrum-belli.com/the-military-doctrine-of-the-russian-federation/. Accessed January 30, 2017.

Thomas, L. Timothy. 2004. “Russia’s Reflexive Control Theory and the Military”. *Journal of Slavic Military Studies,* Vol 17, pp. 237-256. Available at: https://www.rit.edu/~w-cmmc/literature/Thomas_2004.pdf. Accessed January 30, 2017.