Defence Research and Development Canada
Recherche et développement pour la défense Canada

DRDC | RDDC
technologysciencetechnologie

Russian Special Forces and Intelligence Information Effects

Keir Giles
Chatham House

Anthony Seaboyer
Royal Military College of Canada

Prepared by:
Royal Military College of Canada
Department of Political Science
National Defence
P.O. Box 17000, Station Forces
Kingston, Ontario, Canada K7K 7B4

MOU: DND RMCC - Service Level Arrangement with Royal Military College of Canada (RMCC) concerning contribution to DRDC's Program

Technical Authority: Matthew Lauder, DRDC – Toronto Research Centre

Contractor's date of publication: March 2019

Defence Research and Development Canada

Contract Report
DRDC-RDDC-2019-C230
September 2019

Canada

IMPORTANT INFORMATIVE STATEMENTS

This document was reviewed for Controlled Goods by Defence Research and Development Canada using the Schedule to the *Defence Production Act*.

Truth, Duty, Valour • Vérité, Devoir, Vaillance

ROYAL MILITARY COLLEGE OF CANADA • COLLÈGE MILITAIRE ROYAL DU CANADA

PO Box 17000, Station Forces • CP 17000, Succursale Forces • Kingston, Ontario • K7K 7B4

Russian Special Forces and Intelligence Information Effects

Keir Giles and Anthony Seaboyer

Prepared by:
Anthony Seaboyer
Royal Military College of Canada
Department of Political Science
National Defence
P.O. Box 17000,
Station Forces
Kingston, Ontario, Canada K7K 7B4
(613) 985-6111
Anthony.seaboyer@rmc.ca

SLA: RMCC-DRDC Serial #
Annex No

Contract Scientific Authority: Matthew Lauder

Defence R&D Canada, Toronto Research Centre
Contract Report
DRDC-RDDC-2019-CXXX
March 2019

RMC Project Manager and corresponding author: Anthony Seaboyer

Summary

This research report discusses information effects generated by Russian special forces as well as Russian intelligence agencies. After offering a brief introduction into the history of information effects generated by Russian special forces and intelligence agencies the paper discusses the theory and doctrine behind Russian information warfare as well as the evolution of information effects generated after the Cold War. Actors and agencies are introduced before exploring the case studies of information effects generated in Crimea, Eastern Ukraine and Syria are presented. The paper concludes with an examination of Russian tactics, techniques and procedures as well as possible countermeasures.

Résumé

Ce rapport de recherche traite des effets de l'information générés par les forces spéciales russes ainsi que par les agences de renseignement russes. Après une brève introduction à l'histoire des effets de l'information générés par les forces spéciales et les services de renseignement russes, le document examine la théorie et la doctrine de la guerre de l'information russe ainsi que l'évolution des effets de l'information générés après la guerre froide. Les acteurs et les agences sont présentés avant d'explorer les études de cas d'effets sur l'information générés en Crimée, dans l'est de l'Ukraine et en Syrie. Le document se termine par un examen de la tactique, des techniques et des procédures russes, ainsi que des contre-mesures possibles.

Contents

Background and Context

History

The brief war with Georgia in August 2008 prompted critical reviews of all aspects of Russia's performance and capabilities in armed conflict. For the most part, this criticism focused on clear and unambiguous shortcomings in the conduct of kinetic military operations,[1] giving impetus to the fundamental transformations which gripped the Russian Armed Forces for the subsequent decade. One aspect of the conflict though, provoked far more nuanced and uncertain assessments – this was how Russia had acquitted itself in the "information war" with Georgia.

Russian analyses of the information war with Georgia failed to arrive at a consensus on whether that war was actually won or lost.[2] The rapid development of the portrayal of the conflict in Western media, and the mixed success of penetration of the Russian narrative of forced intervention in response to intolerable genocide, were cited as evidence by both sides in the debate.[3] Additionally, while cyber campaigns before and during combat operations in South Ossetia and Abkhazia were not alluded to as a component of Russian overall strategy, it was noted that their contribution to the Russian strategic aims was limited to the information domain - in other words, while elements of Georgian strategic communications were effectively suppressed, broader attacks (for instance on critical national infrastructure) were not in evidence.[4] Regardless of the final conclusion, the common perception among those writing in open sources about the information aspect of the conflict was that the performance of the Russian military needed significant improvement.

"Playing Catch-Up"

Russia had a lot of ground to cover in terms of information warfare capability development. In keeping with a common perception that Russian security agencies moved from a very recent standing-start in operations via the internet, the official history of the Institute for Cryptography, Communications and Information Technology (IKSI, originally training specialists for the FSB[5] security service, SVR intelligence agency, and other bodies, and now part of the FSB Academy) notes the "test use of the Institute's connection to the global Internet network" did not begin

[1] For a summary and overview of Russian deconstructions of the armed conflict, see NATO Defense College reviews, "Understanding the Georgian War, Two Years On" http://www.ndc.nato.int/research/series.php?icode=9.

[2] For a close examination of this ambiguity, see Goble, P. "Defining Victory and Defeat: The Information War Between Russia and Georgia", in Cornell, S. & Starr, F. (eds) *The Guns of August 2008: Russia's War in Georgia*, New York 2009.

[3] See for instance Akhvlediani, M. "The fatal flaw: the media and the Russian invasion of Georgia", in Rich, P. B. (ed.) *Crisis in the Caucasus: Russia, Georgia and the West*, London: Routledge 2010. (Hereafter "Crisis")

[4] Tsyganok, A. "*Informatsionnaya voyna protiv Rossii: kak eto bylo".* Segodnya, 17 April 2009. http://www.segodnia.ru/index.php?pgid=2&partid=13&newsid=8407. The nature of the cyber offensive against Georgia, and its likely origins, have been analysed in depth, most recently at the time of writing by David Hollis in Small Wars Journal. See Hollis, D. "Cyberwar Case Study: Georgia 2008" in Small Wars Journal, 6 January 2011. http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf.

[5] The Federal Security Service (Federalnaya Sluzhba Bezopasnosti (FSB)) is the KGB's main successor in the Russian Federation.

until February 1996.[6] This was not long before, at parliamentary hearings on 17 December 1996, entitled "Russia and the Internet: The Choice of a Future," FAPSI government communications agency First Deputy Director General Vladimir Markomenko, characterised the internet as a whole as a threat to Russian national security.[7]

Certainly, Russia's first real experience with information war utilizing public internet resources, countering Chechen information sources during the first Chechen war, was a sobering experience. Paul Goble noted the experience forced Putin to focus on the role of the internet in deciding the outcome of conflicts. Putin, who acknowledged that Moscow was playing catch-up on this battlefield, stated: "We surrendered this terrain some time ago … but now we are entering the game again."[8]

Despite the head of US Cyber Command, Gen Keith Alexander, describing Russia as a near peer to the US in 2010,[9] the perception that Russia was lagging behind in development of computer network operations was reinforced by the Russian government's emphasis on developing treaties and agreements to restrain state activities in cyberspace (i.e., so-called arms control treaties for information weapons).[10]

These efforts also involved the Ministry of Foreign Affairs of the Russian Federation (MFA) and Directorate K of the Ministry of Internal Affairs (MVD).[11] Professor Igor Panarin of the MFA's Diplomatic Academy is the author of one of the standard works on Russian theory of information war.[12] In his text, Panarin advocates "using the mechanisms of the UN and the mechanisms of Russian-American consultations to create new rules of the game, rules of information balance and rules for protecting our sovereign national information space."[13] It was also persistently argued the 2009 agreement between Shanghai Cooperation Organisation (SCO) states on "cooperation in ensuring international information security," which included a provision for military cooperation, should be used as a template and extended.[14] Taken together, this offensive on a broad front suggests strongly that Russia felt the need to complete its catch-up with foreign states, while further development by those states should be limited by and through international binding agreements.

Some of the proposed treaty limitations make interesting reading when compared with anti-social behaviour in cyberspace, which has emanated from Russia: General

---

[6] *Kompant-dien, posvyashchennyy pyatidesyatiletyu IKSI*, Moscow: Institut Kriptografii, Svyazi i Informatiki, 1999. pp. 195-201.
[7] State Duma proceedings, 17 December 1996.
[8] Goble, P. "Russia: Analysis From Washington -- A Real Battle On The Virtual Front", RF/RL 11 October 1999. http://www.rferl.org/content/article/1092360.html.
[9] "Cyber Threat to Pentagon is Global: China, Russia Near Peers of US", 1 October 2010. http://www.geostrategy-direct.com/geostrategy-direct/secure/2010/10_06/ba.asp.
[10] Gorman, S. "U.S. Backs Talks on Cyber Warfare", Wall Street Journal, 4 June 2010. Available online: http://online.wsj.com/article/SB10001424052748703340904575284964215965730.html.
[11] MVD website: http://www.mvd.ru/struct/10000220/10000221/10000740/.
[12] Panarin, I. *Informatsionnaya voyna i diplomatiya,* Moscow: Gorodets 2004.
[13] BBC Monitoring: "Russian pundit interviewed on US information operations conference", *Rossiya TV* 1950 GMT 27 April 2009.
[14] Boyko, S. M., Dylevskiy I. N., Komov S. A., Korotkov S. V. "*Voyenno-politicheskiye aspekty obespecheniya informatsionnoy bezopasnosti na prostranstve Shankhayskoy organizatsii sotrudnichestva*", *Voyennaya mysl'*, No. 7, July 2010.

Aleksandr Burutin backs “a mutually acceptable multilateral mechanism” which would bind states in “taking responsibility for what is happening in their information space” - a responsibility conspicuously absent in the case of Russia.[15]

Theory and Doctrine

Over the last two decades, the traditional Russian understanding of the nature of war has broadened to include non-military and non-violent means, which are seen to be the equivalent of kinetic activity. Among non-military means, the increasing utility of information as a key instrument of warfare is especially prominent in Russian military thought.[16]

The broadening of the Russian understanding of war has been a long-term evolutionary process. After the onset of the war in Ukraine in 2014, some Western analyses saw a revolution in Russian military thought. However, rather than Ukraine seeing the demonstration of novel Russian military ideas, it was the Western lack of attention to Russian military thought that made them seem novel. In fact, many of the most publicised notions - the blurring of war and peace, that Russia is in an information war, that information can be employed as a weapon, and that non-military means can be as effective as kinetic weapons - were part of the Russian military-theoretical debate long before the invasion of Ukraine.[17]

In order to understand the full range of options available to defence planners in Moscow, it is essential to grasp a key principle of the Russian approach to information warfare: Information itself is important and the object of operations, independent of the channel through which the information is transmitted. The aim of information warfare is to control information in whatever form it takes. In this context, cyber is just a technical representation of information standing among other carriers such as print media, individual or mass consciousness.

This means that a wide range of Russian state agencies, beyond simply the military and intelligence agencies, are expected to engage in information warfare. Influential long-term Duma deputy, and former Secretary of the Security Council and Deputy Minister of Defence (with, intriguingly, a first qualification in radio-electronics from the then Bauman Higher Technical College[18]), Andrey Kokoshin, has been a long-term proponent of the vital importance of information superiority for Russian security.[19] Speaking at the launch of a report entitled, “‘Cyber Wars’ and International Security”[20] in late January 2011, Kokoshin said “the development of issues of information warfare and ‘cyber wars’ must take place on an interdisciplinary level .... The experience of many states shows that information warfare is not just a function of the Armed Forces: other state institutions including the secret services take part in

[15] *Tsentr parlamentskikh kommunikatsiy*, 30 January 2009. http://www.parlcom.ru/index.php?p=MC83&id=27297.
[16] Keir Giles, “Handbook of Russian Information Warfare”, NATO Defense College, November 2016.
[17] See for instance key articles by Military Academy of the General Staff academics Sergey Chekinov and Sergey Bogdanov in the period 2010-2014.
[18] For a biography, see: http://dic.academic.ru/dic.nsf/ruwiki/101812.
[19] As cited in Fitzgerald, M. C. “Russian Views on Electronic and Information Warfare”, Hudson Institute, December 1996.
[20] The report was published jointly by the Institute of International Security Issues of the Russian Academy of Sciences and the Faculty of World Politics of Moscow State University.

it."[21]

This broad, whole of government approach is a principle that has to be borne in mind at all times when considering Russian aims to extract, exfiltrate, manipulate, distort, or insert information, or just isolate a target from sources of information (other than Russian sources). The channels available for doing this are as diverse and include both fake and real news media. Some examples include troll campaigns, official government statements, speeches at rallies or demonstrations, defamatory YouTube videos, direct and text messages, or even just walking up to somebody on the street and telling them something; all of which have been employed in recent Russian influence campaigns.

Evolution

Examining Russian assessments of current events makes it clear that Russia considers itself to be engaged in full-scale information warfare, involving not only offensive but also defensive operations - whether or not its notional adversaries initially noticed that this was the case. This is reflected in the new emphasis on information warfare in Russia's latest military doctrine and approved on 26 December 2014 - although perhaps unsurprisingly, most of the concepts which are recognisable from Russian offensive action in and around Ukraine appear described in purely defensive terms as countering threats to Russia itself.[22]

The current Russian practice of information warfare combines a number of tried and tested tools of influence with a new embrace of modern technology and capabilities. Some underlying objectives and guiding principles are broadly recognisable as reinvigorated aspects of subversion campaigns from the Cold War era,[23] and even earlier.[24] Their recognition as such, not only by Western societies but also by their leaderships, has been slow. In Russian terms, campaigns of this sort are "not new, but old and well forgotten."

This is due to two main factors. First, there is a collective lack of institutional memory among target audiences - a significant proportion of which were not even born when Soviet subversion was a concern. Second, Russia has invested massively in enabling factors to adapt the principles of subversion to the internet age.

These new Russian investments cover three main areas:

1. Both internally- and externally-focused media with a substantial online

[21] "Kokoshin: Kibervoyny ugrozhayut natsional'noy bezopasnosti Rossii", One Russia party website, 26 January 2011. http://er.ru/er/text.shtml?18/2254. This makes an interesting counterpoint to the FSB statement cited elsewhere in this paper which appeared to be suggesting that it was not the business of the Armed Forces at all. The "'Cyber Wars' and International Security" report, according to the Russian Ministry of Defense newspaper Krasnaya Zvezda, "examines primarily US and Chinese policy in this area... The study examines issues such as operations in cyberspace as an integral part of information operations." At the time of writing, the report itself appeared to be unavailable in open sources.

[22] "Military Doctrine of the Russian Federation", approved 26 December 2014. http://news.kremlin.ru/media/events/files/41d527556bec8deb3530.pdf.

[23] "Soviet Propaganda In Western Europe", FCO Research and Analysis Department Background Brief, March 1982. http://www.psywar.org/radSovietPropaganda.php.

[24] Victor Madeira, "Haven't We Been Here Before?", Institute of Statecraft, 30 July 2014. http://www.statecraft.org.uk/research/russian-subversion-havent-we-been-here.

presence, of which RT is the best known but only one example;

2. The use of social media and online fora as force multipliers to ensure Russian narratives achieve broad target audience reach and penetration;

3. Language skills, in order to engage on a broad front with target audiences in the audiences' own languages, as described further below.

How this came about, and how Russian capability developed to a stage which has taken its targets entirely by surprise, is more easily understood by looking at three distinct stages in the evolution of the current Russian approach.[25] Each of these stages involved Russia taking action which was unpopular either at home or abroad, and subsequently realising that it could no longer influence the global narrative about that action in the same way as the USSR could - that the old levers and tools for manipulating global opinion were either unavailable or inoperative, and something new needed to be done. In each case, the resulting shock to the Russian system led to a distinctive response which has shaped Russia's current information warfare capability.

1999

In the Second Chechen War, Russia successfully addressed the failure to dominate the traditional media environment that had proved a strategic challenge in the previous campaign to subdue Chechnya.[26] Russian authorities initially shut down independent reporting, and thereafter took substantive measures to ensure that television and newspaper reporters only filed approved reports from the battlefield, in order to shape both domestic and international perception of the conflict.[27] Russian officials then realised with dismay that in information terms, they were still outmanoeuvred by a notionally weaker and less capable enemy; that is, an enemy that was more adept at the use of the newly-arrived internet, by which "even a small and relatively impoverished adversary could achieve information dominance over a stronger opponent."[28] Despite the fact that the war began with an unprovoked invasion of a Russian republic by jihadist forces from Chechnya, in the international media, Russia found itself incapable of overcoming the adversary's narrative of Russian aggression against heroic Chechen freedom fighters.[29]

The Russian response was twofold. On the one hand, the experience served to reinforce the consistent message from Russian security services, led by the FSB, that the internet as a whole was a dangerous destabilising factor and a threat to national security. Public access to it should be carefully controlled. This was the view

[25] For another assessment of the development of modern Russian information warfare from their historical roots, see Mariia Zaitseva, "Information and security components of the Russian foreign policy", Informacijos mokslai (Information Sciences), Issue 70/2014. pp. 58-68.
[26] Timothy L. Thomas, "Information Warfare in the Second (1999-Present) Chechen War: Motivator for Military Reform?", in "Russian Military Reform 1992-2002", Frank Cass, 2003. pp. 209-233.
[27] Timothy L Thomas, "Manipulating the Mass Consciousness: Russian & Chechen 'Information War' Tactics in the Second Chechen-Russian Conflict", in Anne Aldis (ed.), "The Second Chechen War", Conflict Studies Research Centre, June 2000.
[28] Roland Heickerö, "Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations", FOI, March 2010. pp. 15-16.
[29] Graeme P Herd, "Information Warfare & the Second Chechen Campaign", Conflict Studies Research Centre, 2000.

that led to FAPSI arguing against the internet in Duma hearings in 1996, as described above.[30] At the same time, the security services themselves continued to develop their own means and methods of exploiting the new medium to target adversaries abroad.

2008

The armed conflict in Georgia resulted in a convincing military victory for Russia. At the same time, it exposed serious deficiencies in Russian military performance. Dismay at conventional military failings was accompanied by a failure to agree on who had won the information war but also created a strong consensus that major reform was needed to improve military capability in the information domain.[31] A stark contrast was noted between (then) Georgian President, Mikheil Saakashvili, speaking to Western audiences directly in their own languages (while sitting in front of an entirely misplaced EU flag), and Russia's own belated and stilted attempts at organising press conferences led by the monolingual and uninspiring Deputy Chief of the General Staff, Anatoly Nogovitsyn.

Among other recommendations for overhauling the Russian Armed Forces were calls for the creation of Information Troops, a dedicated branch which could manage the information war from within the military.[32] Reflecting the holistic and full-spectrum nature of the Russian information war concept, these would include hackers, journalists, specialists in strategic communications and psychological operations, and crucially, linguists to overcome Russia's perceived language capability deficit.[33] This combination of skills would enable the Information Troops to engage with a broad range of target audiences:

> *[T]he use of 'mass information armies' conducting a direct dialogue with people on the internet is more effective than a 'mediated' dialogue between the leaders of states and the peoples of the world.*[34]

However, it took nearly a decade for any formed unit known as Information Troops to officially materialise in the Russian order of battle. The notion of the Russian military handling large-scale offensive cyber operations appeared to be publicly rejected by the FSB and the other capabilities referred to earlier, began to develop elsewhere.[35]

---

[30] State Duma proceedings, 17 December 1996. See also Andrei Soldatov, "*Fapsi - obshestvennosti: 'menshe znaesh - krepche spish*'" (FAPSI to the public: the less you know, the sounder you sleep), Segodnya, 12 December 1999.

[31] Timothy L. Thomas, "Russian Information Warfare Theory: The Consequences of August 2008", in Stephen J. Blank and Richard Weitz (eds.), "The Russian Military Today and Tomorrow: Essays In Memory of Mary Fitzgerald", USAWC Strategic Studies Institute, 2010. pp. 265-299.

[32] Keir Giles, "Information Troops - A Russian Cyber Command?", Proceedings of the 3rd International Conference on Cyber Conflict, Tallinn, June 2011.

[33] As reflected, for instance, in complaints over lack of language capacity to influence non-Russian-speaking audiences in the Baltic States. See "Информационные войны с самими собой", Postimees-DZD, 7 November 2011, http://rus.postimees.ee/624820/informacionnye-vojny-s-samimi-soboj.

[34] Col. P. Koayesov, "Theatre of Warfare on Distorting Airwaves. Georgia Versus South Ossetia and Abkhazia in the Field of Media Abuse. Fighting by Their Own Rules," *Voyennyy Vestnik Yuga Rossii*, 18 January 2009.

[35] The shifting fortunes of the Russian army's Electronic Warfare Troops (Voyska REB) as a potential candidate for the role of "Information Troops" can be traced through Ulrik Franke, "War by Non-Military Means: Understanding Russian Information Warfare", FOI report No. FOI-R-4065-SE, March 2015. http://www.foi.se/ReportFiles/foir_4065.pdf.

2011-12

Three years later, protest movements, both at home and abroad, caused a further refining of the approach to information warfare. The Arab Spring demonstrated the power of social media both to mobilise and organise, to the extent of facilitating regime change - a prospect which caused deep alarm at the thought of this being applied to Russia. Meanwhile at home, the election protests of 2011-12 saw Russian attempts to use automated systems to dominate or suppress online debate, or to divert or disrupt social media as a facilitator for organisation.[36] A wide array of pre-positioned Twitterbots, and sporadic but highly targeted DDoS (Distributed Denial of Service) attacks, were combined with old-fashioned dirty tricks (e.g., smear campaigns) against opposition leadership figures to attempt to defuse and discredit the protest movement.

The response to the 2011-12 protests marked a major step forward in Russia's learning to use the means of online mass communication.[37] Examination of the results appears to have reinforced the conclusion that automated systems are insufficient, as dominating mass consciousness online requires the engagement of actual humans.[38] This led to significant investment in human capabilities to direct or prevent online debate and comment.[39] This capability, which previously had only limited targeting and mostly within Russia,[40] was bolstered by the recruitment or training of foreign language speakers (to varying degrees of proficiency) to exploit the hyperconnected nature of online space. Meanwhile, the recruitment of talent for online media saw journalists tempted from their work with traditional media by offers of doubled or tripled salaries. Thus, parts of the original Information Troops concept morphed into the Kremlin Troll Army,[41] in cooperation with state-backed media with a strong internet presence.[42] Automation and machine generation of social media posts and information, while tested and found to have only limited success, was nevertheless incorporated in the overall strategy with its own specific role.

Towards 2014

By 2014, the media element of Russian information campaigns displayed both close coordination of messaging with centralised direction,[43] with an impressive range of

[36] Markku Lonkila, "Russian Protest On- And Offline: The Role Of Social Media In The Moscow Opposition Demonstrations In December 2011", FIIA Briefing Paper 98, February 2012.
[37] See also Margarita Jaitner, "Exercising Power in Social Media", in Jari Rantapelkonen & Mirva Salminen (eds.), The Fog of Cyberwar, Finnish National Defense University, 2013. http://www.doria.fi/bitstream/handle/10024/88689/The%20Fog%20of%20Cyber%20Defence%20NDU%202013.pdf?sequence=1.
[38] See for instance Igor Elkov, "Короткая память", Rossiyskaya gazeta, 17 January 2013. http://www.rg.ru/2013/01/17/ashmanov.html, and "Profilaktika", Mayak radio, 25 December 2012. https://www.youtube.com/watch?v=9yhOKf0J280.
[39] As described in "Городской типаж: блогер-пропагандист", Sobaka.ru, 28 january 2015. http://www.sobaka.ru/city/city/32942/ and Aleksandra Garmazhapova, "Где живут тролли. Как работают интернет-провокаторы в Санкт-Петербурге и кто ими заправляет", Novaya gazeta, 9 September 2013.
[40] Julien Nocetti, "'Digital Kremlin': Power and the Internet in Russia", IFRI Russie.Nei.Visions No. 59, April 2011. pp. 16-17.
[41] Max Seddon, "Documents Show How Russia's Troll Army Hit America", BuzzFeed, 2 June 2014.
[42] "Analysis of Russia's Information Campaign Against Ukraine", NATO StratCom Centre of Excellence (COE), undated document, p. 28 onwards.
[43] "'Anonymous International' Leaks Kremlin's Instructions to Russian TV", GlobalVoices, 28 March 2014, http://globalvoicesonline.org/2014/03/28/anonymous-international-leaks-kremlins-instructions-to-russian-tv/. Stephen Castle, "A Russian TV Insider Describes a Modern Propaganda Machine", New York Times, 13

alternative outlets to address all sectors of the target audience. RT, Sputnik,[44] Russia Direct and other state-controlled media outlets, tailored their level of sophistication and concealed the extent of their propaganda function through subtle imitations of objectivity. They were able to engage - to the expectations of their intended readers and viewers, facilitated by the willingness of unscrupulous or deluded native speakers to serve the Kremlin against the interests of their own nations, whether as editors, correspondents or interviewees.[45] In this way, the media effort reflects the way in which the Russian troll army (i.e., social media operatives) adopts a different approach for different fora, ranging from simple abuse, through confusion with half-truths, to sophisticated argument.

It should be emphasised that Russian information campaigns which are visible to an English-language audience are only part of a broad front covering multiple languages, including not only state-backed media and trolling, but also false flag media, such as sock puppet websites set up to resemble genuine news outlets, which seed their news feeds with false or contentious reporting which ties in with Russian narratives.[46] The false flag approach extends to RT's English language platform, which masquerades as a US broadcaster,[47] and includes clone accounts on social media set up to mimic and discredit genuine Western media outlets.[48]

For Russia, cyber activities in the broad sense are critical to offensive disinformation campaigns, whether establishing sources for disinformation by setting up false media outlets online,[49] or using social media to address targets of opportunity for subversion and destabilisation efforts.[50] These activities are augmented by the ubiquitous activities of social media trolls and bots (accounts run by automated processes), which exploit specific features of the relationship between traditional and social media in order to both disseminate and lend credibility to disinformation.[51] This approach capitalises on the recognition that "digital media are becoming the main - and for a growing number of young people, the only - channel for political information

---

February 2015. http://nyti.ms/1zcDqDq. See also Peter Pomerantsev's "Nothing Is True And Everything Is Possible", PublicAffairs Books, New York, 2014.

[44] Miriam Elder, "Russia Has A New Propaganda Outlet And It's Everything You Thought It Would Be", BuzzFeed, 10 November 2014. http://www.buzzfeed.com/miriamelder/russia-has-a-new-propaganda-outlet-and-its-everything-you-th.

[45] "George Galloway Doubles Pay Packet With Appearances On Russia Today And Al-Mayadeen", The Huffington Post, 11 July 2014. http://www.huffingtonpost.co.uk/2014/07/11/george-galloway-russia-today_n_5577661.html.

[46] Dalibor Rohac, "Cranks, Trolls, and Useful Idiots: Russia's information warriors set their sights on Central Europe", Foreign Policy, 12 March 2015. https://foreignpolicy.com/2015/03/12/cranks-trolls-and-useful-idiots-poland-czech-republic-slovakia-russia-ukraine/.

These fake media are also prone to launching personal attacks on critics of Russia, including this author - for instance "Schweiz Magazin" at http://www.schweizmagazin.ch/nachrichten/schweiz/19717-minutench-diffamiert-Kritiker-als-Putin-gesteuert.html. - an example of fairly low-level sniping compared to the continuing and vicious *ad hominem* attacks on more visible commentators.

[47] Jill Dougherty, "Russian TV's American Face", Huffington Post, 11 April 2014. See also "FULL TRANSCRIPT: Mikhail Kasyanov and Anissa Naouai", CNN, 21 November 2014. http://amanpour.blogs.cnn.com/2014/11/21/full-transcript-mikhail-kasyanov-and-anissa-naouai/

[48] "Clone Twitter Accounts Target RFE/RL", RFE/RL, 17 February 2015. http://www.rferl.org/content/clone-twitter-accounts-target-rferl/26853959.html.

[49] Dalibor Rohac, "Cranks, Trolls, and Useful Idiots: Russia's information warriors set their sights on Central Europe", Foreign Policy, 12 March 2015. https://foreignpolicy.com/2015/03/12/cranks-trolls-and-useful-idiots-poland-czech-republic-slovakia-russia-ukraine/.

[50] Doug Bernard, "America's Adversaries Use Baltimore Unrest to Spread Anti-US Message", VOA News, 30 April 2015. http://www.voanews.com/articleprintview/2743166.html.

[51] Polina Tikhonova, "Russia Hacking Your News", ValueWalk, 14 March 2015. http://www.valuewalk.com/2015/03/russia-hacking-your-news/.

and communication"[52] - and that consequently, "new social media have become the most effective tool for influencing the minds" of target audiences.[53]

Media, Society and Values as a Soft Target

While Ukraine is the topic which brought Russian information warfare to broad public attention, other well-established information campaigns have been running for much longer - as for example in the Baltic States, where Russian-backed media companies and their broadcasting services work in lockstep with the Russian political authorities. Western media organisations more broadly, as well as the populations they serve, were entirely unprepared in early 2014 for a targeted and consistent hostile information campaign that was organised and funded at the state level.[54] The result was initially a startling success for the Russian approach. This was exemplified in Crimea, where reports from journalists on the scene identifying Russian troops often did not reach mainstream audiences because editors in their newsrooms were baffled by the inexplicable Russian denials.[55]

A primary objective of Russian information campaigns is to cause confusion and doubt. The provision of multiple, contradictory alternatives to the truth serves the purpose of undermining trust in objective reporting, and especially in official statements by Russia's adversaries and victims. A key example of this approach followed the shooting down of the Malaysian Airlines Flight MH17 in July 2014.[56] Four days after the crash, by which time it was already clear that Russia held ultimate responsibility for the tragedy, the Russian Ministry of Defence held a press conference to present explanations absolving Russia.[57] The scenarios presented were diverse and mutually exclusive, and did not stand up to the briefest examination by experts with even basic knowledge of the aircraft and missile systems claimed to be involved.[58]

The Russian government was not concerned by international criticism. In fact, rejection of these claims by both foreign and Russian experts did not prevent them being reported in the West, as well as receiving broad coverage within Russia. In the same fashion, almost four months later when Russia issued crudely doctored satellite images suggesting the Malaysian airliner had been downed by a missile attack from a Ukrainian aircraft, these were identified as fake. This did not, however, prevent the claims being reported, initially without qualification, by a range of

[52] Velichka Milina, "Security in a Communications Society: Opportunities and Challenges", Connections, Volume XI, Number 2, Spring 2012. p. 55.
[53] *Ibid.*
[54] Nick Cohen, "Russia Today: why western cynics lap up Putin's TV poison", The Observer, 8 November 2014. http://www.theguardian.com/commentisfree/2014/nov/08/russia-today-western-cynics-lap-up-putins-tv-poison.
[55] Lucy Ash, "How Russia outfoxes its enemies", BBC News, 29 January 2015. http://www.bbc.co.uk/news/magazine-31020283.
[56] Dutch investigators and prosecutors conducting the MH17 air crash investigation have been the targets of intense cyber penetration attempts by Russia; an instance of actions which the West would consider cyber operations being used by Russia for a pure information warfare aim. "Vijf vragen over het MH17-onderzoek", NOS, 3 March 2015. http://nos.nl/artikel/2022540. See also Giles, "With Russia and Ukraine, is all really quiet on the cyber front?", Ars Technica, 11 March 2014. http://arstechnica.com/tech-policy/2014/03/with-russia-and-ukraine-is-all-really-quiet-on-the-cyber-front/.
[57] "Special Briefing by the Ministry of Defense of the Russian Federation on the crash of the Malaysian Boeing 777 in the Ukrainian air space, July 21, 2014", Russian Ministry of Foreign Affairs website, 2014. http://www.mid.ru/brp_4.nsf/0/ECD62987D4816CA344257D1D00251C76.
[58] Keir Giles, "Tales from Two Cities: Moscow and Washington on Flight MH17", Chatham House, 24 July 2014. http://www.chathamhouse.org/expert/comment/15236.

Western media.[59] In other words, the lack of credibility of the claims did not impede Russia's ability to disseminate (dis)information to various target audiences.[60]

To dismiss the importance of Russian denials and other disinformation efforts because they are implausible is also to underestimate the concept and power of the direct lie. Given the habit of leaders in democratic nations to attempt to say something which at least resembles the truth, implausible denials are a ploy which Western media are particularly ill-equipped to respond to and to report appropriately. Thus, when Vladimir Putin denies that Russian troops are in Crimea or in eastern Ukraine, it is not important that what he is saying is clearly untrue - the approach is effective not only in press conferences, especially when unchallenged by a compliant media, as Canadian Premier Stephen Harper found at the G20 summit in Brisbane, it also makes it impossible to confront or engage with President Putin even when face-to-face.[61] In a similar manner, when the German Defence Attaché returned to Moscow with photographs he took of Russian armour and equipment crossing the border into Ukraine, he was simply told by Russian defence officials that the photographs were fakes and he had not taken them.

According to NATO Deputy Secretary General Alexander Vershbow, Russia presents "an endlessly changing storyline designed to obfuscate and confuse, to create the impression that there are no reliable facts and therefore no truth."[62] Vershbow noted:

> *We cannot respond with more propaganda, but only with the truth and facts: by setting the record straight. While this takes time, credibility is our biggest asset to counter hybrid communications.*[63]

This reinforces the point that, instead of convincing Western readers that the disinformation is true, Russian success is defined in two other ways: firstly, isolating the domestic audience from non-approved information so that Russian state actions are permissible; and secondly, influencing foreign decision making by supplying polluted information, exploiting the fact that Western elected representatives receive and are sensitive to the same information flows as their voters. When Russian disinformation is delivered in this manner and becomes part of the framework for decisions, this constitutes success for Moscow, since a key element of the long-standing Soviet and Russian approach of what is referred to as reflexive control, as outlined below, is in place.

Broader Influence

[59] "Is this the moment MH17 was shot down as it flew over Ukraine? Russian state broadcaster produces 'satellite images' showing alleged fighter jet attack", Daily Mail, 14 November 2014. http://www.dailymail.co.uk/news/article-2835088/Is-moment-MH17-shot-flew-Ukraine-Russian-state-broadcaster-produces-satellite-images-showing-fighter-jet-attack.html.
[60] Peter Pomerantsev and Michael Weiss, "The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money", The Interpreter, 22 November 2014. http://www.interpretermag.com/wp-content/uploads/2014/11/The_Menace_of_Unreality_Final.pdf.
[61] Nick Logan, "'Get out of Ukraine': Harper to Putin at G20 Summit in Brisbane", Global News, November 15, 2014. http://globalnews.ca/news/1673290/get-out-of-ukraine-harper-to-putin-at-g20-summit-in-brisbane/. As also reported by Ekho Moskvy radio, 15 November 2014.
[62] "Remarks by NATO Deputy Secretary General Ambassador Alexander Vershbow at the Public Diplomacy Forum 2015", NATO website, 17 February 2015. http://www.nato.int/cps/en/natohq/opinions_117556.htm.
[63] "Remarks by NATO Deputy Secretary General Ambassador Alexander Vershbow at the Public Diplomacy Forum 2015", NATO website, 17 February 2015. http://www.nato.int/cps/en/natohq/opinions_117556.htm.

A related concern is Russia's ability to purchase or co-opt business and political elites into loyal or at least compliant networks. Bribes and business opportunities combine with the appeal of a Russian business culture which embraces opacity and corruption to recruit agents of influence throughout target countries. The result is direct input into political processes through trojan horse individuals or organisations, successfully acquiring influence across Central and Eastern Europe and beyond.[64] This is not a new process. For example, in 2008, a study warned that the UK "should be wary of placing reliance on EU or NATO solidarity, or on national leaders or key figures to act in what would appear to be their own national interests."[65] Following the return of high oil revenues for Russia in the middle of that decade, interference in domestic political systems had become increasingly reflected in financial and other support - transparent or opaque - for individuals and political parties abroad.[66]

Russian geopolitical objectives also encompass providing the appearance of broad-based support for specific government policies or political figures, especially those taking a pro-Russian perspective. Unlike in Soviet times, Russia is no longer restricted in its choice of foreign friends by considerations of ideology, and one notable result is a surge in links with right-wing and anti-EU parties, whose agenda generally aligns with Russian state objectives[67] as well as domestic policies (e.g., Putin's declared support for traditional values).[68]

Russia continues actively to canvas for academic sympathisers,[69] to add to the ranks of individuals, some in influential positions, who for personal motivations are inclined to fall in with Moscow and promote Russian narratives in their own countries at the expense of their own credibility.[70] This approach works in combination with old-school subversive measures such as "NGO diplomacy, or establishing and assisting pro-Russian youth groups, minority and separatist organisations, and think tanks abroad."[71]

The result is that externally, the multiplicity of deceptive narratives put forward by Russian information campaigns finds fertile ground among populations which are not well informed on the realities of history, geography, and the issues at stake in Ukraine and other front-line states. In addition, this network of conscious or unwitting

---

[64] Anne Applebaum, "How Vladimir Putin is waging war on the West - and winning", Spectator, 21 February 2015. http://www.spectator.co.uk/features/9447782/how-vladimir-putin-is-waging-war-on-the-west-and-winning/.
[65] "Russia - Future Directions", Defense Academy of the UK, 1 October 2008.
[66] Elena Servettaz, "Putin's Far-Right Friends in Europe", Institute of Modern Russia, 16 January 2014. http://imrussia.org/en/russia-and-the- world/645-putins-far-right-friends-in-europe.
[67] "«Черный интернационал». Как Москва кормит правые партии по всему миру", The Insider, 27 November 2014, http://theins.ru/politika/2113. Andrew Rettman, "Reports multiply of Kremlin links to anti-EU parties", EUObserver, 26 November 2014. https://euobserver.com/foreign/126676.
[68] See Gabrielle Tétrault- Farber, "Far- Right Europe Has a Crush on Moscow", The Moscow Times, 25 November 2014. http://www.themoscowtimes.com/news/article/far-right-europe-has-a-crush-on-moscow/511827.html. and Peter Tiede, "Für mehr Einfluss auf Europa: Putin greift nach der AfD", Bild, 24 November 2014. http://www.bild.de/politik/inland/wladimir-putin/russlands-praesident-greift-nach-der-afd-kreml-netzwerk-38690092.bild.html.
[69] "The Russian Military Asked Me to Publish Its Propaganda", War Is A Crime.org, 23 March 2015. http://warisacrime.org/print/69356.
[70] Julia Davis, "Dana Rohrabacher claims that the former President of Ukraine was assassinated", The Examiner, 6 April 2015. http://www.examiner.com/article/dana-rohrabacher-claims-that-the-former-president-of-ukraine-was-assassinated. see also James Kirchik, "Putin Bootlickers Assemble in D.C.", The Daily Beast, 31 March 2015. http://www.thedailybeast.com/articles/2015/03/31/report-from-the-belly-of-the-putin-apologetics-beast.html.
[71] Sinikukka Saari, "Russia's public diplomacy: soft tools with a hard edge", Border Crossing (Diplomat Magazine), April 2015.

supporters facilitates the Russian aim of challenging unity among Western allies and creating divisions or exploiting existing ones in order to exert influence.[72]

Effects and Consequences

The pollution of the information framework for decision making is a key element of the long-established Soviet and Russian principle of reflexive control[73] - influencing the decision of your adversary by ensuring that he or she is supplied with specific information or disinformation on which it (the decision) is based.[74] Russian information warfare theorist Col. P. Koayesov explains how this works, both prior to and during conflict:

> *"Information warfare consists in making an integrated impact on the opposing side's system of state and military command and control and its military-political leadership - an impact that would lead even in peacetime to the adoption of decisions favourable to the party initiating the information impact, and in the course of conflict would totally paralyze the functioning of the enemy's command and control infrastructure."*[75]

Danger arises when Russia's successful pollution of the opinion-forming process in the West spills over into influence on the policy-making process itself. At the very least, objective assessment of what Russia is doing is effectively suppressed. Many narratives absolving Russia or placing the blame for the current crisis elsewhere will find willing audiences in those policy circles that wish to appease Russia and return to 'business as usual' as swiftly as possible, as was the case following the armed conflict in Georgia in 2008. Those who decide or guide policy can be influenced either directly (even when not solicited in the course of the concurrent Russian campaign to recruit agents of influence)[76] or indirectly via the electorate. In Western democracies, which are the targets of these campaigns, elected representatives do, at least on occasion, listen to their voters and give attention to their concerns.

As a result, Russian-inspired narratives can appear in surprising and disturbing circumstances. The notion that NATO enlargement is to blame for the Ukraine crisis has spread well beyond academic circles.[77] The accompanying Russian fiction that Moscow was given a promise at the time of German reunification that there would be no NATO enlargement is repeatedly quoted as fact in a range of fora. Other memes that reach politicians through their electorate or media can be more subtle and therefore insidious.[78] The habitual description of conflict in Ukraine as a "civil war"

---

[72] Andrew Higgins, "Waving Cash, Putin Sows E.U. Divisions in an Effort to Break Sanctions", New York Times, 6 April 2015. http://nyti.ms/1ac5osT.
[73] As described in detail in Timothy L. Thomas, "Recasting the Red Star", FMSO, 201. pp. 118-131.
[74] Keir Giles, James Sherr and Anthony Seaboyer, "Russian Reflexive Control", DRDC, October 2018. http://pubs.drdc-rddc.gc.ca/BASIS/pcandid/www/engpub/DDW?W%3DSYSNUM=807769&r=0
[75] Col. P. Koayesov, "Theatre of Warfare on Distorting Airwaves. Georgia Versus South Ossetia and Abkhazia in the Field of Media Abuse. Fighting by Their Own Rules," *Voyennyy Vestnik Yuga Rossii*, 18 January 2009.
[76] "Putin's Secret Friends in Paris", The XX Committee, 9 September 2014. http://20committee.com/2014/09/09/putins-secret-friends-in-paris/.
[77] John J. Mearsheimer, 'Why the Ukraine Crisis Is the West's Fault: The Liberal Delusions That Provoked Putin', Foreign Affairs, September-October 2014. http://www.foreignaffairs.com/ articles/141769/john-j-mearsheimer/why-the-ukraine-crisis-is-the-wests-fault.
[78] To take just one example, a member of the UK Parliament's Foreign Affairs Committee in February 2015 raised the issue of Ukraine, as a failing state, being potentially unable to maintain its nuclear facilities safely - a notion based entirely on unsubstantiated allegations in Russian media coverage such as "Radioactive leak at

and the Russian-backed separatists as “local rebels" represents a success for Russian information operations,[79] as does the dissemination of the highly dangerous argument that the best way to respond to Russian nuclear posturing is to withdraw the last remaining non-strategic nuclear weapons from Western Europe.[80]

Even more dangerously, in circumstances which would require complete Western consensus - such as a decision on collective action to be taken by NATO - Russian information warfare could play a key role by fatally undermining essential unity among Western allies. As explained by Jānis Bērziņš, "The key element of the Russian strategy is the notion that the war is essentially staged in the minds of the participants ... information operations have a great role to play, and they have reached a point where they can take on strategic tasks."[81] A strategic task, such as preventing a NATO consensus on meeting Article 5 commitments when requested, would be the ultimate prize for a Russian information campaign, eliminating NATO's raison d'être at a stroke and immediately justifying Moscow's years of immense investment in information warfare. As noted by Estonian President Toomas Ilves, “It is of such crucial existential importance to NATO that Article 5 be observed ... as soon as Article 5 doesn’t work, every country is on its own, and the only country that can handle being on its own is the United States.”[82]

The threat of Russian information campaigns is such that, in combination with other tools, they prepare the ground for future Russian action which would be directly counter to the interests of Europe and the West. By either undermining the will or support for deterrent measures, or sowing an entirely false impression that Russia is justified in its actions, Russia adjusts key variables in the security calculus determining the risk inherent in future assertive action against its neighbours. In the case of Ukraine, Russia felt the balance was tipped sufficiently in its favour to act, but Ukraine, and Georgia before it, are unlikely to be the last neighbours of Russia to fall victim to this calculation. Current Russian ambitions, if followed to their conclusion, must necessarily lead to a more direct confrontation with the West. Russia now benefits from a highly developed information warfare arsenal which will be a key facilitator in preparing for further actions against its Western neighbours. As noted by Martin Hurt:

> *No matter which country Russia picks on next, it is almost certain that the first phase will be an attempt to harm its international reputation using provocations and dirty tactics in order to isolate it from its EU and NATO allies. For example, heads of governments must be prepared to explain to their publics that social media footage of purportedly murdered Russian children and elderly people are just one of many tactics whose ultimate goal is to dismantle European security.*

---

major Ukrainian nuclear plant - report", RT, 30 December 2014. http://rt.com/news/218807-ukraine-nuclear-plant-leak/.

[79] Rory Finnin and Thomas D. Grant, "Don't call it a civil war - Ukraine's conflict is an act of Russian aggression", The Conversation, 24 August 2015. http://theconversation.com/dont-call-it-a-civil-war-ukraines-conflict-is-an-act-of-russian-aggression-46280.

[80] As reflected in "Rethinking deterrence and assurance", Wilton Park conference report WP1401, 10-13 June 2015.

[81] Jānis Bērziņš, "Russian New Generation Warfare: Implications for Europe", European Leadership Network, 14 October 2014. http://www.europeanleadershipnetwork.org/russian-new-generation-warfare-implications-for-europe_2006.html.

[82] Leonid Bershidsky, "Estonia Did Its Post-Soviet Homework", Bloomberg View, 3 March 2015. http://www.bloombergview.com/articles/2015-03-03/estonia-did-its-post-soviet-homework.

> *This will require European politicians to display qualities of leadership worthy of their responsibility level, and their pay grade.*[83]

Awareness of the destructive potential of hostile information campaigns is also growing in fields which are entirely unrelated to state or non-state adversaries, such as Russia. The phenomenon of source proliferation sowing doubt in authoritative sources has been noted by the scientific community, with the problem of "predatory journals" diluting properly peer-reviewed scientific journal articles with unevaluated material, leading to readers being "unable to distinguish between credible research and junk science."[84] In the UK, controversy over local elections in the London district of Tower Hamlets brought widespread attention to the vulnerabilities of liberal political processes to subversive information campaigns. This incident demonstrated how a dedicated group of individuals can seize political power using concerted efforts to target a specific community's points of susceptibility, by means of intimidation, disinformation, making use of cultural and religious sensitivities, and targeting the disaffected - tapping into existing or manufactured senses of grievance or exclusion.[85] There are other precedents from previous decades which testify to the effectiveness of campaigns specifically intended to undermine Western defence readiness. Exercise HARD ROCK was a 1982 UK emergency exercise at national scale intended to practise responses to a Soviet nuclear strike. The exercise was successfully derailed by a sustained campaign which led to a number of County Councils withdrawing their support.[86]

In short, the mass consciousness of the populations of Western nations is a key arena for confrontation with Russia. In terms of the potentially disastrous effects on domestic audiences, little has changed since a 2008 study of hybrid warfare wrote that:

> *The battle over competing narratives plays out among three audiences: the indigenous population, the home front of the great power, and the wider international community. Great powers risk losing conflicts in which they fail to understand either the human terrain or the "decisive battlegrounds of public opinion at home and abroad."*[87]

This decisive nature of domestic attitudes in the context of military operations was noted in another study written a year later, with the reflection that, "If the story has the potential to erode public support, either domestically or internationally, then it is, in fact, mission critical."[88] It is to this critical point that Russian information warfare seeks to apply persuasive pressure.

---

[83] Martin Hurt, "The potential for hybrid warfare in Central and Western Europe", European Leadership Network, 9 October 2014, http://www.europeanleadershipnetwork.org/the-potential-for-hybrid-warfare-in-central-and-western-europe_1989.html.

[84] Robert E Bartholomew, "Science for sale: the rise of predatory journals", Journal of the Royal Society of Medicine, Vol. 107, Issue 10, 2014. pp. 384-5.

[85] "Judgment In The High Court Of Justice, Queen's Bench Division, In The Matter Of The Representation Of The People Act 1983 And In The Matter Of A Mayoral Election For The London Borough Of Tower Hamlets Held On 22 May 2014". http://news.bbc.co.uk/1/shared/bsp/hi/pdfs/judgment.pdf.

[86] See for example Duncan Campbell, "Bad day at Hard Rock", The New Statesman, 17 September 1982. pp. 6-9.

[87] John J. McCuen, "Hybrid Wars," Military Review, March-April 2008. pp. 107-113.

[88] Cori E. Dauber, "YouTube War: Fighting In A World Of Cameras In Every Cell Phone And Photoshop On Every Computer", U.S. Army War College Strategic Studies Institute, November 2009. p. ix.

Russia's New Emphasis on Information and Influence

Overall, Russia's priorities have shifted from the "accumulation of seemingly unlimited military power to devising new concepts that integrate conventional, nuclear, and unconventional elements of military power in order to build a complex toolkit for facing various contingencies."[89] This new and more precise military instrument can be applied with more finesse than its predecessors, which may increase readiness to use it, given the ability to exert "just enough force to get the policy job done, but not more."[90] The job in question could be coercion through the threat of military force rather than actual application of force, capitalising on the adversary's fear of conflict. According to Mark Galeotti, Russia can now deploy "an extensive, aggressive, and multi-platform attempt to use its military and the threat of force as instruments of coercive diplomacy, intended to divide, distract, and deter Europe from challenging Russia's activities in its immediate neighbourhood."[91]

Similarly, Michael Kofman argues that demonstrations of high-end conventional capabilities are "not meant for the actual fight [but rather] intended to make an impression on the United States. The first goal of the Russian leadership is to make the combat zone its own sandbox, sharply reducing the options for peer adversaries to intervene via direct means."[92] In particular, Russia has demonstrated substantial capability in delivering strikes at ranges in excess of 300 km, with both conventional and non-strategic nuclear weapons deliverable not only by the Navy and the Long-Range Aviation, but also by the Ground Forces.[93] In addition to the Iskander missile system, variants and the Bastion coastal defence missile system for land-attack use, the wide range of theatre missiles and land attack cruise missiles (LACM) available to Russia provide the option of nuclear dominance over NATO nations still observing INF Treaty bans, and reluctant to discuss how to respond to nuclear coercion or to exercise deterrence.

Strategic cyber and information campaigns are becoming so frequent as to be almost commonplace. Russia's increasingly overt use of hostile cyber and information campaigning, as exemplified during the 2016 US presidential election,[94] follows a global trend whereby "Russia is assuming a more assertive cyber posture based on its willingness to target critical infrastructure systems and conduct espionage operations even when detected and under increased public scrutiny."[95] It is also a

[89] Isabelle Facon, "Russia's national security strategy and military doctrine and their implications for the EU", Policy Department, Directorate-General for External Policies, European Parliament, January 2017. p. 15. http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/578016/EXPO_IDA(2017)578016_EN.pdf.
[90] Samuel Charap, "Russia's Use of Military Force as a Foreign Policy Tool: Is There a Logic?", PONARS Policy Memo 443, October 2016. http://www.ponarseurasia.org/memo/russias-use-military-force-foreign-policy-tool-there-logic.
[91] Mark Galeotti, "Heavy Metal Diplomacy: Russia's Political Use of its Military in Europe since 2014", ECFR, 19 December 2016. http://www.ecfr.eu/publications/summary/heavy_metal_diplomacy_russias_political_use_of_its_military_in_europe_since.
[92] Michael Kofman, "A Comparative Guide To Russia's Use Of Force: Measure Twice, Invade Once", War On The Rocks, 16 February 2017. https://warontherocks.com/2017/02/a-comparative-guide-to-russias-use-of-force-measure-twice-invade-once.
[93] Gudrun Persson (ed.), "Russian Military Capability in a Ten-Year Perspective - 2016", FOI, December 2016.
[94] "Report on Russian Active Measures", U.S. Congress House of Representatives Permanent Select Committee on Intelligence, 22 March 2018. https://www.hsdl.org/?abstract&did=809811.
[95] James R. Clapper, "Worldwide Threat Assessment of the US Intelligence Community", Senate Armed Services Committee, 9 February 2016. http://www.armed-services.senate.gov/imo/media/doc/Clapper_02-09-16.pdf.

reflection of a shift in Russian thinking about the potential power of information warfare, which goes to the heart of how wars are won - whether by destroying the enemy, or by rendering the enemy unable to fight.

Traditionally, information activities have played a supporting role, facilitating and enabling kinetic or conventional military operations. Now, with the focus shifting to information as the critical capability targeting the adversary's vulnerabilities and centre of gravity, kinetic operations are frequently undertaken to produce an information effect instead of delivering effect in their own right. In this way the roles of the two domains have been reversed, and rather than an enabler, information campaigns have become the enabled operations.

In effect, Russia's new approach to warfighting can be considered simply a recognition of the primacy of soft power over the kinetic - and that if one side can disrupt the others' will and ability to resist, then the actual strength of their military forces becomes much less relevant, even if not necessarily redundant.

Actors and Agencies

Intelligence and Cyber

Russia habitually refers to its national security agencies, including intelligence, as "special services" (Russian: *spetssluzhby*). What sets them apart compared to other nations' intelligence agencies, with few exceptions, is that rather than being solely or mainly about intelligence gathering and analytical activities, collectively – some more than others - they are much more of an action service, with a unique arsenal of active measures (*aktivnyye meropriyatiya*) – a phenomenon that dates back to the Soviet KGB's long-standing practice of action designed to coerce or influence.

The definitions of active measures are numerous. In practical terms, they could be described as "ranging from simple propaganda and forgery to assassination, terrorism and everything in between."[96] A key to their more general understanding is contained within the definition of intelligence activities referred to by KGB defector Vasili Mitrokhin:

> *A secret form of political struggle which makes use of clandestine means and methods for acquiring secret information of interest and for carrying out active measures to exert influence on the adversary and weaken his political, economic, scientific and technical and military positions.*[97]

Moreover, General Oleg Kalugin, a high-prolife KGB defector, noted: "The heart and soul of the Soviet intelligence was subversion. Not intelligence collection, but subversion: active measures to weaken the West."[98]

---

[96] Steve Abrams, "Beyond Propaganda: Soviet Active Measures in Putin's Russia", Connections, Vol. 15, No. 1, Winter 2016. pp. 12-13, https://www.jstor.org/stable/pdf/26326426.pdf.

[97] Ivo Jurvee. "The resurrection of 'active measures': Intelligence services as a part of Russia's influencing toolbox", Hybrid CoE, April 2018. p. 3. https://www.hybridcoe.fi/wp-content/uploads/2018/05/Strategic-Analysis-2018-4-Juurvee.pdf.

[98] "Inside the KGB – An interview with retired KGB Maj. Gen. Oleg Kalugin," Cold War Experience, CNN, January 1998.
http://web.archive.org/web/20070627183623/http://www3.cnn.com/SPECIALS/cold.war/episodes/21/interviews/k

In the pursuit of this overarching aim - to weaken the West - NATO in general and the United States in particular, were the target of efforts designed "to sow discord among allies" and weaken the US internationally, or in Kalugin's words "to make America more vulnerable to the anger and distrust of other peoples."[99]

It would appear that the same approach, designed to stimulate anger and distrust whether externally or internally, applies now. As information campaigns are waged, the aim of subversion in the West is not to achieve a wholesale change of minds but to move radical fringes to action and suppress votes on one side but motivate them on the other, be it with the help of recruited agents or agents of influence. Yet, while the Russian government can still call upon proxies for action in cyberspace, Russia has invested heavily in what could be generalized as its cyber forces since the armed conflict with Georgia, with the result that its special services have acquired capabilities that are "far beyond what they had in 2008."[100]

As the KGB's main successor in the Russian Federation, the Federal Security Service (*Federalnaya Sluzhba Bezopasnosti, or* FSB) has inherited its forerunner's arsenal of active measures, now adapted to the new geopolitical and technological environment with its resultant new platforms of influence. Moreover, the KGB's doctrine of intelligence as a form of 'political struggle' appears also alive and well, as suggested by the rise in the magnitude of Russia's intelligence activities. The country's security and intelligence agencies are in a state of what has been described as political war against the West,[101] but merely adjusted to the socio-technical realities of the 21st century.

Although little is known about the formal division of responsibilities between the various branches of the Russian security and intelligence apparatus, it is plausible that the FSB's purview extends to what Russia refers to as the 'near abroad' (i.e. parts of the former Soviet Union). By contrast, the agency formerly known as the GRU (from the Russian *Glavnoye Razvedyvatelnoye Upravleniye* or Main Intelligence Directorate), but now officially referred to as the GU (*Glavnoye Upravleniye* or Main Directorate), is responsible for the conduct of military intelligence activities. However, the GU's responsibility extends far further afield and is far broader than its formal remit might suggest. Or, to put more succinctly:

> *"A military intelligence agency that used to be strictly military has now become, if you will, universal."* [102]

Whereas during the Soviet era, the GU was tasked with clandestine operations to build Kremlin influence in the developing world, its role in the West was limited largely to collecting military secrets. The KGB took the lead on political influence

---

alugin/.

[99] *Ibid.*

[100] Jeffrey Carr, "Digital Dao: Russian Cyber Warfare Capabilities in 2014 (We Aren't in Georgia Anymore)", http://jeffreycarr.blogspot.co.uk/2014/03/ russian-cyber-warfare-capabilities-in.html.

[101] Mark Galeotti, 'Russian intelligence is at (political) war', NATO Review Magazine, May 2017. https://www.nato.int/docu/review/2017/also-in-2017/russian-intelligence-political-war-security/en/index.htm.

[102] A Russian activist in Anton Troianovski and Ellen Nakashima, "How Russia's military intelligence agency became the covert muscle in Putin's duels with the West", The Washington Post, 28 December 2018. https://www.washingtonpost.com/world/europe/how-russias-military-intelligence-agency-became-the-covert-muscle-in-putins-duels-with-the-west/2018/12/27/2736bbe2-fb2d-11e8-8c9a-860ce2a8148f_story.html.

operations, while the GU now combines both of the elements above, and much more. As such, it constitutes arguably one of the most important intelligence and influence instruments available to the Kremlin.

The GU's wide spread of responsibilities is accompanied by a seemingly greater appetite for risk, which in turn accords with the mindset of the Kremlin's current occupants. In the words of a former US intelligence officer, "Putin has become more comfortable with risk [and] the GU fits his moment."[103]

In a direct reference to what is today another domain where the GU is highly active, one noted authority observes that, "Historically, the GU has been Russia's main agency for operating in uncontrolled spaces, which has meant civil wars and the like … [and] in some ways, the Internet is today's uncontrolled space."[104]

The GU is now the prime suspect in conducting psychological operations over the Internet and waging cyberattacks, from reportedly the "first known, if somewhat crude, effort by the GU's main psychological-operations division to influence US politicians" in 2015 (an email to a group of Senators from someone purporting to belong to a group of Ukrainian "patriots"), to the hacking of the Democrats' networks in 2016, to deploying a highly disruptive computer virus dubbed NotPetya in 2017.[105] The GU unit behind the emails, known as Unit 54777, or the 72nd Special Service Centre, is the "centre of the Russian military's psychological-warfare capability" and is thought by Western intelligence agencies to work with other psychological operations and cyber units, such as the CyberCaliphate, a "hacking outfit passing itself off as supporters of the Islamic State" but actually a part of the same GU unit that penetrated the Democrats' networks in 2016.[106]

In sum, the characterization of Russia's intelligence services as "the front-line soldiers in Moscow's non-kinetic political war on the West"[107] fully reflects their role in Moscow's influence operations abroad.

Yet the sheer size of Russia's special services, and perhaps even more so the very nature of the system, presents challenges and results in problems. On the one hand, the decentralised and deniable can be characterised as *grey zone activity*. This ambiguity provides the potential for semi-independent intelligence and security actors to take the initiative on the assumption that this is what the leadership wants, sometimes with outcomes that border on or in fact constitute failure. On the other hand, the system is competitive rather than cohesive. In part, this incoherence results from the overlap of baronial jurisdictions in the field of Russia's national security community. Russia's top-down siloed system also leads to a lack of coordination by preventing inter-agency discussions. There is no incentive for sharing information on current operations, still less intelligence, across agencies.

Despite the arrival of the National Defence Control Centre, poor coordination between different levers of power is likely to continue. Moreover, as different

[103] Andrea Kendall-Taylor, a former US deputy national intelligence officer. *Ibid.*
[104] Mark Galeotti, an expert on Russian intelligence at the Institute of International Relations in Prague. *Ibid.*
[105] *Ibid*.
[106] *Ibid*.
[107] Mark Galeotti, 'Russian intelligence is at (political) war', NATO Review Magazine, May 2017. https://www.nato.int/docu/review/2017/also-in-2017/russian-intelligence-political-war-security/en/index.htm.

uncoordinated instruments of Russian state power compete, the situation cannot but increase the level of unpredictability for Russia's adversaries.

Special and Special Operations Forces

The term *Spetsnaz* is an abbreviation of the Russian *Spetsialnogo Naznacheniya* (Special Purpose or 'of Special Designation'). This is a generic term often applied to any non-conventional Russian military or paramilitary unit, and as such covers a wide range of military and state security units with widely varying degrees of training and operational capability. Russia's Army, Navy, National Guard and intelligence services all have their own Spetsnaz units, each with their own allocated range of tasks which can include engaging in or supporting ground hybrid operations.

While the total number of service personnel in different Spetsnaz branches is estimated to be 17,000-18,000,[108] this number includes wide variations in skills and capabilities. Containing around 20-30% conscripts, most units are comparable to elite Western assault troops or specialised light infantry-type units, such as the UK Parachute Regiment or Royal Marines Commando (in the case of naval Spetsnaz), or the US 75th Ranger Regiment.[109] Only a small number of service personnel, estimated to total 1,500-2,000, within the Komandovaniye Sil Spetsialnogo Naznacheniya (KSSO - Special Operations Forces Command) and its regimental-sized operational arm, the 346th Brigade, are considered truly comparable with western Tier 1 SOF (special operations forces).

The Spetsnaz nomenclature also covers internal security actors, such as the FSB units Alfa and Vympel, responsible for anti-terror operations and protection of strategic infrastructure respectively. In addition, the Foreign Intelligence Service (SVR) has its own special unit, Zaslon, responsible for VIP protection.[110] These primary tasks would not limit any of these special forces units from conducting hybrid-like missions abroad. Nevertheless, the primary actor responsible for special ground operations is the GU. The essential responsibilities of the GU are the provision of intelligence for the military- and political decision-makers, but also supervision of the Russian Ground Forces' special operation units.[111] GU specialist training streams focus on a range of capabilities including political operations, military reconnaissance, sabotage, assistance to proxies, and elite infantry integrated with conventional units.

The reorganisation and reallocation of Spetsnaz units in all their various forms and subordinations are continuing at the time of writing.[112]

---

[108] Galeotti, M. 'Operational situation'. Jane's Intelligence Review, IHS Markit, 2018. pp. 12. Bukkvoll, T. "Russian Special Operations Forces in Donbass and Crimea", Aleksanteri Papers, 1, 2016. p. 14-17. https://ssi.armywarcollege.edu/pubs/parameters/issues/Summer_2016/5_Bukkvoll.\pdf

[109] Galeotti, M. (2015) Spetsnaz: Russia's Special Forces. Oxford: Oxford Publishing pp. 54-55.

[110] Bukkvoll, T. 'Russian Special Operations Forces in Donbass and Crimea', Aleksanteri Papers, 1, 2016. p. 13-17. https://ssi.armywarcollege.edu/pubs/parameters/issues/Summer_2016/5_Bukkvoll.pdf.

[111] Defense Intelligence Agency, "Russia Military Power: Building a Military to Support Great Power Aspirations". Military Power Publications, 2017. p.74. http://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Russia%20Military%20Power%20Report%202017.pdf.

[112] In December 2018, for instance, independent Spetsnaz companies were returned to the order of battle of one of the Western Military District's combined-arms armies. See "Return of Independent Spetsnaz Companies", Russian Defense Policy blog, 22 December 2018. https://russiandefpolicy.blog/2018/12/22/return-of-independent-spetsnaz-companies/.

Language Skills

Although contract *Spetsnaz* may learn the customs and language of an area in which they are expected to operate, this is more likely to be a basic operational understanding, possibly enabling them to decipher signals intercepts, translate captured documents and question prisoners. They may gain greater fluency if they later intend to transfer to a GU intelligence role.[113] Language skills are likely to be to a higher standard in the FSB *Spetsnaz,* in particular in *Vympel,* which traditionally focused on overseas operations and previously required its operators to develop fluency in one and basic knowledge of a second language.[114] *Zaslon* unit personnel, providing covert operational support to the Foreign Intelligence Service (SVR), are likely to have the highest standard of foreign language skills.

Organisation and Structure

Briefly, to examine the organisation and structure of *Spetsnaz* forces' order of battle (ORBAT), the bulk of *Spetsnaz* military forces, estimated to number between 15,000 to 17,000 strong, are found in seven Army Brigades (obrSpN), comprising around 19 battalion-sized Detachments (ooSpN). *Spetsnaz* Brigades can number anywhere between 1,500 and 5,500 personnel, consisting of a headquarters, three to four battalions, a communications company and support elements. Between 2010-13, there was a plan to subordinate the various *Spetsnaz* Brigades under the Army territorial commands. This command relationship appears to have been dropped and they remain subordinate to the Fifth Directorate (Operational Reconnaissance) of the GU.[115]

The seven Army GU *Spetsnaz* Brigades (obrSpN) are based in the various Russian Military Districts. Additionally, the 346th *Spetsnaz* Brigade, a regimental-sized operational arm of the KSO Special Operations Command, is based at Prokhladny. The 25th Independent Regiment, responsible for operations in Chechnya and the Northern Caucasus, is based at Stavropol. The 100th Independent Brigade, used to test new weapons, equipment and tactics, is based at Mozdok.[116] Finally, falling under VDV Airborne command is the 45th Guards Independent *Spetsnaz* Airborne Reconnaissance Brigade, based at Kubinka, Moscow, which appears to have a similar role to the UK Special Forces Support Group (SFSG), acting as a force multiplier to the KSO and its 346th Special Forces Brigade. This support role was demonstrated during the seizure of the Crimean Parliament Building, Simferopol, in February 2014. The KSO based at Senezh, northwest of Moscow, also has its own designated Ka-52 (Hokum) combat helicopter and Il-76 (Candid) air transport support at Torzhok Air Base.

1. Western Military District.

    i. 2nd *Spetsnaz* Brigade (obrSpN) - Promezhitsa, Pskov.

[113] See Galeotti, M. "Putin's Hydra: Inside Russia's Intelligence Services", Policy Brief May 2016 European Council on Foreign Relations, May 2016.
[114] Galeotti (2013) *Op.Cit.* pp.40-1.
[115] Galeotti (2015) *Op.Cit.* pp.43-5.
[116] Based on details in Galeotti (2015) *Op.Cit.* p.47.

ii. 16th *Spetsnaz* Brigade (obrSpN) - Chuchkogo/Tambov, Moscow.

2. Southern Military District.

    i. 10th *Spetsnaz* Brigade (obrSpN) - Molkino, Krasnodar.

    ii. 22nd Guards *Spetsnaz* Brigade (obrSpN) - Stepnoi, Rostov.

    iii. 346th *Spetsnaz* Brigade (obrSpN) - Regimental-sized - Prokhladny.

    iv. 25th Independent *Spetsnaz* Regiment (opSpN) - Stavropol.

3. Central Military District.

    i. 3rd Guards *Spetsnaz* Brigade (obrSpN) - Togliatti.

    ii. 24th *Spetsnaz* Brigade (obrSpN) - Irkutsk and Novosibirsk.

4. Eastern Military District.

    i. 14th *Spetsnaz* Brigade (obrSpN) - Ussuriysk.

5. VDV Airborne Command. 45th Guards Independent *Spetsnaz* Airborne Reconnaissance Brigade - Kubinka, Moscow.

Naval *Spetsnaz* are structured into four brigade-sized Reconnaissance Points (omrpSpN), each of which contains its own underwater diversionary combat unit (SpN PDSS) of between 60 and 100 operators.

The Naval Reconnaissance Points reside under their respective Fleet commands:

1. Pacific Fleet. 42nd Independent Special Purpose Naval Reconnaissance Point (omrpSpN) - Vladivostok.

2. Northern Fleet. 420th Independent Special Purpose Naval Reconnaissance Point (omrpSpN) - Severomorsk.

3. Black Sea Fleet. 431st Independent Special Purpose Naval Reconnaissance Point (omrpSpN) - Sevastopol.

4. Baltic Fleet. 561st Independent Special Purpose Naval Reconnaissance Point (omrpSpN) - Kaliningrad.

Information Operations Troops (VIO)

Concept

When reviewing the military's performance in Georgia, deficiencies were noted in

both the information-technical and information-psychological domains, the two main strands of information warfare in Russian thinking.[117] As noted above, the answer proposed was the creation of "Information Troops" within the Russian Armed Forces, who would meet the military's need for *full-spectrum information operations*.

One of the most clearly developed arguments for an entity of this kind was put forward by Igor Panarin, referred to above. Panarin called for "Information Special Forces" who would "prepare for effective operations under potential crisis conditions."[118] These operations would cover all aspects of information operations, including computer network operations and hacking.[119]

The holistic nature of the tasking for these new units, and the way in which the Venn diagram of the Russian information war concept includes much that we might categorise under entirely different headings, was illustrated by further extensive and detailed descriptions of the desired new capability, which inter alia stated:

> *The personnel of the Information Troops should be composed of diplomats, experts, journalists, writers, publicists, translators, operators, communications personnel, web designers, hackers, and others .... To construct information countermeasures, it is necessary to develop a centre for the determination of critically important information entities of the enemy, including* ***how to eliminate them physically****, and how to conduct electronic warfare, psychological warfare, systemic counterpropaganda, and net operations to include hacker training."*[120]

Persuasive press commentaries were followed in due course by Deputy Chief of the General Staff Aleksandr Burutin, noting at the National Information Security Forum that it was "essential to move from analysing the challenges and threats ... to reacting to them and pre-empting them."[121]

Competition

When Col-Gen Anatoly Nogovitsyn suggested that the General Staff should be working on defence against information-technical attack, he was immediately criticised by the Federal Security Service (FSB):

> *It is a strange statement .... Such issues are not under the purview of any one department and should be resolved within the framework of the country's Security Council [a body saturated with serving and former FSB officers]. At the same time, the military cannot but know that we have already created information-protection mechanisms, and they are constantly being*

[117] Thomas, T. L. "Russian Information Warfare Theory: The Consequences of August 2008", in Blank, S. and Weitz, R. *The Russian Military Today and Tomorrow: Essays in Memory of Mary Fitzgerald*, Carlisle: US Army War College Strategic Studies Institute, 2010.
[118] OSC: Panarin, I. "The Information Warfare System: The Mechanism for Foreign Propaganda Requires Renewal", *Voyenno-Promyshlennyy Kuryer* 15 October 2008.
[119] BBC Monitoring: "Russian TV highlights hacker attacks on Georgian sites", *RenTV*, 11 November 2008.
[120] BBC Monitoring: "Russia is Underestimating Information Resources and Losing Out to the West", *Novyy Region*, 29 October 2008 (emphasis added). See also Tsyganok, *op. cit*.
[121] *Tsentr parlamentskikh kommunikatsiy*, 30 January 2009. http://www.parlcom.ru/index.php?p=MC83&id=27297.

improved.[122]

This is indicative of the fact that this capability, which the military felt it lacked, was already well-established in other of Russia's *power ministries* with permanent seats on the Russian Security Council. The Ministry of Internal Affairs (MVD) has its Directorate K, which deals with information crime in the broadest sense, and with a perceived ambiguous role in which kind of cybercrime it will prosecute and which it will permit to continue. Russia did at one point have a dedicated information security agency, the Federal Agency for Government Communications and Information (FAPSI) - described by one leading expert as the unofficial Ministry of Information Warfare.[123]

Although the life-span of FAPSI as an independent entity was relatively short, its components were not disbanded but absorbed into two other agencies - the Federal Protection Service (FSO) and the FSB.[124] While the FAPSI directorate dealing with government communications was transferred to the FSO,[125] the FSB received the Main Directorate for Radio-Electronic Reconnaissance on Communications Networks (*Glavnoye upravlenye radioelektronnoy razvedki sredstv svyazi*, GURRSS). The influence of this body in directing government policy could be inferred from the fact that the former chief of FAPSI and of the GURRSS, Vladislav Sherstyuk, holds the information security portfolio on the Security Council and is also the head of the Department of Information Security at Moscow State University.[126] This department is particularly active in Russia's efforts for international agreements on information and cyber conflict, some of which are referred to above. [127] Thus, a proposal for a new component of the Russian Armed Forces dealing with information warfare had to contend with the fact that it was launched onto a stage already crowded with other information actors, many of which were not particularly willing to share the space with a relative newcomer.

Establishment

After a long period in development, the Information Operations Troops (*Voyska Informatsionnykh Operatsiy,* or VIO) were announced as part of the Russian order of battle in February 2017.[128] These units were expressly intended to fill a gap in Russian information operations capabilities perceived during the armed conflict in Georgia in 2008. The distinction between these line units and those conducting cyber and intelligence operations is important. In keeping with the continuing mismatch between Western and Russian concepts of information operations, Defence Minister Sergei Shoigu's announcement of Information Troops was widely misinterpreted in Western reporting to indicate that these were to provide primarily a cyber capability. Instead, their purpose appears much more in keeping with the

[122] Litovkin, D. "General Staff Prepares for Cyber War", *Izvestia*, 27 February 2009.
[123] Bennett, G. *The Federal Agency of Government Communications & Information*, Conflict Studies Research Centre. Sandhurst: August 2000.
[124] Bennett, G. *FPS & FAPSI - RIP,* Conflict Studies Research Centre. Sandhurst: March 2003.
[125] Official history of the FSO, http://www.fso.gov.ru/histori/histori7.html.
[126] Security Council of the Russian Federation website, http://www.scrf.gov.ru/persons/11.html
[127] See Talbot, D. "Russia's Cyber Security Plans", 16 April 2010.
http://www.technologyreview.com/blog/editors/25050/. for an interview with Sherstyuk discussing "cyber arms control" and the nature of cyber weapons.
[128] "Information Troops Set Up in Russian Federation MoD" [in Russian], Interfax, 22 February 2017.
http://www.interfax.ru/russia/551054.

broad, Russian definition of information warfare, of which cyber is just a part. Russian officers emphasise that the formations tested in various exercises, and already deployed in Syria, are in some cases using techniques "unchanged since the Great Patriotic War," including loudspeaker broadcasts in foreign languages and leaflet drops.[129] At the same time, Russian officers also noted new capabilities of these units, such as UAVs designed to intercept or broadcast data on mobile phone networks. These capabilities are in use for disinformation, demoralisation and propaganda purposes in Syria and Ukraine but have also employed against NATO servicemen in the Baltic states.[130]

The creation of the VIO underscores development in a long tradition of Russian emphasis on information support to ground operations. Although the *maskirovka* plan has always been an integral element of Russian operational orders, recently the overall role of information activities has become increasingly prominent. Although there is strikingly little information publicly available on the operating model of the VIO – or the unit's size and equipment – one assessment indicates their main function is to apply a combination of traditional propaganda, disinformation, psychological manipulation, and strategic communications.[131] The evolution and further formation of the VIO is a notable topic of interest, to be followed closely in the near future as an indicator of how Russia is addressing the increasing importance of information and influence operations.

The recent move to re-establish a Military-Political Directorate within the Russian Ministry of Defence - political officers as they used to be known in the Soviet Union - could also be seen as a means to control the information environment both within the Russian Armed Forces and, to some extent, to shape narratives externally. As Russia hones its ability to act in a way that integrates information operations with both conventional and unconventional military operations, this could also be seen as the recognition of its own vulnerability to similar tactics used against Russia.[132]

At the time of writing, the VIO remain significantly under-studied in open sources both in Russia and abroad, and their activities and organisation insufficiently understood. Given their probable significant role in influence activities at a tactical and operational level, this deficiency should be addressed.

Influence Case Studies: Crimea, Eastern Ukraine, Syria

[129] See also Mikhail Klikushin, "Putin's Army Demands 'NATO Soldiers! Hands Up! Lay Down Your Weapons!'", The Observer, 19 August 2016. http://observer.com/2016/08/putins-army-demands-nato-soldiers-hands-up-lay-down-your-weapons/.
[130] Keir Giles, "Assessing Russia's Reorganized and Rearmed Military", Carnegie, May 2017. https://carnegieendowment.org/2017/05/03/assessing-russia-s-reorganized-and-rearmed-military-pub-69853. For the most recent instances of use of similar techniques at the time of writing, see "Defense Ministry: Russia Sending SMS Messages Asking Residents Of Ukrainian Border Regions To Appear At Nearest Military Units", Ukrainian News, 27 November 2018. https://ukranews.com/en/news/598565-defense-ministry-russia-sending-sms-messages-asking-residents-of-ukrainian-border-regions-to-appear.
[131] Multiple authors. "The Fog of Russian Information Warfare", in *Perception are reality: Historical Case Studies of Information Operations in Large-Scale Combat Operations*, edited by Mark D. Vertuli and Bradley S. Loudon, US Army Press, 2018. pp.40-43. https://www.armyupress.army.mil/Portals/7/combat-studies-institute/csi-books/perceptions-are-reality-lsco-volume-7.pdf.
[132] Mason Clark with Catherine Harris, "Russia's New Tool for Wielding Information", Institute for the Study of War, 15 January 2019. http://iswresearch.blogspot.com/2019/01/russias-tools-for-wielding-information.html.

Crimea

The military operation to take over Crimea in late February 2014, when Russian troops without identifying marks seized government buildings and strategically important points in cities and surrounded Ukrainian military sites, was only the culmination of preparatory measures undertaken using a wide range of non-military measures.[133] The active phase of preparations for the influencing operations had begun at the early stages of the Maidan protests in the Ukrainian capital Kyiv[134], with Russian-state owned media outlets (including in Crimea) promoting anti-Ukraine narratives and describing the illegitimacy of the new government. In addition, Rossotrudnichestvo, the agency responsible for Russian state relations with compatriots abroad, stepped up activity rallying local populations to protests, while a Kremlin-funded puppet "Russian Community of Crimea" issued a written appeal to Russia for military intervention.[135]

Meanwhile, Russian proxies were preparing for the active phase of operations to be conducted by regular forces. These proxies included Cossacks, primarily allocated a force protection role, and the Night Wolves a multinational corporation in the guise of a motorcycle club which engaged in spreading disinformation, organizing civil unrest, collecting intelligence, creating self-protection militias, establishing vehicle checkpoints and roadblocks, and blockading key points.[136] Their activities before and during the seizure of the peninsula indicated strongly that they were centrally coordinated during the planning phase,[137] and at least 11 members of the Night Wolves were awarded the campaign medal "For the Return of Crimea" as though they had been serving in the Russian Armed Forces.[138]

Subsequently, during the overt phase of the intervention, Russia's regular ground forces interacted closely with these proxies. A number of KSSO operators posed as local "self-protection units" during the seizure of the Crimean parliament in order to maintain the pretence that there was no Russian involvement, while elements of the 45th VDV Guards Independent Regiment provided support and security in the surrounding area. Proxies and information preparation of the area of operations, combined with the insertion of special forces, were key enablers for Russia to achieve the seizure of the peninsula with virtually no direct confrontation.

The operations in Eastern Ukraine and Crimea were thus supported by a range of influence actors including non-governmental organisations, media outlets, political parties and businesses. These organisations included local-level actors such as

[133] RAND Corporation, Lessons from Russia's Operations in Crimea and Eastern Ukraine, RAND Corporation, 2017. pp. 5-31. https://www.rand.org/pubs/research_reports/RR1498.html.
[134] Kyiv is the transliterated English spelling of Ukraine's capital. Prior to the fall of the Soviet Union, the Russian transliterated version was used, Kiev.
[135] Lutsevych, O., *Agents of the Russian World: Proxy Groups in the Contested Neighbourhood*, Chatham House, 2016. p. 36-37. https://www.chathamhouse.org/publication/agents-russian-world-proxy-groups-contested-neighbourhood.
[136] Matthew A. Lauder, "'Wolves of the Russian Spring': An Examination of the Night Wolves as a Proxy for the Russian Government", Canadian Military Journal, Vol. 18, No. 3, Summer 2018. http://www.journal.forces.gc.ca/vol18/no3/PDF/CMJ183Ep5.pdf.
[137] RAND Corporation, Lessons from Russia's Operations in Crimea and Eastern Ukraine, RAND Corporation, 2017. pp. 5-31. https://www.rand.org/pubs/research_reports/RR1498.html.
[138] Irene Chalupa, "Direct Translation: Meet the Ex-Convicts, Bullies, and Armed Bikers Who Helped Seize Crimea," Atlantic Council, 19 June 2014. http://www.atlanticcouncil.org/blogs/new-atlanticist/direct-translation-the-kremlin-celebrates-secretlythe-ex-convicts-bullies-and-bikers-who-helped-itcapture-crimea.

Moscow mayor Yuri Luzhkov's Moscow-Sevastopol and Moscow-Crimea organisations as well as more broad-based groups including ethnic, ideological, historical, religious and extremist patriotic movements supported by Russian business individuals, policy-makers and entities with close links to the Kremlin.[139] Information operations were carried out both by applying cognitive and social cyber actions such as social media influencing, and through technical cyber operations by groups including the so-called Cyberberkut.[140]

A distinctive aspect of information operations in Ukraine itself, and one with important implications for how cyber war may be waged in future, is the way Russian activity in the cyber domain facilitates broader information warfare aims. One manifestation of this is the spearphishing of Ukrainian officials[141] for exploitation, but also in specific uses of malware in the conflict.[142] A particular example is the redirection of malware originally intended for cybercrime to manipulating viewer figures to promote pro-Russian video clips.[143] But potentially even more significant for the nature of future cyber operations is the new interface between cyber and kinetic operations.

During the seizure of Crimea, Russia sought to influence three distinct audiences: the local population, the Ukrainian armed forces in Crimea, Western leaders and decision-makers, and Russia's own domestic population. Three key aspects of the hybrid intervention provided the ingredients for the influence mix calibrated and tailored to each audience.

Information isolation

When Russia wished to isolate Crimea from news from the outside world, no sophisticated cyber exploits were required. Instead, in addition to gaining pre-emptive control of television and radio broadcasters and print media in Crimea, during the intervention Russian special forces with embedded telecommunications engineers simply took over Crimea's main Simferopol internet exchange point (IXP), and elsewhere selectively disrupted cable connections to the mainland.[144] Russia's consequent total information dominance of the region, and accompanying information campaigns including such basic measures as speeches at rallies, ensured that no information from other than Russian sources was available to the population of Crimea, with the result that significant sections of Crimean society were

[139] Lutsevych, O., *Agents of the Russian World: Proxy Groups in the Contested Neighbourhood*, Chatham House, 2016. https://www.chathamhouse.org/publication/agents-russian-world-proxy-groups-contested-neighbourhood.
[140] RAND Corporation, Lessons from Russia's Operations in Crimea and Eastern Ukraine, RAND Corporation, 2017. pp. 33-62. https://www.rand.org/pubs/research_reports/RR1498.html.

[141] Undated PowerPoint presentation by SBU (Security Service of Ukraine), entitled 'В умовах військової агресії з боку Російської Федерації, війна ведеться не лише на землі, в повітрі та в дипломатичних колах, вперше в історії війн застосовані нові форми ведення агресії - гібридна війна з використанням кіберпростору України'
[142] Geers, Kenneth, 'Strategic Analysis: As Russia-Ukraine Conflict Continues, Malware Activity Rises', FireEye, 28 May 2014. https://www.fireeye.com/blog/threat-research/2014/05/strategic-analysis-as-russia-ukraine-conflict-continues-malware-activity-rises.html.
[143] Kogan, R. 'Bedep trojan malware spread by the Angler exploit kit gets political', Trustwave, 29 April 2015. https://www.trustwave.com/Resources/SpiderLabs-Blog/Bedep-trojan-malware-spread-by-the-Angler-exploit-kit-gets-political/.
[144] 'Кримські регіональні підрозділи ПАТ «Укртелеком» офіційно повідомляють про блокування невідомими декількох вузлів зв'язку на півострові', Ukrtelekom, 28 February 2014. http://www.ukrtelecom.ua/presscenter/news/official?id=120327.

happy to welcome Russian troops because they were "convinced that bandits and fascists were coming from Kiev to kill them". In addition, the surrounded Ukrainian garrisons were unable to communicate with their higher command in Kyiv[145]. This greatly facilitated influence both on the population (to see the Russian troops as protectors against conflict rather than invaders) and on the Ukrainian armed forces (limiting their situational awareness to their interactions with surrounding Russian troops). In short, complex and expensive information weapons are entirely unnecessary in situations where the adversary can gain physical control of infrastructure, and embed the engineering expertise of telecoms with its special forces in order to exploit them.

Disinformation to induce paralysis

Russia's use of special forces without identifying marks, and its denial that these forces were Russian, were not at any point plausible but created sufficient temporary confusion among Western news media, and consequently for Western political leaders, for Russia to achieve its goals without threat of immediate countermeasures from outside Ukraine.

Fait accompli

Due to the speed of movement of Russia's armed forces, taking advantage of preparations by non-military agencies such as the Night Wolves motorcycle outfit[146], both Ukraine and Western states were presented with a situation where Russian troops already controlled key points and would have to be dislodged (with the strong likelihood of open conflict) rather than prevented from taking control.

Russian planners exploited the key conditions and weaknesses of the adversary including local culture, political unrest, and unpreparedness while maximising self-effectiveness by deploying highly-trained small units as a way to avoid direct confrontation as well as being under constant information support.[147] The main objective was to win the hearts and minds of the local population. The presence of proxy actors alongside regular forces was an essential feature to increase the so-called "hybridness" of the operation.

Cross-domain coercion as exercised by hybrid actors aims to manipulate the adversary's perception, to manoeuvre its decision-making process, and to influence its strategic behaviour while minimising, compared to the industrial warfare era, the scale of kinetic force use, and increasing the non-military measures of strategic influence.[148]

Eastern Ukraine

[145] Kyiv is the transliterated English spelling of Ukraine's capital. Prior to the fall of the Soviet Union, the Russian transliterated version was used, Kiev, hence the variation between the quote and the text.
[146] Matthew A. Lauder, "'Wolves of the Russian Spring': An Examination of the Night Wolves as a Proxy for the Russian Government", Canadian Military Journal, Vol. 18, No. 3, Summer 2018. http://www.journal.forces.gc.ca/vol18/no3/PDF/CMJ183Ep5.pdf.
[147] RAND Corporation, Lessons from Russia's Operations in Crimea and Eastern Ukraine, RAND Corporation, 2017. pp. 13-25. https://www.rand.org/pubs/research_reports/RR1498.html.
[148] Dima Adamsky, "Cross-Domain Coercion: The Current Russian Art of Strategy," IFRI Proliferation Papers, No. 54, November 2015.

Russia's ground operations in eastern Ukraine have involved a complex and variable mix of forces, including conventional regular units, proxies, paramilitaries, elements of Rosgvardiya, special forces and intelligence operatives.[149] Conventional ground forces, while not always directly involved in the conflict, played a key role from its early stages. Moscow startled and alarmed the West by moving large amounts of its land forces quickly and effectively to the border with Ukraine. For much of 2014-2016, the main role of those forces was to sit on the border, augmenting and depleting as required in order to focus the attention of the West like a hypnotist's watch while only small Russian SOF groups actually conducted warfare inside Ukraine.

The early formation of the proxy Luhansk and Donetsk "People's Republics" began soon after the annexation of Crimea in the spring of 2014, when armed insurgents and local volunteers were brought together under Russian control and re-formalised as an umbrella organisation for a variety of different paramilitary groups closely associated with non-state actors such as Night Wolves, Cossack networks and Wagner PMC. These paramilitary forces have been responsible for different tasks including policing, recruitment, direct combat, as well as war crimes.[150] They were utilised in a way designed to create a perception of Ukraine being a polarised and a failed state. In information warfare terms, both mainstream and social media influencing were key instruments in shaping not only local sentiments but also the perception in the West about the situation in the conflict zone.[151]

GU and FSB special operation forces have been present in eastern Ukraine since early March 2014 mainly in full-spectrum and overt reconnaissance, sabotage, infiltration, and training roles while avoiding direct combat contact. Meanwhile units from both battalion tactical groups and special operations forces have been effectively unified into the newly formed 1st and 2nd Army Corps, which also include paramilitary forces.[152] One analysis suggests that in the current division of responsibilities in eastern Ukraine, the FSB has taken the lead role in exercising control over the Luhansk sector, while the Donetsk sector is mostly coordinated by the GU.[153]

Russia's cross-border combined-arms offensives of August 2014 and January 2015

[149] Bukkvoll, T. 'Russian Special Operations Forces in Donbass and Crimea', Aleksanteri Papers, 1, 2016. p. 17-20. https://ssi.armywarcollege.edu/pubs/parameters/issues/Summer_2016/5_Bukkvoll.pdf.
Multiple Authors, 'Russian Presence', in *Donbass in Flames*, edited by Alina Maiorova, Security Environment Research Center, 2017. pp. 67-82. https://prometheus.ngo/wp-content/uploads/2017/04/Donbas_v_Ogni_ENG_web_1-4.pdf.

[150] Amnesty International, Torture and Summary Killings in Eastern Ukraine, Amnesty.org, 2015. p. 13. https://www.amnesty.org/download/Documents/EUR5016832015ENGLISH.pdf.
And see: Bingham, J., "Crossing the line", Jane's Intelligence Review, IHS Markit, 2018. pp. 13-15. Shortened version: https://www.janes.com/images/assets/018/78018/Private_companies_engage_in_Russias_non-linear_warfare.pdf. And see: Lauder, M.A. 'Wolves of the Russian Spring': An Examination of the Night Wolves as a Proxy for the Russian Government, Canadian Military Journal, 2018. pp. 5-13. http://www.journal.forces.gc.ca/vol18/no3/PDF/CMJ183Ep5.pdf.
And see: RAND Corporation, Lessons from Russia's Operations in Crimea and Eastern Ukraine, RAND Corporation, 2017. pp. 33-62. https://www.rand.org/pubs/research_reports/RR1498.html.

[151] RAND Corporation, Lessons from Russia's Operations in Crimea and Eastern Ukraine, RAND Corporation, 2017. https://www.rand.org/pubs/research_reports/RR1498.html.

[152] Multiple Authors, 'Russian Presence', in *Donbass in Flames*, edited by Alina Maiorova, Security Environment Research Center, 2017. p. 67. https://prometheus.ngo/wp-content/uploads/2017/04/Donbas_v_Ogni_ENG_web_1-4.pdf.

[153] Mark Galeotti, 'Operational situation'. Jane's Intelligence Review, IHS Markit, 2018. pp. 13.

introduced a dramatically new dynamic into the conflict but confirmed the role of ground forces as just one of many elements combining to achieve Russia's objectives. In August 2014, regular forces formed in battalion tactical groups, were required to prevent a catastrophic defeat of Russia's proxies by the unexpectedly robust Ukrainian military. Close interaction with irregular forces was observed. The main role of the BTGs was to serve as spearhead combat units to take and hold ground while being supported by paramilitary guard forces responsible for securing flanks and logistical routes and screening the main force.[154] The January 2015 offensive in particular represented escalations of influence as much as of conventional war-fighting. It formed the backdrop to threats delivered by Putin during peace negotiations to escalate the conflict to unspecified levels if his demands were not met. Combined with a largely successful information campaign aimed at convincing the West that Ukraine was to blame for the failure to implement the Minsk protocols, this drove Russia's interlocutors, German Chancellor Angela Merkel and French President François Hollande, towards the imposition of the Minsk II agreement and the 'Normandy process', which continues to this day despite Russia's failure to honour any of the Minsk II provisions.[155] Overall, Russia's combining conventional kinetic activity with a sustained and multi-dimensional information campaign brought it success in ensuring a permissive environment for ongoing destabilising activity against Ukraine, condoned by a notional ceasefire ensuring Russia's baseline interests were protected.

Specific episodes in the course of the Ukrainian conflict also further demonstrate use of combined (or "hybrid") actions by a wide range of state and non-state agencies in order to deliver influence. On 5 August 2014, the Russian Foreign Ministry announced that Russia was going to organise "an international humanitarian mission for the southeast of Ukraine." The operation made use of a range of Russian government agencies in addition to Russia's well-developed disinformation capabilities (the convoy used Emergencies Ministry vehicles, with crews from the armed forces, while the Foreign Ministry undertook noisy diplomatic activity in support of the convoy to further divert attention). Almost the entire Russia-watching foreign media accredited in Moscow, and a substantial proportion of the Western diplomatic corps in Moscow, watched the progress of the resulting convoy towards Ukraine, with a primary focus on the potential Ukrainian reaction and the likelihood of conflict once it reached the border.[156] This was a highly successful distraction operation, which allowed Russia to prepare and launch its mid-August cross-border offensive into Ukraine practically unnoticed.

Syria

Russian involvement in ground operations in Syria presented a further refinement of selective integration between regular military forces and irregular enablers, reducing the exposure of the main ground forces to combat to a minimum. Despite the

[154] Nicolas Fiore, *Defeating the Russian Battalion Tactical Group*, Fort Benning, 2017. p. 2. http://www.benning.army.mil/armor/eARMOR/content/issues/2017/Spring/2Fiore17.pdf.
[155] See James Sherr, '*Geopolitics and Security' in The Struggle for Ukraine*, Chatham House, August 2017. pp 11-13.
[156] Detailed in Katri Pynnöniemi, "Metanarratives of Russian Strategic Deception", in Katri Pynnöniemi and András Rácz (eds.), *Fog of Falsehood: Russian Strategy of Deception and the Conflict in Ukraine*, FIIA Report 45, p. 79. On this and other Russian disinformation efforts in Ukraine, see Edward Lucas and Peter Pomerantsev, "Winning the Information War", CEPA, p. 16.

deliberate rotation through Syria of as many Russian professional service personnel as possible to gather experience of operational conditions, the Russian approach strongly emphasised outsourcing of actual combat. Special operations forces, artillery, forward air controllers and support units such as military police focused on enhancing the combat potential of Syrian government troops and coordinating with Syrian and Iranian partners. In addition to regular forces and PMCs, Russia deployed a number of other irregular and paramilitary entities in Syria, including Muslim volunteer militias such as the Turan Battalion consisting of ethnic-Turkish volunteer fighters.[157] The combined use of regular, irregular and private military contractor forces, with heavy emphasis on partnership with local and especially Muslim forces, facilitated Russia's approach to expanding the territory under government control. This targeted engagement with communities was used to conclude local truce agreements, with the alternative of devastating airstrikes. Russia's "reconciliation centres", designed to end fighting by granular engagement with local leaders, consequently achieved successes that would have been impossible if Russia's presence had solely consisted of regular military forces.[158]

Shortly after Russia's involvement in Syria was first observed in September 2015, when Russian air force assets were deployed to Hmeymim airfield and an intensive air campaign followed, the necessity for a ground deployment became clear. Russia began to deploy three distinct categories of forces from early December 2015: first, special operations forces from the KSSO, GU Spetsnaz, FSB Spetsnaz, SVR Zaslon and 431st Naval Reconnaissance Regiment; battalion tactical groups including from the 810th Independent Naval Infantry Brigade; and support elements such as military police and advisor groups.[159] Each different category was tasked with distinct missions and responsibilities. The main role of the SOF and KSSO operators in particular was the execution of joint air-to-ground control and reconnaissance missions for the extensive air and artillery operations, intelligence gathering and provision of kinetic support to ground combat operations.

The use of Private Military Companies (PMCs), another noteworthy element, ranged from urban offensive, reconnaissance and fire support, to defensive roles.[160] Evidence suggests that in 2017, the Wagner PMC specifically took part in the recapture of Deir Ez-Zour and the retaking of Palmyra from Islamic State.[161]

It appears likely that the combined use of regular, irregular and contractor elements will be an enduring feature of Russian land operations, as a means both to broaden the scope, reduce the cost, and if applicable enhance the deniability of each

[157] Fainberg, S. 'Russian Spetsnaz, Contractors, and Volunteers in the Syrian Conflict', Russia.Nei.Visions No.105. IFRI, 2017. p. 19. https://www.ifri.org/sites/default/files/atoms/files/fainberg_russian_spetsnaz_syrian_conflict_2017.pdf.
[158] Tim Ripley, *Operation Aleppo: Russia's War in Syria*, Telic-Herrick Publications, Lancaster, 2018. See also Sanu Kainikara, *In The Bear's Shadow: Russian Intervention in Syria*, Air Power Development Centre, Canberra, 2018.
[159] Fainberg, S. "Russian Spetsnaz, Contractors, and Volunteers in the Syrian Conflict", in Russia.Nei.Visions No.105, IFRI, 2017. p. 10-22. https://www.ifri.org/sites/default/files/atoms/files/fainberg_russian_spetsnaz_syrian_conflict_2017.pdf.
[160] Bingham, J., "'Crossing the line", Jane's Intelligence Review, IHS Markit, 2018. pp. 13-15. Shortened version : https://www.janes.com/images/assets/018/78018/Private_companies_engage_in_Russias_non-linear_warfare.pdf.
[161] J. Miller, "Putin's Attack Helicopters and Mercenaries Are Winning the War for Assad", Foreign Policy, 30 March 2016. http://foreignpolicy.com/2016/03/30/putins-attack-helicopters-and-mercenaries-are-winning-the-war-for-assad/.

operation.

Tactics, Techniques and Procedures

Other incidents and trends provide an insight into the range of capabilities which Russia may be preparing for action. These range from high-level macro approaches, including targeting communications infrastructure at a strategic level, to much more focused targeting of individuals on a personal basis.

Information Isolation

The circumstances in which Russia achieved total information isolation of Crimea were unique, and not only because of the peninsula's distinctive internet geography. Russian planners will have noted the striking success in gaining information control over the region and will be looking for where it can be applied elsewhere. There are two important implications for planning for future crises with Russia. First, both civil and military contingency planning should include scenarios where friendly access to the internet is degraded or absent. Second, civilian internet infrastructure - including IXPs, and in particular undersea cables and their termination points - needs at least as much defence and protection as other strategic assets.

Intensified Russian interest in civilian internet communications infrastructure is one possible indicator of future plans. After a long prehistory in the classified domain, Russian investigation of subsea communications cables is now of a sufficiently high profile that it has reached substantial public reporting in the West. Highly visible commentary in, for example, the New York Times[162] has been accompanied by more detailed investigations in Finnish[163] and Polish[164] media. This is an indication that the subsea activity which is the subject of recent media attention is not just limited to the area around the continental United States, but also extends to the Baltic Sea and elsewhere.[165] The technologies for accessing data from subsea cables are well established.[166] Targeting them would meet a wide range of Russian objectives. According to former SACEUR Jim Stavridis, these would include "a rich trove of intelligence, a potential major disruption to an enemy's economy, and a symbolic chest thump for the Russian Navy."[167]

Unsurprisingly, nations have been reticent about revealing exactly what is known about Russian subsea activity in their immediate environment. The precise capabilities available to Western nations for detecting what is happening in the

[162] David E. Sanger and Eric Schmitt, "Russian Ships Near Data Cables Are Too Close for U.S. Comfort", The New York Times, 25 October 2015. http://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html.
[163] Laura Halminen, "Venäjä nuuskii nyt lännen tietoliikennettä - Krimillä liikennekaapelit vain tärveltiin", Helsingin Sanomat, 7 November 2015. http://www.hs.fi/ulkomaat/a1446879570779.
[164] TVN24 (Poland), "Kable, bez których stanie świat", TVN24, 9 November 2015. http://www.tvn24.pl/weekend/tvn24-na-weekend,12/kable-bez-ktorych-stanie-swiat,237.
[165] Nicole Starosielski, "In our Wi-Fi world, the internet still depends on undersea cables", The Conversation, 3 November 2015. https://theconversation.com/in-our-wi-fi-world-the-internet-still-depends-on-undersea-cables-49936.
[166] Olga Khazan, "The Creepy, Long-Standing Practice of Undersea Cable Tapping", The Atlantic, 16 July 2013. http://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/.
[167] Jim Stavridis, "A New Cold War Deep Under the Sea?", Huffington Post, 28 October 2015. http://www.huffingtonpost.com/admiral-jim-stavridis-ret/new-cold-war-under-the-sea_b_8402020.html.

subsea environment are classified, just as the Russian activities there are. In the case of Finland, the only official statement as to the nature of the underwater intruder which was detected in April 2015 was that it was "not a submarine" - leading to speculation that it was a remotely operated vehicle.

Sophisticated subsea technologies may not be necessary in all cases. Finland in particular has seen media reporting with alarm at the apparently systematic acquisition by Russian interests of land and properties in key locations near strategically important facilities, including "locations related to telecommunication links".[168] The Turku archipelago, in the narrowest stretch of water between southern Finland and Sweden, is highlighted as a key location where communications cables and energy interconnectors are vulnerable.[169]

Potentially hostile activity by Russian assets in space, however, is much more visible, thanks to the involvement of commercial companies in space operations, and to amateurs reporting on what they observe. The unusual manoeuvres carried out by Russian space vehicles in the vicinity of communications satellites has a number of possible explanations. At worst, this could be practice for attack runs for deploying anti-satellite weapons in order to degrade Western communications at a critical moment. At the other extreme, the most charitable explanation is that this provides an opportunity for close observation and investigation of Western communication satellites.[170] In either case, this is a further example of intensified Russian interest in communications infrastructure.[171]

As has been noted above, the very distinctive nature of Crimean internet geography means that replicating this success in information dominance elsewhere would by no means be as straightforward for Russia. Even Crimea itself is now directly connected to the Russian internet, removing one of its key vulnerabilities of a single point of failure for internet connections.[172]

Increasingly, the close Russian interest displayed in communications infrastructure in other areas of the world can have a range of hostile implications. Investigating vulnerabilities of this infrastructure can facilitate espionage operations, isolation, or means of planting disinformation - or a combination of all of these. In addition, information interdiction of the kind demonstrated in Crimea should also be thought of in a broader context. Capabilities displayed in eastern Ukraine include a much-enhanced electronic warfare (EW) capability, including for GPS jamming,[173] which unofficial reports suggest has already been directed from Russia at US and NATO

[168] Ari Pesonen, "Tietoliikenneyhteyksien katkaiseminen olisi Venäjälle tehokasta sodankäyntiä", Uusi Suomi, 27 October 2015. http://aripesonen1.puheenvuoro.uusisuomi.fi/205516-tietoliikenneyhteyksien-katkaiseminen-olisi-venajalle-tehokasta-sodankayntia.
[169] Iltalehti (Finland), "Suomen vesiväylät "motissa" - venäläisfirma osti maat", Iltalehti, 19 January 2015. http://www.iltalehti.fi/uutiset/2015011919044524_uu.shtml, and see:
Iltalehti (Finland), "Maakauppoja strategisissa kohteissa", Iltalehti, 12 March 2015. http://www.iltalehti.fi/uutiset/2015031119338528_uu.shtml.
[170] For detail see Brian Weeden, "Dancing in the dark redux: Recent Russian rendezvous and proximity operations in space", The Space Review, 5 October 2015. http://www.thespacereview.com/article/2839/1.
[171] Capabilities both discussed further in Mike GUss, "Space Surveillance Sats Pressed into Early Service", SpaceNews, 18 September 2015. http://spacenews.com/space-surveillance-sats-pressed-into-early-service/.
[172] Doug Madory, "No turning back: Russia activates Crimean cable", Dyn Research, 31 July 2015. http://research.dyn.com/2014/07/no-turning-back-russia-crimea/.
[173] See “Russia overtaking US in cyber-warfare capabilities,” SC Magazine, 30 October 2015. http://www.scmagazine.com/russia-overtaking-us-in-cyber-warfare-capabilities/article/450518/.

military units visiting border regions of the Baltic states.

Holistic approach

Significantly for the nature of possible future Russian information operations, the method used to achieve information dominance in Crimea was simply taking physical control of the internet and telecoms infrastructure,[174] and selectively disrupting cable connections to the mainland.[175]

This argues that suitable telecoms expertise was available to the Russian special forces involved in the operation, and points to an entirely new interface between cyber, information, and kinetic operations, and one which Western planners should study closely. This combining of capabilities has been demonstrated further in ongoing operations in eastern Ukraine. According to Maj-Gen. Stephen Fogarty, head of the US Army's Cyber Center of Excellence, "Russian activities in Ukraine... really are a case study in the potential for CEMA, cyber-electromagnetic activities… It's not just cyber, it's not just electronic warfare, it's not just intelligence, but it's really effective integration of all these capabilities with kinetic measures to actually create the effect that their commanders [want] to achieve."[176] Meanwhile, by contrast, the US Army itself is reported to be only at an early stage of working towards this effective integration.[177]

More generally, what could be described as Russia's comprehensive approach to the domain of military information technology and the military ("cyber" is just one of the elements integrated with kinetic operations) is unlike anything seen in the West. Rather than referring to cyberspace, Russia refers to 'information space' and includes in this space both computer and human information processing, in effect the cognitive domain. Russian doctrine embraces computer network operations alongside psychological operations and intelligence, counterintelligence, *maskirovka*, disinformation, electronic warfare (EW), debilitation of communications, degradation of navigation support, psychological pressure, and destruction of enemy computer capabilities. Whereas developing Western doctrine on cyberspace such as EW-cyber integration aims to create greater convergence between cyberspace and 'traditional' warfighting, Russia is not faced with the challenge of convergence because - thanks to the holistic and integrated approach to information warfare - they never went through a process of divergence in the first place.[178]

---

[174] Ukraine Telecom,"Unidentified uniformed personnel again block several communication nodes in Crimea", Ukrtelecom, 1 March 2014. http://www.ukrtelecom.ua/presscenter/news/official?id=120389.

[175] Ukraine Telecom, "PJSC Ukrtelecom's Crimean regional branches officially announce the blocking of several communication nodes on the peninsula by unidentified personnel", Ukrtelecom, 28 February 2014. http://www.ukrtelecom.ua/presscenter/news/official?id=120327.

[176] Sydney J. Freedberg, "Army Fights Culture Gap Between Cyber & Ops: 'Dolphin Speak'", Breaking Defense, 10 November 2015. http://breakingdefense.com/2015/11/army-fights-culture-gap-between-cyber-ops-dolphin-speak/.

[177] Jen Judson, "Army Learning How Cyber Support Plays Role In Tactical Operations", Defense News, 10 November 2015. http://www.defensenews.com/story/defense/land/army/2015/11/10/army-learning-how-cyber-support-plays-role-in-tactical-operations/75545442/. With respect to integrating cyber and EW capabilities, see also Joel Harding, "Army Puts 'Cyber Soldiers' In The Mud", To Inform is to Influence, 13 November 2015. http://toinformistoinfluence.com/2015/11/14/army-puts-cyber-soldiers-in-the-mud/.

[178] Keir Giles, "Handbook of Russian Information Warfare," NATO Defence College NDC Fellowship Monograph Series 9, 2016. p. 9.

Targeting Personnel

Another campaign for which Russia appears to be developing, testing, and accumulating capabilities is the targeting of foreign military and defence personnel, whether individually or *en-masse*.

Again, a series of apparently isolated incidents indicate an underlying trend. In mid-2015, US soldiers on rotation through frontline states as part of Operation ATLANTIC RESOLVE, intended to both deter Russia and reassure the host nations, began to be harassed by Russian intelligence operatives recounting details of their personal lives gleaned from social media. This followed a series of incidents, including unsubstantiated allegations of child rape in Russian-backed media against specific named US Army officers visiting Kyiv, effectively highlighting the very personal nature and impact of hostile Russian activities.

At the same time, and despite detailed guidance on use of social media and avoiding presenting vulnerabilities through indiscreet posting, many Western military and defence personnel remain unaware that by using smartphones in hostile information environments - including, for example, Ukraine - they are presenting hostile intelligence services not only with their social media posts, but also with their personal details – in particular their security authentication for any application they logged into at the time. Russia thus does not need to undertake painstaking individual targeting when identities, and credentials, can be harvested and processed on an a relatively industrial scale.

Examples of the impact of these activities are already available, such as the mass telephoning of Polish military personnel in November 2015.[179] Other instances of selecting and then simultaneously contacting a large number of specific individuals include government messaging to Russian internet users who accessed a mail service from Egypt,[180] and a well-documented instance of intimidating SMS messages to individuals taking part in the Maidan protests in Kyiv in January 2014. The messages, including “Dear subscriber, you are registered as a participant in a mass disturbance”, appeared to be from the individuals' local phone service provider but was apparently accomplished without the provider’s involvement (likely using an international mobile subscriber-catcher, or IMSI-catcher, which is a device used to intercept mobile phone traffic).[181]

Since 2014, this capability has been developed and refined, making use of the vast repositories of information on individuals represented by social media and online

[179] Matthew Day, Roland Oliphant, "'Thousands' of Polish soldiers receive mysterious call from Russian number", Daily Telegraph, 3 November 2015. http://www.telegraph.co.uk/news/worldnews/europe/poland/11972391/Thousands-of-Polish-soldiers-receive-mysterious-call-from-Russian-number.html.

[180] Kevin Rothrock, "Russia's Most Popular Social Network Just Sent 20,000 Users a Private Message From the Government", Global Voices, 8 November 2015. https://globalvoices.org/2015/11/08/russias-most-popular-social-network-just-sent-20000-users-a-private-message-from-the-russian-government/print/.

[181] Heather Murphy, "Ominous Text Message Sent to Protesters in Kiev Sends Chills Around the Internet", The New York Times, 22 January 2014. http://thelede.blogs.nytimes.com/2014/01/22/ominous-text-message-sent-to-protesters-in-kiev-sends-chills-around-the-internet/. See also analysis by Andrey Soldatov and Irina Borogan in "The Red Web", available in excerpt at http://uk.businessinsider.com/heres-how-facebook-kicked-off-the-euromaidan-revolution-2015-7.

fora. Campaigns have been observed targeting military personnel directly through LinkedIn,[182] as well as targeting military spouses through spearphishing.[183] The implication is that service personnel are not only vulnerable as a result of their own online behaviour, but their families, friends and colleagues (in fact, anyone the original target connected with via social media or a mobile device) should also be considered targets for collection of information.

The capability is therefore available to message targeted individuals on a mass scale, with information that appears to them to be coming from a trusted source, whether by SMS, social media posting, or email. The implication is that in time of crisis, if the defence forces of a frontline state decided to mobilise in response to a direct and immediate threat from Russia, it might find that its personnel - and government officials more broadly – receive seemingly trustworthy instructions to remain at home and offer no resistance. In the crucial and decisive first few hours that might decide a conflict with Russia, this could be a critical disabling factor.

Targeting Connected Devices

A key means by which Russia could deliver this trusted content to users would be through manipulation of information they receive on their cell phones, tablets and other connected/mobile devices.

Specific Russian systems are designed for intercepting, jamming or spoofing civilian mobile phone communications, including broadcasting content to smartphones.[184] Russian officers report that systems like this have proven highly effective in information operations in Syria, and cite the example of delivering tailored content to opposition fighters intended to demoralise them by detailing "how much their commanders earn and where their bank accounts are and where they go on holiday".[185] In Ukraine, Russian forces use SMS messages to text Ukrainian frontline troops to “demoralise their frontline forces - which even includes references to their wives and children back in Kyiv … [and] “threaten them."[186]

The reach and mobility of cell phone spoofing systems is greatly extended by mounting them on UAVs. As described in early 2017:

> *The Leer-3 complex is composed of three Orlan-10 UAVs and a command and control post on a KamAZ-5350 truck. The unmanned aerial vehicles' primary mission is to suppress cellular communication towers. To do this, special 'jammers' have been installed onboard the Orlan-10 UAVs, and also disposable jammers, which they drop onto the ground. Having jammed the base stations, the old Orlan-10 UAVs were able to send instant messages to subscribers under certain conditions...But the new drones can easily handle*

[182] Jeff Stein, "How Russia Is Using LinkedIn as a Tool of War Against Its U.S. Enemies", Newsweek, 3 August 2017. http://www.newsweek.com/russia-putin-bots-linkedin-facebook-trump-clinton-kremlin-critics-poison-war-645696.
[183] "Threat Group-4127 Targets Google Accounts", Secureworks, 26 June 2016. https://www.secureworks.com/research/threat-group-4127-targets-google-accounts.
[184] Aleksey Ramm and Vladimir Zykov, “The Russian Army Has Obtained a Cellular Weapon: The Modernized Leer-3 Complex Will Be Able to Send Instant Messages and Audio and Video Messages,” Izvestia, 25 January 2017, https://iz.ru/news/659503.
[185] Author's conversations, March 2017.
[186] Glen Howard, Jamestown Foundation, by e-mail, March 2017.

those targets. They 'jam' base stations and take their place, while becoming virtual cellular stations.[187]

In keeping with the already well-developed intelligence and disinformation targeting of NATO troops in the Baltic states and elsewhere, it should be assumed that NATO personnel within reach of Russian UAVs will be subjected to similar information activities, regardless of whether any form of overt hostilities are taking place.

Outlook and Recommendations

In addition to the tactics and capabilities described above (such as the information isolation of a target audience or specific area of the country, or highly personalised disinformation delivered simultaneously to a mass military audience), the following possible methods should be prepared for when conflict with Russia is imminent or already under way.

1. Social media manipulation to spark rather than to exploit an already existing conflict. Russia will have watched with interest instances of community violence breaking out in response to entirely false information circulated via social media, and will be considering how to exploit this capability against its adversaries.[188]

2. Limited kinetic activity at a tactical level for strategic information effect. This trend has already been observed in Syria. UK Army Maj-Gen. Felix Gedney, commenting after completion of his tour as deputy commander of Operation Inherent Resolve in October 2018, noted how "military operations [were] being conducted for the sole reason of getting the picture or the footage those people wanted."[189] Given the perceived success of this approach, further application in other theatres can be expected.

Countermeasures and Policy Recommendations

Based on this analysis, the following countermeasures and policy recommendations are offered:

1. Exercises should simulate coordinated cyber, information and kinetic effects in a range of combinations and roles, where both information effects facilitate kinetic outcomes and vice versa;

2. Civilian internet infrastructure must be accorded the same degree of

[187] Aleksey Ramm and Vladimir Zykov, "The Russian Army Has Obtained a Cellular Weapon: The Modernized Leer-3 Complex Will Be Able to Send Instant Messages and Audio and Video Messages," Izvestia, 25 January 2017. https://iz.ru/news/659503.

[188] As for instance in Marcos Martínez, "Burned to death because of a rumour on WhatsApp", BBC Monitoring, 12 November 2018, https://www.bbc.co.uk/news/world-latin-america-46145986. See also Yemisi Adegoke and BBC Africa Eye, "Like. Share. Kill.: Nigerian police say false information on Facebook is killing people", BBC.co.uk, 13 November 2018. https://www.bbc.co.uk/news/resources/idt-sh/nigeria_fake_news.

[189] Katie Bo Williams, "Russia is Winning the Information War in Iraq and Syria: UK General", Defense One, 8 October 2018. https://www.defenseone.com/threats/2018/10/information-warfare/151855/.
See also Paul McLeary, "Russia Winning Info & Electronic War In Syria, US & UK Generals Warn", Breaking Defense, 9 October 2018. https://breakingdefense.com/2018/10/russia-winning-information-electronic-war-over-syria-us-uk-generals-warn/.

protection, both before and during a crisis, as other strategically important assets;

3. Western governments, and their defence and security forces, must be fully prepared to operate in an environment where access to internet resources is degraded or absent - including for the purposes of communicating with their own civilian populations and military/defence personnel;

4. This applies in equal measure to using any other friendly capabilities which may be compromised by lack of access to the electromagnetic spectrum, including to GPS signals;

5. At the same time false messaging on a mass scale, including from apparently trusted sources, should be expected and countermeasures established;

6. Social media intelligence capabilities should be invested in, in order to provide indicators and warnings of future Russian activity in the information domain;

7. NATO forces should be training and exercising with the assumption that they will be under not only electronic and cyberattack, but also individual and personalised information attack, including exploitation of personal data harvested from any connected device brought into an operational area;

8. Detection and countering of Russian data and information interception and manipulation capabilities, whether cross-border or locally installed, should be prioritised. This should accompany rigid enforcement of policies intended to prevent personal connected devices being brought into hostile information security environments;[190] and,

9. It should also be remembered that an overt state of conflict with Russia need not necessarily exist in order for Russian information warfare capabilities to be deployed and utilized.

[190] In the case of Finland, this has led to generations of young conscripts buying their first wristwatch ahead of their period of army service, since they will no longer be able to use their phones to tell the time. See Yle Uutiset (Finland), "Tällainen on varusmiehen uusin vakiovaruste – inttirolex komeilee nyt lähes jokaisen varusmiehen ranteessa", Yle Uutiset, 15 January 2019. https://yle.fi/uutiset/3-10594869.

BIBLIOGRAPHY

Abrams, Steve, "Beyond Propaganda: Soviet Active Measures in Putin's Russia", Connections, Vol. 15, No. 1 (Winter 2016), pp. 12-13, https://www.jstor.org/stable/pdf/26326426.pdf

Adamsky, Dima, “Cross-Domain Coercion: The Current Russian Art of Strategy,” IFRI Proliferation Papers, No. 54, November 2015.

Adegoke, Yemisi and BBC Africa Eye, “Like. Share. Kill.: Nigerian police say false information on Facebook is killing people”, BBC.co.uk, 13 November 2018. https://www.bbc.co.uk/news/resources/idt-sh/nigeria_fake_news.

Akhvlediani, M. “The fatal flaw: the media and the Russian invasion of Georgia”, in Rich, P. B. (ed.) *Crisis in the Caucasus: Russia, Georgia and the West*, London: Routledge 2010.

Amanpour, Christina, “Mikhail Kasyanov and Anissa Naouai Interview”, CNN, 21 November 2014. http://amanpour.blogs.cnn.com/2014/11/21/full-transcript-mikhail-kasyanov-and-anissa-naouai/

Amnesty International, “Torture and Summary Killings in Eastern Ukraine”, Amnesty.org, 2015. https://www.amnesty.org/download/Documents/EUR5016832015ENGLISH.pdf.

Applebaum, Anne, "How Vladimir Putin is waging war on the West - and winning", Spectator, 21 February 2015. http://www.spectator.co.uk/features/9447782/how-vladimir-putin-is-waging-war-on-the-west-and-winning/.

Ash, Lucy, "How Russia outfoxes its enemies", BBC News, 29 January 2015. http://www.bbc.co.uk/news/magazine-31020283.

Bartholomew, Robert E., "Science for sale: the rise of predatory journals", Journal of the Royal Society of Medicine, Vol. 107, Issue 10, 2014. pp. 384-5.

BBC Monitoring: “Russia is Underestimating Information Resources and Losing Out to the West”, *Novyy Region*, 29 October 2008.

BBC Monitoring: “Russian pundit interviewed on US information operations conference”, *Rossiya TV,* 27 April 2009.

BBC Monitoring, “Russian TV highlights hacker attacks on Georgian sites”, *RenTV*, 11 November 2008.

Bennett, G., *FPS & FAPSI - RIP,* Conflict Studies Research Centre. Sandhurst: March 2003.

Bennett, G., *The Federal Agency of Government Communications & Information*, Conflict Studies Research Centre. Sandhurst: August 2000.

Bernard, Doug, "America's Adversaries Use Baltimore Unrest to Spread Anti-US Message", VOA News, 30 April 2015. http://www.voanews.com/articleprintview/2743166.html.

Bershidsky, Leonid, "Estonia Did Its Post-Soviet Homework", Bloomberg View, 3 March 2015. http://www.bloombergview.com/articles/2015-03-03/estonia-did-its-post-soviet-homework.

Bērziņš, Jānis, "Russian New Generation Warfare: Implications for Europe", European Leadership Network, 14 October 2014. http://www.europeanleadershipnetwork.org/russian-new-generation-warfare-implications-for-europe_2006.html.

Bingham, J., "Crossing the line", Jane's Intelligence Review. (IHS Markit, 2018), pp. 13-15. Shortened version : https://www.janes.com/images/assets/018/78018/Private_companies_engage_in_Russias_non-linear_warfare.pdf

Boyko, S. M., Dylevskiy I. N., Komov S. A., Korotkov S. V. "*Voyenno-politicheskiye aspekty obespecheniya informatsionnoy bezopasnosti na prostranstve Shankhayskoy organizatsii sotrudnichestva*", *Voyennaya mysl'*, No. 7, July 2010.

Bukkvol, T., "Russian Special Operations Forces in Donbass and Crimea", Aleksanteri Papers, 1 (2016). p. 17-20. https://ssi.armywarcollege.edu/pubs/parameters/issues/Summer_2016/5_Bukkvoll.pdf.

Campbell, Duncan, "Bad day at Hard Rock", The New Statesman, 17 September 1982. pp. 6-9.

Carr, Jeffrey, "Digital Dao: Russian Cyber Warfare Capabilities in 2014 (We Aren't in Georgia Anymore)", http://jeffreycarr.blogspot.co.uk/2014/03/ russian-cyber-warfare-capabilities-in.html.

Castle, Stephen, "A Russian TV Insider Describes a Modern Propaganda Machine", The New York Times, 13 February 2015. http://nyti.ms/1zcDqDq.

Chalupa, Irene, "Direct Translation: Meet the Ex-Convicts, Bullies, and Armed Bikers Who Helped Seize Crimea", Atlantic Council, 19 June 2014. http://www.atlanticcouncil.org/blogs/new-atlanticist/ direct-translation-the-kremlin-celebrates-secretlythe-ex-convicts-bullies-and-bikers-who-helped-itcapture-crimea.

Charap, Samuel, "Russia's Use of Military Force as a Foreign Policy Tool: Is There a Logic?", PONARS Policy Memo 443, October 2016. http://www.ponarseurasia.org/memo/russias-use-military-force-foreign-policy-tool-there-logic.

Clapper, James R., "Worldwide Threat Assessment of the US Intelligence

Community", United States Senate Armed Services Committee, 9 February 2016. http://www.armedservices.senate.gov/imo/media/doc/Clapper_02-09-16.pdf.

Clark, Mason and Harris, Catherine, “Russia's New Tool for Wielding Information”, Institute for the Study of War, 15 January 2019. http://iswresearch.blogspot.com/2019/01/russias-tools-for-wielding-information.html.

CNN, “Inside the KGB – An interview with retired KGB Maj. Gen. Oleg Kalugin,” Cold War Experience, CNN, January 1998. http://web.archive.org/web/20070627183623/http://www3.cnn.com/SPECIALS/cold.war/episodes/21/interviews/kalugin/.

Cohen, Nick, "Russia Today: why western cynics lap up Putin’s TV poison", The Observer, 8 November 2014. http://www.theguardian.com/commentisfree/2014/nov/08/russia-today-western-cynics-lap-up-putins-tv-poison.

Daily Mail, "Is this the moment MH17 was shot down as it flew over Ukraine? Russian state broadcaster produces 'satellite images' showing alleged fighter jet attack", Daily Mail, 14 November 2014. http://www.dailymail.co.uk/news/article-2835088/Is-moment-MH17-shot-flew-Ukraine-Russian-state-broadcaster-produces-satellite-images-showing-fighter-jet-attack.html.

Dauber, Cori E., "YouTube War: Fighting In A World Of Cameras In Every Cell Phone And Photoshop On Every Computer", U.S. Army War College Strategic Studies Institute, November 2009. p. ix.

Davis, Julia, "Dana Rohrabacher claims that the former President of Ukraine was assassinated", The Examiner, 6 April 2015. http://www.examiner.com/article/dana-rohrabacher-claims-that-the-former-president-of-ukraine-was-assassinated.

Day, Matthew and Oliphant, Roland, "'Thousands' of Polish soldiers receive mysterious call from Russian number", Daily Telegraph, 3 November 2015. http://www.telegraph.co.uk/news/worldnews/europe/poland/11972391/Thousands-of-Polish-soldiers-receive-mysterious-call-from-Russian-number.html.

Defence Academy of the United Kingdom, "Russia - Future Directions", Defence Academy of the UK, 1 October 2008.

Defense Intelligence Agency, ‘Russia Military Power: Building a Military to Support Great Power Aspirations’. Military Power Publications, 2017. p.74. http://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Russia%20Military%20Power%20Report%202017.pdf.

Dougherty, Jill, "Russian TV's American Face", Huffington Post, 11 April 2014.

Elder, Miriam, "Russia Has A New Propaganda Outlet And It's Everything You Thought It Would Be", BuzzFeed, 10 November 2014. http://www.buzzfeed.com/miriamelder/russia-has-a-new-propaganda-outlet-and-its-everything-you-th.

Elkov, Igor, "Короткая память", Rossiyskaya gazeta, 17 January 2013. http://www.rg.ru/2013/01/17/ashmanov.html.

Facon, Isabelle, “Russia’s national security strategy and military doctrine and their implications for the EU”, Policy Department, Directorate-General for External Policies, European Parliament, January 2017. p.15. http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/578016/EXPO_IDA(2017)578016_EN.pdf

Fainberg, S., “Russian Spetsnaz, Contractors, and Volunteers in the Syrian Conflict”, Russia.Nei.Visions No.105. IFRI, 2017. p. 19. https://www.ifri.org/sites/default/files/atoms/files/fainberg_russian_spetsnaz_syrian_conflict_2017.pdf.

Federal Security Service of the Russian Federation, “Official history of the FSO”, FSO.gov.ru, undated. http://www.fso.gov.ru/histori/histori7.html.

Finnin, Rory and Grant, Thomas D, "Don't call it a civil war - Ukraine's conflict is an act of Russian aggression", The Conversation, 24 August 2015. http://theconversation.com/dont-call-it-a-civil-war-ukraines-conflict-is-an-act-of-russian-aggression-46280.

Fiore, Nicolas, Defeating the Russian Battalion Tactical Group. Fort Benning, 2017. p. 2. http://www.benning.army.mil/armor/eARMOR/content/issues/2017/Spring/2Fiore17.pdf

Fitzgerald, M. C., “Russian Views on Electronic and Information Warfare”, Hudson Institute, December 1996.

Franke, Ulrik, "War by Non-Military Means: Understanding Russian Information Warfare", FOI report No. FOI-R-4065-SE, March 2015. http://www.foi.se/ReportFiles/foir_4065.pdf.

Freedberg, Sydney J., "Army Fights Culture Gap Between Cyber & Ops: ‘Dolphin Speak’", Breaking Defense, 10 November 2015. http://breakingdefense.com/2015/11/army-fights-culture-gap-between-cyber-ops-dolphin-speak/.

Galeotti, Mark, "Heavy Metal Diplomacy: Russia’s Political Use of its Military in Europe since 2014", ECFR, 19 December 2016. http://www.ecfr.eu/publications/summary/heavy_metal_diplomacy_russias_political_use_of_its_military_in_europe_since.

Galeotti, Mark, “Operational situation”, Jane’s Intelligence Review, IHS Markit, 2018.

Galeotti, Mark, “Putin’s Hydra: Inside Russia’s Intelligence Services”, Policy Brief, May 2016, European Council on Foreign Relations, May 2016.

Galeotti, Mark, “Russian intelligence is at (political) war”, NATO Review Magazine, (May 2017). https://www.nato.int/docu/review/2017/also-in-2017/russian-intelligence-political-war-security/en/index.htm.

Galeotti, Mark, (2015) “Spetsnaz: Russia’s Special Forces”. Oxford: Oxford Publishing pp. 54-55.

Garmazhapova, Aleksandra, "Где живут тролли. Как работают интернет-провокаторы в Санкт-Петербурге и кто ими заправляет", Novaya gazeta, 9 September 2013.

Geers, K., “Strategic Analysis: As Russia-Ukraine Conflict Continues, Malware Activity Rises”, FireEye, 28 May 2014. https://www.fireeye.com/blog/threat-research/2014/05/strategic-analysis-as-russia-ukraine-conflict-continues-malware-activity-rises.html.

GeoStrategy Direct, “Cyber Threat to Pentagon is Global: China, Russia Near Peers of US”, GeoStrategy, 1 October 2010. http://www.geostrategy-direct.com/geostrategy-direct/secure/2010/10_06/ba.asp.

Giles, Keir, "Assessing Russia’s Reorganized and Rearmed Military", Carnegie, May 2017. https://carnegieendowment.org/2017/05/03/assessing-russia-s-reorganized-and-rearmed-military-pub-69853.

Giles, Keir, “Handbook of Russian Information Warfare”, NATO Defense College, November 2016.

Giles, Keir, "Information Troops - A Russian Cyber Command?", Proceedings of the 3rd International Conference on Cyber Conflict, Tallinn, June 2011.

Giles, Keir, "Tales from Two Cities: Moscow and Washington on Flight MH17", Chatham House, 24 July 2014.
http://www.chathamhouse.org/expert/comment/15236.

Giles, Keir, "With Russia and Ukraine, is all really quiet on the cyber front?", Ars Technica, 11 March 2014. http://arstechnica.com/tech-policy/2014/03/with-russia-and-ukraine-is-all-really-quiet-on-the-cyber-front/.

Giles, Keir, Sherr, James and Seaboyer, Anthony, "Russian Reflexive Control", DRDC, October 2018.
http://pubs.drdc-rddc.gc.ca/BASIS/pcandid/www/engpub/DDW?W%3DSYSNUM=807769&r=0.

Global Voices, "‘Anonymous International’ Leaks Kremlin's Instructions to Russian TV", GlobalVoices, 28 March 2014.
http://globalvoicesonline.org/2014/03/28/anonymous-international-leaks-kremlins-instructions-to-russian-tv/.

Goble, P. “Russia: Analysis From Washington -- A Real Battle On The Virtual Front”, RF/RL 11 October 1999. http://www.rferl.org/content/article/1092360.html.

Goble, P. “Defining Victory and Defeat: The Information War Between Russia and Georgia”, in Cornell, S. & Starr, F. (eds) *The Guns of August 2008: Russia’s War in Georgia*, New York 2009.

Gorman, S. “U.S. Backs Talks on Cyber Warfare”, Wall Street Journal, 4 June 2010. http://online.wsj.com/article/SB10001424052748703340904575284964215965730.html.

GUss, Mike, "Space Surveillance Sats Pressed into Early Service", SpaceNews, 18 September 2015. http://spacenews.com/space-surveillance-sats-pressed-into-early-service/.

Halminen, Laura, "Venäjä nuuskii nyt lännen tietoliikennettä - Krimillä liikennekaapelit vain tärveltiin", Helsingin Sanomat, 7 November 2015. http://www.hs.fi/ulkomaat/a1446879570779.

Harding, Joel, "Army Puts ‘Cyber Soldiers’ In The Mud", To Inform is to Influence, 13 November 2015,. http://toinformistoinfluence.com/2015/11/14/army-puts-cyber-soldiers-in-the-mud/.

Heickerö, Roland, "Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations", FOI, March 2010. pp. 15-16.

Herd, Graeme P., "Information Warfare & the Second Chechen Campaign", Conflict Studies Research Centre, 2000.

Higgins, Andrew, "Waving Cash, Putin Sows E.U. Divisions in an Effort to Break Sanctions", The New York Times, 6 April 2015. http://nyti.ms/1ac5osT.

Hollis, David, "Cyberwar Case Study: Georgia 2008", Small Wars Journal, 6 January 2011. http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf.

Howard Glen, Jamestown Foundation, e-mail, March 2017.

Huffington Post, "George Galloway Doubles Pay Packet With Appearances On Russia Today And Al-Mayadeen", Huffington Post, 11 July 2014. http://www.huffingtonpost.co.uk/2014/07/11/george-galloway-russia-today_n_5577661.html.

Hurt, Martin, "The potential for hybrid warfare in Central and Western Europe", European Leadership Network, 9 October 2014. http://www.europeanleadershipnetwork.org/the-potential-for-hybrid-warfare-in-central-and-western-europe_1989.html.

Iltalehti (Finland), "Suomen vesiväylät "motissa" - venäläisfirma osti maat", Iltalehti, 19 January 2015. http://www.iltalehti.fi/uutiset/2015011919044524_uu.shtml.

Illtalehti (Finland), "Maakauppoja strategisissa kohteissa", Iltalehti, 12 March 2015.

http://www.iltalehti.fi/uutiset/2015031119338528_uu.shtml.

Institut Kriptografii, *Kompant-dien, posvyashchennyy pyatidesyatiletyu IKSI*, Moscow: Institut Kriptografii, Svyazi i Informatiki, 1999; pp. 195-201.

Interfax News Agency (Russia), “Information Troops Set Up in Russian Federation MoD” [in Russian], Interfax, 22 February 2017. http://www.interfax.ru/russia/551054.

Institute of International Security Issues of the Russian Academy of Sciences and the Faculty of World Politics of Moscow State University.

Jaitner, Margarita, "Exercising Power in Social Media", in Jari Rantapelkonen & Mirva Salminen (eds.), The Fog of Cyberwar, Finnish National Defense University, 2013.
http://www.doria.fi/bitstream/handle/10024/88689/The%20Fog%20of%20Cyber%20Defence%20NDU%202013.pdf?sequence=1.

Judson, Jen, "Army Learning How Cyber Support Plays Role In Tactical Operations", Defense News, 10 November 2015.
http://www.defensenews.com/story/defense/land/army/2015/11/10/army-learning-how-cyber-support-plays-role-in-tactical-operations/75545442/.

Jurvee, Ivo, “The resurrection of ‘active measures’: Intelligence services as a part of Russia’s influencing toolbox”, Hybrid CoE, April 2018. p. 3.
https://www.hybridcoe.fi/wp-content/uploads/2018/05/Strategic-Analysis-2018-4-Juurvee.pdf.

Kainikara, Sanu, “In The Bear’s Shadow: Russian Intervention in Syria”, Air Power Development Centre, Canberra, 2018.

Khazan, Olga, "The Creepy, Long-Standing Practice of Undersea Cable Tapping", The Atlantic, 16 July 2013.
http://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/.

Kirchik, James, "Putin Bootlickers Assemble in D.C.", The Daily Beast, 31 March 2015. http://www.thedailybeast.com/articles/2015/03/31/report-from-the-belly-of-the-putin-apologetics-beast.html.

Klikushin, Mikhail, “Putin’s Army Demands ‘NATO Soldiers! Hands Up! Lay Down Your Weapons!’”, The Observer, 19 August 2016.
http://observer.com/2016/08/putins-army-demands-nato-soldiers-hands-up-lay-down-your-weapons/.

Koayesov, Col. P., “Theatre of Warfare on Distorting Airwaves. Georgia Versus South Ossetia and Abkhazia in the Field of Media Abuse. Fighting by Their Own Rules,” *Voyennyy Vestnik Yuga Rossii*, 18 January 2009.

Kofman, Michael, "A Comparative Guide To Russia’s Use Of Force: Measure Twice, Invade Once", War On The Rocks, 16 February 2017.

https://warontherocks.com/2017/02/a-comparative-guide-to-russias-use-of-force-measure-twice-invade-once.

Kogan, R., ‘Bedep trojan malware spread by the Angler exploit kit gets political’, Trustwave, 29 April 2015. https://www.trustwave.com/Resources/SpiderLabs-Blog/Bedep-trojan-malware-spread-by-the-Angler-exploit-kit-gets-political/.

Lauder, Matthew A., ‘Wolves of the Russian Spring’: An Examination of the Night Wolves as a Proxy for the Russian Government, Canadian Military Journal, Vol. 18, No. 3, Summer 2018. pp. 5-13. http://www.journal.forces.gc.ca/vol18/no3/PDF/CMJ183Ep5.pdf.

Litovkin, D. “General Staff Prepares for Cyber War”, *Izvestia*, 27 February 2009.

Logan, Nick, "‘Get out of Ukraine': Harper to Putin at G20 Summit in Brisbane", Global News, November 15, 2014. http://globalnews.ca/news/1673290/get-out-of-ukraine-harper-to-putin-at-g20-summit-in-brisbane/.

Lonkila, Markku, "Russian Protest On- And Offline: The Role Of Social Media In The Moscow Opposition Demonstrations In December 2011", FIIA Briefing Paper 98, February 2012.

Lucas, Edward and Pomerantsev, Peter, “Winning the Information War”, CEPA, p. 16

Lutsevych, O., *Agents of the Russian World: Proxy Groups in the Contested Neighbourhood*. (Chatham House, 2016. https://www.chathamhouse.org/publication/agents-russian-world-proxy-groups-contested-neighbourhood.

Madeira, Victor, "Haven't We Been Here Before?", Institute of Statecraft, 30 July 2014. http://www.statecraft.org.uk/research/russian-subversion-havent-we-been-here.

Madory, Doug, "No turning back: Russia activates Crimean cable", Dyn Research, 31 July 2015. http://research.dyn.com/2014/07/no-turning-back-russia-crimea/.

Maiorova, Alina, (ed.), “Russian Presence”, in *Donbass in Flames*, Security Environment Research Center, 2017. p. 67-82. https://prometheus.ngo/wp-content/uploads/2017/04/Donbas_v_Ogni_ENG_web_1-4.pdf.

Martínez, Marcos, “Burned to death because of a rumour on WhatsApp”, BBC Monitoring, 12 November 2018. https://www.bbc.co.uk/news/world-latin-america-46145986.

McCuen, John J., “Hybrid Wars,” Military Review, March-April 2008. pp. 107-113.

McLeary, Paul, "Russia Winning Info & Electronic War In Syria, US & UK Generals Warn", Breaking Defense, 9 October 2018. https://breakingdefense.com/2018/10/russia-winning-information-electronic-war-over-

syria-us-uk-generals-warn/.

Mearsheimer, John J., "Why the Ukraine Crisis Is the West's Fault: The Liberal Delusions That Provoked Putin", Foreign Affairs, September-October 2014. http://www.foreignaffairs.com/ articles/141769/john-j-mearsheimer/why-the-ukraine-crisis-is-the-wests-fault.

Velichka, Milina, "Security in a Communications Society: Opportunities and Challenges", Connections, Volume XI, Number 2, p Spring 2012. p. 55.

Military Academy of the General Staff academics Sergey Chekinov and Sergey Bogdanov in the period 2010-2014.

Miller, J. "Putin's Attack Helicopters and Mercenaries Are Winning the War for Assad", Foreign Policy, 30 March 2016. http://foreignpolicy.com/2016/03/30/putins-attack-helicopters-and-mercenaries-are-winning-the-war-for-assad/.

Murphy, Heather, "Ominous Text Message Sent to Protesters in Kiev Sends Chills Around the Internet", The New York Times, 22 January 2014. http://thelede.blogs.nytimes.com/2014/01/22/ominous-text-message-sent-to-protesters-in-kiev-sends-chills-around-the-internet/.

MVD website at http://www.mvd.ru/struct/10000220/10000288/.

MVD website: http://www.mvd.ru/struct/10000220/10000221/10000740/.

NATO Defense College reviews, "Understanding the Georgian War, Two Years On", 2010. http://www.ndc.nato.int/research/series.php?icode=9.

NATO StratCom Centre of Excellence, "Analysis of Russia's Information Campaign Against Ukraine", NATO StratCom Centre of Excellence (COE), undated document.

Nocetti, Julien, "'Digital Kremlin': Power and the Internet in Russia", IFRI Russie.Nei.Visions No. 59, April 2011. pp. 16-17.

NOS (Netherlands), "Vijf vragen over het MH17-onderzoek", NOS, 3 March 2015. http://nos.nl/artikel/2022540.

Odivizion (Russia) YouTube Channel [Отдельный Дивизион], Игорь Ашманов в гостях у «Профилактики»"Profilaktika", Mayak radio, 25 December 2012. https://www.youtube.com/watch?v=9yhOKf0J280.

One Russia Party Website, "Kokoshin: Kibervoyny ugrozhayut natsional'noy bezopasnosti Rossii", One Russia party website, 26 January 2011. http://er.ru/er/text.shtml?18/2254.

Panarin, I., *Informatsionnaya voyna i diplomatiya,* Moscow: Gorodets 2004.

Panarin, I., "The Information Warfare System: the Mechanism for Foreign Propaganda Requires Renewal", *Voyenno-Promyshlennyy Kuryer* ,15 October 2008.

Persson, Gudrun (ed.), "Russian Military Capability in a Ten-Year Perspective - 2016", FOI, December 2016.

Pesonen, Ari, "Tietoliikenneyhteyksien katkaiseminen olisi Venäjälle tehokasta sodankäyntiä", Uusi Suomi, 27 October 2015. http://aripesonen1.puheenvuoro.uusisuomi.fi/205516-tietoliikenneyhteyksien-katkaiseminen-olisi-venajalle-tehokasta-sodankayntia.

Pomerantsev, Peter, *Nothing Is True And Everything Is Possible*, PublicAffairs Books, New York, 2014.

Pomerantsev, Peter and Weiss, Michael, "The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money", The Interpreter, 22 November 2014. http://www.interpretermag.com/wp-content/uploads/2014/11/The_Menace_of_Unreality_Final.pdf.

Postime Estonia, "Информационные войны с самими собой", Postimees-DZD, 7 November 2011. http://rus.postimees.ee/624820/informacionnye-vojny-s-samimi-soboj.

PsyWar.org, "Soviet Propaganda In Western Europe", FCO Research and Analysis Department Background Brief, March 1982. http://www.psywar.org/radSovietPropaganda.php.

Pynnöniemi, Katri, “Metanarratives of Russian Strategic Deception”, in Katri Pynnöniemi and András Rácz (eds.), *Fog of Falsehood: Russian Strategy of Deception and the Conflict in Ukraine*, FIIA Report 45, p. 79.

Radio Free Europe/Radio Liberty, "Clone Twitter Accounts Target RFE/RL", RFE/RL, 17 February 2015. http://www.rferl.org/content/clone-twitter-accounts-target-rferl/26853959.html.

Ramm, Aleksey and Zykov, Vladimir, “The Russian Army Has Obtained a Cellular Weapon: The Modernized Leer-3 Complex Will Be Able to Send Instant Messages and Audio and Video Messages,” Izvestia, 25 January 2017. https://iz.ru/news/659503.

RAND Corporation, “Lessons from Russia's Operations in Crimea and Eastern Ukraine”, RAND Corporation, 2017. https://www.rand.org/pubs/research_reports/RR1498.html .

Rettman, Andrew, "Reports multiply of Kremlin links to anti-EU parties", EUObserver, 26 November 2014. https://euobserver.com/foreign/126676.

RIA Novosti (Russia), "В Белоруссии начались учения 'Нерушимое братство-2016'" (Unbreakable Brotherhood 2016 exercise begins in Belarus), RIA, 23 August 2016. https://ria.ru/world/20160823/1475032583.html.

Ripley, Tim, “Operation Aleppo: Russia’s War in Syria”, Telic-Herrick Publications,

Lancaster, 2018.

Rohac, Dalibor, "Cranks, Trolls, and Useful Idiots: Russia's information warriors set their sights on Central Europe", Foreign Policy, 12 March 2015. https://foreignpolicy.com/2015/03/12/cranks-trolls-and-useful-idiots-poland-czech-republic-slovakia-russia-ukraine/.

Rothrock, Kevin, "Russia's Most Popular Social Network Just Sent 20,000 Users a Private Message From the Government", Global Voices, 8 November 2015. https://globalvoices.org/2015/11/08/russias-most-popular-social-network-just-sent-20000-users-a-private-message-from-the-russian-government/print/.

RT, "Radioactive leak at major Ukrainian nuclear plant - report", RT, 30 December 2014. http://rt.com/news/218807-ukraine-nuclear-plant-leak/.

Russian Defense Policy Blog, “Return of Independent Spetsnaz Companies", Russian Defense Policy blog, 22 December 2018. https://russiandefpolicy.blog/2018/12/22/return-of-independent-spetsnaz-companies/.

Russian Federation Centre for Parliamentary Communication, *Tsentr parlamentskikh kommunikatsiy*, 30 January 2009. http://www.parlcom.ru/index.php?p=MC83&id=27297.

Russian Federation Ministry of Defence, “Military Doctrine of the Russian Federation", approved 26 December 2014. http://news.kremlin.ru/media/events/files/41d527556bec8deb3530.pdf.

Russian Federation Ministry of Foreign Affairs, "Special Briefing by the Ministry of Defense of the Russian Federation on the crash of the Malaysian Boeing 777 in the Ukrainian air space, July 21, 2014", MID.ru, 2014. http://www.mid.ru/brp_4.nsf/0/ECD62987D4816CA344257D1D00251C76.

Russian Federation State Duma proceedings, 17 December 1996.

Sanger, David E. and Schmitt, Eric, "Russian Ships Near Data Cables Are Too Close for U.S. Comfort", The New York Times, 25 October 2015. http://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html.

SC Magazine, “Russia overtaking US in cyber-warfare capabilities,” SC Magazine, 30 October 2015. http://www.scmagazine.com/russia-overtaking-us-in-cyber-warfare-capabilities/article/450518/.

Schweiz Magazin, “17-minutench-diffamiert-Kritiker-als-Putin-gesteuert”, SchweizMagazin.ch, undated. http://www.schweizmagazin.ch/nachrichten/schweiz/19717-minutench-diffamiert-Kritiker-als-Putin-gesteuert.html.

Secureworks, "Threat Group-4127 Targets Google Accounts", Secureworks, 26 June 2016. https://www.secureworks.com/research/threat-group-4127-targets-google-

accounts.

Security Service of Ukraine, Power Point Presentation, entitled ‘В умовах військової агресії з боку Російської Федерації, війна ведеться не лише на землі, в повітрі та в дипломатичних колах, вперше в історії війн застосовані нові форми ведення агресії - гібридна війна з використанням кіберпростору України, undated.

Security Council of the Russian Federation website, http://www.scrf.gov.ru/persons/11.html

Seddon, Max, "Documents Show How Russia’s Troll Army Hit America", BuzzFeed, 2 June 2014.

Servettaz, Elena, "Putin’s Far-Right Friends in Europe", Institute of Modern Russia, 16 January 2014. http://imrussia.org/en/russia-and-the- world/645-putins-far-right-friends-in-europe.

Sherr, James, ‘Geopolitics and Security’ in *The Struggle for Ukraine*, Chatham House, August 2017. pp 11-13.

Sinikukka, Saari, "Russia’s public diplomacy: soft tools with a hard edge", Border Crossing (Diplomat Magazine), April 2015.

Sobaka, "Городской типаж: блогер-пропагандист", Sobaka.ru, 28 january 2015. http://www.sobaka.ru/city/city/32942/.

Soldatov, Andrey, “*Fapsi - obshestvennosti: ‘menshe znaesh - krepche spish*’” (FAPSI to the
public: the less you know, the sounder you sleep), Segodnya, 12 December 1999.

Soldatov, Andrey and Borogan, Irina, The Red Web: Here’s How Facebook Kicked Off the Euromaidan Revolution, July 2015. http://uk.businessinsider.com/heres-how-facebook-kicked-off-the-euromaidan-revolution-2015-7.

Starosielski, Nicole, "In our Wi-Fi world, the internet still depends on undersea cables", The Conversation, 3 November 2015. https://theconversation.com/in-our-wi-fi-world-the-internet-still-depends-on-undersea-cables-49936.

Stavridis, Jim, "A New Cold War Deep Under the Sea?", Huffington Post, 28 October 2015. http://www.huffingtonpost.com/admiral-jim-stavridis-ret/new-cold-war-under-the-sea_b_8402020.html.

Stein, Jeff, "How Russia Is Using LinkedIn as a Tool of War Against Its U.S. Enemies", Newsweek, 3 August 2017. http://www.newsweek.com/russia-putin-bots-linkedin-facebook-trump-clinton-kremlin-critics-poison-war-645696.

Talbot, D., “Russia's Cyber Security Plans”, Technology Review, 16 April 2010. http://www.technologyreview.com/blog/editors/25050/.

Tétrault- Farber, Gabrielle, "Far- Right Europe Has a Crush on Moscow", The Moscow Times, 25 November 2014. http://www.themoscowtimes.com/news/article/far-right-europe-has-a-crush-on-moscow/511827.html.

The High Court of Justice, Queen's Bench Division (UK), "Judgment In The High Court Of Justice, Queen's Bench Division, In The Matter Of The Representation Of The People Act 1983 And In The Matter Of A Mayoral Election For The London Borough Of Tower Hamlets Held On 22 May 2014", Via BBC.co.uk, 2014. http://news.bbc.co.uk/1/shared/bsp/hi/pdfs/judgment.pdf.

The Insider (Russia), "«Черный интернационал». Как Москва кормит правые партии по всему миру", The Insider, 27 November 2014. http://theins.ru/politika/2113.

The XX Committee, "Putin's Secret Friends in Paris", The XX Committee, 9 September 2014. http://20committee.com/2014/09/09/putins-secret-friends-in-paris/.

Thomas, Timothy L., "Information Warfare in the Second (1999-Present) Chechen War: Motivator for Military Reform?", in *Russian Military Reform 1992-2002*, Frank Cass, 2003. pp. 209-233.

Thomas, Timothy L., "Manipulating the Mass Consciousness: Russian & Chechen 'Information War' Tactics in the Second Chechen-Russian Conflict", in Anne Aldis (ed.), *The Second Chechen War*, Conflict Studies Research Centre, June 2000.

Thomas, Timothy L., "Recasting the Red Star", FMSO, 2011. pp. 118-131.

Thomas, Timothy L., "Russian Information Warfare Theory: The Consequences of August 2008", in Blank, S. and Weitz, R. *The Russian Military Today and Tomorrow: Essays in Memory of Mary Fitzgerald*, Carlisle: US Army War College Strategic Studies Institute, 2010.

Tiede, Peter, "Für mehr Einfluss auf Europa: Putin greift nach der AfD", Bild, 24 November 2014. http://www.bild.de/politik/inland/wladimir-putin/russlands-praesident-greift-nach-der-afd-kreml-netzwerk-38690092.bild.html.

Tikhonova, Polina, "Russia Hacking Your News", ValueWalk, 14 March 2015. http://www.valuewalk.com/2015/03/russia-hacking-your-news/.

Troianovski, Anton and Nakashima, Ellen, "How Russia's military intelligence agency became the covert muscle in Putin's duels with the West", The Washington Post, 28 December 2018. https://www.washingtonpost.com/world/europe/how-russias-military-intelligence-agency-became-the-covert-muscle-in-putins-duels-with-the-west/2018/12/27/2736bbe2-fb2d-11e8-8c9a-860ce2a8148f_story.html.

Tsyganok, A., "*Informatsionnaya voyna protiv Rossii: kak eto bylo"*. Segodnya, 17 April 2009. http://www.segodnia.ru/index.php?pgid=2&partid=13&newsid=8407.

TVN24 (Poland), "Kable, bez których stanie świat", TVN24, 9 November 2015.

http://www.tvn24.pl/weekend/tvn24-na-weekend,12/kable-bez-ktorych-stanie-swiat,237.

Ukraine Telecom, “PJSC Ukrtelecom’s Crimean regional branches officially announce the blocking of several communication nodes on the peninsula by unidentified personnel”, Ukrtelecom, 28 February 2014, http://www.ukrtelecom.ua/presscenter/news/official?id=120327

Ukraine Telecom, "Unidentified uniformed personnel again block several communication nodes in Crimea", Ukrtelecom, 1 March 2014. http://www.ukrtelecom.ua/presscenter/news/official?id=120389.

Ukraine Telekom, ‘Кримські регіональні підрозділи ПАТ «Укртелеком» офіційно повідомляють про блокування невідомими декількох вузлів зв'язку на півострові’, Ukrtelekom, 28 February 2014. http://www.ukrtelecom.ua/presscenter/news/official?id=120327.

Ukrainian News, "Defense Ministry: Russia Sending SMS Messages Asking Residents Of Ukrainian Border Regions To Appear At Nearest Military Units", Ukrainian News, 27 November 2018. https://ukranews.com/en/news/598565-defense-ministry-russia-sending-sms-messages-asking-residents-of-ukrainian-border-regions-to-appear.

US House of Representatives Permanent Select Committee on Intelligence, “Report on Russian Active Measures”, US Congress House of Representatives Permanent Select Committee on Intelligence, 22 March 2018. https://www.hsdl.org/?abstract&did=809811.

Vershbow, Alexander, "Remarks by NATO Deputy Secretary General Ambassador Alexander Vershbow at the Public Diplomacy Forum 2015", NATO website, 17 February 2015. http://www.nato.int/cps/en/natohq/opinions_117556.htm.

Vertuli, Mark D. and Loudon, Bradley S., (eds.), ‘The Fog of Russian Information Warfare’ , in *Perception are reality: Historical Case Studies of Information Operations in Large-Scale Combat Operations*, US Army Press, 2018. https://www.armyupress.army.mil/Portals/7/combat-studies-institute/csi-books/perceptions-are-reality-lsco-volume-7.pdf.

War is A Crime.org, "The Russian Military Asked Me to Publish Its Propaganda", War Is A Crime.org, 23 March 2015. http://warisacrime.org/print/69356.

Weeden, Brian, "Dancing in the dark redux: Recent Russian rendezvous and proximity operations in space", The Space Review, 5 October 2015. http://www.thespacereview.com/article/2839/1.

Williams, Katie Bo, "Russia is Winning the Information War in Iraq and Syria: UK General", Defense One, 8 October 2018. https://www.defenseone.com/threats/2018/10/information-warfare/151855/.

Wilton Park Conference Report, "Rethinking deterrence and assurance", Wilton Park

conference report WP1401, 10-13 June 2015.

Yle Uutiset (Finland), "Tällainen on varusmiehen uusin vakiovaruste – inttirolex komeilee nyt lähes jokaisen varusmiehen ranteessa", Yle Uutiset, 15 January 2019. https://yle.fi/uutiset/3-10594869.

Zaitseva, Mariia, "Information and security components of the Russian foreign policy", Informacijos mokslai (Information Sciences), Issue 70/2014. pp. 58-68.

DOCUMENT CONTROL DATA

*Security markings for the title, authors, abstract and keywords must be entered when the document is sensitive

1. ORIGINATOR (Name and address of the organization preparing the document. A DRDC Centre sponsoring a contractor's report, or tasking agency, is entered in Section 8.)

Royal Military College of Canada
Department of Political Science
National Defence
P.O. Box 17000, Station Forces
Kingston, Ontario, Canada K7K 7B4

2a. SECURITY MARKING (Overall security marking of the document including special supplemental markings if applicable.)

CAN UNCLASSIFIED

2b. CONTROLLED GOODS

NON-CONTROLLED GOODS
DMC A

3. TITLE (The document title and sub-title as indicated on the title page.)

Russian Special Forces and Intelligence Information Effects

4. AUTHORS (Last name, followed by initials – ranks, titles, etc., not to be used)

Giles, K.; Seaboyer, A.

5. DATE OF PUBLICATION (Month and year of publication of document.)	6a. NO. OF PAGES (Total pages, including Annexes, excluding DCD, covering and verso pages.)	6b. NO. OF REFS (Total references cited.)
March 2019	56	181

7. DOCUMENT CATEGORY (e.g., Scientific Report, Contract Report, Scientific Letter.)

Contract Report

8. SPONSORING CENTRE (The name and address of the department project office or laboratory sponsoring the research and development.)

DRDC – Toronto Research Centre
Defence Research and Development Canada
1133 Sheppard Avenue West
Toronto, Ontario M3K 2C9
Canada

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)
05cc – Influence Activities in support of Joint Targeting	MOU: DND RMCC - Service Level Arrangement with Royal Military College of Canada (RMCC) concerning contribution to DRDC's Program

10a. DRDC PUBLICATION NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)
DRDC-RDDC-2019-C230	

11a. FUTURE DISTRIBUTION WITHIN CANADA (Approval for further dissemination of the document. Security classification must also be considered.)

Public release

11b. FUTURE DISTRIBUTION OUTSIDE CANADA (Approval for further dissemination of the document. Security classification must also be considered.)

12. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Use semi-colon as a delimiter.)

Russia; Russian political warfare; Russian Military Developments; information warfare; adversarial intent; active measures

13. ABSTRACT/RÉSUMÉ (When available in the document, the French version of the abstract must be included here.)

This research report discusses information effects generated by Russian special forces as well as Russian intelligence agencies. After offering a brief introduction into the history of information effects generated by Russian special forces and intelligence agencies the paper discusses the theory and doctrine behind Russian information warfare as well as the evolution of information effects generated after the Cold War. Actors and agencies are introduced before exploring the case studies of information effects generated in Crimea, Eastern Ukraine and Syria are presented. The paper concludes with an examination of Russian tactics, techniques and procedures as well as possible countermeasures.

Ce rapport de recherche traite des effets de l'information générés par les forces spéciales russes ainsi que par les agences de renseignement russes. Après une brève introduction à l'histoire des effets de l'information générés par les forces spéciales et les services de renseignement russes, le document examine la théorie et la doctrine de la guerre de l'information russe ainsi que l'évolution des effets de l'information générés après la guerre froide. Les acteurs et les agences sont présentés avant d'explorer les études de cas d'effets sur l'information générés en Crimée, dans l'est de l'Ukraine et en Syrie. Le document se termine par un examen de la tactique, des techniques et des procédures russes, ainsi que des contre-mesures possibles.