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

CAN UNCLASSIFIED

DRDC | RDDC
technologysciencetechnologie

The Russian Information Warfare Construct

Keir Giles
Chatham House

Anthony Seaboyer
Royal Military College of Canada

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

Contractor Document Numbers: SLA: RMCC-DRDC Serial # 2014-007-SLA; Annex No: PA16011

Contract Number: DND RMCC - Service Level Arrangement with Royal Military College of Canada (RMCC) concerning contribution to DRDC's Program
Technical Authority: Matthew Lauder, Defence Scientist
Contractor's date of publication: March 2019

Defence Research and Development Canada

Contract Report
DRDC-RDDC-2019-C241
October 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

The Russian Information Warfare Construct

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 # 2014-007-SLA
Annex No: PA16011

Contract Scientific Authority: Matthew Lauder

Defence R&D Canada, Toronto Research Centre
Contract Report
DRDC-RDDC-2019-C241
March 2019

RMC Project Manager and corresponding author: Anthony Seaboyer

Abstract

This report discusses the Russian information warfare construct by tracing the concept of Russian information warfare back to the enduring principles of the Russian approach to competition between states. This report argues that the current Russian information warfare construct is in no way a new phenomenon. Instead, the construct is only extensively updated and renewed as part of Russia's recent preparations for conflict in conditions of overall conventional inferiority. After introducing essential concepts and important terminology, the report focuses on discussing particularly aims and objectives of current Russian information warfare.

Abstrait

Ce rapport traite de la construction de la guerre de l'information russe en retraçant le concept de guerre de l'information russe jusqu'aux principes durables de l'approche russe de la concurrence entre États. Ce rapport affirme que la construction actuelle de la guerre de l'information en Russie n'est en aucun cas un phénomène nouveau. Au lieu de cela, le concept n'est actualisé et renouvelé que dans le cadre des récents préparatifs de la Russie en vue d'un conflit dans des conditions d'infériorité conventionnelle globale. Après avoir introduit des concepts essentiels et une terminologie importante, le rapport se concentre sur les buts et objectifs de la guerre de l'information en Russie.

Summary

This report discusses the Russian information warfare construct by tracing the concept of Russian information warfare back to the enduring principles of the Russian approach to competition between states. This report argues that the current Russian information warfare construct is in no way a new phenomenon. Instead, the construct is only extensively updated and renewed as part of Russia's recent preparations for conflict in conditions of overall conventional inferiority. After introducing essential concepts and important terminology, the report focuses on discussing the aims and objectives of current Russian information warfare. The report concludes that, while the current Russian information warfare construct is not new, it is not static but is continuously evolves, develops, and adapts. Russia should not be expected to fight the last war when employing an information warfare component in a new conflict. This report argues that nations that believe they understand Russian information warfare on the basis of current studies and are responding by preparing for currently visible threats and capabilities are likely out of date and may be surprised by Russian operations in the information space. An evolving awareness of the challenge, capabilities and tactics is the most potent defence against Russian information warfare.

Introduction

> *"A new type of war has emerged, in which armed warfare has given up its decisive place in the achievement of the military and political objectives of war to another kind of warfare - information warfare."*[1]

Along with other instruments of power, the concept of Russian information warfare has become the subject of sudden and intense interest in the West since the start of the crisis over Ukraine in 2014. However, also in common with other instruments of power, which had been largely disregarded since the end of the Soviet Union, Russian information warfare is by no means a new phenomenon. Instead, it reflects enduring principles of the Russian approach to competition between states, extensively updated and renewed as part of Russia's recent preparations for conflict in conditions of overall conventional inferiority. As described by President Vladimir Putin, "We must take into account the plans and directions of development of the armed forces of other countries… Our responses must be based on intellectual superiority, they will be asymmetric, and less expensive."[2]

In the Russian construct, information warfare is not an activity limited to wartime (i.e., declared wars). It is not even limited to the "initial phase of conflict" before hostilities begin, which includes information preparation of the battle space.[3] Instead, it is an ongoing activity regardless of the state of relations with the opponent[4] and, "in contrast to other forms and methods of opposition, information confrontation is waged constantly in peacetime."[5] The entry for "information war" (*informatsionnaya voyna*) in a glossary of key information security terms produced by the Military Academy of the General Staff makes a clear distinction between the Russian definition - broad, and not limited to wartime - and the Western definition – which it describes as limited, tactical information operations carried out during hostilities.[6] For Russia, the contest for political supremacy with the West in the information domain has already begun.

Furthermore, information warfare can cover a vast range of different activities and processes seeking to steal, plant, interdict, manipulate, distort or destroy information. The channels and methods available for doing this cover an equally broad range, including computers, smartphones, real or invented news media, statements by leaders or celebrities, online troll campaigns, text messages, vox pops (snapshots of local opinions) by concerned citizens, YouTube videos, or direct approaches to individual human targets.

The overall effect of these tools and instruments in the information domain is repeatedly described in Russian sources as being capable of addressing highly ambitious 'strategic

---

[1] V. Kvachkov, Спецназ России (Russia's Special Purpose Forces), Voyennaya Literatura, 2004. http://militera.lib.ru/science/kvachkov_vv/index.html. Vladimir Kvachkov is a former GRU officer, whose "theory of special operations", including information operations, has reportedly been adopted as the basis for Russian military instructional and training materials.

[2] V. Putin, "Солдат есть звание высокое и почетное" ('Soldier' is an honourable and respected rank), excerpts from annual Address to the Federal Assembly of the Russian Federation, *Krasnaya zvezda*, May 11, 2006. http://old.redstar.ru/2006/05/11_05/1_01.html.

[3] Pavel Antonovich, "Cyberwarfare: Nature and Content", *Military Thought*, Vol.20, no. 3, 2011. pp. 35-43.

[4] Roland Heickerö, "Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations", Swedish Defence Research Establishment (FOI), 2010. www.foi.se/ReportFiles/foir_2970.pdf. p. 20.

[5] V.I. Slipchenko, "Future War (A Prognostic Analysis)", January 1998.

[6] "*Slovar' terminov i opredeleniy v oblasti informatsionnoy bezopasnosti*", *Voyennaya Akademiya General'nogo Shtaba*, 2nd Edition, Moscow Voyeninform, 2008.

tasks.' A strategic task, such as preventing a NATO consensus on meeting Article 5 commitments, would be the ultimate prize for a Russian information campaign.

Essential Concepts and Terminology

For Russia, *information warfare* (also referred to as *information confrontation*) is a broad and inclusive concept covering a wide range of different activities.[7] It covers hostile activities using information as a tool, or a target, or a domain of operations.

Consequently, the concept carries within it computer network operations alongside disciplines, such as psychological operations (PsyOps), strategic communications, influence operations, along with "intelligence, counterintelligence, *maskirovka* (military deception, or operational masking), disinformation, electronic warfare, debilitation of communications, degradation of navigation support, psychological pressure, and destruction of enemy computer capabilities."[8] Taken together, these activities form, "a whole of systems, methods, and tasks to influence the perception and behavior of the enemy, population, and international community on all levels."[9]

Russia sees superiority in this broad application of information warfare as a key enabler for victory in current and future conflict against the West:

> *Wars will be resolved by a skilful combination of military, nonmilitary, and special nonviolent measures that will be put through by a variety of forms and methods and a blend of political, economic, informational, technological, and environmental measures, primarily by taking advantage of information superiority. Information warfare in the new conditions will be the starting point of every action now called the new type of warfare, or hybrid war, in which broad use will be made of the mass media and, where feasible, global computer networks (blogs, various social networks, and other resources).*[10]

This blending and coordination of different tools and techniques is a distinctive feature of how Russia aspires to prosecute information warfare. Critics of NATO practice suggest that within the Alliance, this coordination is – by contrast – conspicuously absent, as is a coherent overall approach to the execution of activities in the information domain.[11] According to one

---

[7] The distinction between информационное противоборство, (*informatsionnoye protivoborstvo)*, information confrontation, and информационная война *(informatsionnaya voyna*), information war, is the subject of detailed debate in official Russian sources. The distinctions are of little practical impact for assessing Russian approaches, and for simplicity, "information war" is the term adopted throughout this paper.

[8] K. Mshvidobadze, "The Battlefield On Your Laptop", Radio Free Europe/Radio Liberty, 21 March 2011. http://www.rferl.org/articleprintview/2345202.html.

[9] A.J.C. Selhorst, "Russia's Perception Warfare", *Militaire Spectator*, Vol. 185, No. 4, 2016. p. 151.

[10] S. G. Chekinov and S. A. Bogdanov, "Прогнозирование характера и содержания войн будущего: проблемы и суждения" (Forecasting the nature and content of wars of the future: problems and assessments), *Voennaya Mysl'* (Military Thought), No. 10, 2015. p. 44-45.
Col. (Rtd) Sergey Chekinov is cited repeatedly in this handbook. This reflects both his extensive range of publications on this subject, and his position as head of the Centre for Military Strategic Research of the Russian General Staff Academy and hence as a reliable indicator of current trends of thought within the General Staff.

[11] While at first glance, the information-related capabilities (IRCs) employed by the Russian military appears to be similar to that of NATO (e.g., the existence of psychological operations, strategic communications, influence operations, electronic warfare, and military deception, etc.), there are a number of conceptual and structural differences that set Russia apart from NATO. First, NATO does not use the term 'information warfare' to describe its own capabilities or activities conducted in and designed to affect the information environment, but

assessment of NATO's own definitions:

> *There is still a lack of consensus when it comes to defining all the elements that make up the strategic application of power in the information domain. Regarding the use of terms like Information Warfare (IW), Psychological Operations (PsyOps), Influence Operations (IO), Strategic Communications (STRATCOM), Computer Network Operations (CNO), and Military Deception (MILDEC), there is a lot of confusion as there are numerous conflicting definitions, and these terms are used in different contexts to describe different objectives and actions.*[12]

Yet, in the Russian context, all these different disciplines form a unified whole under the heading of information warfare.

The Ukraine conflict provides a clear demonstration of how Russia sees cyber activity as a subset, and sometimes facilitator, of the much broader domain of information warfare, with a particular focus on generating psychological effects.[13] In fact, the techniques visible in and around the Ukraine conflict represent the culmination of an evolutionary process in Russian information warfare theory and practice, seeking to revive well-established Soviet techniques of subversion and destabilisation and update them for the internet age.[14] For all their innovative use of social media, current Russian approaches have deep roots in long-standing Soviet practice.[15] As pointed out by Jolanta Darcewska, in a detailed review of coverage of information warfare in Russia's new Military Doctrine, "doctrinal assumptions about information warfare demonstrate not so much a change in the theory of its conduct... but rather a clinging to old methods (sabotage, diversionary tactics, disinformation, state terror, manipulation, aggressive propaganda, exploiting the potential for protest among the local population)."[16]

---

rather 'information operations.' When the term 'information warfare' is used by NATO, it is generally in reference to adversary capabilities and tactics, or the conduct of adversarial activities impacting the information environment. Second, while information operations are a coordination function of information-related capabilities within NATO, public affairs are (traditionally) considered to be a 'separate but related' capability; in other words, public affairs reside outside of the conceptual frame of information operations. Although an effort is underway in NATO to move public affairs into the realm of information operations, this conceptual divide implies that Russia has achieved a greater degree of information capability integration than that of NATO. The last significant difference between Russia and NATO is twofold. First, the responsibility for the design and execution of information warfare in the Russia government falls to the intelligence community and special forces (e.g., GRU, FSB, etc.), which effectively combines intelligence collection operations (espionage) with psychological warfare, including elements of direct action (subversion, sabotage, and assassination). Second, Russian information warfare draws upon and utilizes the full breadth of military, civilian, and non-governmental agencies, including non-state actors (e.g., private business, organized crime, patriotic groups, etc.), in what can be referred to as a 'whole-of-society' approach.

[12] P. Brangetto and M. A. Veenendaal, "Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations", in N.Pissanidis et. al. (eds.), *8th International Conference on Cyber Conflict*, NATO Cooperative Cyber Defence Centre of Excellence, June 2016. https://ccdcoe.org/sites/default/files/multimedia/pdf/CyCon_2016_book.pdf.

[13] For analysis of how this is implemented, see chapters in Kenneth Geers (ed.), "Cyber War in Perspective: Russian Aggression against Ukraine", NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), December 2015.

[14] Examined in greater detail in Keir Giles, "Russia's Toolkit", chapter in "The Russian Challenge", Chatham House, London, June 2015.

[15] Cliff Kincaid, "How Putin Uses KGB-style 'Active Measures'", Accuracy in Media, 9 April 2014. http://www.aim.org/aim-column/how-putin-uses-kgb-style-active-measures/.

[16] Jolanta Darczewska, "The Devil Is In The Details: Information Warfare In The Light Of Russia's Military Doctrine", OSW Point of View No. 50, May 2015.

The basic principles of the Russian approach to information security and information threats have been consistently clear from Russian declaratory policy,[17] and the development of their implementation can be traced through a wealth of official Russian documents laying out the approach to information security.[18] Public military discussion of the integration and utilisation of cyberspace to facilitate the compromise of adversary decision-making channels, as well as command and control networks, has a prehistory in Russia dating back to at least the early 1990s.[19] But, as with Russia's military transformation, this evolution accelerated following the war with Georgia in 2008, when limited performance in the information domain was one of the many criticisms aimed at the Russian Armed Forces. The proposal within Russia at that time was to establish dedicated Information Troops, whose purpose "would be the creation of an information domain that makes international reality responsive to Russia's interests."[20] By the beginning of 2014, and prior to the Russian annexation of Crimea, it was clear that, "information operations, which may encompass broad, socio-psychological manipulation ... are comfortably in the mainstream of Russian military thought."[21]

Russian Cyber Warfare

One fundamental distinction between Russian and Western approaches to information activities is the categorisation of computer network operations (CNO) and other activities in cyberspace.

Unlike the West, cyber is not a separate function or domain in the Russian information warfare concept. The delineation of activities in the cyber domain from other activities processing, attacking, disrupting or stealing information is seen as artificial in Russian thinking. In this context, “[d]istributed denial of services attacks (DDoS), advanced [cyber] exploitation techniques and Russia Today television are all related tools of information warfare.”[22]

The phrase *cyber warfare* in Russian writing describes foreign concepts and activities, which generally observe and reinforce the distinction between information activities on computers and networks and those in the physical and psychological domain. Consequently, searches for *cyber* and *cyber warfare* in Russian sources primarily return references to Western doctrine and thinking. It follows that any research on Russian capabilities and intentions which includes cyber or cyber warfare risks providing fundamentally misleading results.

By extension, research on Russia's *cyber command, cyber doctrine,* and *cyber capabilities* is also often a misdirected effort, since these entities and concepts, even if they exist, are not named or described in these terms. Persistent reporting that "Russia's Ministry of Defense is

[17] For example, "Basic Principles for State Policy of the Russian Federation in the Field of International Information Security to 2020, Approved by the President of the Russian Federation July 24, 2013."
[18] Keir Giles, "Russia’s Public Stance on Cyberspace Issues", in C. Czosseck, R. Ottis, K. Ziolkowski (Eds.), 2012 *4th International Conference on Cyber Conflict*, Tallinn, June 2012. pp. 63-75.
[19] See V.M. Lisovoy, "*O zakonakh razvitiya vooruzhennoy bor'by i nekotorykh tendentsiyakh v oblasti oborony*", *Voyennaya Mysl',* Issue 5, 1993.
[20] "Russia is underestimating information resources and losing out to the West", unattributed article, Novyy Region, 29 October 2008.
[21] Stephen Blank, "Signs of New Russian Thinking About the Military and War", Eurasia Daily Monitor, 12 February 2014.
[22] D. J. Smith. ‘How Russia Harnesses Cyberwarfare,’ Defense Dossier, American Foreign Policy Council, Issue 4, August 2012. p. 8. http://www.afpc.org/files/august2012.pdf.

establishing its own cyber command,"[23] and related reports on boosting military cyber capabilities,[24] appear to refer to very different organisations and notions than in the West, in particular NATO.

At the same time, it must be emphasised that verification of open source reporting of organisational developments in the parts of the Russian Armed Forces and other government departments and agencies that prosecute CNO and other aspects of information warfare is extremely challenging, largely due to their classified nature.[25] Detailed and factual public announcements, of the kind made by the US when setting up Twenty-Fourth Air Force (24 AF) or the UK when establishing 77 Brigade, simply do not happen in Russia. As a result, discussions based on open sources of how Russia organises, plans and directs its information warfare efforts – in effect, who does what and how within the Russian system – is largely speculative.

Instead of cyberspace, Russia refers to and uses the term *information space*, and includes in this concept both *computer* and *human information processing* (i.e., decision-making and cognition), in effect the psychological domain.[26] The closest Russian thinking comes to separating out CNO from other activities in the information space is division into the *information-technical* and *information-psychological* domains, the two main strands of information warfare in Russian thinking.[27] As explained in one authoritative Russian textbook:

> *Depending on the target of action, information warfare consists of two types:*
>
> - *Information-psychological warfare (to affect the personnel of the armed forces and the population), which is conducted under conditions of natural competition, i.e. permanently;*
>
> - *Information-technology warfare (to affect technical systems which receive, collect, process and transmit information), which is conducted during wars and armed conflicts.*[28]

It should be noted that cyber activities do not map directly to the information-technological domain; as an integral part of information warfare overall, cyber activities are also inherent and utilised in information-psychological operations. It is also important to note that some

[23] J. R. Clapper, US Director of National Intelligence, Worldwide Threat Assessment of the US Intelligence Community, Senate Armed Services Committee Statement for the Record, 26 February 2015.
[24] Eugene Gerden, "Russia to spend $250m strengthening cyber offensive capabilities", SC Magazine UK, 4 February 2016. http://www.scmagazineuk.com/russiatospend250mstrengtheningcyberoffensivecapabilities/printarticle/470733/.
[25] Russia did at one point have a separate dedicated information security agency, the Federal Agency for Government Communications and Information (FAPSI) – described in 2000 by one leading expert as "the unofficial Ministry of Information Warfare of the Russian Federation" – but this is long defunct, and its functions absorbed into other government departments. See G. Bennett, *The Federal Agency of Government Communications & Information*, Conflict Studies Research Centre, Sandhurst, August 2000.
[26] T.L.Thomas, "Information Security Thinking: A Comparison of U.S., Russian, And Chinese Concepts", Foreign Military Studies Office, July 2001. http://fmso.leavenworth.army.mil/documents/infosecu.htm.
[27] T. L. Thomas. "Russian Information Warfare Theory: The Consequences of August 2008", in S. Blank and R. Weitz (eds.). *The Russian Military Today and Tomorrow: Essays in Memory of Mary Fitzgerald*, Carlisle, US Army War College Strategic Studies Institute 2010.
[28] V. Kvachkov, Спецназ России (Russia's Special Purpose Forces), Voyennaya Literatura, 2004. http://militera.lib.ru/science/kvachkov_vv/index.html.

operations in both domains are undertaken permanently – regardless of the notional state of cooperation or hostility (i.e., during wars and armed conflicts) between the opposing sides.

The key word, therefore, is *information*. In the Russian conceptual framework, information can be stored anywhere and transmitted by any means – so information in print media, or on television, or in somebody's head, is subject to the same targeting concepts and methods as that are used on an adversary's computer or mobile device. Similarly, the transmission or transfer of this information can be by any means (e.g., traditional media, new media, electronic warfare, etc.). Thus, introducing corrupted data into a computer across a network or from a flash drive is – conceptually – no different from placing disinformation in a media outlet, or causing it to be repeated in public by a key influencer.

In keeping with the broader Russian understanding of information space, the term *information weapon* has an impressively broad application. Information weapons can be used in many more domains than cyber, in particular the human-cognitive domain.[29] Even within CNO, an information weapon need not necessarily have a destructive real-world effect in the style of Stuxnet[30] that led to the physical destruction of centrifuges. Instead, in keeping with information warfare objectives more broadly, "influencing the transfer and storage of data means that the physical destruction of your opponent's facilities is no longer required."[31]

Importantly, multiple senior Russian officials have reinforced the point that the initiation of informational activities is not contingent upon a declaration of war or a recognized state of armed conflict. For example, former Deputy Chief of the General Staff Lt-Gen Aleksandr Burutin noted in January 2008 that information weapons can be, "used in an efficient manner in peacetime as well as during war."[32] This points to another obvious asymmetry with NATO practice. As pointed out by Mark Laity, Chief of Strategic Communications, Supreme Headquarters Allied Powers Europe (SHAPE):

> *The Russians use information from a covert stage through six phases of warfare to the re-establishment of victory. Information confrontation is conducted in every phase, including covertly, in peace and in war. Our doctrines do not allow us to do a lot of this stuff till the fighting basically starts.*[33]

At the same time, some previous Russian writers while discussing the permanent nature of information warfare have drawn a distinction between its nature in peacetime and wartime. According to this categorisation, peacetime is mostly characterised by covert measures, reconnaissance, espionage, building capabilities and degrading those of the adversary, and manoeuvring for advantage in information space. Wartime measures, by contrast, are inherently aggressive, and include "discrediting [adversary] leadership, intimidating military personnel and civilians ... falsification of events, disinformation, hacking attacks and so

[29] K. Giles and W. Hagestad, "Divided by a Common Language: Cyber Definitions in Chinese, Russian and English", in K. Podins et al (eds.), 5th International Conference on Cyber Conflict, CCDCOE, Tallinn, 2013. https://ccdcoe.org/publications/2013proceedings/d3r1s1_giles.pdf.
[30] R. Pfeffercorn, "Security Risks of Government Hacking", The Center for Internet and Society, September 2018. https://cyberlaw.stanford.edu/files/publication/files/2018.09.04_Security_Risks_of_Government_Hacking_Whitepaper.pdf.
[31] Prof. V. Lisovoy, speaking at Swedish Defence Research Agency, Stockholm, 5 October 2010.
[32] Interfax-AVN news agency, 31 January 2008.
[33] "Russia: Implications for UK defence and security", First Report of Session 2016–17, House of Commons Defence Committee, UK Parliament, 5 July 2016. p. 17.

forth".[34] Furthermore, the main effort of information warfare is "concentrated on achieving political or diplomatic ends, and influencing the leadership and public opinion of foreign states, as well as international and regional organisations."[35] If measured by these criteria, recent Russian activities in the information space would indicate that Russia already considers itself to be in a state of [undeclared] war.[36]

War and Peace

One of the most striking elements of this evolution has been in the Russian approach to the relationship between information warfare and the traditional state of war. The erosion of the conceptual distinction between war and peace, and the emergence of a *grey zone* (whereby the origins, nature and participants in a conflict remain fuzzy or blurred), is noted repeatedly throughout recent Russian military writing on the nature of warfare – including, but not limited to, the presentation by Chief of General Staff Valery Gerasimov, which widely referred to by Western military analysts and journalists as the *Gerasimov doctrine*.[37] According to a 2011 analysis by Pavel Antonovich, the "dividing lines between war and peace can be eroded conveniently in cyberspace [and] … [d]amage (whatever its nature) can actually be done to an adversary without overstepping formally the line between war and peace."[38] An exceptional study of Russian views on information warfare (IW) conducted by Sweden's FOI defence research agency in 2010, noted:

> *Regarding network and computer operations in peacetime IW, viruses and other malware are important in order to compromise the information assets of the engineering systems of the enemy. Other aspects of IW are accumulating (stealing) information on the enemy, by intelligence gathering, while developing and testing one's own IW weapons.*[39]

This, however, is a radical departure from previous Russian views of the status of information warfare. In the mid-1990s, Timothy L. Thomas and Lester Grau argued:

> *[F]rom a military point, the use of Information Warfare against Russia or its armed forces will categorically not be considered a non-military phase of a conflict…. [In response to] the possible catastrophic use of information warfare means by an enemy, whether on economic or state command and control systems, or on the combat*

[34] I. Sharavov, "К вопросу об информационной войне и информационном оружии" (On the issue of information war and information weapons), *Zarubezhnoye voyennoye obozreniye*, No. 10, 2000. pp. 2-5. And see: V. Malyshev, "Использование возможностей средств массовой информации в локальных вооруженных конфликтах" (Making use of the media in local armed conflicts), *Zarubezhnoye voyennoye obozreniye*, No. 7, 2000. pp. 2-8.

[35] Yu. E. Donskov, O. G. Nikitin, "Место и роль специальных информационных операций при разрешении военных конфликтов" (The place and role of special information operations in resolving military conflicts) *Voyennaya mysl'*, No. 6, 2005. pp. 17-23.

[36] Multiple indicative examples include CNO targeting the United States in a practically overt manner, and Russia's new lack of concern at accompanying damage to its international reputation. See Max Fisher, "In D.N.C. Hack, Echoes of Russia's New Approach to Power", The New York Times, 25 July 2016. http://www.nytimes.com/2016/07/26/world/europe/russia-dnc-putin-strategy.html.

[37] Valeriy Gerasimov, "*Tsennost nauki v predvidenii*" (The Value Of Science Is In Foresight), *Voyenno-promyshlennyy kuryer*, No. 8 (476), 27 February 2013.

[38] Pavel Antonovich, "Cyberwarfare: Nature and Content", *Military Thought*, Vol.20, No.3, 2011. pp. 35-43.

[39] Roland Heickerö, "Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations", Swedish Defence Research Establishment (FOI), 2010. www.foi.se/ReportFiles/foir_2970.pdf. p. 20.

> *potential of the armed forces .... Russia retains the right to use nuclear weapons first against the means and forces of information warfare, and then against the aggressor state itself.*[40]

This, and similar developments in Russian information warfare thinking,[41] laid the groundwork for the creative approach to achieving information dominance, which was clearly demonstrated in Crimea.

Implications

The scope and potentiality of the Russian conceptualization of information warfare should not be measured against Western concepts of information operations or information activities, nor should it be confused with cyber operations. The Ukraine conflict has provided clear demonstrations of how Russia understands and operationalizes cyber activity as a subset, and sometimes facilitator, of the much broader domain of information warfare.[42]

Since 2014, Russian information warfare has commonly come to be identified in non-specialist literature (e.g., mainstream and popular media, etc.) with the simple distribution of disinformation. The Russian approach, however, is much broader than sowing lies, deceit and denial; for instance, maintaining that Russian troops and equipment are not where they plainly are, such as in Crimea. Instead, Russian state and non-state actors have exploited history, culture, language, nationalism, disaffection and other psychological, social and political factors to carry out cyber-enhanced disinformation campaigns with broad strategic objectives. In an article written by Tim Thomas in 1998, he notes:

> *[Russia's] different prisms of logic may offer totally different conclusions about an information operation's intent, purpose, lethality, or encroachment on sovereignty; and this logic may result in new methods to attack targets in entirely non-traditional and creative ways."*[43]

The Western approach to cyber defence has typically focused on technical responses to what are largely perceived as technical threats and has dismissed the interface with information warfare more broadly. This approach is entirely apt for some persistent threats, but not always sufficient for a wider and more holistic approach, such as the one adopted by Russia.[44]

In other words, the West may be prepared to face pure, technological cyber challenges, but the capabilities and intentions embraced by Russia indicate that it also needs to prepare for

---

[40] Lester Grau, Timothy L. Thomas, T. (1996) "A Russian View of Future War: Theory and Direction", *Journal of Slavic Military Studies*, issue 9.3, September 1996. pp. 501–518.
[41] As examined on the eve of the Ukraine conflict by Tim Thomas in "Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?", The Journal of Slavic Military Studies, 10 March 2014. pp. 101-130.
[42] For analysis of how this is implemented, see chapters in Kenneth Geers (ed.), "Cyber War in Perspective: Russian Aggression against Ukraine", NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), December 2015. See also M. Aaltola, "Cyber Attacks Go Beyond Espionage: The Strategic Logic of State-sponsored Cyber Operations in the Nordic-Baltic Region", Finnish Institute of International Affairs Briefing Paper 200 (2016), 29 August 2016. http://www.fiia.fi/en/publication/606/cyber_attacks_go_beyond_espionage/.
[43] Timothy L. Thomas, "Dialectical versus Empirical Thinking: Ten Key Elements of the Russian Understanding of Information Operations", *Journal of Slavic Military Studies*, Vol.11, No.1, 1998. pp. 40-62.
[44] Patrik Maldre, "The Many Variants of Russian Cyber Espionage", Atlantic Council, 28 August 2015. http://www.atlanticcouncil.org/blogs/natosource/the-many-variants-of-russian-cyber-espionage.

information war, especially when these are integrated with disinformation, subversion, kinetic and electronic warfare (EW) operations.

Aims and Objectives

Recently published Russian military theory gives information warfare an increasingly prominent role in contemporary interstate conflict and specifically as a means of assuring victory in armed conflict by predetermining the outcome:

> *Information and psychological warfare will come on top of all forms and methods of operations in future wars to achieve superiority in troop and weapon control and to erode the morale and psychological spirit of the opposing side's armed forces personnel and population. Indeed, information warfare and psychological operations lay much of the groundwork for victory.*[45]

Information warfare is also considered capable of avoiding the necessity of armed conflict altogether by achieving strategic goals on its own. As noted by Mark Galeotti:

> *[Russia has given] primacy to non-kinetic operations, especially information warfare. The traditional [Western] assumption has been that subversion, deception, and the like are all 'force multipliers' to the combat arms, not forces in their own right. At present, though, Russia is clearly seeing the kinetic and the non-kinetic as interchangeable and mutually supporting.*[46]

Information warfare campaigns can have a range of aims and objectives, both offensive and defensive, which are not necessarily mutually exclusive. Broad categories of objective are listed below in decreasing order of ambition, from use as a stand-alone tool for achieving geopolitical goals to simple weakening of the adversary without necessarily any specific end state in mind.

Strategic Victory

Studies that consider the strategic effects of information warfare have tended to conclude that for the West, "IW is almost by definition counter command and control warfare."[47] But this is a more limited construct than the Russian approach, which is far more ambitious and comprehensive. Recent authoritative Russian papers on military theory state:

> *Under today's conditions, means of information influence have reached a level of development such that they are capable of resolving strategic tasks;*[48]

And,

---

[45] S. G. Chekinov and S. A. Bogdanov, "Прогнозирование характера и содержания войн будущего: проблемы и суждения" (Forecasting the nature and content of wars of the future: problems and assessments), *Voennaya Mysl'* (Military Thought), No. 10, 2015. pp. 44-45.

[46] Mark Galeotti, "Hybrid, ambiguous, and non-linear? How new is Russia's 'new way of war'?", Small Wars & Insurgencies, Vol. 27 No. 2, 2016. p. 291.

[47] S. Blank, "Can Information Warfare Be Deterred?" *Defense Analysis*, Vol. 17, No. 2, 2001. p. 132.

[48] S. G. Chekinov and S. A. Bogdanov, "Влияние непрямых действий на характер современной войны" (The influence of the indirect approach on the nature of modern warfare), *Voyennaya mysl'*, No. 6 2011. pp. 3-13.

> *Winning information confrontations will result in the achievement of strategic and political goals and in the defeat of an enemy's armed forces (and the capture of his territory, destruction of his economic potential, and overthrow of his political system).*[49]

Information activities as preparation for open conflict are also nothing new. As noted by James Sherr:

> *One of the aims of the Russians pursuing what they have long called the initial period of war is to incapacitate a state as much as possible before that state is even aware that a conflict has started. In Ukraine, this was done very effectively. So at one dimension of activity, we are dealing with something which is unfamiliar to us, but has been around in Russian thinking since the 1920s.*[50]

In more recent constructs of information warfare, involvement of conventional military forces is reduced to a minimum, and they are replaced by effective use of the internet:

> *Of great importance here is the use of the global internet network to exert a massive, dedicated impact on the consciousness of the citizens of states that are the targets of the aggression. Information resources have become one of the most effective types of weapon. Their extensive employment enables the situation in a country to be destabilized from within in a matter of days…. In this manner, indirect and asymmetric actions and methods of conducting hybrid wars enable the opposing side to be deprived of its actual sovereignty without the state's territory being seized.*[51]

In fact, senior Russian officers have suggested that information effects – including using the internet to affect mass consciousness – can, in some cases, replace armed intervention altogether.[52]

It can be seen that the ultimate aim of information warfare is that of regime change. Importantly, this is achieved not only by targeting the ruling regime itself, or its armed forces, but also the population as a whole. As noted by Kuleshov, a Russian military theorist:

> *The main aim of information-psychological conflict is regime change in the adversary country (through destroying the organs of government); by means of mass influence*

---

[49] V. Slipchenko, "Информационный ресурс и информационное противоборство" (Information Resources and Information Confrontation) *Armeyskiy sbornik*, October 2013. p. 52.

[50] Oral evidence: Russia: Implications for UK Defence and Security, HC 763, House of Commons Defence Committee, 1 March 2016.
http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/defence-committee/russia-implications-for-uk-defence-and-security/oral/29915.html.

[51] V. Gerasimov, "По опыту Сирии" (Based on the experience of Syria), *Voyenno-promyshlennyy kur'er*, 9 March 2016. http://vpk-news.ru/sites/default/files/pdf/VPK_09_624.pdf.

[52] A. V. Kartapolov, "Уроки военных конфликтов, перспективы развития средств и способов их ведения. Прямые и непрямые действия в современных международных конфликтах" (Lessons of military conflicts and prospects for the development of means and methods of conducting them. Direct and indirect actions in contemporary international conflicts," *Vestnik Akademii Voennykh Nauk* (Bulletin of the Academy of Military Science), No. 2 2015. pp. 28-29.
At the time of writing, Col-Gen Andrey Kartopolov is the commander of Russia's NATO-facing Western Military District, whose forces have been substantially augmented under his command. His previous post was head of the Main Operations Directorate of the General Staff. As such, it can be assumed that he is one of the best-informed individuals in Russia on plans to initiate or resist confrontation with NATO.

on the military-political leadership of the adversary achieving as a minimum an increase in the amount of time available for taking command decisions and lengthening the operational cycle; by means of influence on the mass consciousness of the population – directing people so that the population of the victim country is induced to support the aggressor, acting against its own interests.[53]

Permissive Environment

Russia seeks to influence foreign decision-making by creating and maintaining a polluted information environment, exploiting the fact that Western elected representatives receive and are sensitive to the same information flows as their voters. The threshold for a successful information warfare campaign is the delivery of disinformation into the decision-making framework of a target nation.

However, even if disinformation is not successfully inserted into the policy-making chain, and only spreads in mass and social media, the effect can be to create a permissive public opinion environment whereby Russian narratives are presented as factual. In this case, Moscow's potential gain is to win public support in adversary nations, and thereby attenuate resistance to future actions planned by Russia.

In some cases, rather than challenging or promoting specific facts, these efforts are aimed at framing an ongoing debate in a manner favourable to the end state desired by Russia.[54] This can include the promotion of specific narratives designed to constrain or limit NATO freedom of action.[55]

Even responsible media reporting can inadvertently lend authority to false Russian disinformation. For example, in reporting on Canada's status as a framework nation for NATO's multinational presence in Latvia, Canadian state funded broadcaster, CBC published a report quoting a German view that the presence could be seen as "a provocation," especially since NATO had "signed a treaty" with Russia in which it "explicitly agreed not to station troops along the Russian border in former satellite states."[56] These are the terms in which Russia would wish the NATO-Russia Founding Act to be interpreted, rather than what is written in the Act. The result is that the Canadian public was inadvertently informed by an arm's length, state funded media outlet that Canada's actions were in breach of NATO treaty commitments to Russia.[57]

Individual examples like this may appear trivial, but in order to gauge their effect, they have to be considered *en masse* and across all NATO nations.

---

[53] Yu. Kuleshov et al., "Информационно-психологическое противоборство в современных условиях: теория и практика" (Information-Psychological Warfare In Modern Conditions: Theory And Practice), *Vestnik Akademii Voyennykh Nauk*, Vol. 46, No. 1, 2014. p. 106.

[54] As described in a study focusing on the Czech Republic: T. Wesolowsky, "Kremlin Propaganda In Czech Republic Plays Long Game To Sow Distrust In EU", RFE/RL, 16 June 2016. http://www.rferl.org/content/czech-kremlin-propaganda-plays-long-game-sow-eu-distrust/27802234.html.

[55] Karl-Heinz Kamp, "Russia's myths about NATO: Moscow's propaganda ahead of the NATO Summit", Federal Academy for Security Policy Working Paper No. 15, 2016. https://www.baks.bund.de/sites/baks010/files/working_paper_15_2016.pdf.

[56] Murray Brewster, "Canada to send troops to Latvia for new NATO brigade", CBC, 30 June 2016. http://www.cbc.ca/news/politics/nato-canadian-troops-baltics-1.3659814.

[57] For a detailed and insightful study on the roots of confusion over this section of the NATO-Russia Founding Act, see W. Alberque, "'Substantial Combat Forces' in the Context of NATO-Russia Relations", NATO Defense College Research Paper No. 131, July 2016. http://www.ndc.nato.int/download/downloads.php?icode=493.

These narratives need not be specifically related to current events; historical events can also be distorted or selectively presented in order to inculcate a world view which justifies Russian actions. As described by Estonia's Internal Security Service, "Russia's influence operations in the field of history have always been an integral part of Moscow's foreign policy."[58]

Subversion and Destabilisation

At the lower end of the scale of ambition of Russian information warfare comes broad-based, long-term weakening and undermining of adversary societies overall, without necessarily any specific short-term goal other than increasing Russia's relative strength in a classic zero-sum approach.

The underlying approaches of activities utilized by Russia, and the guiding principles, are broadly recognisable as reinvigorated aspects of subversion campaigns from the Cold War era.[59] During the Cold War, aspects of these information-based campaigns were referred to as *active measures*. According to a Finnish study, active measures constitute:

> *[C]ertain overt and covert techniques for influencing events and behaviour in, and the actions of, foreign countries. [They] may entail the following objectives:*
>
> - *influencing the policies of another government;*
> - *undermining confidence in its leaders and institutions;*
> - *disrupting the relations between other nations;*
> - *discrediting and weakening governmental and nongovernmental opponents.*[60]

A key element of subversion campaigns is "spreading disinformation among the population about the work of state bodies, undermining their authority, and discrediting administrative structures."[61] This contributes to the *dismay effect* in former NATO press officer Ben Nimmo's short characterisation of Russian disinformation (which he argues aims to dismiss, distort, distract, dismay)[62] and can be achieved by exploiting vulnerabilities in the target society, particularly freedom of expression and democratic principles. The range of targets is broad. Subversion campaigns can aim to:

> *[I]nvolve all public institutions in the country it intends to attack, primarily the mass media and religious organizations, cultural institutions, nongovernmental organizations, public movements financed from abroad, and scholars engaged in*

[58] Annual Review 2015, Estonian Internal Security Service (aka KAPO), 2015. https://kapo.ee/sites/default/files/public/content_page/Annual%20Review%202015.pdf. pp. 12-15.
[59] 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.
And see: 'Soviet Propaganda In Western Europe', UK Foreign & Commonwealth Office, March 1982. http://www.psywar.org/radSovietPropaganda.php.
[60] K. Pynnöniemi and A. Rácz (eds.), *Fog of Falsehood: Russian Strategy of Deception and the Conflict in Ukraine*, FIIA Report No. 45, undated. p. 38.
[61] Yu. Kuleshov et al., "Информационно-психологическое противоборство в современных условиях: теория и практика" (Information-Psychological Warfare In Modern Conditions: Theory And Practice), *Vestnik Akademii Voyennykh Nauk*, Vol. 46, No. 1, 2014. pp. 106.
[62] Ben Nimmo, "Anatomy of an Info-War: How Russia's Propaganda Machine Works, and How to Counter It", 19 May 2015. http://www.stopfake.org/en/anatomy-of-an-info-war-how-russia-s-propaganda-machine-works-and-how-to-counter-it/.

research on foreign grants. All these institutions and individuals may be involved in a distributed attack and strike damaging point blows [sic; presumably точечные удары, more commonly translated as surgical strikes] at the country's social system with the purported aims of promoting democracy and respect for human rights.[63]

An obvious target for distributing disinformation is the mainstream news media, and a direct link is seen between news media campaigns and a society's capacity to resist:

The mass media today can stir up chaos and confusion in government and military management of any country and instil ideas of violence, treachery, and immorality, and demoralize the public. Put through this treatment, the armed forces personnel and public of any country will not be ready for active defense.[64]

But bodies and organisations other than the news media can also be targeted. At the time of writing, the US Senate Intelligence Committee is advocating the reconstitution of an organisation within the intelligence community that, among its duties, "would also investigate the funding of front groups — or cover organizations for Russian operations — 'covert broadcasting, media manipulation' and secret funding."[65]

Direct links between Russia and political parties representing the dissatisfied population at either end of the political spectrum have become increasingly well documented.[66] But a much wider range of organisations than established political parties can be used for subversive purposes:

It is preferable to have a foreign nonprofit nongovernmental organization (NGO) that could best contribute to the attainment of the goal of a hybrid operation. It can be established beyond the Russian Federation under the rules of a foreign country [and] can draw its members from residents of the disputed territory and its political objectives will include discrediting the current government agencies, eroding the prestige and public standing of the law enforcement agencies, particularly the armed forces, buying up the mass media and conducting information operations purportedly to protect democracy, and nominating delegates for local government elections, and infiltrating them into the elected government authorities.[67]

Once again it should be emphasised that when Russian military theorists are describing these

[63] S.G. Chekinov and S.A. Bogdanov, "The Nature and Content of a New-Generation War", *Military Thought* (English edition), No. 4, 2013. Emphasis as in original publication.
[64] S. G. Chekinov and S. A. Bogdanov, "Initial Periods of Wars and Their Impact on a Country's Preparations for a Future War", *Military Thought* (English edition), No 4, 2012. pp. 24-25.
[65] Ali Watkins, "Senate Committee Looks To Revive Cold-War Era Body To Catch Russian Spies", Buzzfeed, 21 June 2016. https://www.buzzfeed.com/alimwatkins/senate-committee-looks-to-revive-cold-war-era-body-to-catch.
[66] As in A. Klapsis, "An Unholy Alliance: The European Far Right and Putin's Russia", Wilfried Martens Centre for European Studies, undated. http://www.martenscentre.eu/sites/default/files/publication-files/far-right-political-parties-in-europe-and-putins-russia.pdf. See also P. Foster and M. Holehouse, "Russia accused of clandestine funding of European parties as US conducts major review of Vladimir Putin's strategy", Daily Telegraph, 16 January 2016. http://www.telegraph.co.uk/news/worldnews/europe/russia/12103602/America-to-investigate-Russian-meddling-in-EU.html. And see: Alina Polyakova, "Why Europe Is Right to Fear Putin's Useful Idiots", Foreign Policy, 23 February 2016. http://foreignpolicy.com/2016/02/23/why-europe-is-right-to-fear-putins-useful-idiots/.
[67] I. N. Vorobyov and V. A. Kiselev, "Гибридные операции как новый вид военного противоборства" (Hybrid operations as a new form of armed conflict), *Voyennaya mysl'*, No. 5, 2015. pp. 41-49.

approaches, they are – in the majority of cases – presented as campaigns planned by the West against Russia, rather than as measures which Russia itself is implementing. In addition, funding political parties or other organisations with a view to promoting a specific agenda can hardly be said to be a Russian invention. Nevertheless, Russia can be seen adopting and adapting these lessons from the West, within the framework of existing information warfare theory. Furthermore, the adoption of damaging actions with no set or specific geopolitical objective beyond weakening and undermining competitor societies should not be seen as a recent innovation, but rather a mainstream Russian approach adopted from the Soviet Union.

Defensive Measures

Awareness of the destructive potential of the techniques outlined above has led Russia to re-institute control over the information space to which its own population is exposed.

For Russia, this was part of implementing the requirements of its information security doctrine of "securing national information space," and protecting it against "breaches". Both of these isolationist concepts are unfamiliar for the West but were traditional security preoccupations for Russia both during and before Soviet times, recognizing the enduring concern that, "the political system of Russia could not withstand twenty years of free communication with Western Europe."[68]

Foreign ownership of media outlets has been limited, rebroadcasting licences withdrawn, and independent sources of news closed or constrained.[69] One consistent element in this process is commercial control over media companies being acquired by Kremlin-friendly individuals, who then directly or subtly steer the editorial approach.[70] What remains of Russia's free media has largely been marginalised or intimidated into compliance.[71] In many cases mainstream journalism has reverted to its former role of transporting leadership messages into the public space.

The key role of television in influencing Russian society is well documented, and research confirms the driving role of this government-controlled medium in forming opinion even on the (comparatively) free internet.[72] The alternative reality broadcast on Russian television is unrecognisable from real life.[73] As noted by Michael Birnbaum, Russian "[s]tate television — the well-funded and primary news source for most Russians — broadcasts slickly-produced programs that focus on news that is either at sharp variance with that available in the West or is cherry-picked to bolster the Kremlin's image."[74] But contrary to Western

[68] A. de Custine, *Lettres de Russie: La Russie en 1839*, P. Nora (ed.), Gallimard, 1975.
[69] M. Tsvetkova and P. Devitt, "Russian editors 'fired over stories that irked officials'", Reuters, 13 July 2016. http://www.reuters.com/article/us-russia-newspaper-idUSKCN0ZT0EU.
[70] The Economist, 'Russian media firms: Interesting news', *The Economist*, 8 November 2014. http://www.economist.com/node/21631057/print.
[71] Andrei Malgin, 'Russia's State Media Get Away With Murder', *Moscow Times*, 4 November 2014. http://www.themoscowtimes.com/opinion/article/russia-s-state-media-get-away-with-murder/510619.html. See also 'Russian media firms: Interesting news', *The Economist*.
[72] Christina Cottiero, Katherine Kucharski, Evgenia Olimpieva and Robert W. Orttung, 'War of words: the impact of Russian state television on the Russian Internet', *Nationalities Papers: The Journal of Nationalism and Ethnicity*, March 2015.
[73] Gary Shteyngart, 'Out of My Mouth Comes Unimpeachable Manly Truth', *New York Times*, 18 February 2015. http://www.nytimes.com/2015/02/22/magazine/out-of-my-mouth-comes-unimpeachable-manly-truth.html.
[74] Michael Birnbaum, "Russia's Putin signs law extending Kremlin's grip over media", The Washington Post, 15 October 2014. https://www.washingtonpost.com/world/europe/russias-putin-signs-law-extending-kremlins-

expectations, this does not automatically lead to its content or narratives being rejected, even by the educated and well-travelled sections of the Russian-speaking audience.[75]

Information control is further tightened by measures, such as censoring school textbooks, so that the Russian domestic audiences develop the approved vision not only of current events but also of history.[76] And in a direct echo of Soviet and Tsarist repression of thought, Russia has already begun the criminalisation of alluding to historical facts which are inconvenient for current state narratives.[77] There is an important distinction between this process and a Western academic tradition which can now accept 'history' as a competition of narratives and interpretations rather than a collection of facts. Rather than selective emphasis and open debate, the current (and traditional) Russian approach is reliant instead on enforced amnesia regarding inconvenient events, and promotion of officially-sponsored falsifications.

The regaining of control over domestic information space has been a continuous process dating almost from the arrival in power of President Putin in 2000. In recent years it has both accelerated and spread to the previously unrestricted internet. Russian domestic audiences have become dramatically more isolated from alternative sources of information.[78] This isolation is not total and hermetic in the same way as during periods of the Cold War – it is still possible for interested Russian domestic audiences to access foreign media via the internet, if they wish. Internet usage monitoring, filtering and misleading translation of foreign media reports online, also contribute to the isolating effect.[79] The Russian Security Council is reported even to have considered the implications of the country operating without internet access altogether.[80]

The consequences for NATO nations are twofold. First, the challenge to strategic communications is evident; it is hard to counter Russian disinformation about the role, nature and activities of NATO among the Russian population when the Russian state is working hard to prevent or influence their access to this kind of undesirable information. In addition, isolation facilitates distortion. It is easy for Russian media outlets to provide accounts or translations of statements by foreign leaders or organisations which are misleading or entirely false, without being challenged within the country.[81]

Second, these efforts to isolate the Russian domestic population from a true picture of events both in the outside world and in their own country help Russian authorities promote the

---

grip-over-media/2014/10/15/6d9e8b2c-546b-11e4-809b-8cc0a295c773_story.html.

[75] J. Szostek, "News media repertoires and strategic narrative reception: A paradox of dis/belief in authoritarian Russia", *New Media & Society*, 7 July 2016. http://nms.sagepub.com/content/early/2016/07/01/1461444816656638.abstract.

[76] Sasha Mordovets and Steven Lee Myers, 'Putin's Friend Profits in Purge of Schoolbooks', The New York Times, 1 November 2014. http://mobile.nytimes.com/2014/11/02/world/europe/putins-friend-profits-in-purge-of-schoolbooks.html.

[77] Halya Coynash, "Russian fined for reposting that the USSR & Nazi Germany invaded Poland", Human Rights in Ukraine, 1 July 2016, http://khpg.org/en/index.php?id=1467327913.

[78] See also the extensive review of this process by Jill Dougherty, 'How the Media Became One of Putin's Most Powerful Weapons', The Atlantic, 21 April 2015. http://www.theatlantic.com/features/archive/2015/04/how-the-media-became-putins-most-powerful-weapon/391062/.

[79] Keir Giles, "Putin's troll factories: How Moscow controls access to western media", *The World Today*, July 2015. https://www.academia.edu/14901643/The_information_war_Putins_troll_factories.

[80] Keir Giles, 'As sanctions bite, could Russia isolate itself by switching off the net?', *The World Today*, November 2014.

[81] "Lies, Damn Lies and Translation: Mucking With Quotes in Russian", Stopfake.org, 10 June 2016. http://www.stopfake.org/en/lies-damn-lies-and-translation-mucking-with-quotes-in-russian/.

notion of a Russia under threat from an aggressive, expansionist West, by preventing domestic media users from measuring against reality. The result is broad acceptance, at least in public, of the version of reality endorsed by the Russian state. One damaging consequence is the tendency of the Russian political and military leadership to come to believe their own propaganda.

> *[P]sychological tendency to accept ultimately as real an image of the external world which may have been utilized originally for purely domestic purposes... the leadership may very well believe what it tells its subjects about the external non-Soviet world and yet also recognize the usefulness of this image as a means of exacting greater sacrifices from them.*[82]

The most dangerous implication of the Russian leadership believing what they tell the Russian domestic population is the possibility that they could also then act on that belief.

Outlook and Conclusions

The challenge of Russian information warfare is, however, not a static situation, but a developing and evolving process. The Russian approach evolves, develops, adapts, and - just like other Russian operational approaches - identifies success and reinforces it, and conversely abandons failed attempts and moves on. The result is that Russia should not be expected to fight the last war when it next decides to use an information warfare component in a new conflict. In other words, those nations or organisations that think they understand Russian information warfare on the basis of current studies and are responding by preparing for currently visible threats and capabilities, are out of date and will be surprised once again by what happens next.

At the same time, awareness of the challenge of Russian information warfare is the most potent defence against it. Western nations were initially slow to respond to the multifaceted nature of Russia's developing online capabilities. Until recently, the focus in the West was almost exclusively on countering technical threats in the cyber realm, while neglecting the additional capabilities that Russia was building up in other areas of information warfare. But the striking difference in effect between Russian attempts to influence the US and French presidential elections in 2016 and 2017 point to the power of public recognition of the threat, allowing society, media and government to put in place appropriate defences.

Another essential first step to countering information warfare threats is to establish whether, and where, they have the potential to cause real damage when the aim is less ambitious than high-level political influence. There has been little visible effort in the West to quantify just how successful and effective Russia's subversion and disinformation campaigns really are. This raises the risk of resources and countermeasures being misdirected against threats that are ineffective and can reasonably be simply monitored, while others cause actual harm but are overlooked.

Broad but detailed study of mass consciousness to assess its resilience while under concentrated foreign attack would be challenging for Western societies but not unprecedented.[83] But another

[82] John Reshetar, Problems of Analyzing and Predicting Soviet Behavior, New York: Doubleday, 1955, p. 9.
[83] Mass Observation Archive, Mass Observation 1937-1950s, MassObs.org.uk, undated. http://www.massobs.org.uk/mass-observation-1937-1950s.

key element of measurement is tracking Russian information campaigns through into the policy-making space, to determine whether and to what extent actual decisions are influenced by Moscow. On a computer, antivirus software monitors the integrity of critical systems and processes, assessing whether they have been affected by malicious data introduced from outside. Proper assessment of the effect, or lack of it, of Russian subversion requires an analogous system of monitoring for Western governments and political systems.

The allocation of responsibility for managing the challenge needs to be clear. Just as hybrid threats exploit the seams of responsibility between the armed forces and civilian agencies, blended technical and psychological attacks exploit the disconnect between technical defensive measures and those (if any) that are focused on societal resilience. Russia's holistic approach to use of cyber capability requires a closely coordinated response from government agencies which have traditionally focused on distinct areas of vulnerability.

The involvement of corporations provides an additional layer of complexity, and it must be recognised that the primary objective of entities such as Facebook and Twitter is generating profits rather than defending Western political systems. There are clear limits to the amount of pressure that can be brought on major internet corporations even through invocation of corporate social responsibility, but there are also some commonalities of interest in reducing their role in facilitating Russian information warfare campaigns. There can be no reasonable objection to social media taking firmer steps to prevent the hijacking of profiles of legitimate organisations and individuals for disinformation aims.[84] And it is in the interest of internet companies to accept cooperation with intelligence agencies, if this leads to greater understanding of technical security challenges[85] and how their systems are abused to carry out organised deceit of their users.[86]

In order to address the specific problem of disinformation - including in its new characterisation as fake news - social media should continue partnering with journalists and fact checkers to build trust,[87] even though this is only effective among media-literate users who take the time and effort to assess the legitimacy of sources.[88] Proposals for an open review and verification system for online media[89] with the aim of establishing a gold standard of fact checking and objectivity should be pursued, but they must recognise that any such system needs protection against the same kind of gaming and abuse as any other open forum to which Russia will have access. When

[84] Dean Obeidallah, "How Russian Hackers Used My Face to Sabotage Our Politics and Elect Trump", The Daily Beast, 27 September 2017. https://www.thedailybeast.com/how-russian-hackers-used-my-face-to-sabotage-our-politics-and-elect-trump.
[85] Jim Stavridis and Dave Weinstein, Obama's Disclosure About Russian Hacking Is A Cybersecurity Gold Mine, Huffington Post, 3 January 2017. https://www.huffingtonpost.com/entry/the-disclosure-of-russias-hacking-is-a-gold-mine-for-cybersecurity_us_5866b4cfe4b0eb5864894ed6.
[86] Mike Allen, How Big Tech is prepping for Russian propaganda backlash, Axios, 26 September 2017. https://www.axios.com/how-big-tech-is-prepping-for-backlash-on-russian-propaganda-2489717745.html.
[87] Amol Rajan, "Germany Leads Fightback Against Fake News", BBC News, 16 February 2017. http://www.bbc.co.uk/news/entertainment-arts-38991973.
[88] Eileen Brown, "9 out of 10 Americans don't fact-check information they read on social media", ZDNet, 10 May 2017. http://www.zdnet.com/article/nine-out-of-ten-americans-dont-fact-check-information-they-read-on-social-media/.
[89] Geoff Mulgan, "Truth and the media: a modest proposal", Nesta.org, 6 January 2017. http://www.nesta.org.uk/blog/truth-and-media-modest-proposal.

countering disinformation, the response should be as engaging and interesting as the original fake news. Simple explanations that news is fake are not sufficient to engage target audiences. Countermeasures should focus not on the detail, but on the deceit - letting ordinary users know they have been taken as fools by Russia, rather than engaging in dry and detailed explanations of how it was done.

Finally, countermeasures must be flexible and adaptable; with a range of capabilities tested by Moscow but not yet deployed, success in countering one set of Russian tactics will cause a switch to another. If defenders are not prepared to be alert and agile, then as noted above they will once more be taken by surprise.

REFERENCES

Aaltola, M., "Cyber Attacks Go Beyond Espionage: The Strategic Logic of State-sponsored Cyber Operations in the Nordic-Baltic Region", Finnish Institute of International Affairs Briefing Paper 200 (2016), 29 August 2016. http://www.fiia.fi/en/publication/606/cyber_attacks_go_beyond_espionage/.

Alberque, W., "'Substantial Combat Forces' in the Context of NATO-Russia Relations", NATO Defense College Research Paper No. 131, July 2016. http://www.ndc.nato.int/download/downloads.php?icode=493.

Allen, Mike, How Big Tech is prepping for Russian propaganda backlash, Axios, 26 September 2017. https://www.axios.com/how-big-tech-is-prepping-for-backlash-on-russian-propaganda-2489717745.html.

Antonovich, Pavel, "Cyberwarfare: Nature and Content", *Military Thought*, No.3, Vol.20, 2011. pp. 35-43.

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

Birnbaum, Michael, "Russia's Putin signs law extending Kremlin's grip over media", The Washington Post, 15 October 2014. https://www.washingtonpost.com/world/europe/russias-putin-signs-law-extending-kremlins-grip-over-media/2014/10/15/6d9e8b2c-546b-11e4-809b-8cc0a295c773_story.html.

Blank, Stephen, "Can Information Warfare Be Deterred?", Defense Analysis, Volume 17, No. 2, 2001. p. 132.

Blank, Stephen, "Signs of New Russian Thinking About the Military and War", Eurasia Daily Monitor, 12 February 2014.

Brangetto, P. and Veenendaal, M.A., "Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations", in N.Pissanidis et. al. (eds.), *8th International Conference on Cyber Conflict*, NATO Cooperative Cyber Defence Centre of Excellence, June 2016. https://ccdcoe.org/sites/default/files/multimedia/pdf/CyCon_2016_book.pdf.

Brewster, Murray, "Canada to send troops to Latvia for new NATO brigade", CBC News, 30 June 2016. http://www.cbc.ca/news/politics/nato-canadian-troops-baltics-1.3659814.

Brown, Eileen, "9 out of 10 Americans don't fact-check information they read on social media", ZDNet, 10 May 2017. http://www.zdnet.com/article/nine-out-of-ten-americans-dont-fact-check-information-they-read-on-social-media/.

Chekinov, S. G. and Bogdanov, S.A., "Влияние непрямых действий на характер современной войны" (The influence of the indirect approach on the nature of modern warfare), *Voyennaya mysl'*, No. 6, 2011. pp. 3-13.

Chekinov, S. G. and Bogdanov, S.A., “Прогнозирование характера и содержания войн будущего: проблемы и суждения” (Forecasting the nature and content of wars of the future: problems and assessments), *Voennaya Mysl’, Military Thought*, No. 10, 2015. pp. 44-45.

Chekinov, S. G. and Bogdanov, S.A., “Initial Periods of Wars and Their Impact on a Country's Preparations for a Future War”, *Military Thought* (English edition), No 4 2012. pp. 24-25.

Chekinov, S. G. and Bogdanov, S.A., “The Nature and Content of a New-Generation War", *Military Thought* (English edition), No. 4, 2013.

Cottiero, Christina, Kucharski, Katherine, Olimpieva, Evgenia and Orttung, Robert W., “War of words: the impact of Russian state television on the Russian Internet”, *Nationalities Papers: The Journal of Nationalism and Ethnicity*, March 2015.

Coynash, Halya, "Russian fined for reposting that the USSR & Nazi Germany invaded Poland", Human Rights in Ukraine, 1 July 2016. http://khpg.org/en/index.php?id=1467327913.

Darczewska, Jolanta, "The Devil Is In The Details: Information Warfare In The Light Of Russia’s Military Doctrine", OSW Point of View No. 50, May 2015.

De Custine, A., *Lettres de Russie: La Russie en 1839*, P. Nora (ed.), Gallimard, 1975.

Donskov, Yu. E. and Nikitin, O.G., "Место и роль специальных информационных операций при разрешении военных конфликтов" (The place and role of special information operations in resolving military conflicts) *Voyennaya mysl'*, No. 6, 2005. pp. 17-23.

Dougherty, Jill, ‘How the Media Became One of Putin’s Most Powerful Weapons’, *The Atlantic*, 21 April 2015. http://www.theatlantic.com/features/archive/2015/04/how-the-media-became-putins-most-powerful-weapon/391062/.

Ennis, Stephen, "Russia's fixation with 'information war'", BBC News, 26 May 2016. http://www.bbc.co.uk/monitoring/russias-fixation-with-information-war.

Estonian Internal Security Service, Annual Review 2015, Estonian Internal Security Service (KAPO), 2015. pp. 12-15. https://kapo.ee/sites/default/files/public/content_page/Annual%20Review%202015.pdf.

Fisher, Max, "In D.N.C. Hack, Echoes of Russia’s New Approach to Power", The New York Times, 25 July 2016. http://www.nytimes.com/2016/07/26/world/europe/russia-dnc-putin-strategy.html.

Foster, P. and Holehouse, M., "Russia accused of clandestine funding of European parties as US conducts major review of Vladimir Putin's strategy", Daily Telegraph, 16 January 2016. http://www.telegraph.co.uk/news/worldnews/europe/russia/12103602/America-to-investigate-Russian-meddling-in-EU.html.

Galeotti, Mark, "Hybrid, ambiguous, and non-linear? How new is Russia's 'new way of war'?", Small Wars & Insurgencies, Vol. 27 No. 2, 2016. p. 291.

Geers, Kenneth (ed.), "Cyber War in Perspective: Russian Aggression against Ukraine", NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), December 2015.

Gerasimov, Valeriy, "*Tsennost nauki v predvidenii*" (The Value Of Science Is In Foresight), *Voyenno-promyshlennyy kuryer*, No. 8 (476), 27 February 2013.

Gerasimov, Valeriy, "По опыту Сирии" (Based on the experience of Syria), *Voyenno-promyshlennyy kur'er*, 9 March 2016. http://vpk-news.ru/sites/default/files/pdf/VPK_09_624.pdf.

Gerden, Eugene, "Russia to spend $250m strengthening cyberoffensive capabilities", SC Magazine UK, 4 February 2016. http://www.scmagazineuk.com/russiatospend250mstrengtheningcyberoffensivecapabilities/printarticle/470733/.

Giles, Keir, "As sanctions bite, could Russia isolate itself by switching off the net?", The World Today, November 2014.

Giles, Keir, "Putin's troll factories: How Moscow controls access to western media", The World Today, July 2015. https://www.academia.edu/14901643/The_information_war_Putins_troll_factories.

Giles, Keir, "Russia's Public Stance on Cyberspace Issues", in C. Czosseck, R. Ottis, K. Ziolkowski (Eds.), *2012 4th International Conference on Cyber Conflict*, Tallinn, June 2012. pp. 63-75.

Giles, Keir, "Russia's Toolkit", chapter in "The Russian Challenge", Chatham House, London, June 2015.

Giles, Keir, and Hagestad, W., "Divided by a Common Language: Cyber Definitions in Chinese, Russian and English", in K. Podins et al (eds.), *5th International Conference on Cyber Conflict*, CCDCOE, Tallinn, 2013, https://ccdcoe.org/publications/2013proceedings/d3r1s1_giles.pdf.

Grau, Lester and Thomas, Timothy L., "A Russian View of Future War: Theory and Direction", *Journal of Slavic Military Studies*, issue 9.3, September 1996. pp. 501–518.

Heickerö, Roland, "Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations", FOI, March 2010. p. 20. www.foi.se/ReportFiles/foir_2970.pdf.

House of Commons of the United Kingdom, Oral evidence: Russia: Implications for UK Defence and Security, HC 763, House of Commons Defence Committee, 1 March 2016. http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/defence-committee/russia-implications-for-uk-defence-and-security/oral/29915.html.

House of Commons of the United Kingdom, "Russia: Implications for UK defence and security", First Report of Session 2016–17, House of Commons Defence Committee, UK

Parliament, 5 July 2016, p. 17.

Interfax-AVN news agency, 31 January 2008.

Kamp, Karl-Heinz, "Russia's myths about NATO: Moscow's propaganda ahead of the NATO Summit", Federal Academy for Security Policy Working Paper No. 15, 2016. https://www.baks.bund.de/sites/baks010/files/working_paper_15_2016.pdf.

Kartapolov, A. V., "Уроки военных конфликтов, перспективы развития средств и способов их ведения. Прямые и непрямые действия в современных международных конфликтах" (Lessons of military conflicts and prospects for the development of means and methods of conducting them. Direct and indirect actions in contemporary international conflicts," *Vestnik Akademii Voennykh Nauk* (Bulletin of the Academy of Military Science), No. 2 2015. pp. 28-29.

Kincaid, Cliff, "How Putin Uses KGB-style 'Active Measures'", Accuracy in Media, 9 April 2014. http://www.aim.org/aim-column/how-putin-uses-kgb-style-active-measures/.

Klapsis, A. "An Unholy Alliance: The European Far Right and Putin's Russia", Wilfried Martens Centre for European Studies, undated. http://www.martenscentre.eu/sites/default/files/publication-files/far-right-political-parties-in-europe-and-putins-russia.pdf.

Kuleshov, Yu. et al., "Информационно-психологическое противоборство в современных условиях: теория и практика" (Information-Psychological Warfare In Modern Conditions: Theory And Practice), *Vestnik Akademii Voyennykh Nauk* No. 1 (46), 2014. pp. 106.

Kuzio, Taras, "When an academic ignores inconvenient facts", New Eastern Europe, 21 June 2016. http://www.neweasterneurope.eu/articles-and-commentary/books-and-reviews/2035-when-an-academic-ignores-inconvenient-facts.

Kvachkov,V., *Спецназ Россиu (Russia's Special Purpose Forces),* Voyennaya Literatura, 2004. http://militera.lib.ru/science/kvachkov_vv/index.html.

Lisovoy, V.M., "*O zakonakh razvitiya vooruzhennoy bor'by i nekotorykh tendentsiyakh v oblasti oborony*", *Voyennaya Mysl',* Issue 5, 1993.

Lisovoy, V.M., Speech to the Swedish Defence Research Agency, Stockholm, 5 October 2010.

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.

Maldre, Patrik, "The Many Variants of Russian Cyber Espionage", Atlantic Council, 28 August 2015. http://www.atlanticcouncil.org/blogs/natosource/the-many-variants-of-russian-cyber-espionage

Malgin, Andrei, 'Russia's State Media Get Away With Murder', Moscow Times, 4 November 2014. http://www.themoscowtimes.com/opinion/article/russia-s-state-media-get-away-with-murder/510619.html.

Malyshev, V., "Использование возможностей средств массовой информации в локальных вооруженных конфликтах" (Making use of the media in local armed conflicts), *Zarubezhnoye voyennoye obozreniye*, No. 7, 2000, pp. 2-8.

Mass Observation Archive, Mass Observation 1937-1950s, MassObs.org.uk, undated. http://www.massobs.org.uk/mass-observation-1937-1950s.

Military Academy of the General Staff of the Armed Forces of the Russian Federation, "*Slovar' terminov i opredeleniy v oblasti informatsionnoy bezopasnosti*", Voyennaya Akademiya General'nogo Shtaba, 2nd Edition, Moscow Voyeninform, 2008.

Mordovets, Sasha and Lee Myers, Steven, 'Putin's Friend Profits in Purge of Schoolbooks', *The New York Times*, 1 November 2014. http://mobile.nytimes.com/2014/11/02/world/europe/putins-friend-profits-in-purge-of-schoolbooks.html.

Mshvidobadze, K., "The Battlefield On Your Laptop", Radio Free Europe/Radio Liberty, 21 March 2011. http://www.rferl.org/articleprintview/2345202.html.

Mulgan, Geoff, "Truth and the media: a modest proposal", Nesta.org, 6 January 2017. http://www.nesta.org.uk/blog/truth-and-media-modest-proposal.

Nimmo, Ben, "Anatomy of an Info-War: How Russia's Propaganda Machine Works, and How to Counter It", 19 May 2015. http://www.stopfake.org/en/anatomy-of-an-info-war-how-russia-s-propaganda-machine-works-and-how-to-counter-it/.

Novyy Region, "Russia is underestimating information resources and losing out to the West", Novyy Region, 29 October 2008.

Obeidallah, Dean, "How Russian Hackers Used My Face to Sabotage Our Politics and Elect Trump", The Daily Beast, 27 September 2017. https://www.thedailybeast.com/how-russian-hackers-used-my-face-to-sabotage-our-politics-and-elect-trump.

Pfeffercorn, R. "Security Risks of Government Hacking", The Center for Internet and Society, September 2018. https://cyberlaw.stanford.edu/files/publication/files/2018.09.04_Security_Risks_of_Government_Hacking_Whitepaper.pdf.

Polyakova, Alina, "Why Europe Is Right to Fear Putin's Useful Idiots", Foreign Policy, 23 February 2016. http://foreignpolicy.com/2016/02/23/why-europe-is-right-to-fear-putins-useful-idiots/.

Putin, Vladimir, "Солдат есть звание высокое и почетное" ('Soldier' is an honourable and respected rank), excerpts from annual Address to the Federal Assembly of the Russian Federation, *Krasnaya zvezda*, 11 May 2006. http://old.redstar.ru/2006/05/11_05/1_01.html.

Pynnöniemi, Katri and Rácz, A., (eds.), *Fog of Falsehood: Russian Strategy of Deception*

and the Conflict in Ukraine, FIIA Report No. 45, undated. p. 38.

Rajan, Amol, "Germany Leads Fightback Against Fake News", BBC News, 16 February 2017. http://www.bbc.co.uk/news/entertainment-arts-38991973.

Reshetar, John, *Problems of Analyzi Problems of Analyzing and Predicting Soviet Behavior*, New York: Doubleday, 1955. p. 9.

RT, "Intellectual level of British leadership so low, it's shocking - European politics scholar", RT, 19 February 2016. https://www.rt.com/shows/sophieco/332958-intellectual-level-british-leadership/.

Russian Federation, "Basic Principles for State Policy of the Russian Federation in the Field of International Information Security to 2020, Approved by the President of the Russian Federation", 24 July 2013.

Selhorst, A.J.C. ,"Russia's Perception Warfare", *Militaire Spectator*, 185 No. 4, 2016. p. 151.

Sharavov, I., "К вопросу об информационной войне и информационном оружии" (On the issue of information war and information weapons), *Zarubezhnoye voyennoye obozreniye*, No. 10, 2000. pp. 2-5.

Shteyngart, Gary, 'Out of My Mouth Comes Unimpeachable Manly Truth', The *New York Times*, 18 February 2015. http://www.nytimes.com/2015/02/22/magazine/out-of-my-mouth-comes-unimpeachable-manly-truth.html.

Slipchenko, V.I., "Future War (A Prognostic Analysis)", January 1998.

Slipchenko, V.I., "Информационный ресурс и информационное противоборство" (Information Resources and Information Confrontation) *Armeyskiy sbornik*, October 2013. p. 52.

Smith, D. J., "How Russia Harnesses Cyberwarfare", Defense Dossier, American Foreign Policy Council, Issue 4, August 2012. p. 8, http://www.afpc.org/files/august2012.pdf.

Stavridis, Jim and Weinstein, Dave, Obama's Disclosure About Russian Hacking Is A Cybersecurity Gold Mine, Huffington Post, 3 January 2017. https://www.huffingtonpost.com/entry/the-disclosure-of-russias-hacking-is-a-gold-mine-for-cybersecurity_us_5866b4cfe4b0eb5864894ed6.

StopFake, "Lies, Damn Lies and Translation: Mucking With Quotes in Russian", Stopfake.org, 10 June 2016. http://www.stopfake.org/en/lies-damn-lies-and-translation-mucking-with-quotes-in-russian/.

J. Szostek, "News media repertoires and strategic narrative reception: A paradox of dis/belief in authoritarian Russia", *New Media & Society*, 7 July 2016. http://nms.sagepub.com/content/early/2016/07/01/1461444816656638.abstract.

The Economist, 'Russian media firms: Interesting news', *The Economist*, 8 November 2014.

http://www.economist.com/node/21631057/print.

Thomas, Timothy L., “Dialectical versus Empirical Thinking: Ten Key Elements of the Russian Understanding of Information Operations”, *Journal of Slavic Military Studies*, Vol.11, No.1, 1998. pp. 40-62.

Thomas, Timothy L., “Information Security Thinking: A Comparison of U.S., Russian, And Chinese Concepts”, Foreign Military Studies Office, July 2001. http://fmso.leavenworth.army.mil/documents/infosecu.htm.

Thomas, Timothy L., "Russia’s Information Warfare Strategy: Can the Nation Cope in Future Conflicts?", The Journal of Slavic Military Studies, 10 March 2014. pp. 101-130.

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

Tsvetkova, M. and Devitt, P. "Russian editors 'fired over stories that irked officials'", Reuters, 13 July 2016. http://www.reuters.com/article/us-russia-newspaper-idUSKCN0ZT0EU.

UK Foreign and Commonwealth Ministry, “Soviet Propaganda In Western Europe’, UK Foreign & Commonwealth Office via PsyWar.org, March 1982. http://www.psywar.org/radSovietPropaganda.php.

United States Senate Armed Services Committee, James R. Clapper, US Director of National Intelligence, Worldwide Threat Assessment of the US Intelligence Community, Senate Armed Services Committee Statement for the Record, 26 February 2015.

Vorobyov, I. N. and Kiselev, V. A., "Гибридные операции как новый вид военного противоборства" (Hybrid operations as a new form of armed conflict), *Voyennaya mysl'*, No. 5, 2015. pp. 41-49.

Watkins, Ali, “Senate Committee Looks To Revive Cold War Era Body To Catch Russian Spies”, Buzzfeed, 21 June 2016. https://www.buzzfeed.com/alimwatkins/senate-committee-looks-to-revive-cold-war-era-body-to-catch.

Wesolowsky, T. "Kremlin Propaganda In Czech Republic Plays Long Game To Sow Distrust In EU", RFE/RL, 16 June 2016, http://www.rferl.org/content/czech-kremlin-propaganda-plays-long-game-sow-eu-distrust/27802234.html.

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.)

The Russian Information Warfare Construct

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	29	89

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	

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-C241	

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.)

Russian Political Warfare; Russia; Influence; Information Warfare; Cyber warfare; Active Measures

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

This report discusses the Russian information warfare construct by tracing the concept of Russian information warfare back to the enduring principles of the Russian approach to competition between states. This report argues that the current Russian information warfare construct is in no way a new phenomenon. Instead, the construct is only extensively updated and renewed as part of Russia's recent preparations for conflict in conditions of overall conventional inferiority. After introducing essential concepts and important terminology, the report focuses on discussing particularly aims and objectives of current Russian information warfare.

Ce rapport traite de la construction de la guerre de l'information russe en retraçant le concept de guerre de l'information russe jusqu'aux principes durables de l'approche russe de la concurrence entre États. Ce rapport affirme que la construction actuelle de la guerre de l'information en Russie n'est en aucun cas un phénomène nouveau. Au lieu de cela, le concept n'est actualisé et renouvelé que dans le cadre des récents préparatifs de la Russie en vue d'un conflit dans des conditions d'infériorité conventionnelle globale. Après avoir introduit des concepts essentiels et une terminologie importante, le rapport se concentre sur les buts et objectifs de la guerre de l'information en Russie.