Russian Information Warfare: Lessons from Ukraine

by

Margarita Jaitner

Chapter 10 in
Kenneth Geers (Ed.), Cyber War in Perspective:
Russian Aggression against Ukraine,
NATO CCD COE Publications, Tallinn 2015

CCDCOE

NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

Swedish Defence University researcher Margarita Jaitner highlights current Russian Information Warfare (IW) theory in Chapter 10. She contends that Moscow has an inherent belief in the power of information control to advance its political and military goals. In Russian doctrine, cyber security is subordinate to information security, and cyberspace is only one part of the 'information space'. National security planners are concerned with both 'technical' and 'cognitive' attacks, and recognise that achieving information superiority involves everything from propaganda to hacking to kinetic military operations. Margarita Jaitner argues that the annexation of Crimea was a textbook case in information superiority.

NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

Russian Information Warfare: Lessons from Ukraine

Margarita Levin Jaitner
Swedish Defense University

1 Introduction

'Information is now a species of weapon',[1] write Russians Maj. Gen. (R) Ivan Vorobyev and Col. (R) Valery Kiselyov. Closer to the truth is that Russia has a long history of using information as a weapon – both in the context of mobilising its own population[2] and in demonising foreign powers.[3]

Therefore, it is only natural that Russia has employed Information Warfare (IW) in Ukraine: from the onset of the 'Euromaidan' demonstrations, to the annexation of Crimea, and as a dimension of ongoing military operations in eastern Ukraine. And it is equally unsurprising that, in the internet era, Moscow has developed effective tactics for waging IW in cyberspace.

This chapter discusses contemporary Russian IW theory and analyses Russian IW activities on the ground in Crimea and in eastern Ukraine. While the dynamic and diffuse nature of IW makes it difficult to gauge its precise impact, this chapter argues that Russian IW in Crimea and in eastern Ukraine has been highly successful, and that the West is currently playing catch up vis-à-vis Russia in this arena.

1 Vorobyov, I. and Kiseljov, V. 'Russian Military Theory: Past and Present.' *Military Thought* 2013 (3).
2 Peter Kenez. *The birth of the propaganda state: Soviet methods of mass mobilization, 1917-1929* (Cambridge University Press, 1995).
3 David M. Glantz. *Surprise and Maskirovka in Contemporary War.* Soviet Army Studies Office, Army Combined Arms Center, Fort Leavenworth KS, 1988). http://www.dtic.mil/get-tr-doc/pdf?Location=U2&doc=GetTRDoc.pdf&AD=ADA216491.

2 Information Security and Cyber Security in Russian Military Theory

In Russian government and academic circles, information is understood to be a form and source of great power. This was true well before the advent of the internet and cyberspace – which have not changed Russian IW strategy, but only its tactics.

In the West, cyber security and information security are considered to be two different things. In Russia, however, cyber is subordinate to information security, which allows national security planners to oversee both technical data (e.g. the integrity of password files) and cognitive data (e.g. political information on websites). Thus, any information found on the World Wide Web could be a 'missile' fired at Russia that is more dangerous than a typical cyber attack as currently understood in the West.

The logical consequence of this Russian perspective is to define and to protect the borders of the Russia's 'information space' (*информационное пространство*), and this philosophy is to be found easily in Russian doctrines, strategies, and activities both at home and abroad – including in Ukraine.

For example, Russia's *National Security Strategy 2020* states that 'nationalist, separatist, radical religion' is a danger to nation-states, and that a 'global information struggle' is now intensifying. The document proposes to counter this threat by disseminating 'truthful' information to Russian citizens, including via the promotion of native internet platforms encompassing social media.[4]

As for the importance of cyberspace, numerous official documents describe computer network operations as an integral part of Russian information security, including: *Information Security Doctrine of the Russian Federation*,[5] *Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space*,[6] and *Basic Principles for State Policy of the Russian Federation in the Field of International Information Security*.[7]

> *Information superiority in cyberspace is an essential goal.*

Academic discourse within the Russian military is similar. From a historical perspective, progress in computer science has wrought a new generation of warfare in which the achievement of information superiority in cyberspace is an essential goal. Within any desired zone of influence, this includes attacks against and defence of

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

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

6 Ministry of Defence of the Russian Federation. *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) (Moscow, 2011).

7 Security Council of the Russian Federation. *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.) (Moscow, 2013).

both technical data and cognitive information, as well as and psychological operations, or PSYOPS.

Maj. Gen. (R) Ivan Vorobyev and Col. (R) Valery Kiselyov have written that information is 'not just an addition to firepower, attack, manoeuvre, but transforms and unites all of these'.[8] Col. (R) Sergei Chekinov and Lt. Gen. (R) Sergei Bogdanov go even further: 'Today the means of information influence reached such perfection that they can tackle strategic tasks'.[9]

Information can disorganise governance, delude adversaries and reduce an opponent's will to resist.

Checkinov and Bogdanov point out – in the aftermath of the annexation of Crimea and the current destabilisation of Ukraine – that information can be used to disorganise governance, organise anti-government protests, delude adversaries, influence public opinion, and reduce an opponent's will to resist. Furthermore, it is critical that such activities begin prior to the onset of traditional military operations.[10]

At least since Soviet times, Russia considers itself to be a victim of IW, engaged in a battle between the 'historical Russian world' (of which Ukraine is a part) and the West where the US is its principal antagonist.[11] Professor Igor Panarin has described a 'first information war' during the Cold War that resulted in the demise of the Soviet Union. Today, he sees an 'Operation ANTI-PUTIN' modelled on an earlier 'Operation ANTI-STALIN'. He contends that Western IW was behind both the Arab Spring[12] and Euromaidan, and that WikiLeaks' Julian Assange is an agent of the British MI6.[13] Panarin believes there is a 'second information war' taking place against countries such as Russia and Syria which began at least by the time of the Russo-Georgian war in 2008.[14] Russian President Vladimir Putin has characterised the rift between Russia and the West as an incompatibility of values («*духовные ценности*»).[15]

Panarin is far from being the only contemporary Russian military thinker arguing this line. A group of five authors recently wrote in Russia's *Military Thought* that 'The NATO countries led by the US … have set up a powerful information operations (IO) system and are going on expanding and improving it'.[16]

8 Vorobyov and Kiseljov 'Russian Military Theory: Past and Present.' *Military Thought,* 2013 (3).

9 Sergei G. Checkinov and Sergei A. Bogdanov. 'Asymmetrical Actions to Maintain Russia's Military Security.' *Military Thought,* 2010 (1).

10 Sergei G. Checkinov and Sergei A. Bogdanov. 'The Art of War in the Early 21st Century: Issues and Opinions.' *Military Thought,* 2015 (24).

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

12 *Ibid*.

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

14 Igor Panarin. 2014a.

15 Vladimir Putin. '*Путин защитит традиционные семейные ценности*. (Putin to defend traditional family values).' Vesti, 12 December, 2013a. http://www.vesti.ru/doc.html?id=1166423; Vladimir Putin. '*Наши духовные ценности делают нас единым народом*' (Our values unite us as peoples. Speech in Kyiv 27.07.2013.). YouTube, 2013b. https://www.youtube.com/watch?v=YW1WYh_gvJg Accessed 20 December 2014.

16 Dylevski, I.N., Elyas, V.P., Komov, S.A., Petrunin, A.N. & Zapivakhin V.O.'Political and Military Aspects of the Russian Federation's State Policy on International Information Security.' *Military Thought,* 2015 (24).

Even Russia, however, is not a monolith.[17] Some military scholars have criticised the prevailing view and have suggested that a distinction should be drawn between attacks on technical and cognitive data, detailing a 'technospheric war' largely corresponding to the Western perception of 'cyber war'.[18] Similarly, a publicly available draft of the next *Cyber Security Strategy of the Russian Federation* problematises the difference between the Russian and the Western views on the matter, suggesting that cyber security and information security be treated as distinct challenges. However, to date these remain unimplemented proposals.

3 Russian IW in Crimea and Novorossiya[19]

Russian IW in Ukraine began well before the current conflict. The Security Services of Ukraine (SBU) warned that its government officials had been targeted by Russian espionage malware (variously called 'Snake', 'Uroboros' or 'Turla') since 2010.[20,21,22] Successful cyber espionage can have a strategic impact. In a military context, it can be directly linked to a desire to gain information superiority on the battlefield,[23] and can sometimes be easy to associate with ongoing military operations.[24]

In Crimea, just as soon as insignia-less armed fighters appeared on the scene (the same dynamic later occurred in eastern Ukraine), Russian media referred to them as 'friendly people' who were 'good to civilians',[25] while the Ukrainian side called them the 'little green men' from Russia. For weeks, Vladimir Putin[26] and

> *The course of events was enveloped in a sophisticated effort to control the flow of information.*

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

18 Yurii Starodubtsev, Vladimir Bukharin and Sergei Semenov (2012). Техносферная война (War in the technosphere). *Военная Мысль (Military Thought) 2012(7).*

19 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.

20 Security Service of Ukraine, SBU. 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. http://www.sbu.gov.ua/sbu/control/uk/publish/article?art_id=132039&cat_id=39574.

21 '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/.

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

23 James J. Coyle. 'Russia Has Complete Information Dominance in Ukraine.' *Atlantic Council*,12 May 2015. http://www.atlanticcouncil.org/blogs/new-atlanticist/russia-has-complete-informational-dominance-in-ukraine.

24 'Operation Armageddon: Cyber Espionage as a Strategic Component of Russian Modern Warfare.' *Lookingglass*, 28 April 2015. https://lgscout.com/wp-content/uploads/2015/04/Operation_Armageddon_FINAL.pdf.

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

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

Russian Defence Minister Sergei Shoigu[27] denied the participation of Russian troops in the Crimea takeover – even though Ukrainian troops on the peninsula were forced into a quick, large-scale surrender.[28][29]

In warfare, there has always been a tight relationship between IW and traditional military operations. In Crimea, the entire course of events – from the takeover of the Simferopol parliament to the disputed referendum and the Russian annexation of Crimea – was enveloped in a sophisticated effort to control the flow of information. Russian IW extended across the entire spectrum of communication in both the cyber and non-cyber domains, targeting its physical, logical, and social layers.

In early March, *Ukrtelecom* reported kinetically damaged fiber-optic trunk cables, as well as the temporary seizure of its company's offices. Further disclosures detailed the jamming of Ukrainian naval communications.[30] SBU Chief Valentyn Nalyvaichenko declared that Ukrainian government officials' mobile communications were subjected to an 'IP-telephonic attack'.[31] And on the World Wide Web, government sites and news portals suffered Distributed Denial of Service (DDoS) attacks and defacements – all of which contributed to a significant information blackout.[32],[33]

The 'hacktivist' group *Cyberberkut*[34] has repeatedly claimed to have gained access to telephone recordings and e-mail correspondence between Ukrainian, European Union (EU) and US officials – and released some content to prove it. *Cyberberkut* also allegedly attacked the Ukrainian electronic voting system and defaced several NATO websites.[35]

The importance of gaining information superiority in warfare can be seen in how much time and resources have been spent in creating official, semi-official, and unofficial sources of war-related information, including dedicated channels on YouTube.[36]

The success of IW is hard to gauge, but these attacks likely made it more difficult for Kyiv to gain a clear picture of what was happening in Crimea – which in turn presumably hampered its decision-making process. Even unsophisticated cyber attacks tend to generate significant media attention, and as a bonus can sow general distrust in systems and their security architecture.[37]

---

27 Sergey Shoigy. 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. http://www.bbc.co.uk/russian/russia/2014/03/140305_crimea_troops_shoigu.

28 Yuzhniy Kurier. 'Все. Украинские солдаты в Крыму сдаются. (The End. Ukrainian soldiers in Crimea surrender.).' *Yuzhniy Kur'er*, March 19, 2014. http://courier.crimea.ua/news/courier/vlast/1146781.html.

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

30 Tim Maurer and Scott Janz. 'The Russia-Ukraine Conflict: Cyber and Information Warfare in a Regional Context.' *The International Relations and Security Network*, 17 October 2014. http://www.isn.ethz.ch/Digital-Library/Articles/Detail/?id=184345.

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

32 Tim Maurer and Scott Janz. 'The Russia-Ukraine Conflict: Cyber and Information Warfare in a Regional Context.'

33 Piret Pernik. '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/.

34 'Киберберкут' http://cyber-berkut.org/en.

35 Pierluigi Paganini. 'Crimea – The Russian Cyber Strategy to Hit Ukraine.'

36 'YouTube.' 2014. Database query: 'Новости Новороссии'. Accessed 13 December 2014.

37 Tim Maurer and Scott Janz. 'The Russia-Ukraine Conflict: Cyber and Information Warfare in a Regional Context.'

Ukrainian military commentator Dmitry Tymchuk, speaking on behalf of the 'Information Resistance' group,[38] accused the interim government in Kyiv of lacking clarity and moving too slowly,[39] and Ukrainian parliament (Verhovna Rada) member Gennady Moskal complained that Ukrainian troops had not received permission to use their weapons in time.[40]

Today, the war in eastern Ukraine can also be described as a hall of IW smoke and mirrors. On 17 April, 2014, Vladimir Putin referred to the south-eastern part of Ukraine as *Novorossiya*, and a similarly named 'confederation' was formally created on May 24, 2014.[41] However, an analysis of web data shows that cyber preparations were made prior to this announcement: *Novorossiya* websites such as novorus.info and novorossia.su were registered with who.is in March 2014, and the official websites of the People's Republics of Donetsk and Lugansk were registered before the entities came into being.[42] Finally, Moscow has consistently denied that its military personnel are engaged in Ukraine, but web-based studies have found evidence of their deployments to Ukraine[43] as well as their involvement in the crash of the Malaysian Airlines flight 17,[44] via social media and imagery analysis.[45]

4 The Unique Characteristics of Russian IW

The Russian political narrative – aimed at both domestic and foreign audiences – describes a 'Russian World' (*Русский Мир*), 'Russian values', and even a 'Russian soul'. The narrative's articulation begins at the very top, in the person of Vladimir Putin, and flows downward in a pyramidal fashion through traditional media and cyberspace all the down to the grassroots level. It targets not just Russian citizens but the entire Russian-speaking population of planet Earth. Beyond that, it is expected that the narrative's influence will organically spread outside the diaspora.

The basic storyline is easy to comprehend and to convey, and is intended to be become a foundation for the interpretation of current and future world events. In this narrative, Russia is a misunderstood and misjudged superpower, and a necessary counterweight to Western liberal values. By contrast, the West has experienced

38 '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.

39 Dimitro Tymchuk. 'О предательстве (On betrayal).' *Gazeta.ua*, March 2014. http://gazeta.ua/ru/blog/42707/o-predatelstve.

40 Yuzhniy Kurier. 'Все. Украинские солдаты в Крыму сдаются. (The End. Ukrainian soldiers in Crimea surrender.).' *Yuzhniy Kurier*, 19 March 2014. http://courier.crimea.ua/news/courier/vlast/1146781.html.

41 Vladimir Putin. 'Прямая линия с Владимиром Путиным.' Phone-in with Vladimir Putin. (Transcript). 17 April 2014. http://kremlin.ru/news/20796.

42 See who.is listings for novorus.info (http://who.is/whois/novorus.info), novorossia.su (http://who.is/whois/novorossia.su)

43 'Selfie Soldiers: Russia Checks in to Ukraine.' *Vice News*, 16 June, 2015.

44 'Bellingcat.com' By and for citizen investigative journalists: Russia. http://www.bellingcat.com/tag /russia/.

45 NATO ACO – Allied Command Operations. 'New Satellite Imagery Exposes Russian Combat Troops Inside Ukraine'. *NATO Allied Command Operations: News,* 28 August 2014. http://aco.nato.int/new-satellite-imagery-exposes-russian-combat-troops-inside-ukraine.aspx.

a decay of 'traditional values' and acts hypocritically in the international arena. As a result, the West's philosophy, systems, and actions should not be trusted.

At the bottom of the pyramid, the Russian political narrative is absorbed into individual group ideologies in different ways. For example, nationalists focus on Russia's historic power, while communist groups decry capitalism. Each group self-selects and customises the narrative in unique ways that correspond to their own natural biases. And this stovepiping dynamic also tends to bypass critical peer review from the wider public.

This group dynamic capitalises on the pre-established interpersonal trust characteristic of online social media – a by-product of information overload in the internet era. There are many groups which are naturally sceptical of mainstream information channels, such as the population of the Former Soviet Union, where citizens have long had little trust in official media. In Moscow, the word of friends and colleagues is immeasurably more important than that of mass media.[46]

One of the latest developments in this arena has been the rise of professional 'trolls' and other (sometimes anonymous) 'opinion agents'. Such operations (in Russian military terminology 'maskirovka' (*маскировка*), or denial and deception) can be countered through the effective analysis of open source information, but usually not in a timely manner. Therefore, analysts and scholars must exercise caution, because online persona, images, messages, and campaigns can be wholly fabricated.

5 Conclusion

The global internet offers military and intelligence agencies the opportunity to expand and enhance IW, and it simultaneously presents their targets and victims with novel challenges. Russian IW – both in traditional media and in cyberspace – tangibly contributed to the successful annexation of Crimea, and is playing an important role in the ongoing crisis in eastern Ukraine. On balance, this author believes that Russia, and not the West, currently has the lead in contemporary IW.

Unlike propaganda in Soviet times, which was largely a unidirectional, top-down phenomenon, today's IW encompasses a worldwide audience that is both narrative-bearing and narrative-developing. Domestic, diaspora, and foreign audiences interact with current events in real time as they travel through online platforms such as social media. This dynamic makes it more challenging for propagandists to predict how and where the narrative will evolve, but to some degree it is possible to presume how certain political groups will interpret the narrative and how they will describe it to their followers.

In sum, the traditional 'fog of war' has changed in the internet era. The ubiquity and anonymity of internet communications offer all nations including Russia

46 Markku Lonkila. 'Russian Protest On-and Offline: The role of social media in the Moscow opposition demonstrations in December 2011.' *UPI FIIA Briefing Papers* 98, 2012.

In sum, the traditional 'fog of war' has changed in the internet era.

new IW opportunities, even as defenders also have more tools and tactics at their disposal to counter hostile actions. In Ukraine, 'conventional' cyber attacks by Russia were negligible,[47] but social media-based, narrative-focused attacks including disinformation have been common. And while it is possible to counter adversary operations with accurate open source analysis (for journalists,[48] scholars, and activists[49]), this is unfortunately difficult to do in a timely manner.

47 However, even unsophisticated cyber attacks such as DDoS and website defacements tend to garner widespread media exposure, and can sow distrust in the security of systems. This occurred during the invasion of Crimea, when Russia sought to capitalise on events that unfolded far too quickly for methodical information analysis to take place.

48 Jessikka Aro.'Yle Kioski Investigated: This is How Pro-Russia Trolls Manipulate Finns Online – Check the List of Forums Favored by Propagandists'. *YLE Kioski*, 24 June 2015. http://kioski.yle.fi/omat/troll-piece-2-english.

49 Sites such as www.stopfake.org were launched inviting people to join the 'struggle against fake information about events in Ukraine' by verifying online allegations. 'Stopfake.org.' 2015. Accessed: 14 June 2015. http://www.stopfake.org; 'Bellingcat kontert Kritik mit neuen Satellitenbildern'. *Zeit Online*. 12 June 2015. www.zeit.de/politik/ausland/2015-06/bellingcat-russland-mh17-satellitenfotos-manipulation; Dmitry Volchek and Claire Bigg. 'Ukrainian bloggers use social media to track Russian soldiers fighting in east'. *The Guardian*, 3 June 2015. http://www.theguardian.com/world/2015/jun/03/bloggers-social-media-russian-soldiers-fighting-in-ukraine.