National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

# NATO VULNERABILITIES: NON-KINETIC THREATS IN THE BALTIC STATES

Maj Agris Liepiņš

| JCSP 44 | PCEMI 44 |
|---|---|
| Exercise *Solo Flight* | Exercice *Solo Flight* |

**Disclaimer**

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

**Avertissement**

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES
JCSP 44 – PCEMI 44
2017 – 2018

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

# NATO VULNERABILITIES: NON-KINETIC THREATS IN THE BALTIC STATES

Maj Agris Liepiņš

# NATO VULNERABILITIES:
# NON-KINETIC THREATS IN THE BALTIC STATES

## INTRODUCTION

The following essay analyzes the use of non-kinetic threats in Eastern Europe. The focus will be on the most recent activities in the information and cyber domains occurring in the Baltic states. Therefore, this paper will look at the doctrinal aspects of non-kinetic and influence activities and how they can be best applied to reach maximal effects. The doctrinal review will be followed by an assessment of the Russian way of war and an analysis of recent incidents in the non-kinetic environment of the Baltic states. Finally, the paper will present a recent review of developments and intentions from NATO and their potential for better solutions to counter information warfare.

NATO has successfully deployed troops in order to protect their Eastern border from Russian aggression; however, this has not been effective at protecting the Baltic States and NATO against non-kinetic threats.

## NON-KINETIC WARFARE

Non-kinetic warfare makes up a large part of military activities in the 21st century. The pinnacle of its use was during the Cold War when Eastern and Western countries competed through non-lethal means. Since the 1990s this strategy can also be identified in information dissemination, influence activities, messaging and the use of propaganda for internal and external use in order to dominate the post-Soviet era in Eurasia.[1] What is currently happening on NATO's Eastern border is an example of Sun Tzu's method of offensive strategy: "To win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill."[2] From a doctrinal perspective, the current situation could be characterized by the conduct of influence activities "integration of designated information-related capabilities in order to synchronize themes, messages, and actions with operations to inform… global audiences, influence foreign audiences, and affect adversary and enemy decision-making."[3] NATO doctrine only espouses influence activities in a war time whereas Russia uses them over the full peace time to war time spectrum.

Non-kinetic warfare includes influence activities, applied to as information operations (IO) in the most current doctrine manuals. In *US Field Manual 3-13* IO "is the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own."[4] In *Canadian Forces, Joint Publication 01* information is a "strategic resource vital to pursuing national interests…. Information readily available from multiple sources influences domestic and foreign audiences including citizens, adversaries, and governments."[5] IO includes many capabilities such as Psychological operations (PSYOPS), Public and Civil affairs, Electronic Warfare,

[1] Jolanta Darczewska*, THE ANATOMY OF RUSSIAN INFORMATION WARFARE,* The Crimean operation, A Case Study, Point of View Nr.42, Warsaw (Center for Eastern Studies, 2014), 10-25.

[2] Samuel B.Griffith, *Sun Tzu The Art of War. Offensive strategy* ch.3*,* Oxford University Press, (1963), 77.

[3] Field Manual 3-13, *Information operations,* Headquarters Department of the Army Washington, DC (25 January 2013), ch.1, 1-1.

[4] Field Manual 3-13, *Information operations,* Headquarters Department of the Army Washington, DC (14 June 2016), 1-2.

[5] *Canadian Forces Joint Publication, CFJP 01 Canadian Military Doctrine* (Her Majesty the Queen as represented by the Minister of National Defence, 2009), ch.2, 2-1. http://publications.gc.ca/collections/collection_2010/forces/D2-252-2009-eng.pdf.

Cyberspace operations, Military Deception and others. IO has a very important role throughout all phases of military operations. IO through the informational environment creates necessary effects, which enables other elements to achieve their goals and mission success. The informational environment is closely related to the operational environment and can impact one or many parts of it.[6] The "Informational environment consists of three aspects: physical, informational and cognitive. Within the physical dimension of the information environment is the connective infrastructure that supports the transmission, reception, and storage of information."[7] Physical aspects can be patrols and reconnaissance elements which gather information. Informational aspects are more about the content: data, text and images. "Within the cognitive dimension are the minds of those who are affected by and act upon information. These minds range from friendly commanders and leaders, to foreign audiences affecting or being affected by operations, to enemy, threat or adversarial decision makers."[8] This shows how information warfare is a great tool that can be used before and during the conduct of kinetic operations in order to support the achievement of operational objectives.

Nowadays modern forces have developed sophisticated Electronic Warfare (EW) capabilities. Those capabilities consist of protection, support and offensive activities such as electronic attack. EW compliments IO in order to gain the freedom of action.[9] EW "is essential for protecting friendly operations and denying adversary operations within the [Electromagnetic Spectrum] EMS throughout the operational environment. EW can influence

[6] Field Manual 3-13, (14 June 2016) ... 1-2, 1-3.

[7] Field Manual 3-13, (14 June 2016) ... 1-2.

[8] Ibid.

[9] Joint Publication 3-13.1, *Electronic Warfare,* Department of Defense (8 February 2012), vii-ix.

the adversary, friendly population, and neutral population."[10] EW, although can have kinetic effects, is a proven method in the spectrum of non-kinetic actions.

Cyberspace operations are a critical element of 21st century warfare, and in Joint Publication (JP) 3-13, *Information Operations* states that it "is a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers."[11] Cyberspace and EW operations complement each other and can create better effects when properly executed and synchronized.[12]

Loren B. Thompson, of the Lexington Institute, shows that the Pentagon is going to investigate and conduct research in EW and cyber capabilities. The future will be different and a non-kinetic approach will be key. Thompson stressed the importance of innovations in Cyber warfare and the use of computers in order to reach military objectives. EW and Cyber warfare will play dominant roles in future campaigns.[13]

## RUSSIAN WAY OF WAR

Russia is waging war with an outlook at least 10 years from now. It is not recognized as a conventional war where war has traditionally been declared and both sides are fighting with uniformed and known armies with insignias. It is a hybrid threat which consists of conventional and irregular elements which also include covert and deniable activities. An

[10] Ibid.

[11] Joint Publication 3-13, *Information operations,* Department of Defense (20 November 2014), II-9.

[12] Joint Publication 3-13.1, *Electronic Warfare* ... viii-ix

[13] Loren B. Thompson, Ph. D, *Pentagon Study Signals Growing Awareness Of "Non-Kinetic" Threats& Opportunities,* Lexington Institute (17 December 2012). http://www.lexingtoninstitute.org/pentagon-study-signals-growing-awareness-of-non-kinetic-threats-opportunities.

historical example was in 1998 with the Russian invasion of Georgia: a state that openly wanted to join NATO. Later, in 2014, "green men" undeclared from Russia invaded Ukraine and annexed Crimea. Also in 2014, a civilian Malaysian airplane was shot down from a Russian missile and instead of acknowledging the factual results of an international investigation, President Putin publicly blamed Ukraine.[14]

In the *Handbook of Russian Information Warfare*, the Russian doctrine states that non-kinetic warfare is information warfare which is not just restricted in wartime. Therefore, it is also not restricted just in "phase zero"  which in *US Joint Publication 5-0* means  "Joint and multinational operations—inclusive of normal and routine military activities—and various interagency activities are performed to dissuade or deter potential adversaries and to assure or solidify relationships with friends and allies".[15] Influence activities must be conducted during peace time and that is the biggest practical difference between Eastern and Western forces. The strategic goal of information warfare is to discredit NATO, weaken NATO coherence and to deny the application of NATO Article 5.[16]  Latvian policy researcher Janis Berzins says "The Russians have placed the idea of influence at the very center of their operational planning and used all possible levers to achieve this: the skillful internal communications; deception operations; psychological operations and well-constructed external communications."[17] The use of IO during peacetime must be strictly controlled; moreover, there is an urgent need to review international law, particularly the

[14] Max Boot*, Russia's been waging war on the West for years. We just haven't noticed.* Washington Post *( 15 March 2018). https://www.washingtonpost.com/opinions/russias-been-waging-war-on-the-west-for-at-least-a-decade-we-just-havent-noticed/2018/03/15/83926c78-2875-11e8-bc72077aa4dab9ef_story.html?utm_ term=.294d47d1160c.*

[15] Joint Publication 5-0, *Joint Operation Planning,* Department of Defense (11 August 2011), xxiii-xxiv.

[16] Keir Giles*, Handbook of Russian Information Warfare,* NATO Defense Collage, NDC Fellowship Monograph Ser. 9 (November 2016), 1-13; article 5 is a NATO country's mechanism to initiate NATO defense from all NATO countries against an aggressor.

[17] Jānis Bērziņš, *Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy,* National Defense Academy of Latvia, Center for Security and Strategic Research, Policy Paper No. 2, (April 2014), p. 6.

Laws Of Armed Conflict, to prevent state sponsor IO activities that currently exploit legal grey zones or gaps.

Former Russian Intelligence service officer Vladimir Kvachkov has said about modern information warfare that “A new type of war has emerged, in which armed warfare has given up its decisive place in the achievement of the military and political objectives of war to another kind of warfare - information warfare.”[18] Even during peace time Russia views “cyber-capabilities as tools of information warfare, which combines intelligence, counterintelligence, maskirovka, disinformation, electronic warfare, debilitation of communications… psychological pressure, and destruction of enemy computer capabilities”[19]

The war in Ukraine demonstrated Russian capabilities in information and psychological warfare; moreover, they were seen by the whole world. To conduct influence activities Russia mainly used state-controlled television, radio, newspapers, the internet and it was supported by Russian diplomats, politicians and experts. The Crimean invasion showed excellent use of information warfare. Moscow’s information aggression nowadays uses historically perfected and developed propaganda techniques.[20]

It is essential to be aware of the after effects of overwhelming information warfare and what steps were taken by recipients. For example, both during and right after Russia’s Zapad 2013 exercises there were clandestine moves of the Russian military to invade Ukraine.[21] In the article *Russia’s Zapad 2013 Military Exercise* it reads “Moscow uses such large-scale exercises as a smoke-screen to obscure the deployment of its Armed Forces to

[18] V.Kvachkov, Спецназ России (Russia’s Special Purpose Forces), Voyennaya Literatura, 2004. http://militera.lib.ru/science/kvachkov_vv/index.html (accessed 21 July 2016).

[19] K.Mshvidobadze, *The Batlefield On Your Laptop*, Radio Free Europe Radio Liberty (21 March 2011), https://www.rferl.org/a/commentary_battlefield_on_your_desktop/2345202.html.

[20] Jolanta Darczewska*, THE ANATOMY OF RUSSIAN INFORMATION WARFARE,* The Crimean operation, A Case Study, Point of View Nr.42, Warsaw (Center for Eastern Studies, 2014), 10-25.

[21] *Russian Zapad 2013 Military exercise, Lessons for Baltic Regional Security* (The Jamestown Fundation. December, 2015), iv, 1-4.

regional hotspots beyond borders… Almost certainly, Moscow will utilize such a modus operandi in future conflicts as well."[22] This demonstrates that NATO must follow all Russian non-kinetic steps that are being used as precursors to its military kinetic activities.

## NON-KINETIC THREATS IN THE BALTIC STATES

Threats to Eastern NATO members generally come from Russia. President Putin laments the collapse of Soviet Union, stating that "the collapse of the Soviet Union was the biggest geopolitical collapse of century."[23] Soft power has been used in the Baltic states in order to change attitudes towards Russian regime. Putin uses public diplomacy together with propaganda tools in order to divide and undermine the local populations of the Baltic states. Propaganda and controlled news is an accessible and valuable way of influencing the Baltic States "The news are presented in them is moderated by political technology specialists, who decide which information could help achieve certain goals and which should be blocked as harmful."[24] Russia tries to change political and social behaviours in order to reach its foreign policy objectives. The Baltic states' integration into NATO and the European Union is perceived as a peril to the Russian Federation.[25] Russia is seeking to undermine NATO and Russia's primary aim in its foreign policy is to control and influence post-Soviet countries. In its doctrine it is said that "Russia should be able to control either militarily or politically neighboring spaces and countries. In a more contemporary approach, such a control has been viewed as the key to Russia asserting itself as one of the 'centers of influence' in the

[22] Ibid., 1.

[23] *Russia's Public Diplomacy in Latvia: Media and Non-governmental Intstitutions* (Eastern Europe Political Science Center, 2014), 3-15.

[24] Jolanta Darczewska*, THE ANATOMY* ... 25-26.

[25] Isaak Park*, Russian Soft Power in the Baltics: in the Frameworks of Neoliberalism,* University of Tennessee (August2016), vol. 7, 157-165, http://trace.tennessee.edu/cgi/viewcontent.cgi?article=1319&context=pursuit.

world."[26] NATO must focus more on countering Russia's non-kinetic activities in order to maintain cohesion between member states and balance in the Baltic region.

The Russian form of hybrid warfare mainly uses cyber and information operations; however, the covert and deniable nature of these activities is of grave concern for the Baltic States. The concern is that the adversary will use a combination of many activities like propaganda, support of hostilities and criminal activities, use of security services and military in irregular ways to reach its political goals. There are reasonable worries that Russia will infiltrate in the Baltic governments and thus will try to demonstrate failure of alliance efforts.[27] Scholar J.Berzins says that there are "three categories of hybrid scenarios in the Baltics: nonviolent subversion, which seeks to use propaganda, covert action, and other nonviolent means to undermine or influence the governments of the Baltic states…and other forms of irregular warfare."[28]

Disinformation, which also includes fake news fabricated media outlets, is Russia's main tool and the aim is to mislead and divide populations. Russian influence activities during peace time is closely connected to the military and supported by politicians.[29] Russian hackers meddle with election processes overseas, their military jets are flying in the UK's air-space, their state-sponsored media outlets are spreading false stories, seeking to destabilize the principles of good journalism.[30]

[26] Isabelle Facon, *Russia's national security strategy and military doctrine and their implications for EU.* Directorate-General for External Policies. Policy Department. (European Parliament, January 2017), 7, http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/578016/EXPO_IDA(2017)578016_EN.pdf.

[27] Andrew Radin*, Hybrid Warfare in the Baltics. Threats and potential responses,* Research report by Strategy and Doctrine Program of RAND (2017), 5-15. https://www.rand.org/content/dam/rand/pubs/research_reports/RR1500/RR1577/RAND_RR1577.pdf.

[28] Andrew Radin*, Hybrid Warfare in the Baltics …* 19.

[29] *Fake News: A Roadmap,* NATO Strategic Communications Center of Excellence (25 February 2018), 40-55. https://www.stratcomcoe.org/fake-news-roadmap.

[30] Ibid., 50-64.

One recent example of fake news is the situation in Latvia where the Latvian Central Bank governor was accused of taking bribes. The story was accompanied by fake photos which probably were made by Russian ”trolls”. “Corruption allegations that led to the suspension of Latvia’s central bank governor on Tuesday may be part of a disinformation campaign aimed at damaging trust in the country and influencing October elections.”[31] By saying “trolls” it is understood that “their task is to control debate and stifle dissent in forums and on social media.”[32] More comments on this particular event came from the Ministry of Defense of Latvia declaring “there is a high probability that massive information operation from outside is conducted, which is identical in structure and execution to information operations which were observed in France, Germany and the USA before elections.”[33] This latest report is another example of how the Russian propaganda machine works in order to disrupt stable governments in the Baltics states.

An example of the use of EW was seen in Latvia in 2017 when Intelligence services spotted a Russian attack on telecommunication services and the event is still under investigation: the “…loss of service resulted from a Russian electronic attack; a Russian ship equipped for electronic warfare was reportedly just offshore at the time.”[34] Similarly, in Norway an attack was noted where “…their country suffered an electronic attack in September that they say came from Russia, with GPS signals on flights in northern Norway being jammed just as Moscow was carrying out its massive Zapad military exercise in the

[31] Gederts Gelzis, *Latvian Defense Ministry says corruption claims may be disinformation campaign, Reuters* (20 February 2018), https://www.reuters.com/article/us-latvia-banking/latvian-defense-ministry-says-corruption-claims-may-be-disinformation-campaign-idUSKCN1G41KG.

[32] N. Hermant, *“Inside Russia’s Troll Factory: Controlling debate and stifling dissent in Internet forums and social media”* (ABC, 13.08.2015) http://www.abc.net.au/news/2015-08-12/inside-russia's-troll-factory-internet-forums-social-media/6692318.

[33] Ministry of Defense of Latvia, *Information Operation Conducted Against Latvia*, (19 February 2018), http://www.mod.gov.lv/Aktualitates/Preses_pazinojumi/2018/02/20-01.aspx.

[34] Reid Standish, *Russia’s Neighbors Respond to Putin’s ‘Hybrid War’, Baltic and Nordic countries turn to education as much as military hardware to counter Moscow’s hybrid threats*, (Foreignpolicy,12 October, 2017). http://foreignpolicy.com/2017/10/12/russias-neighbors-respond-to-putins-hybrid-warlatvia-estonia-lithuania-finland.

neighborhood."[35] The principal warfare tools in Lithuania were cyber attacks: they "…faced a constant stream of cyberattacks against its government departments since 2014, while Russian jets routinely violated national airspace in the Baltics."[36] These examples show that EW attacks are a reality in modern warfare and a problem in wider region.

Research document produced by the Strategy and Doctrine Program of the RAND corporation suggests that in the future the United States and NATO must use proper strategic communication through the Baltic governments and Russian language media. Moreover, a public relations campaign must be conducted that explains the reasons why NATO forces are there and that they are not threat to the Russian Federation and their minorities in Baltic States..[37]

In recent history Lithuania was victim to many incidents in the Cyber domain: "In recent years, a number of attempts to use cyber-attacks for affecting the outcomes of democratic elections in other states were brought to light in Europe and the West. In the last year alone, Lithuania registered over 50 thousand cyber-attacks."[38] In order to counter Russian aggression Lithuania is building Cyber teams which will be able to rapidly react on aggression against Lithuania. "The European Council also endorsed the list of 17 collaborative defense projects. Lithuania will manage the project on the establishment of Cyber Rapid Response Teams. The President tabled the initiative to establish the teams in Tallinn a few months ago."[39] This is a great example of countering non-kinetic threats; however, there is room for more improvements and developments in the future to protect NATO.

[35] Ibid.

[36] Ibid.

[37] Andrew Radin*, Hybrid Warfare in the Baltics…*1-5.

[38] Homepage of President of Republic of Lithuania, https://www.lrp.lt/en/press-centre/press-releases/lithuania-to-manage-the-establishment-of-eu-cyber-teams/29038.

[39] Ibid.

From Russian perspective, NATO is a threat to Russia because of its activities close to the border. "Increasing military activity of the states of block; enlargement of the alliance; the placement of its military infrastructure close to Russian borders create a threat to [Russia's] national security."[40] However, those activities in NATO are only defensive in nature because of recent annexation in Crimea; therefore, could not be perceived as a danger to Russia.

## CONCLUSION

NATO doctrine encompasses non-kinetic warfare and there can be positive effects when it is implemented wholesomely. The importance of information operations is recognized through the integrated employment with other capabilities and lines of operations in the future and the necessity of development of Cyber capabilities. More critically, information operations as a non-kinetic warfare tool need to be used beyond the wartime spectrum to have the most comprehensive impact.

Russia conducts a form of hybrid warfare that consists of conventional and irregular elements, and those elements can include the covert activities witnessed in Georgia and Ukraine. Russia's strategic goal is to discredit NATO coherence and it will continue to use peace time in operational planning deception, psychological operations and well prepared communication means during times of peace. It will continue to use information warfare to accomplish military and political objectives and cyber capabilities will be its main tool in this kind of warfare.

[40] I.Berzina, M.Cepuritis, D.Kaljula, I.Juurvee, *Russia's Footprint in the Nordic – Baltic Informational Environment,* Research project by NATO Strategic Communications Center of Excellence (2016/17), 21. https://www.stratcomcoe.org/russias-footprint-nordic-baltic-information-environment-0.

In 1990 the Soviet Union lost their control over Baltic states and President Putin leverages that and wants to regain regional power in Eastern Europe. His main tools are diplomacy, propaganda and other influence activities. Disinformation, fake news, Cyber-attacks have been conducted against Baltic states by civilian "trolls" and these techniques have been recognized as information operations that are part of bigger plans like for example the disruption of elections.

There has been a lot of effort to counter adversary activities; however, there is a need for more diplomatic and military approach from the NATO side in order to create better conditions and to act against Russian aggression and unlawful employment of their military and non-military tools. NATO has successfully deployed an Enhanced Forward Presence units in order to protect its Eastern border with "boots on the ground" and reached its strategic success in deterring Russian kinetic aggression; however, it is not completely effective to protect the Baltic states and other NATO members from non-kinetic, unconventional and irregular threats. NATO must put more resources and effort into leveraging non-kinetic warfare tools during the full spectrum of peacetime to wartime in order to properly protect its membership and interests abroad from a subversive adversary.

# BIBLIOGRAPHY

Berzina I., Cepuritis M., Kaljula D., Juurvee I., Russia's Footprint in the Nordic – Baltic Informational Environment, Research project by NATO Strategic Communications Center of Excellence, 2017. https://www.stratcomcoe.org/russias-footprint-nordic-baltic-information-environment-0.

Bērziņš Jānis, Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy, National Defense Academy of Latvia, Center for Security and Strategic Research, Policy Paper No. 2, April 2014.

Boot Max, Russia's been waging war on the West for years. We just haven't noticed. Washington Post, March 2018. https://www.washingtonpost.com/opinions/russias-been-waging-war-on-the-west-for-at-least-a-decade-we-just-havent-noticed/2018/03/15/83926c78-2875-11e8-bc72077aa4dab9ef_story.html?utm_ term=.294d47d1160c

Darczewska Jolanta, THE ANATOMY OF RUSSIAN INFORMATION WARFARE, The Crimean operation, A Case Study, Point of View Nr.42, Warsaw, Center for Eastern Studies, 2014.

Facon Isabelle, Russia's national security strategy and military doctrine and their implications for EU. Directorate-General for External Policies. Policy Department, European Parliament, January 2017. http://www.europarl.europa.eu/RegData/ etudes/IDAN/2017/578016/EXPO_IDA(2017)578016_EN.pdf.

Field Manual 3-13, Information operations, Headquarters Department of the Army Washington, DC, June 2016.

Field Manual 3-13, Information operations, Headquarters Department of the Army Washington, DC, January 2013.

Field Manual 5-0, Operations process, Headquarters Department of the Army, March 2010.

Field Manual 6-0, Commander and Staff Organization and Operations, Headquarters Department of the Army, March 2014.

Field Manual 100-2-1, The Soviet Army Operations and Tactics, Headquarters Department of the Army, July 1984.

Field Manual 100-2-3, The Soviet Army: Troops, Organization, Equipment, Headquarters Department of the Army, June 1991.

Canadian Forces Joint Publication, CFJP 01 Canadian Military Doctrine (Her Majesty the Queen as represented by the Minister of National Defence, 2009. http://publications.gc.ca/collections/collection _2010/forces/D2-252-2009-eng.pdf.

Gederts Gelzis, Latvian Defense Ministry says corruption claims may be disinformation campaign, Reuters, February 2018. https://www.reuters.com/article/us-latvia-banking/latvian-defense-ministry-says-corruption-claims-may-be-disinformation-campaign-idUSKCN1G41KG.

Giles Keir, Handbook of Russian Information Warfare, NATO Defense Collage, NDC Fellowship Monograph Ser. 9, 2016.

Griffith B.Samuel, Sun Tzu The Art of War. Offensive strategy ch.3, Oxford University Press, 1963.

Homepage of President of Republic of Lithuania, https://www.lrp.lt/en/press-centre/press-releases/lithuania-to-manage-the-establishment-of-eu-cyber-teams/29038.

Hermant N., "Inside Russia's Troll Factory: Controlling debate and stifling dissent in Internet forums and social media", ABC, August 2015. http://www.abc.net.au/news/2015-08-12/inside-russia's-troll-factory-internet-forums-social-media/6692318.

Joint Publication 3-13.1, Electronic Warfare, Department of Defense, February 2012.

Joint Publication 3-13, Information operations, Department of Defense, November 2014.

Joint Publication 5-0, Joint Operation Planning, Department of Defense, August 2011.

Kvachkov V., Спецназ России (Russia's Special Purpose Forces), Voyennaya Literatura, 2004, http://militera.lib.ru/science/kvachkov_vv/index.html (accessed 21 July 2016).

Mshvidobadze K., The Batlefield On Your Laptop, Radio Free Europe Radio Liberty, March 2011.https://www.rferl.org/a/commentary_battlefield_on_your_desktop/2345202.html .

Ministry of Defense of Latvia, Information Operation Conducted Against Latvia, February 2018. http://www.mod.gov.lv/Aktualitates/Preses_pazinojumi/2018/02/20-01.aspx.

NATO Strategic Communications Center of Excellence, Fake News: A Roadmap, February 2018. https://www.stratcomcoe.org/fake-news-roadmap.

Park Isaak, Russian Soft Power in the Baltics: in the Frameworks of Neoliberalism, University of Tennessee, August 2016. http://trace.tennessee.edu/cgi/viewcontent.cgi?article=1319&context=pursuit.

Radin Andrew, Hybrid Warfare in the Baltics. Threats and potential responses, Research report by Strategy and Doctrine Program of RAND, 2017. https://www.rand.org/content/dam/rand/pubs/research_reports/RR1500/RR1577/RAND_RR1577.pdf.

Russian Zapad 2013 Military exercise, Lessons for Baltic Regional Security, The Jamestown Foundation, December, 2015.

Russia's Public Diplomacy in Latvia: Media and Non-governmental Intstitutions, Eastern Europe Political Science Center, 2014.

Standish Reid, Russia's Neighbors Respond to Putin's 'Hybrid War', Baltic and Nordic countries turn to education as much as military hardware to counter Moscow's hybrid threats, Foreignpolicy, October 2017. http://foreignpolicy.com/2017/10/12/russias-neighbors-respond-to-putins-hybrid-warlatvia-estonia-lithuania-finland.

Thompson B. Loren, Ph. D, Pentagon Study Signals Growing Awareness Of “Non-Kinetic” Threats& Opportunities, Lexington Institute, December 2012. http://www.lexingtoninstitute.org/pentagon-study-signals-growing-awareness-of-non-kinetic-threats-opportunities.