National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

SOF IN MODERN WARFARE

Maj Agris Liepiņš

JCSP 44

SERVICE PAPER

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.

PCEMI 44

ÉTUDE MILITAIRE

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

SERVICE PAPER - ÉTUDE MILITAIRE

SOF IN MODERN WARFARE

Maj Agris Liepiņš

Word Count: 2573

Compte de mots: 2573

SOF IN MODERN WARFARE

AIM

1. The following service paper analyzes the complexity of modern warfare and argues for changes in the use of NATO Special Operation Forces (SOF). This paper focuses on the key tasks and proposes adjustments to the approach to SOF employment in a contemporary, non-kinetic environment and for future operations in Eastern Europe.

INTRODUCTION

2. In recent military writings the following terms are all being used: New Generation Warfare, Hybrid Warfare, Modern Warfare, Fourth Generation Warfare, and in reality they are all describing the same thing. *The Oxford Handbook of War* describes Modern Warfare as a "combination of regular and irregular violent warfare."[1] However, scholar Maciej Bartkowsky from Hopkins University in Washington says that "hybrid warfare has come to be equated only with violence and fails to capture other nonviolent actions."[2] Modern Warfare is full of complexities involving both kinetic and non-kinetic means, which are evident in recent conflicts such as Afghanistan, Syria and Ukraine. It is in these complex threat environments where SOF plays a key role to facilitate the outcome of conflicts. The SOF community is small compared with conventional forces and in proportion to its impacts; therefore, it is necessary to take a closer look at the tasks they perform.

---

[1]Lindley-French Julia, *The Oxford Handbook of War,* (Arlington Virginia, December 2012), 358

[2]Bartkowsky Maciej, *Nonviolent Civilian Defense to Counter Russian Hybrid Warfare*, (2015) http://advanced.jhu.edu/wp-content/uploads/2015/02/GOV1501_WhitePaper_Bartkowski.pdf

3. Recent history in Afghanistan and Iraq shows that in kinetic and short-term operations SOF are highly successful. SOF are trained to kill or capture terrorists and secure hostages. These capabilities are still vital and it is necessary to maintain them. However, prior to the conflict in Ukraine no friendly SOF units were employed, which shows that the approach to employment of SOF in the early stage of a conflict must be reconsidered. Bartkowsky said that Russia "seems to have made the most extensive use of collective nonviolent actions in support of its geopolitical and military objectives. As we shall see, this occurred in the course of its … hybrid conflict against Ukraine in 2014."[3] Currently, a very similar situation is unfolding in Eastern Europe – the Baltic States and Poland – where these countries are being pressured by Russia's hegemonic expansion. The Baltic region is a place of strategic interest for Russia, and non-kinetic instruments of modern warfare such as propaganda, information war and cyber-attacks have already been used for several decades. In Ukraine some of those methods were used by SOF and other agencies; however, we do not have proof that SOF are used in Baltic region.

DISCUSSION

4. **Need for refocusing.** SOF units must be able to execute more than just raids like they did in Afghanistan. In order to broaden their strategic impacts, they need to focus more on influencing Host Nation governments and information exchange, work closely with civilian organizations and conduct information operations. The Washington think tank *The Council on Foreign Relations* (CFR) concludes that a "…new vision for special operations forces that shifts from a tactical focus on achieving sustained political-military effect…"[4] is necessary. To

[3]Bartkowsky Maciej, *Nonviolent Civilian Defense to Counter Russian Hybrid Warfare*, (2015) http://advanced.jhu.edu/wp-content/uploads/2015/02/GOV1501_WhitePaper_Bartkowski.pdf

[4]Robinson Linda, *The Future of U.S. Special Operations Forces*, Council Special Report No. 66 (April, 2013), 4

empower SOF in the future the focus needs to be on the broader development of SOF non-kinetic and political-military outcomes.

5. As an Infantry Officer author of the Service Paper worked with many SOF units in both domestic and multinational operations and while on various deployments including in Afghanistan. In order to integrate better in a multinational, joint, interagency framework, SOF must change their attitude and be more open and ready to exchange information in order to facilitate mission success in future operations. Their attitude towards conventional forces must be changed, and closer cooperation, training and a cooperative working environment must be created. SOF should participate in joint exercises alongside conventional forces and in doing so will normalize an environment where in the future it will be possible to conduct operations in a more synchronized manner. In his research paper on SOF, Major Theo Heuthorst said "…integration of SOF and conventional forces can only be achieved if the two currently disparate groups train together in a realistic environment."[5] Moreover, he added that "…if SOF remain isolated from conventional forces, then their capabilities cannot be effectively employed by the joint force commander, who is responsible for mission success. Special and conventional forces must be integrated in all levels."[6] New ways and means must be developed for SOF and conventional forces to conduct small-footprint operations together. In that case, the limited SOF resources will not be wasted and special capabilities can be enhanced more effectively integrating conventional resources.

---

[5]Heuthorst Theo T.W, *Deeds and Words:An Integrated Special Operations Doctrine for the Canadian Forces*, MDS research project (2007), 56

[6]Ibid, 62

6. Allied forces need to establish closer relationships and better intelligence information sharing. Doing so will improve the collective understanding of the intent and aim of would be adversaries even before any kinetic actions occur and create better and broader allied situational awareness. Intelligence exchange between allies was not timely before the Ukrainian conflict. The lessons learned were not effectively captured from this situation and the same thing will happen in Eastern Europe where even more intelligence information is needed for the larger environment and a greater number of NATO allies with protective interests in the area. There is huge space for SOF to take advantage of this opportune and nascent pre-conflict environment and facilitate the necessary intelligence resources to empower allied forces with situational awareness and influence before any violent conflict or land grabs arise.

7. Many former SOF tasks could be done either by conventional forces or in conjunction and close cooperation with conventional forces. For example, from authors experience in two rotations in Afghanistan as Operational Mentor Liaison Team (OMLT) leader some advisory tasks to Host Nation military and police units could have been done by Army leadership instead of SOF. In Afghanistan and Iraq, small OMLTs were created from conventional forces. Those teams proved that it is possible to train military, police and border guards effectively with conventional force units. Moreover, the OMLT was able to fight together with Host Nation forces in difficult conditions like in Eastern Afghanistan, close to the Pakistan border – in Kunar and Nuristan provinces, and other places. For future modern warfare it is advisable to consider the use of more conventional forces for similar types of missions in order to preserve the limited and highly valuable resources in SOF.

8. The 2009 *Capstone Concept for SOF* says that "CANSOF must be able to deter, pre-empt, disrupt and destroy the adversaries that would do harm to Canadians or our allies" [7] All those functions are well understood with respect to kinetic means. However, less emphasis has been placed on those capabilities that could be employed by NATO SOF in Eastern Europe. Non-kinetic activities such as information sharing with Allies, force training, security force assistance, special reconnaissance, information operations, cyber and contra-cyber and civil affairs operations should be a part of the NATO mission in Eastern Europe.

9. **Latest non-kinetic methods.** Russia uses the information domain in order to influence people in Eastern Europe. Nowadays we can see that Russia exploits the information domain very well against the U.S., the Baltic States, Poland and in other countries around the world. Russia believes that "the collapse of the Soviet Union was the biggest geopolitical collapse of the century."[8] Russia realized that they did not have enough global power and influence and therefore President Putin concentrated his focus on gaining it back and demonstrating to the world that Russia is still a global power.

10. Russia uses propaganda through social media every day and conducts informational warfare against the Latvian population and other Baltic states. They want to influence the Latvian population and government decisions.[9]

---

[7] *CANSOFCOM Capstone Concept for Special Operations 2009,* (Her Majesty the Queen, 2009), 2

[8] *Russia's Public Diplomacy in Latvia: Media and Non-Governmental Institutions* (Eastern Europe Political Science Center), 30

[9] Ibid, 3-30

11. Russia has a *troll army* that has been used for a long time against U.S. and European countries mainly through internet means. They have an Internet Research Agency which has been known as *troll factory*.[10] The aim of the *troll army* is to discredit population and government and "their task is to control debate and stifle dissent in forums and on social media."[11] Data from various research agencies shows that the "proportion of troll's messages in some cases even exceeded half of posted comments."[12] In an interview from a former troll factory worker said it was revealed that "around 250 people work 12- hour shifts, writing in blogs 24/7, working mostly in the Russian blogging platform Livejournal, Facebook, social network Vkontakte. This is full-cycle production: some write the posts, others comment on them."[13] All those Russian *troll* activities must be countered and the best way could be to use some elements of SOF or creation of new countering unit.

12. Electronic warfare is a common Russian tool in terms of cyber-attacks and it is directed by SOF leadership and various agencies. The Latvian military gets under those attacks almost every day and Russia is trying to expand it towards other NATO countries.[14] Recently, Russian Wessel jammed cellular services in Latvia for close to 24 hours.[15] Electronic warfare activities were also recently observed in Norway when GPS signals were jammed during the Russian

---

[10]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

[11]Ibid

[12]*Internet Trolling as A Tool of Hybrid Warfare: The Case Of Latvia,* Research (NATO Strategic Center of Excellence, 25 January 2016), 17-24, https://www.stratcomcoe.org/internet-trolling-hybrid-warfare-tool-case-latvia-0

[13]Harding Joel*, Thriving on Forums, Paid Kremlin Trolls Move Into New Offices,* DP.ru article (6 November 2014), https://toinformistoinfluence.com/2014/11/06/thriving-on-forums-paid-kremlin-trolls-move-into-new-offices/

[14]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/

[15]Ibid

exercise ZAPAD.[16] Cyber is used as one of the tools for Russian offensive activities. Moreover, hackers have disrupted multinational firms, ports and public services.[17] Currently, in Latvia there are troops from Canada, Spain, Italy, Slovakia and other countries. However, there are no declared capabilities which could counter Russian offensive cyber activities; therefore, a broad opportunity exists for NATO SOF to focus non-kinetic actions.

13. **Counter methods.** With the rise of technology, informational and electronic warfare methods will continue to expand in the future warfare domain. Therefore, the development of capabilities and tools to counter those methods is imperative.

14. To counter adversary non-kinetic activities there exists a requirement for a dedicated unit that can detect, protect against and defend against cyber-attacks. The unit must be formed with skillful technicians that know how networks and information within them flows and how to analyze it. These specialized personnel should be under command of SOF and well-compensated for their skills in order to be focused, dedicated and more agile in their mandate. A second course of action for placement of a cyber-defense unit is under conventional forces command.

15. Some tasks for the cyber unit should include to protect the information domain, the analyze news in the media, and protection from cyber-attacks. Additionally, offensive tasks such as influence activities and cyber-attacks against the adversary should be employed. To do those

---

[16]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/

[17]Harding Joel*, Thriving on Forums, Paid Kremlin Trolls Move Into New Offices,* DP.ru article (6 November 2014), https://toinformistoinfluence.com/2014/11/06/thriving-on-forums-paid-kremlin-trolls-move-into-new-offices/

tasks there must be changed roles. For example, if it is evident that a cyber-attack came from the adversary there must be regulated contra steps. Those steps will defend the informational and cyber domains and facilitate a safer future for populations. We can argue that those tasks could to other EW units; however, to maximize results they should do at least in cooperation with SOF elements, especially when we talk about offensive cyber-attacks.

16. **SOF against SOF**. It is difficult to find open source information about Russian SOF activities. The conflict in Ukraine can be studied to understand how Russian SOF operate in order to counter their activities. It is known that adversary SOF forces crossed the border many times before and during conflict in Ukraine. There is no question that they are in Ukraine, but it is not clear what they are doing.[18] NATO must adapt to these risks and realities and create a better posture for collective situational awareness and a force prepared to counter similar activities in other NATO countries when necessary.

17. Allied SOF must be ready to counter the sudden and rapid deployment of adversary SOF. Most likely Russian SOF and agencies will infiltrate into the Host Nation government and population. Covert operations will be conducted by Russian SOF in order to influence local leaders and stir up rebellion. Indications of possible rebellion must be known ahead of time. Russian SOF in Ukraine exploited vulnerabilities in the local population in the early stages of the conflict because of historic ties and the sway of local Russian minorities.[19] Allied SOF must be ready to identify the sympathetic vulnerabilities in populations and the informational domain

[18]Tor Bukkvoll, *Russian Special Operations Forces in Crimea and Donbas,* (2016), http://ssi.armywarcollege.edu/pubs/parameters/issues/summer_2016/5_bukkvoll.pdf

[19]Ibid

prior to any adversary activities. Moreover, SOF priorities in future warfare must be on *phase zero* - before actual conflict arises- and with capabilities to predict and disrupt adversary forces.

CONCLUSION

18. In this paper the adjustments of focus in SOF activities in modern warfare were analyzed. The author has prescribed looking at and implementing lessons learned from recent conflicts in Afghanistan and Ukraine, as well as in the non-kinetic battlespace of Eastern Europe.

19. SOF needs to focus more on influencing Host Nation governments, work closely with civilian organizations and conduct information operations. The focus must be on achieving a pre-emptive and sustained political-military effect prior to conflict development.

20. SOF needs to work more closely with conventional forces. In order to achieve mission success there is a need for more integrated exercises between both forces. Many SOF tasks such as the training of Host Nation forces could be reconsidered and effectively done by conventional forces. Moreover, if there is a requirement for more specialized training of conventional forces it should be done with closer cooperation. Adopting recommended changes to SOF tasks will ensure that they are ready to work together with conventional forces, and that will lead to the more efficient and symbiotic employment of joint forces in future warfare.

21. For future warfare in Eastern Europe there must be more non-kinetic operations prior to conflict development. The studied development of the Ukraine conflict must be leveraged to learn better practices for the future. Russian propaganda through social media and fake news

must be countered. Electronic warfare in terms of cyber-attacks are the future. It is recommended that a specialized unit be created under control of SOF or conventional forces that will be able to perform tasks that include information protection, the analysis of news media, protection from cyber-attacks, and the conduct of offensive cyber-attack and influence activities.

22. Lastly the author suggests to focus on events prior to Ukraine's conflict where Russian SOF together with other agencies infiltrated the Host Nation government and population, influenced local leadership and facilitated violent rebellions. Modern SOF must be ready to deploy prior to conflicts, identify vulnerabilities of Host Nations, enhance situational awareness and be ready to counter activities against adversary SOF.

RECOMMENDATIONS

23. Conventional units should be employed more in building partner nations capacity. Training tasks to Host Nation forces could be given to conventional forces and in that case SOF would preserve their personnel and concentrate more on things they are uniquely suited to. Moreover, small-footprint operations should be considered and exercised with conventional leadership and force involvement.

24. SOF and conventional forces need to train in a realistic environment and in a more integrated manner in order to be ready to deploy together. Both services must be trained together more than before and that will create mutual understanding for future operations.

25. Consider to create a unit similar to the Russian *troll factory* under SOF or conventional forces command that are capable to conduct information operations and electronic warfare to include information protection, influence activities, counter-propaganda, news media analysis, protection against cyber-attacks and the execution of cyber-attacks.

26. Empower allied nations with intelligence capabilities to discern and share about the adversary's aims and movements in Eastern Europe. Conduct security force assistance, special reconnaissance, information operations, civil affairs operations, cyber and contra-cyber operations.

27. Create a capability for SOF to operate against adversary SOF in *phase zero* of future warfare. Those operations must be conducted in a covert manner where it is necessary to deny the adversary's ability to infiltrate in governments and populations and to counter their efforts to create rebellions.

BIBLIOGRAPHY

Bartkowsky Maciej, *Nonviolent Civilian Defense to Counter Russian Hybrid Warfare*, 2015,http://advanced.jhu.edu/wpcontent/uploads/2015/02/GOV1501_WhitePaper_Bartkowski.pdf

Bukkvoll Tor, *Russian Special Operations Forces in Crimea and Donbas,* 2016, http://ssi.armywarcollege.edu/pubs/parameters/issues/summer_2016/5_bukkvoll.pdf

Eastern Europe Political Science Center, *Russia's Public Diplomacy in Latvia: Media and Non-Governmental Institutions*, 2016

Heuthorst Theo T.W, *Deeds and Words:An Integrated Special Operations Doctrine for the Canadian Forces*, MDS research project, 2007

Her Majesty the Queen, *CANSOFCOM Capstone Concept for Special Operations 2009*, 2009

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

Harding Joel*, Thriving on Forums, Paid Kremlin Trolls Move Into New Offices,* DP.ru article*,* 2014, https://toinformistoinfluence.com/2014/11/06/thriving-on-forums-paid-kremlin-trolls-move-into-new-offices/

Kiras D.James, *Special Operations and Strategy, From World War II to the War on Terrorism*, 2006

Lindley-French Julia, *The Oxford Handbook of War,* Arlington Virginia, 2012

NATO Strategic Center of Excellence, *Internet Trolling as A Tool of Hybrid Warfare: The Case Of Latvia,* Research*,* 2016, https://www.stratcomcoe.org/internet-trolling-hybrid-warfare-tool-case-latvia-0

Robinson Linda, *The Future of U.S. Special Operations Forces*, Council Special Report No. 66, 2013

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, 2017, http://foreignpolicy.com/2017/10/12/russias-neighbors-respond-to-putins-hybrid-warlatvia-estonia-lithuania-finland/