2015 7th International Conference on Cyber Conflict:
Architectures in Cyberspace
M.Maybaum, A.-M.Osula, L.Lindström (Eds.)
2015 © NATO CCD COE Publications, Tallinn

Russian Information Warfare of 2014

Margarita Jaitner
Department of Military Studies
Swedish Defence University
Stockholm, Sweden
Margarita.jaitner@fhs.se

Dr. Peter A. Mattsson
Department of Military Studies
Swedish Defence University
Stockholm, Sweden
peter.mattsson@fhs.se

Abstract: The belief in the power of information is deeply ingrained in the minds of the Russian top leadership, which operates under the premise that public opinion can be effectively influenced in order to reach desired outcomes domestically as well as on foreign soil. Ever since the beginning of the Euromaidan demonstrations, Russia has been seeking to promote its own narrative domestically, in Ukraine, and beyond, making use of the unique features of the cyberspace. As the crisis deepened in early spring of 2014, information operations played an important role in facilitating the de facto annexation of the Crimean peninsula to the Russian Federation, as well as throughout the continuation of the crisis.
This paper sets out to examine the information-related events of early 2014 with a particular focus on the annexation of Crimea. The aim is twofold. First, it provides an insight into the Russian world of ideas regarding information and its power applying the concept of information superiority and how it connects cyber and information warfare. Second, this paper exemplifies how Russia or pro-Russian entities make use of a wide array of tools and methods – kinetic, cyber, and informational – with the purpose of achieving information superiority. The paper concludes with a discussion regarding the impact of cyber within Russian Information Warfare as experienced in Ukraine.

Keywords: *information operations, information warfare, cyberspace, social media, Russia, Ukraine*

1. INTRODUCTION

"All warfare is based on deception," wrote Sun Tzu in "The Art of War". Information and communication have always played a role in conflict: ever since antiquity, symbols, rhetoric, and (mis)information have been used to gain advantage by frightening and misleading the enemy. Knowledge of the opponent's plans and capabilities, on the other hand, has the potential to balance differences between the combatants' firepower, contributing to victories. Russia has a long history of using misinformation and misdirection in conflict to create benefits for domestic

and foreign policy (Glantz 1988) as well as of using agitation and propaganda to mobilize its population (Kenetz 1985). Therefore, it is hardly surprising that the country's current leadership seeks to exploit the new complex networked information environment to its advantage. When the Ukraine crisis came to its first peak with the annexation of the Crimean peninsula, it became clear that Russia was conducting intense Information Operations (IOs), and, more so, that it was yielding success with these. The Information Warfare (IW) as such, however, had begun much earlier and gained intensity ever since the first Euromaidan demonstration.

IOs exist in a direct context with other types of operations such as military action, as experienced throughout the crisis in the Ukraine. In this light, the relatively bloodless but disinformation-rich annexation of Crimea must be seen as an absolute success. Still, because of the diffuse nature, it is difficult to estimate the exact impact of IOs. While areas with more exposure to other-than-Russian narratives are likely to be more resilient to Russian IOs, it is safe to say that Russia will continue to make use of its IW capabilities and that these are likely to have an impact on physical events. The present article aims to provide an overview over Russian application of IO/IW during the 2014 crisis in Ukraine and, to the extent it is possible, identify what contributes to their success. An essential element herein is to describe how information warfare converges with other types of warfare, in particular with cyber. The article is limited to cover pro-Russian activities during 2014; however, referenced to past events are made when deemed necessary. While examples of IOs against other countries are used, the paper's focus is on Ukraine.

2. INFORMATION AND CYBER SECURITY IN RUSSIAN (MILITARY) THEORY

The Russian policy and academic view on information as a source of power provides important background for the country's conduct of IOs. Russian focus on information and "information superiority" ("информационное превосходство") is an important element in the country's doctrines and strategies. The "National Security Strategy 2020" (Security Council of the Russian Federation 2009), for example, states in its analysis of future threats that the "global information struggle will intensify". In the same context, "nationalist, separatist, radical religion" and another agitation is deemed to become a danger to the Russian state. The strategy proposes to counter these threats by disseminating "truthful" information to citizens as well as promoting development of native platforms – such as own social media. Other official documents, such as the Information Security Doctrine of the Russian Federation (Security Council of the Russian Federation 2000), the Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space (Ministry of Defence of the Russian Federation 2011) as well as the Basic Principles for State Policy of the Russian Federation in the Field of International Information Security (Security Council of the Russian Federation 2013), treat Computer Network Operations as an inherent part of information security without distinction. This is also evident in the terminology used in Russian strategies, doctrines. Instead of the Western "cyber security", "information security" ("информационная безопасность") is central. Thus, the Russian perspective cares not only about the technical wholeness of information but also about the cognitive wholeness of information. Message –

towards the state, its executives and the population – can be the gunpowder in the cyberspace. Furthermore, there is also a strong perception of Russia already being the target of an ongoing IW, which is to a significant part waged in the cyberspace (Panarin 2012, 2014a). Hence, the desire to define and safeguard the borders of the Russian "information environment" or "information space" ("информационное пространство") appears to be a logical consequence. Russia is well aware of the discrepancies in the use of terminology, which is evident in the publicly available draft of the Cyber Security Strategy of the Russian Federation (Russian Federation Security Council 2014).

Similarly, the academic discourse grants a lot of focus to information. "Information has become a weapon. It is not just an addition to firepower, attack, manoeuvre, but transforms and unites all of these," say Ivan Vorobyev and Valery Kiselyov (2013) in an academic article on Russian military theory. Sergei Chekinov and Sergei Bogdanov (2011) ascribe even more power to information: "Today, the means of information influence reached such perfection that they can tackle strategic tasks." At the same time, other scholars are trying to make sense of the Western views on cyber and struggling towards an adequate terminology, which would be necessary to counter foreign developments (Balybin, Donskov & Boyko 2014). Still, it seems fairly unlikely that the technical aspects of cyberspace will be divided from the message anytime soon.

The potential power of information is firmly rooted in the Russian military and political thinking. More so, Russia also considers itself to be a target of ongoing IW: Russian academic literature makes clear that there is a perception of a rift between Russia, or the "historical Russian world", of which Ukraine is part, and "the West" with the US as the principle antagonist. This rift is both ideological and cultural, signified by an incompatibility of values ("духовные ценности") (Putin 2013a, 2013b). It is also perceived that the US continuously conducts IOs against other countries. The revolutions of recent years, such as the Arab Spring, are then explained with such operations. Professor Igor Panarin's (2014) book "Information Warfare and Communications" ("Информационная война и коммуникации") provides an example for this line of thought. The fall of the Soviet Union is a result of what Panarin calls the "first information war". According to him, the US currently engages in a "second information war" against, amongst others, Russia and Syria, to which the five-day war in Georgia in August 2008 was the clearest prelude. Further, Panarin speculates about the existence of an "Operation ANTI-PUTIN", which he compares to "Operation ANTI-STALIN" which was allegedly central to the "first information war". Panarin (2014b) also believes that Wikileaks' Julian Assange is an agent of the British MI-6 and that Euromaidan is the result of Western IOs. The focus on information and its power is not new, but a relic of the Soviet era (Glantz, 1988). In today's networked world, however, there are many more means to disseminate information than ever before.

3. BATTLESPACE (SOCIAL) MEDIA

In recent years, the Russian media landscape has changed significantly. As Freedom House (2014) noted, press freedom declined since Putin was re-elected as president in 2012. Relatively few media outlets feature critical political debate and Kremlin controls many news outlets, either through state-owned companies or aligned business owners. With the advancement

of technological development, traditional media sought to extend to new communications platforms. Many large and a high number of small newspapers, radio and TV channels are today present on the web. The step into the cyberspace also paved the way for the media to reach out to the world. Media outlets like RIA Novosti provide versions in English and other languages in addition to Russian-language content. Further, purely externally focusing media such as RT have gained audience abroad. RT is deeply integrated with social media through direct interfaces, the communication possibilities in the comment field. Similarly, the newest Russian media project, Sputnik, seems to be well integrated technically. According to the head of Rossiya Segodnya, Dmitry Kiselyov (2014), Sputnik was created by the Russian government to counter "propaganda promoting a unipolar world".

The Kremlin-aligned Russian traditional media has ever since the beginning of the crisis painted a negative picture of Euromaidan and Kiev. For example, Russian media claimed that hundreds of refugees were leaving Ukraine to seek asylum in Russia as a result of Ukrainian brutality towards the (Russian-speaking) population (TASS 2014a, 2014b, 2014c). In several cases, these reports were accompanied by photo and video material from the Ukrainian-Polish, not the Ukrainian-Russian border (Figure 1). Among other inaccuracies, there were also claims that the Ukrainian Navy frigate Hetman Sahaydachniy defected. Upon refutation, Russian media merely reported that the frigate had loaded NATO intelligence equipment (Sivkova 2014, TASS 2014d).

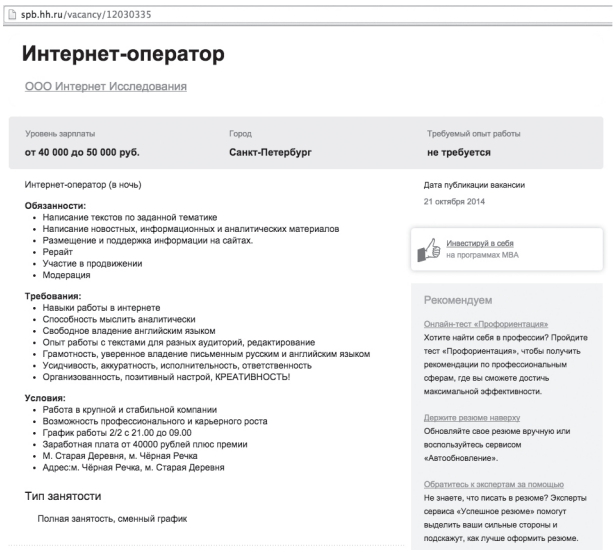
FIGURE 1: RUSSIAN CHANNEL 1 REPORTS ABOUT MASSES OF UKRAINIAN REFUGEES TRYING TO CROSS THE BORDER TO RUSSIA, SHOWING VIDEO FOOTAGE FROM BORDER CHECKPOINT BETWEEN UKRAINE AND POLAND (UMANEC 2014).

Social media constitutes an integral part of the Russian media landscape. In this context, the term "Runet" is interesting. Summing up the entirety of Russian-language content, this term describes the interconnectedness of the various parts. This includes pages that are maintained in Russia as well as pages operated by Russian-speakers abroad, traditional and new media, and other types of pages. All of these constitute nodes in a single large network. The phrase "in the Runet" ("в Рунете") describes how information migrates between different nodes. The term can also gain significance in the light of the Russian desire to define and defend "Russian

information space". Seddon (2014) describes the Russian government's approach to the Internet and social media as filled with fear towards an environment that is outside of control.

Since the early 2000s, the Internet has provided a space for political blogs, groups, and forums of varying ideology (Polyanskaya, Krivov & Lomko 2003). Social media was a key driver during the 2011/2012 demonstrations against the re-elections of Edinaya Rossiya and Vladimir Putin. During these demonstrations, pro-Kremlin online groups engaged in political debate, but also worked intensely to discredit the opposition and even to disrupt the organization of anti-government protests (Jaitner 2013). The opposition coined the term "Kremlin's trolls" to describe these groups. It has long been speculated that Kremlin itself employs and pays these "trolls" to spread pro-government discourse and to disrupt the opposition (Polyanskaya, Krivov & Lomko 2003, 2009; Fitzpatrick 2014). In 2014, the Finnish Defence Forces Research Institute confirmed the existence of paid "internet trolls", pointing at a St. Petersburg based company (Myös 2014). At the time of writing, this company continues to recruit employees to "work with social media" (Figure 2).

FIGURE 2: LLC "INTERNET RESEARCH" LOOKING TO HIRE AN "INTERNET OPERATOR". DUTIES: WRITING POSTINGS FOR SOCIAL MEDIA ON A DESIGNATED TOPIC. KNOWLEDGE OF ENGLISH LANGUAGE AND THE INTERNET, AS WELL AS CREATIVITY AND ABILITY TO THINK ANALYTICALLY ARE REQUIRED (HEADHUNTER.RU 2014).


spb.hh.ru/vacancy/12030335

Интернет-оператор

ООО Интернет Исследования

Уровень зарплаты
от 40 000 до 50 000 руб.

Город
Санкт-Петербург

Требуемый опыт работы
не требуется

Интернет-оператор (в ночь)

Обязанности:
- Написание текстов по заданной тематике
- Написание новостных, информационных и аналитических материалов
- Размещение и поддержка информации на сайтах.
- Рерайт
- Участие в продвижении
- Модерация

Требования:
- Навыки работы в интернете
- Способность мыслить аналитически
- Свободное владение английским языком
- Опыт работы с текстами для разных аудиторий, редактирование
- Грамотность, уверенное владение письменным русским и английским языком
- Усидчивость, аккуратность, исполнительность, ответственность
- Организованность, позитивный настрой, КРЕАТИВНОСТЬ!

Условия:
- Работа в крупной и стабильной компании
- Возможность профессионального и карьерного роста
- График работы 2/2 с 21.00 до 09.00
- Заработная плата от 40000 рублей плюс премии
- М. Старая Деревня, м. Чёрная Речка
- Адрес:м. Чёрная Речка, м. Старая Деревня

Тип занятости

Полная занятость, сменный график

Дата публикации вакансии
21 октября 2014

Инвестируй в себя
на программах MBA

Рекомендуем

Онлайн-тест «Профориентация»
Хотите найти себя в профессии? Пройдите тест «Профориентация», чтобы получить рекомендации по профессиональным сферам, где вы сможете достичь максимальной эффективности.

Держите резюме наверху
Обновляйте свое резюме вручную или воспользуйтесь сервисом «Автообновление».

Обратитесь к экспертам за помощью
Не знаете, что писать в резюме? Эксперты сервиса «Успешное резюме» помогут выделить ваши сильные стороны и подскажут, как лучше оформить резюме.

Interestingly, some of the social media accounts that can be linked to use by trolls have been created long in advance while the first activity of these Internet personas was recorded during the crisis. According to the "hacktivist" group "Anonymous", up to 600 paid "trolls" work in St. Petersburg (Baltic News Network 2014).

The troll activity is not limited to Runet with intense pro-Russian discourse appearing in commentaries on Western traditional and social media (Sindelar 2014). The Baltic countries

see themselves as particularly vulnerable: paid "Kremlin-trolls" are working not only from St. Petersburg but also in Estonia and Latvia (Baltic News Network 2014; The Lithuanian Tribune 2014).

Ukraine, with its large Russian speaking population, has long been an integral part of the Russian traditional and social media's audience. It is difficult to draw a definitive line between Runet and Ukrainian-language Internet. For example, before the crisis took place, the Russian equivalent of Facebook, VKontakte, was the most popular social media site amongst Ukrainian users. Another favourite social media is Odnoklassniki, or "Classmates" (ok.ru, 2014), where roughly 20 million profiles claim that they reside in Ukraine. However, the use of Russia-associated social media declined since the beginning of the crisis in favour of the Western alternative, Facebook (Unian 2014). Still, a mix of Russian and Ukrainian languages, as well as attitudes, is observable in political and other discussions throughout the social media. Antimaidan-discourse has been persistent throughout the crisis (Security Service of Ukraine 2015). The topics in this discourse correspond largely with the reporting in traditional Kremlin-leaning media. Herein, significant attention is given to nationalist and fascist participation in Euromaidan demonstrations (Anpilov 2013, RIANovosti 2014a, 2014b). Unsurprisingly, potential threats to "ethnic Russians" and the status of the Russian language are hot topics. These were fuelled by the attempt to amend Ukraine's legislation in the latter matter shortly after the interim government was installed. Although the bill was unsuccessful, it provided the pro-Kremlin debaters with "sufficient evidence" for hostility towards the Russian-speaking minority.

4. CASE CRIMEA AND NOVOROSSIYA[1]

When uniformed, armed individuals wearing no insignia appeared on the Crimean peninsula and later also in eastern Ukraine, Russian-leaning media nicknamed them "friendly people" who were "good to civilians" (Leonov 2014). The Ukrainian side called them "little green men", immediately identifying them as troops under Russian order. For weeks, Vladimir Putin (2014b) denied the participation of Russian troops in the Crimea take over and Defense Minister Sergei Shoigu (2014) called the rumours "nonsense and provocation". Nevertheless, the Russian-language media proceeded to portray these "soldiers of the future" as extremely well equipped and professional (Leonov, 2014). Meanwhile, Ukrainian troops stationed in Crimea were offered to pledge allegiance to the Russian Federation or alternatively to leave the peninsula or resign from their military careers. Russian media was then quick to report about large-scale surrender by Ukrainian troops (Yuzhniy Kurier 2014, CNN 2014). In retrospect, Verhovna Rada member Gennady Moskal (2014) blamed the fact that the Ukrainian troops had not received permission to use their weapons in time. Dmitry Tymchuk (2014) – Ukrainian military commentator and the front figure of the "Information Resistance" group[2], which gained a lot of popularity during the crisis – commented the events by accusing the interim government

1 Novorossiya – historically a region north of the Black Sea, annexed by the Russian Empire following the Russo-Turkish wars. The term was revived to denote a confederation of the self-proclaimed Donetsk People's Republic and Lugansk People's Republic in eastern Ukraine.

2 "Information Resistance" is, according to its own description on http://sprotyv.info/en/about-us, a non-governmental project that aims to counteract external threats to the informational space of Ukraine". The group provides operational data and analytics. As one of the project's front figures, Dmitry Tymchuk has provided analysis to, amongst others, Kyiv Post and Huffington Post.

in Kiev of having handled the situation in Crimea slowly and without sufficient clarity. However, the totality of IW in Crimea might have significantly added to Kiev's difficulties getting a clear picture of the events on the ground and thus have slowed down the decision making process.

The events in Crimea that unfolded in spring of 2014 provide important clues for the interplay between IOs and kinetic activity. The course of events – from the takeover of parliament in Simferopol and dismantling of the Ukrainian military presence on the peninsula, to the disputed referendum and the de facto annexation of the area to the Russian Federation – was accompanied by intense activity aimed to control the flow of information. This activity extended across the entire spectrum of communication and included kinetic, cyber and IOs targeting the physical, logical and social layers of communication.

In early March, Ukrtelecom reported kinetically damaged fiber optic cables and a temporary seizure of the company's offices; further disclosures described jammed naval communication (Maurer & Janz 2014). The head of Security Services of Ukraine also confirmed that government officials' mobile communications fell victim to an "IP-telephonic attack" (Paganini 2014). Some argued that attacking Ukrainian telecommunication equipment was a relatively easy task due to similarity to its Russian counterparts (Maurer & Janz 2014). However, this is also likely to be true for other critical infrastructure in the Ukraine. Still, communication channels appeared to be the primary target. In addition, there were reports of Distributed Denial of Service (DDoS) attacks as well as website defacements targeting political, government, and news websites (Maurer & Janz 2014, Pernik 2014). Examining cases of cyber attacks against Ukraine at that time, it quickly becomes evident that publicity was a crucial factor in the selection of possible targets. The "hacktivist" group "CyberBerkut" ("Киберберкут" http://cyber-berkut.org/en) claimed to have attacked the Ukrainian electronic voting system and later to have also successfully defaced several NATO websites (Maurer & Janz 2014, Paganini 2014). While these attacks are technically not very advanced, they suit to make a statement and are difficult to interpret for laymen, as in the case with NATO websites, or to sow distrust in systems, as in the case with the voting system. What is more, such attacks create speculations regarding the attackers' overall capabilities without revealing their full arsenal (Maurer & Janz 2014).

Striving for information superiority also implies the desire to access adversary's information. Cyberberkut repeatedly claimed to have gained access to telephone recordings and e-mail correspondence between Ukrainian, EU, and US officials and disclosed the content. In addition, the SBU (2014) warned that Ukrainian officials are targets of espionage malware distributed via e-mail. The espionage malware "Snake", "Uroboros" or "Turla", discovered in Ukrainian networks and forensically linked to Russia, remained the most advanced cyber activity against Ukraine. While it still largely aims at information, it cannot be linked to the immediate Ukrainian conflict directly because it appears to have been residing in Ukrainian networks since 2010 (Infosecurity Magazine 2014, Symantec 2014).

In many cases, it is difficult to distinguish information (or disinformation) that originates centrally from content that is created and disseminated by individuals based on their own opinion and experience. Throughout the crisis, pro-Russian activists and fighters have created and uploaded videos, photographs as well as written testimonies and continue to do so. Once

content is made available online, it is disseminated across various nodes, often taken out of its original context and given a new, sometimes contradictory, meaning by individuals or in an organized manner. Such intense activity naturally helps creating what can be called "the fog of information war", which fosters polarization amongst the spectators, who in turn influence the higher political levels' ability to act.

The importance of information superiority becomes apparent when looking at how much planning and resources were put into creating "official" as well as semi-official "information agencies". Among these are even several YouTube (2014) channels reaching relatively large audiences. Websites related to "Novorossiya" are particularly interesting: novorus.info and novorossia.su were, according to who.is, registered in March 2014. The use of this term, however, was popularized at a later point in time: Putin used the historical concept to describe the southeastern parts of Ukraine for the first time in a live phone-in on April 17, 2014 (Putin 2014a) and the so-called confederation Novorossiya was formally created on May 24, 2014. Similarly, the "official" websites of the People's Republics Donetsk and Lugansk were registered before the entities were self-proclaimed.

Online pro-Russian content also fills another auxiliary function: recruitment of combatants as well as supporting supply and logistics. This includes calls for monetary donations, necessities for children, medical supplies as well as practical information for those willing to travel to combat zones. Activists of extremely varying ideologies recruit combatants to join the rebel forces in eastern Ukraine. An interesting observation in this context is how various ideologies converge for a "universal goal". For example, a thread on a Stalinist forum ("17th of March Movement" or "Общесоюзное движение 17 марта" 2014) features recruitment information provided by imperialists, communists, nationalists as well as "orthodox patriots". Even volunteers from the North Caucasus have found their way to the conflict – video clips on various social media testify Kadyrov's followers' ("Кадыровцы") involvement in the fighting in eastern Ukraine. The individual posts differ rhetorically. Based on on a common slim narrative, different elements characterize the evilness of the foe with a common denominator: a fight for the "good" values and fraternity with the people of eastern Ukraine. Depending on the individual ideology, activists use communist slogans, prayers and "Russian-orthodox" values as well as grave anti-Semitic speech. While the various groups' discourse differs significantly, the lowest common denominator appears to be the mention of fascism as a foe. Given the constantly upheld memory of the Great Patriotic War, this is hardly surprising – even though the term is interpreted differently within the individual groups. Another notable factor is that, despite the convergence, there is little evidence for hostility between groups of conflicting ideology – a common foe unites.

5. THE ANATOMY OF RUSSIAN INFORMATION WARFARE

Ever since the dawn of the Ukraine crisis, the physical events were accompanied by an intense information struggle, a struggle to establish a narrative but also to mislead the opponents. Despite its likely origin at the top political level, this struggle differs from the pre-Internet

and pre-globalization propaganda in some important aspects. Unlike propaganda during Soviet times, which relied heavily on narratives designed at the top level as well as on isolation, today's Russian IW incorporates the audience as a narrative-bearing and a narrative-developing factor. Furthermore, today's countless interfaces between various audiences – such as domestic, diaspora, and foreign – present a probably insurmountable obstacle for conveying individual narratives to different audiences. Therefore, anything that the top leadership aims to share with domestic audience is almost instantly shared with the foreign population. This creates a requirement to tailor narratives to fit a large audience.

The interplay between different levels of information – from the political leadership of President Putin at the tip, via the traditional media to the grassroots level in social media – appears to be an important core element of the Russian IW. One of the core narratives surrounds Russia's position in the world: a misunderstood counterweight to Western liberal values and a misjudged historic superpower. This narrative is slim and can be easily absorbed by the general population and even groups abroad. Being slim and universal, this narrative provides a perspective or a foundation for interpretation of further events. Once it reaches the grassroots level, it can be customized to fit various groups' individual ideologies. Elements can be highlighted or refilled with attributes in accordance with a group's opinions – by the group itself. For example, nationalist groups focus on Russia's historical position of power, while communist groups discuss Russian antagonism to capitalism with reference to the Soviet era. Applying such pyramid method has at least two advantages. First, since individual flavours of narratives are created at group level, their competition is less exposed to the general public. Second, there is no need to design individual narratives and inject these into groups. Instead, already existing group dynamic is utilized, including the group's opinion-makers' position of trust within the group.

Because the narrative at its origin aims at both domestic as well as foreign audience, the mechanism also serves its purpose outside the country. The idea of a "Russian World" ("Русский Мир") as the bearer of "Russian soul" and "Russian values", which does not only include ethnic Russians but the world's "Russian-speaking population", is continuously maintained and serves as a unifying factor. In extension, the message is also transported beyond the Russian-speaking diaspora. The narrative for the world outside Russia and former Soviet area is complemented by information that aims to seed doubts and distrust towards the Western systems. Western "hypocritical behaviour" and "decay of traditional values" are two of the frequently recurring topics, which particularly gain attention within system-critical groups.

A particular focus on the grassroots level is detectable, evident by the use of "trolls" or "opinion agents". Such practice indicates an inherent understanding of how to penetrate societies that are naturally sceptic towards mainstream information channels. It also implies an awareness of the importance of popular opinion, as well as an understanding of the significance of "private" or interpersonal channels of communication. In the post-Soviet environment where the population has little trust in official information, interpersonal communication gains importance. Information shared by an acquaintance enjoys more trust than the message provided through media (Lonkila 2012). Meanwhile, in open societies, this methodology can successfully create doubts in regard to objectivity that is desired from the mainstream media. Due to the relative

anonymity in the cyberspace, trolls can operate by blending into the crowd, being difficult to detect by laymen. Similarly, cyber events of little technical harm, such as DDoS, website defacements, or mere suggestion that a system has been compromised by an intrusion, can present themselves as far more impactful to laymen. This in turn sows distrust in established systems, especially when paired with efforts to create an informational blackout, as seen in Crimea. The (partial) blackout itself then hinders the attacked side to gain an overview of events and, at the same time, allows the attacking side to promote its own narrative.

Inside the Russian sphere of influence, the younger generation that grew up in the post-Soviet era is seen as a weak link, evident through concern with the youth being receptive to undesired influences (Putin 2014c). Having inherited their parents' distrust in mainstream media, they also enjoy a greater access to non-Russian content and thus are, according to Kremlin's line of thought, exposed to influence from the West. At the same time, it is possible to reach the younger generation via social media in urban centres, where both Internet penetration and affiliation with Western values are high. Russian IW strategists likely see these areas as most problematic. A certain level of criticism and counter-narrative may be desired to be able to relate propagated narrative to an antithesis, and to maintain an illusion of freedom. The impact of IW at the grassroots aiming on the younger population in urban centres in post-Soviet countries appears to be a particularly interesting subject to scrutinize in detail, possibly in the context of vulnerability of open societies in general.

6. CONCLUSIONS: THE ROLE OF CYBER IN RUSSIAN IW

Technological developments of the recent decades have presented new possibilities to enhance and expand IW geographically, while also presenting those who want to engage in IW activities with new challenges. Russian leadership appears to have adapted to the new, networked environment, putting a large focus on efforts throughout the crisis on information and control thereof. Here, physical efforts converge with cyber attacks and other influence activities. Particularly during the seizure of Crimea a twofold use of cyber could be observed: attacks against telecommunication equipment and media channels appear to have contributed to a communication blackout, while other attacks aimed at influencing the opinion of domestic and foreign audiences. In this context, technically less advanced attacks, such as DDoS or website defacements can be argued to constitute a part of cyber IW. Also, while the Uroboros spyware cannot be absolutely attributed to the particular crisis, it is an instrument for gaining information superiority. In this perspective, cyber has contributed to the course of the events as a part of overall IW efforts. Meanwhile, the cyberspace as such has required adaptation in Russian IW practices. Probably most obvious adaptations are the use of a slim narrative and the utilization of "trolls" who thrive in an environment of relative anonymity. Furthermore, the networked reality enhances the influence-bearing factor of any action, such as the deployment of troops. Russian IW seeks to utilize these factors by providing a narrative as a base for interpretation of events.

Overall, IW has significantly contributed to the successful annexation of Crimea, as well as to the creation of the Novorossiya concept and thus to the continuation of the crisis. This in turn highlights the need to address the new ways IW is conducted. The convergence between malicious cyber activities and IW deserve professional and policy attention. What might be called conventional cyber attacks by Russia were almost negligible; however, these new cyber aspects must be considered as an integral part of new information warfare.

REFERENCES

Anpilov, V. 2013. "Анпилов: Фашисты захватывают Майдан. (Anpilov: Fascists taking over Maidan.)" *Pravda*. Accessed 10 December 2014. http://www.pravda.ru/world/formerussr/ukraine/10-12-2013/1184934-anpilov-0/

Baltic News Network. 2014. "Latvia overrun by Kremlin-financed internet trolls." *Delphi by The Lithuanian Tribune*, 4 December 2014. Accessed 20 December 2014. http://en.delfi.lt/nordic-baltic/latvia-overrun-by-kremlin-financed-internet-trolls.d?id=66577080

Balybin, C. Donskov, Yu. and Boyko A. 2014. "Electronic Warfare Terminology in the Context of Information Operations." *Military Thought* 23 (3).

Checkinov, S. & Bogdanov S. 2010. "Asymmetrical Actions to Maintain Russia's Military Security." *Military Thought* 2010 (1).

CNN. "CNN: Украинские войска в Крыму сдаются силам самообороны. (Ukrainian troops surrender to Crimean self-defence forces.)" *edited by RT*, 19 March 2014. Accessed 17 December 2014. http://russian.rt.com/inotv/2014-03-19/CNN-Ukrainskie-vojska-v-Krimu

Fitzpatrick, C. 2014. "Russia This Week: The Kremlin's Growing Army of Internet Trolls." *The Interpreter*, 14 November 2014. Accessed 21 November 2014. http://www.interpretermag.com/russia-this-week-the-kremlins-growing-army-of-internet-trolls/

Freedom House. 2014. Russia. Freedom of press 2013, 2014. *Freedom House*. https://www.freedomhouse.org/report/freedom-press/2013/russia - .VH74sJPF800:

Glantz, D. 1988. "Surprise and Maskirovka in Contemporary War." *Army Combined Arms Center Fort Leavenworth KS Soviet Army Studies Office*. Accessed 13 November 2014. http://www.dtic.mil/get-tr-doc/pdf?Location=U2&doc=GetTRDoc.pdf&AD=ADA216491

Headhunter.ru. 2014. "Интернет Оператор. (Internet Operator.)" *HeadHunter.ru.* Accessed 17 November 2014. http://spb.hh.ru/vacancy/12030335

InfoSecurity, Magazine. 2014. "Snake Cyber-espionage Campaign Targetting Ukraine is Linked to Russia." *InfoSecurity Magazine*, 11 March 2014. http://www.infosecurity-magazine.com/news/snake-cyber-espionage-campaign-targetting-ukraine/

Jaitner, M. 2013. "Exercising Power in Social Media." *The fog of cyber defence*., edited by J. Rantapelkonen, & Salminen, M. Julkaisusarja 2. Artikkelikokoelma no: 10.

Kenez, P. 1985. *The birth of the propaganda state: Soviet methods of mass mobilization, 1917-1929*. : Cambridge University Press.

Kiselyov, D. 2014. Дмитрий Киселёв представил международный проект "Спутник". (Dmitri Kiselyov introduces the international project "Sputnik".) *YouTube.* Accessed: 20 December 2014. https://www.youtube.com/watch?v=WR6qEi8I-IE

Leonov, A. 2014. “Солдаты будущего: чем вооружены «вежливые люди» в Крыму. (Future soldiers: The friendly men’s equipment in Crimea.)” *Forbes,* 7 March 2014. Accessed 20 December 2014. http://m.forbes.ru/article.php?id=251676

Lonkila, M. 2012. “Russian Protest On-and Offline: The role of social media in the Moscow opposition demonstrations in December 2011.” *UPI FIIA Briefing Papers* 98 (2012).

Maurer, T. & Janz, S. 2014. “The Russia-Ukraine Conflict: Cyber and Information Warfare in a Regional Context.“ *The International Relations and Security Network*, 17 October 2014. Accessed 14 December 2014. http://www.isn.ethz.ch/Digital-Library/Articles/Detail/?id=184345

Ministry of Defence of the Russian Federation. 2011. Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве. (Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space.)

Paganini, P. 2014. “Crimea – The Russian Cyber Strategy to Hit Ukraine.” *InfoSec Institute*, 11 March 2014. http://resources.infosecinstitute.com/crimea-russian-cyber-strategy-hit-ukraine/

Panarin, I. 2012. “О Доктрине информационного противоборства России. (On the Russian doctrine of Information Defence.)” *Voyennoye Obozreniye*, 18 July 2012. Accessed 10 December 2014. http://topwar.ru/16540-o-doktrine-informacionnogo-protivoborstva-rossii.html

Panarin, I. 2014a. *Информационная война и коммуникации. (Information warfare and communications.)* Moskva, Russia: Goryachaya Liniya - Telekom.

Panarin, I. 2014b. Posting on Facebook, 29 June 2014. Accessed 19 December 2014. http://www.facebook.com/permalink.php?story_fbid=487886764691548&id=100004106865632&fref=ts

Pernik, P. 2014. “Is All Quiet on the Cyber Front in the Ukrainian crisis?” *RKK ICDS International Centre for Defence and Security*, 7 March 2014. http://www.icds.ee/et/blogi/artikkel/is-all-quiet-on-the-cyber-front-in-the-ukrainian-crisis/

Polyanskaya, A., Krivov A. & Lomko I. 2003. “Виртуальное око старшего брата. (Big Brother’s virtual eye.)” *Zhurnal Vestnik*, 3 April 2003.

Polyanskaya, A., Krivov A. & Lomko I. 2009. “The Kremlin’s Virtual Squad.” *Open Democracy*, 19 March 2009.

Putin, V. 2013a. “Путин защитит традиционные семейные ценности. (Putin to defend traditional family values.)” *Vesti*, 12 December 2013. Accessed 20 December 2014. http://www.vesti.ru/doc.html?id=1166423

Putin, V. 2013b. “Наши духовные ценности делают нас единым народом (Our values unite us as peoples.)” Speech in Kiev 27 June 2013.” *YouTube.* Accessed 20 December 2014. https://www.youtube.com/watch?v=YW1WYh_gvJg

Putin, V. 2014a. Прямая линия с Владимиром Путиным. Phone-in with Vladimir Putin. (Transcript). 17 April 2014. Accessed 15 December 2014. http://kremlin.ru/news/20796

Putin, V. 2014b. Путин: “В Крыму нет российских солдат. Это самооборона Крыма. (Putin: There are no Russian soldiers. This is Crimeas popular defense.)” *YouTube*. Accessed 20 December 2014. https://www.youtube.com/watch?v=qzKm7uxK8ws

Putin, V. 2014c Security Council meeting 20 November 2014. Transcript. Accessed 21 November 2014. http://kremlin.ru/news/47045

RIANovosti. 2014a. “ ‘Фашисты’ и ‘террористы’: СМИ США выясняют, кто есть кто на Украине. (‘Fascists’ and ‘terrorists’ Media in the US sorts out who is who in the Ukraine.)” *RIA Novosti*, 18 May 2014. Accessed 20. December 2014. http://ria.ru/world/20140518/1008297621.html

RIANovosti. 2014b. “Более 140 тысяч граждан уехали из Украины в Россию, заявил сенатор. (Senator: More than 140k Ukrainians left for Russia.)” *RIA Novosti*, 1 March 2014. Accessed 13 December 2014. http://ria.ru/world/20140301/997697055.html

Security Council of the Russian Federation. 2000. Доктрина информационной безопасности Российской Федерации. (Information Security Doctrine of the Russian Federation.)

Security Council of the Russian Federation. 2009. Стратегия национальной безопасности Российской Федерации до 2020 года. (National Security Strategy to 2020.)

Security Council of the Russian Federation. 2013. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года. (Basic Principles for State Policy of the Russian Federation in the Field of International Information Security to 2020.)

Security Council of the Russian Federation. 2014. Концепция стратегии кибербезопасности Российской Федерации. (Cyber Security Strategy of the Russian Federation – Concept.)

Seddon, M. 2014. “Documents Show How Russia’s Troll Army Hit America.” *Buzzfeed*, 2 June 2014. Accessed 20 December 2014. http://www.buzzfeed.com/maxseddon/documents-show-how-russias-troll-army-hit-america

Security Service of Ukraine, SBU 2014. Служба безпеки України попереджає про “фейкові” електронні розсилки від імені державних органів. (Security Service of Ukraine warns of “fake” e-mails on behalf of public authorities.) 26 September 2014. Accessed 15 December 2014. http://www.sbu.gov.ua/sbu/control/uk/publish/article?art_id=132039&cat_id=39574

Security Service of Ukraine, SBU 2015. СБУ: власники інтернет-спільноти “Антимайдан” знаходяться у Криму. (SBU: online community “Antimaidan” located in Crimea.) 13 March 2015. Accessed 15 March 2015. http://www.ssu.gov.ua/sbu/control/uk/publish/article;jsessionid=379798D64EB113AED76BBA26C5AE26A6.app1?art_id=138947&cat_id=39574

Shoigy, S. 2014. “Шойгу о российской технике в Крыму: ‘чушь и провокация’. (Shoigu on Russian military in Crimea: ‘nonsense and provocation’.)” *BBC Russkaya Sluzhba*, 5 March 2014. Accessed 2 December 2014. http://www.bbc.co.uk/russian/russia/2014/03/140305_crimea_troops_shoigu

Sindelar, D. “The Kremlin’s Troll Army.” *The Atlantic*, 12 August 2014. Accessed 20 December 2014. http://www.theatlantic.com/international/archive/2014/08/the-kremlins-troll-army/375932/

Sivkova, A. 2014. “Флагман ВМФ Украины «Гетман Сагайдачный» перешел на сторону России. (Flagship the Ukrainian Navy, “Getman Sagaidachny“ defected to Russia.)” *Izvestiya*, 1 March 2014. Accessed 20. December 2014. http://izvestia.ru/news/566817

Symantec. 2014. Turla: Spying tool targets governments and diplomats. *Symantec*, 7 August 2014. Accessed 7 December 2014. http://www.symantec.com/connect/blogs/turla-spying-tool-targets-governments-and-diplomats

TASS. 2014a. “Число обращений граждан Украины в ФМС в Краснодарском крае увеличилось на 100%. (Number of requests for asylum by Ukrainians doubles in Krasnodar region.)” *TASS*, 26 March 2014. Accessed 20 December 2014. http://itar-tass.com/obschestvo/1075504

TASS. 2014b. “Граждане Украины просят временное убежище в Новгородской области. (Ukrainians request temporary asylum in Novgorod.)” *TASS*, 26 March 2014. Accessed 20 December 2014. http://itar-tass.com/spb-news/1076617

TASS. 2014c. “ФМС: за временным убежищем в РФ обратились более 245 тыс. граждан Украины. (FMS: Over 245k Ukrainians ask for asylum in Russia.)” *TASS*, 4 December 2014. Accessed 20 December 2014. http://itar-tass.com/obschestvo/1616949

TASS. 2014d. “Ukrainian frigate Hetman Sahaidachny carries NATO’s intelligence equipment — source.” *TASS*, 05 March 2014 Accessed 20 December 2014. http://tass.ru/en/world/722267

The Lithuanian Tribune. 2014. “Lithuania’s State Security Department warns citizens to beware of propaganda from Russia.” *The Lithuanian Tribune*, 5 September 2014. Accessed 17 December 2014. http://en.delfi.lt/lithuania/society/lithuanias-state-security-department-warns-citizens-to-beware-of-propaganda-from-russia.d?id=65761684

Tymchuk, D. 2014. “О предательстве. (On betrayal.)” *Gazeta.ua*, March 2014. Accessed 20 December 2014. http://gazeta.ua/ru/blog/42707/o-predatelstve

Unian. 2014. “Російські соціальні мережі втрачають популярність в Україні. (Russian Social Media loses popularity in the Ukraine.)” *Unian*, 30 July 2014. Accessed 20 December 2014. http://www.unian.ua/science/945549-rosiyski-sotsialni-mereji-vtrachayut-populyarnist-v-ukrajini.html

Umanec, V. 2014. “Як лоханувся телеканал ОРТ. (TV channel ORT failed.)” *Podglyad*, 2 March 2014. Accessed 17 December 2014. http://poglyad.te.ua/podii/yak-lohanuvsya-telekanal-ort/

Vorobyov, I. & Kiseljov V. 2013 “Russian Military Theory: Past and Present.” *Military Thought* 2013 (3).

YouTube. 2014. Database query: “Новости Новороссии”. *YouTube*. Accessed 13 December 2014.

Yuzhniy Kurier. 2014. “Все. Украинские солдаты в Крыму сдаются. (The End. Ukrainian soldiers in Crimea surrender.)” *Yuzhniy Kuri’er*, March 19, 2014. Accessed 20. December 2014. http://courier.crimea.ua/news/courier/vlast/1146781.html