NATO Defense College
Collège de Défense de l'OTAN

HANDBOOK OF RUSSIAN INFORMATION WARFARE

Keir Giles

FELLOWSHIP MONOGRAPH

RESEARCH DIVISION
NATO DEFENSE COLLEGE

9

November 2016

Keir Giles is an Associate Fellow of the Royal Institute of International Affairs (Chatham House) in London. He also works with Conflict Studies Research Centre, a group of subject matter experts in Eurasian security based in Cambridge.

Handbook of Russian Information Warfare

NATO DEFENSE COLLEGE
COLLEGE DE DEFENSE DE L'OTAN
Fellowship Monograph

Handbook of Russian Information Warfare

Keir Giles

Rome, November 2016

NATO DEFENSE COLLEGE

NATO Defense College Cataloguing in Publication-Data:
Handbook of Russian Information Warfare

(NATO Defense College "NDC Fellowship Monograph Series")

Fellowship Monograph 9
by Keir Giles

ISBN: 978-88-96898-16-1

The Research Division (RD) of the NATO Defense College provides NATO's senior leaders with sound and timely analyses and recommendations on current issues of particular concern for the Alliance. Papers produced by the Research Division convey NATO's positions to the wider audience of the international strategic community and contribute to strengthening the Transatlantic Link.

The RD's civil and military researchers come from a variety of disciplines and interests covering a broad spectrum of security-related issues. They conduct research on topics which are of interest to the political and military decision-making bodies of the Alliance and its member states.

The opinions expressed are those of the authors and do not necessarily reflect the opinions of the North Atlantic Treaty Organization or the NATO Defense College.

Printed copies of this paper can be obtained by contacting Mary Di Martino at
m.dimartino@ndc.nato.int

Limited print copies of this Fellowship Monograph may be obtained directly from:
NATO Defense College, Research Division
Via Giorgio Pelosi 1 – 00143 Rome, Italy
Jeffrey A. Larsen, PhD, Director

Website: http://www.ndc.nato.int
Follow us on twitter, https://twitter.com/NDC_Research

Printed and bound by
DeBooks Italia srl
V.le G. Mazzini 41, 00195 Rome, Italy
www.debooks.us

Table of Contents

Notes on the Text

This handbook provides an introductory guide to the Russian concept of information warfare, including elements of cyber warfare. The handbook's target audience is NATO servicemen and officials who have not previously studied Russian principles of warfighting, but require an introduction to current and projected Russian operations in the information and cyber domains. The guide also functions as a source book for further detailed research as required.

The period since the Russian seizure of Crimea in early 2014 has seen a large number of new publications on the topic of Russian cyber and information warfare, of widely varying quality. Most of these works discuss a specific aspect of the challenge, and many were highly time-sensitive and are therefore already outdated. The aim of this handbook is instead to circumvent the need for extensive *ab initio* research by providing a guide to the Russian approach which is both comprehensive and durable.

The guide takes as its basis material already in the public domain; this material has been collated from a wide range of disparate and sometimes obscure publications in Russian and other languages. Where possible, key concepts and approaches are illustrated and explained by direct quotations from senior members of the Russian defence and security communities. Unless otherwise specified, quotations in the text are from Russian sources, in many cases authoritative papers and essays on the theory and practice of warfare from military journals and conferences. Although not all the sources quoted are ordinarily available to the public, no classified material has been used.

It should be noted that the majority of these Russian sources present their research and findings as describing not Russia's own approaches, but the approaches which they say are adopted by foreign

powers seeking to harm Russia. In some cases, the principles described reflect not home-grown theory, but Russian adoption of what it believes to be Western practice.

In addition to extensive citations in footnotes, each section concludes with a list of recommended reading for deeper research on specific topics. Russian-language titles here and in the citations have been translated into English. URLs for online access to publications have been provided where they are known and available.

Translations from Russian are the author's own unless otherwise specified.

Handbook of Russian Information Warfare

1. 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 Russian instruments of power, the concept of information warfare has become the subject of sudden intense interest in the West since the start of the crisis over Ukraine in 2014. However, also in common with aspects of Russian power which had been largely disregarded since the end of the Soviet Union, it 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]

Sections in this guide cover the basic concepts and terminology of Russian information warfare; its aims and objectives; the history and development of the current approach, and what can be learned from it; features of current implementation by Russia; and finally, rapid and ongoing evolution and possible future challenges. Two themes recur

1 V. Kvachkov, Спецназ России (Russia's Special Purpose Forces), Voyennaya Literatura, 2004, http://militera.lib.ru/science/kvachkov_vv/index.html (accessed 21 July 2016). 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 (accessed 22 June 2016).

throughout the handbook: the waging of information warfare during notional peacetime; and the holistic, all-encompassing nature of the "information" that is both the subject and the medium of the conflict.

In the Russian construct, information warfare is not an activity limited to wartime. 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] "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 one – which it describes as limited, tactical information operations carried out during hostilities.[6] For Russia, contest with the West in the information domain has already begun. Ongoing information warfare is "a regular feature of the country's news and current affairs coverage."[7]

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 by concerned citizens, YouTube videos, or direct approaches to individual human targets. Recent Russian campaigning provides examples of all of the above and more.

---

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

4 R. Heickerö, "Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations," Swedish Defence Research Establishment (FOI), 2010, w*ww.foi.se/ReportFiles/foir_2970.pdf,* p. 20.

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

6 Словарь терминов и определений в области информационной безопасности, *Voyennaya Akademiya General'nogo Shtaba*, 2nd Edition, Moscow Voyeninform, 2008.

7 As described in a BBC Monitoring media survey. See Stephen Ennis, "Russia's fixation with 'information war,'" BBC News, 26 May 2016, http://www.bbc.co.uk/monitoring/russias-fixation-with-information-war (accessed 6 July 2016).

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 tasks." 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.

2. Essential Concepts and Terminology

For Russia, "information confrontation" or "information war" is a broad and inclusive concept covering a wide range of different activities.[8] 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, along with "intelligence, counterintelligence, *maskirovka*, disinformation, electronic warfare, debilitation of communications, degradation of navigation support, psychological pressure, and destruction of enemy computer capabilities."[9] Taken together, this forms "a whole of systems, methods, and tasks to influence the perception and behavior of the enemy, population, and international community on all levels."[10]

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

> *"Wars will be resolved by a skillful 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,*

8 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.

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

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

various social networks, and other resources).”[11]

This blending and coordination between different informational tools 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 conspicuous by its absence, as is a coherent overall approach. According to one 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.

“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.

“Cyber” as a separate function or domain is not a Russian concept.

---

11 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.

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 (accessed 20 June 2016).

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, "Distributed denial of services attacks (DDoS), advanced [cyber] exploitation techniques and Russia Today television are all related tools of information warfare."[13]

The phrase "cyber warfare" in Russian writing describes foreign concepts and activities, which do observe this distinction between information activities on computers and networks and those "in real life." Consequently, searches for "cyber" in Russian sources primarily return references to Western doctrine and thinking. It follows that any research on Russian capabilities and intentions which includes the word "cyber" 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 establishing its own cyber command,"[14] and related reports on boosting military cyber capabilities,[15] even when they have any basis in fact, appear to refer to very different organisations and notions than the words suggest to NATO ears.

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 bodies which prosecute not only CNO but other aspects of information warfare is extremely challenging, given their deeply classified nature.[16] Detailed and factual public announcements,

13 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 (accessed 15 July 2016).

14 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.

15 Eugene Gerden, "Russia to spend $250m strengthening cyberoffensive capabilities," SC Magazine UK, 4 February 2016, http://www.scmagazineuk.com/russiatospend250mstrengtheningcyberoffensivecapabilities/printarticle/470733/ (accessed 14 June 2016).

16 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

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, discussion based on open sources of how Russia organises and directs its information warfare efforts – in effect, who does what within the Russian system – is largely speculative, and consequently is not included in this handbook.

Instead of cyberspace, Russia refers to "information space," and includes in this space both computer and human information processing, in effect the cognitive domain.[17] Within information space, the closest Russian thinking comes to separating out CNO from other activities is division into the information-technical and information-psychological domains, the two main strands of information warfare in Russian thinking.[18] 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."*[19]

It should be noted that "cyber" activities do not map directly to the "information-technological" domain: as an integral part of information warfare overall, they are also inherent and utilised in information-

functions absorbed into other government departments. See G. Bennett, *The Federal Agency of Government Communications & Information*, Conflict Studies Research Centre, Sandhurst, August 2000.

17 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 (accessed 15 July 2016).

18 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.

19 V. Kvachkov, Спецназ России (Russia's Special Purpose Forces), *op. cit*.

psychological operations. It is also important to note that some operations in both domains are undertaken "permanently" – regardless of the notional state of cooperation or hostility between the opposing sides.

The key word therefore is *information*. In the Russian conceptual framework, this 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 as that held on an adversary's computer or smartphone. Similarly, the transmission or transfer of this information can be by any means: so 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, crucially including the human cognitive domain.[20] But even within CNO, an information weapon need not necessarily have a destructive real-world effect in the style of Stuxnet. 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."[21]

Importantly, multiple senior Russian officials have reinforced the point that open conflict need not have been declared for hostile activity in information space to begin. To take just one example, this includes former Deputy Chief of the General Staff Lt-Gen Aleksandr Burutin, who noted in January 2008 that information weapons can be "used in an efficient manner in peacetime as well as during war."[22] This points

20 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 (accessed 4 July 2016).

21 Prof. V. Lisovoy, speaking at Swedish Defence Research Agency, Stockholm, 5 October 2010.

22 Interfax-AVN news agency, 31 January 2008.

to another obvious asymmetry with NATO practice. As put 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."*[23]

At the same time, some previous Russian writers while discussing the permanent nature of information confrontation 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 overtly aggressive, and include "discrediting [adversary] leadership, intimidating military personnel and civilians... falsification of events, disinformation, hacking attacks and so forth."[24] Furthermore, "the main effort 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."[25] If measured by these criteria, recent Russian activities in the information domain would indicate that Russia already considers itself to be in a state of war.[26]

---

23 "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.

24 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; 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.

25 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.

26 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,

Implications

The scope and potentiality of information warfare in the Russian conception should not be measured against more recent Western concepts of information operations, or information activities, and in particular it should not be confused with cyber operations. The Ukraine conflict has provided clear demonstrations of how Russia sees cyber activity as a subset, and sometimes facilitator, of the much broader domain of information warfare.[27]

In the period since 2014, Russian information warfare has commonly come to be identified in non-specialist literature with the simple distribution of disinformation. But the Russian approach is much broader than simply sowing lies and denial, for instance maintaining that Russian troops and equipment are not where they plainly are. Instead, Russian state and non-state actors have exploited history, culture, language, nationalism, disaffection and more to carry out cyber-enhanced disinformation campaigns with much wider objectives. According to veteran US scholar of Russian information warfare principles Tim Thomas, writing in 1998:

> *[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.*[28]

The Western approach to cyber defence has typically focused on technical responses to technical threats, largely disregarding the interface

---

"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 (accessed 15 September 2016).

27 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/ (accessed 15 September 2016).

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

with information warfare in the broad sense. This approach is entirely apt for some persistent or background threats, but not always sufficient for a wider and more holistic approach like the one adopted by Russia.[29]

In other words, the West may be prepared to face "pure" cyber challenges, but the capabilities and intentions embraced by Russia and discussed in detail in later chapters show that it also needs to be prepared for information war when these are melded with disinformation, subversion, kinetic and EW operations, with highly ambitious aims up to and including regime change in the target state.

Further Reading

In English

- Dr A. Foxall, *Putin's Cyberwar: Russia's Statecraft in the Fifth Domain*, Policy Paper No. 9 (2016), Henry Jackson Society Russia Studies Centre, May 2016.

  (Provides a convenient list of recent targeted Russian cyber attacks.)

- T. Thomas, *Thinking Like a Russian Officer: Basic Factors and Contemporary Thinking on the Nature of War*, Foreign Military Studies Office, April 2016, http://fmso.leavenworth.army.mil/documents/Thinking%20Like%20A%20Russian%20Officer_monograph_Thomas%20(final).pdf (accessed 22 June 2016).

  (A guide to key elements of the framework of Russian planning and evaluation at the strategic and operational level, in information warfare and beyond.)

- K. Giles, "Russia's Public Stance on Cyberspace Issues," in C. Czosseck et al (eds.), *2012 4th International Conference on Cyber Conflict*, NATO CCDCOE, Tallinn, June 2012, https://ccdcoe.org/publications/2012proc

29 P. 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

eedings/2_1_Giles_RussiasPublicStanceOnCyberInformationWarfare.pdf (accessed 13 July 2016).

- "Stage 5: Information Warfare" in A. Grigas, *Beyond Crimea: The New Russian Empire*, Yale University Press, 2016, pp. 44-56.

- Unwala and S. Ghori, "Brandishing the Cybered Bear: Information War and the Russia-Ukraine Conflict," *Military Cyber Affairs*, Volume 1, Issue 1, http://scholarcommons.usf.edu/mca/vol1/iss1/7

- J. Weedon and L. Galante, "Intelligence Analysts Dissect the Headlines: Russia, Hackers, Cyberwar! Not So Fast," *FireEye Blogs*, March 12, 2014, https://www.fireeye.com/blog/executive-perspective/2014/03/intel-analysts-dissect-the-headlinesrussia-hackers-cyberwar-not-so-fast.html

- J. Darczewska, "Russia's armed forces on the information war front. Strategic documents," OSW Studies, 27 June 2016, http://www.osw.waw.pl/en/publikacje/osw-studies/2016-06-27/russias-armed-forces-information-war-front-strategic-documents

In Russian

- "Словарь терминов и определений в области информационной безопасности" (Dictionary of terms and definitions in the field of information security), *Voyennaya Akademiya General'nogo Shtaba*, 2nd Edition, Moscow Voyeninform, 2008.

  (This glossary of key Russian information security concepts is highly instructive, especially as it illustrates clearly many of the divergences between Russian and Western thinking on the nature of information warfare and computer network operations. In particular, it includes no entry for the term "cyber warfare.")

- "Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве" (Conceptual Views on the Activity of the Russian Federation Armed Forces in Information Space), *Russian Ministry of Defence*, 22 December 2011, http://ens.mil.ru/

science/publications/more.htm?id=10845074@cmsArticle (accessed 22 June 2016).

(A Russian military cyber proto-doctrine. Its explanation of how the Russian Armed Forces see their role in cyberspace is interesting but incomplete, focusing on situational and threat awareness and force protection, with no mention whatsoever of offensive cyber or information activity.)

3. Aims and objectives

Recently published Russian military theory gives information warfare an increasingly prominent role. Recognition that Russia cannot compete directly in conventional terms with NATO has led to persistent emphasis in public statements on finding asymmetric responses. Information warfare is presented as one of these responses, 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."*[30]

But in its more ambitious descriptions, information warfare is considered capable of avoiding the necessity of armed conflict altogether by achieving strategic goals on its own. As put by Mark Galeotti, Russia is showing

> *"willingness to give 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."*[31]

Information warfare campaigns can have a range of aims and objectives, both offensive and defensive, all of which are not necessarily mutually exclusive. Broad categories of objective are listed here in decreasing order of ambition, from use as a stand-alone tool for achieving geopolitical

30 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), *op. cit.*, pp. 44-45.

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

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 countercommand and control warfare."[32] But this is a more limited construct than the Russian approach, which is far more ambitious. Recent authoritative Russian papers on military theory state as follows:

- "Under today's conditions, means of information influence have reached a level of development such that they are capable of resolving strategic tasks."[33]
- "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)."[34]

Information activities as preparation for open conflict are nothing new. As put 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."*[35]

32 S. Blank, "Can Information Warfare Be Deterred?" *Defense Analysis* 17, No. 2 (2001), p. 132.

33 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.

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

35 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/

But in more recent constructs, 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."*[36]

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.[37]

It can be seen that the ultimate aim of this highly ambitious implementation of information warfare is in effect 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:

> *"…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 on the military-political leadership of the*

---

evidencedocument/defence-committee/russia-implications-for-uk-defence-and-security/oral/29915.html (accessed 5 July 2016).

36 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 (accessed 22 June 2016).

37 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.

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."[38]

"Reflexive control"

Reflexive control is the term used to describe the practice of predetermining an adversary's decision in Russia's favour, by altering key factors in the adversary's perception of the world.[39] As such, it represents a key asymmetric enabler to gain critical advantages, neutralising the adversary's strengths by causing him to choose the actions most advantageous to Russian objectives.[40]

Significantly, the phrase "reflexive control" is far more frequently encountered in recent Western writing about Russian information warfare principles than in original Russian sources. In Russian public discussion, the term appears to have been superseded, and at least partially replaced by "perception management" with a meaning similar to the Western understanding of this approach. The Russian phrase "рефлексивное управление" (additionally, "рефлексивный контроль") now primarily refers to "reflexive practice" in an educational or personnel management context. Nevertheless, given its widespread application in Western analysis, and the absence of a suitable replacement, "reflexive

38 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* No. 1 (46), 2014, p. 106.

39 An accessible summary of the Russian-language literature on principles of reflexive control is available in C. Kasapoglu, *Russia's Renewed Military Thinking: Non-Linear Warfare and Reflexive Control*, Research Paper 121, NATO Defense College, 25 November 2015, http://www.ndc.nato.int/news/news.php?icode=877 (accessed 23 June 2016).

40 See M. Snegovaya, "Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare." Institute for the Study of War, Russia Report I, September 2015, p. 9.

control" continues to offer a suitable descriptor for information activity of this kind.

An information campaign within this category need not be limited to influencing a single decision. Similarly to a skilful barrister cross-examining a witness, reflexive control can lead the adversary to make a series of decisions that successively discard options that would improve their position, until they are finally faced with a choice between bad and worse, either of which options would favour Russia.

Senior British analyst Charles Blandy describes the process as follows:

> *"Traditionally the Russian military mind, as embodied in the General Staff, looks further ahead than its Western counterpart, on the basis that 'foresight implies control.' Having made the 'decision,' the military mind works backwards from the selected objective to its present position. Subsidiary goals are identified for achieving the objective. The Soviet and Russian General Staffs over a long period of time have studied the application of reflexive control theory both for deception and disinformation purposes in order to influence and control an enemy's decision making processes, for:*
>
> *Control of an opponent's decision is achieved by means of providing him with the grounds by which he is able logically to derive his own decision, but one that is predetermined by the other side. This can be achieved:*
>
> - *By applying the pressure of force.*
> - *By assisting the opponent's formulation of an appreciation of the initial situation.*
> - *By shaping the opponent's objectives.*
> - *By shaping the opponent's decision making algorithm.*
> - *By the choice of the decision making moment."*[41]

41 C. Blandy, *Provocation, Deception, Entrapment: The Russo-Georgian Five Day War*, Defence Academy of the United Kingdom, March 2009, http://conflictstudies.org.uk/files/04.pdf (accessed 23 June 2016). This

This is a far broader approach than pure deception, or providing an adversary commander with false operational information on which to base his decision. Instead of consisting simply of disinformation, reflexive control implies a compound programme of targeting decision-making factors through multiple vectors. The Russian General Staff Military Academy's glossary of information security terms defines "agitation" (агитация) as "one of the forms of information-psychological influence on the emotional plane of the target or group of targets with the aim of achieving a specific psychological state which will lead to active and specific actions being taken."[42] More general and less specific propaganda and counter-propaganda efforts also play a role in establishing the information background for decision-making.

Critically, as with strategic objectives above, the target for reflexive control activity need not be limited to key decision-makers, but can include broader sections of the population as well – mass as well as individual cognitive domains:

> *"The targets for influence are both mass and individual consciousness. Those 'honoured' with individual influence are those persons whose decisions determine issues of interest to the adversary party (i.e. the president, the prime minister, head of the Ministry of Foreign Affairs, diplomatic representatives, commanders of military formations and so on). Information influence involves distorting facts, or envisages imposing on the target person emotional impressions which are favourable to the influencer."*[43]

---

case study argues that reflexive control was in play against Georgia in the lead-up to the armed conflict with Russia in August 2008.

42 *"Словарь терминов и определений в области информационной безопасности*" (Dictionary of terms and definitions in the field of information security), *Voyennaya Akademiya General'nogo Shtaba*, 2nd Edition, Moscow Voyeninform, 2008, p. 6.

43 Yu. Kuleshov et al., "Информационно-психологическое противоборство в современных условиях: теория и практика" (Information-Psychological Warfare In Modern Conditions: Theory And Practice), *op. cit.*, p. 105.

Permissive environment

Russia seeks to influence 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 disinformation delivered in this manner is part of the framework for decisions, this constitutes success for Moscow, because a key element of reflexive control is in place.

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 where Russian narratives are presented as factual. Moscow's potential gain at this level of influence is to win public support in adversary nations, and thereby attenuate resistance to actions planned by Russia, in order to increase their chances of success and reduce the likelihood of damaging adverse reactions by the international community.

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.[44] This can include the promotion of specific narratives designed to constrain NATO freedom of action to make defensive preparations,[45] some of which have achieved striking success in penetrating academic debate.[46]

Even responsible media reporting can inadvertently lend authority to false Russian arguments. To take one example which is topical at the

44 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 (accessed 24 June 2016).

45 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, undated, https://www.baks.bund.de/sites/baks010/files/working_paper_15_2016.pdf (accessed 24 June 2016).

46 As, to take just one example, in "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/ (accessed 24 June 2016). See also Taras Kuzio, "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 (accessed 24 June 2016).

time of writing, in reporting on Canada's status as a framework nation for NATO's multinational presence in Latvia, Canadian state broadcaster CBC informed the public that the move "could be seen as a provocation," 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."[47] These are the terms in which Russia would wish the NATO-Russia Founding Act to be interpreted, rather than what the Act actually says; and description as "a provocation" is characteristic of Russian statements. The result is that the Canadian public has now been informed by its state media that Canada's actions are in breach of NATO treaty commitments to Russia.[48]

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. The effect is even greater when, as in the CBC example above, Russian narratives are repeated and validated by official and trusted national media sources.

These narratives need not be specifically related to current events. Historical events too can 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."[49]

Subversion and Destabilisation

At the lower end of the scale of ambition of information warfare

47 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 (accessed 15 July 2016).

48 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 (accessed 15 September 2016).

49 Annual Review 2015, Estonian Internal Security Service, 2015, https://kapo.ee/sites/default/files/public/content_page/Annual%20Review%202015.pdf pp. 12-15 (accessed 4 July 2016).

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 like this, and some guiding principles, are broadly recognisable as reinvigorated aspects of subversion campaigns from the Cold War era and earlier.[50] At that time, aspects of these campaigns were referred to as "active measures" in a sometimes misleading adoption of Soviet terminology of the time. According to a major Finnish study, active measures constitute:

> *"certain 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."*[51]

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."[52] This contributes to the "dismay" effect in former NATO press officer Ben Nimmo's short characterisation of Russian disinformation aims as to "dismiss, distort, distract, dismay,"[53] and can be achieved by exploiting vulnerabilities in

50 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; 'Soviet Propaganda In Western Europe', UK Foreign & Commonwealth Office, March 1982, http://www.psywar.org/radSovietPropaganda.php.

51 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

52 Yu. Kuleshov et al., "Информационно-психологическое противоборство в современных условиях: теория и практика" (Information-Psychological Warfare In Modern Conditions: Theory And Practice), *op. cit.,* pp. 106.

53 Ben Nimmo, "Anatomy of an Info-War: How Russia's Propaganda Machine Works, and How to

the target society, particularly freedom of expression and democratic principles. The range of targets is broad. Subversion campaigns can aim:

> *"to involve 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 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."*[54]

An obvious target for distributing disinformation is the media, and a direct link is seen between 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 instill 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."*[55]

But bodies and organisations other than the 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."[56]

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/ (accessed 27 June 2016).

54 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.

55 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.

56 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-

Direct links between Russia and political parties representing the dissatisfied at either end of the political spectrum have become increasingly well documented.[57] 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."*[58]

Once again it should be emphasised that when Russian military theorists are describing these approaches, they are in the majority of cases (including this last citation) presented as campaigns planned by a hostile 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

---

war-era-body-to-catch (accessed 22 June 2016).

57 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 (accessed 18 July 2016). 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 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/ (both accessed 18 July 2016)

58 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.

damaging actions with no specific objective in mind beyond weakening and undermining competitor societies should not be seen as a recent innovation, but rather in the mainstream of Russian approaches from Soviet times and even before. As described in 1839:

> *"Russia sees Europe as a prey which our dissensions will sooner or later deliver up to her; she foments anarchy among us in the hope of profiting by a corruption she promotes because it is favourable to her views."*[59]

Defensive Measures

Awareness of the destructive potential of the techniques outlined above has led Russia to re-institute control over the information 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."[60]

Foreign ownership of media outlets has been limited, rebroadcasting licences withdrawn, and independent sources of news closed or constrained.[61] One repeated 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.[62] What remains of Russia's free media has largely been either marginalized or intimidated

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

60 *Ibid.*

61 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 (accessed 14 July 2016).

62 'Russian media firms: Interesting news', *The Economist*, 8 November 2014, http://www.economist.com/node/21631057/print.

into compliance.[63]

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.[64] The alternative reality broadcast on Russian television is unrecognisable from real life.[65] "State 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."[66] But contrary to Western 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.[67]

Information control is further tightened by measures such as censoring school textbooks, so that Russians develop the approved vision not only of current events but also of history.[68] And in a direct echo of Soviet and Tsarist repression of thought, Russia has already begun the

63 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*.

64 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.

65 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.

66 Michael Birnbaum, Russia's Putin signs law extending Kremlin's grip over media, 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 (accessed 14 July 2016).

67 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 (accessed 15 September 2016).

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

criminalisation of alluding to historical facts which are inconvenient for current state narratives.[69] 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; but in recent years it has both accelerated and spread to the previously unrestricted internet. Russians have become dramatically more isolated from alternative sources of information.[70] This isolation is not total and hermetic in the same way as during periods of the Cold War – it is still possible for interested Russians to access foreign media via the internet if they wish. But internet usage monitoring, and filtering and misleading translation of foreign media reports online, also contribute to the isolating effect.[71] The Russian Security Council is reported even to have given consideration to the implications of the country operating without internet access altogether.[72]

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,

69 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 (accessed 7 July 2016).

70 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/.

71 K. 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 (accessed 23 June 2016).

72 K. Giles, 'As sanctions bite, could Russia isolate itself by switching off the net?', *The World Today*, November 2014.

isolation facilitates distortion. It is easy for Russian media to provide accounts or translations of statements by foreign leaders or organisations which are misleading or entirely false, without being challenged within the country.[73]

Second, these efforts to isolate the Russian population from a true picture of events both in the outside world and in their own country help the Russian authorities promote the 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 Russian leadership figures to come to believe their own propaganda. In this way too, there are echoes of Soviet times, when one analyst could describe Soviet leaders':

> *"psychological 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."*[74]

The most dangerous implication of Russian leaders believing what they tell their subjects is the possibility that they could also then act on that belief.

Further Reading

General Principles:

- E. Lucas and B. Nimmo, "Information Warfare: What Is It and How to Win

73 "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/ (accessed 19 July 2016).

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

It?" CEPA Infowar Paper No. 1, November 2015.

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

- P. Koshkin, "The paradox of Kremlin propaganda: How it tries to win hearts and minds," *Russia Direct*, 2 April 2015, http://www.russia-direct.org/analysis/paradox-kremlin-propaganda-how-it-tries-win-hearts-and-minds (accessed 30 June 2016).

- K. Giles, *Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power*, Chatham House, March 2016, https://www.chathamhouse.org/publication/russias-new-tools-confronting-west (accessed 15 July 2016).

Current Implementation:

- B. Nimmo, "Anatomy of an info-war: How Russia's propaganda machine works, and how to counter it," *CEPolicy.org*, 15 May 2015, http://www.cepolicy.org/publications/anatomy-info-war-how-russias-propaganda-machine-works-and-how-counter-it

- M. van Herpen, *Putin's Propaganda Machine: Soft Power and Russian Foreign Policy*, Lanham, Rowman & Littlefield Publishers, 2015.

- S. D. Bachmann and H. Gunneriusson, "Russia's Hybrid Warfare in the East: The Integral Nature of the Information Sphere," *Georgetown Journal of International Affairs*: International Engagement on Cyber V (2015).

History and Background:

- 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, US Army War College Strategic Studies Institute, July 2010, http://www.strategicstudiesinstitute.army.mil/pdffiles/pub997.pdf (accessed 23 June 2016). pp. 265-300.

- "Soviet Influence Activities: A Report on Active Measures and Propaganda, 1986-87," US Department of State, August 1987.

4. History and Development

As with other domains of warfare, Russia's current approach to information war "grows from indigenous military and political traditions."[75] This follows the general principle explained by Tim Thomas that "in Russian, discussions of armed conflict [terms and definitions] are associated with thinking from decades ago, indicating a strong continuity of thought in Russian military theory."[76]

The techniques and approaches currently on display 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.[77] For all their innovative use of social media and the internet, current Russian methods have deep roots in long-standing Soviet practice.[78] Importantly, this continuity of thought from former generations of information activity practice is not replicated in the West, where two generations after the end of the Cold War, Russian practices of information warfare have caused widespread surprise.

The development of thought on new methods of transmission of information warfare effects can be traced to initial recognition of the transformative effect of digitisation on warfighting itself, stemming from discussion of the Revolution in Military Affairs and in particular observation of United States operations in the 1991 Gulf War and subsequent campaigns. Early analysis in this trend emphasised precision guided munitions as the defining factor of a new generation of warfare, but

75 M. Galeotti, "Hybrid, ambiguous, and non-linear? *op. cit.*, pp. 282-301.

76 T. Thomas, *Thinking Like a Russian Officer: Basic Factors and Contemporary Thinking on the Nature of War*, Foreign Military Studies Office, April 2016, http://fmso.leavenworth.army.mil/documents/Thinking%20Like%20A%20Russian%20Officer_monograph_Thomas%20(final).pdf (accessed 22 June 2016).

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

78 C. 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/

already recognised that "one attribute of future war will be 'information confrontation'... [since] information is becoming the very same kind of weapon as missiles, bombs, torpedoes and so on."[79] Some Russian military thinkers were alert from the earliest stages to the opportunities provided by the Internet for extending information warfare practice into a new domain, in particular to attack adversary decision-making structures and command and control networks.[80]

This was followed by recognition of the potential of hyperconnectivity offered by the internet for providing direct accessibility to target audiences for "information-psychological" as well as "information-technical" effect. The realisation that "it turns out that one can penetrate a state's information networks in the simplest way through Internet channels in addition to the traditional channels of radio, television and the mass media"[81] implied that mass audiences could be reached with much greater impact, and much less expense and effort, than previous techniques of planting and disseminating disinformation; in effect, by means of "the use of 'mass information armies' conducting a direct dialogue with people on the internet."[82] The perception of information activities as an asymmetric enabler was reinforced by their potentially very high return on investment: "Information has become the same kind of weapon as a missile, a bomb and so on [but it] allows you to use a very small amount of matter or energy to begin, monitor and control processes whose matter and energy parameters are many orders of magnitude larger."[83]

In parallel with the attenuated power and capability of its conventional armed forces, Russia's capabilities in the information warfare domain were

79 V.I. Slipchenko, "Future War," *op. cit*.

80 See V.M. Lisovoy, О законах развития вооруженной борьбы и некоторых тенденциях в области обороны, Issue 5, 1993.

81 V.I. Slipchenko, "Future War," *op. cit*.

82 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.

83 Vladimir Mukhin, "История завоевания 'четвертого фронта'" (History of conquering the "fourth front"), *Nezavisimoye voyennoye obozreniye*, 22 July 2016, http://nvo.ng.ru/realty/2016-07-22/10_4front.html (accessed 15 September 2016).

repeatedly exposed as deficient in the 1990s and early 2000s. Repeated setbacks resulted from a failure both to realise that the previously available networks of subversion, disinformation and malign influence which were used by the Soviet Union were no longer available; and to realise the true nature and utility of the internet in a timely manner.

Significant steps in the evolution of Russian thinking in this area took place with each failure to achieve desired results in international information campaigns. Specific examples were the first and second Chechen wars, each of which took place in a distinct media environment at an early stage in the expansion and globalisation of the World Wide Web.[84] Russia's performance in the information domain during the first intervention in Chechnya in 1994-6 was officially characterized as "the quintessence of helplessness in the information sphere."[85]

But it was the armed conflict with Georgia in August 2008 which provided the impetus to overhaul and transform Russia's information warfare effort, along with the whole of the Russian armed services.[86] It was at this point that Russia significantly stepped up efforts to exploit the internet as another medium for controlling information. Open debate on the best response to the challenge included calls for the creation of Information Troops, a dedicated branch that could manage the information war from within the military.[87] Reflecting the full-spectrum nature of the Russian information war concept, these troops would

84 For more detail on this process, see K. Giles, *Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power*, Chatham House, March 2016, https://www.chathamhouse.org/publication/russias-new-tools-confronting-west (accessed 15 July 2016).

85 Speech by then Defence Minister Sergey Ivanov at plenary meeting of Russian Academy of Military Sciences, 18 January 2003.

86 Despite this complete overhaul, one analysis has identified a number of techniques and approaches already applied by Russian state media at this stage which are identifiable as the prototypes of later efforts in 2014-16. See J. Rogoża and A. Dubas, 'Russian Propaganda War: Media as a Long- and Short-range Weapon,' *Centre for Eastern Studies* Commentary, Issue 9, 11 September 2008, http://mercury.ethz.ch/serviceengine/Files/ISN/91705/ipublicationdocument_singledocument/9970722d-84ca-4f45-8ec1-a3d77ad75e48/en/commentary_09.pdf (accessed 1 July 2016).

87 K. Giles, "Information Troops – A Russian Cyber Command?" *Proceedings of the Third International Conference on Cyber Conflict*, Tallinn, June 2011.

include hackers, journalists, specialists in strategic communications and psychological operations, and, crucially, the essential linguists to overcome Russia's now perceived language capability deficit. Heavy investment in language capabilities began, in order to reach non-Russian-speaking target audiences directly.

Russia's "lessons learned" process after this conflict included close study of the U.S. experience of maintaining active psychological operations units within the Armed Forces, contrasted with Russia's failure to do so in the post-Soviet period.[88] It is suggested that this was subsequently addressed by "the revival of psychological operations units both at army and frontline levels, subordinated directly to the GRU." The careful, long-term and well-funded development of these capabilities contributes to their effectiveness by comparison with countermeasures with Ukraine, which has attempted to replicate the same processes from a standing start and consequently launches disinformation and propaganda efforts that can appear crude, clumsy and counter-productive.

But throughout this process the mainstream of Russian security thought about the nature of information, and its potential as both an opportunity and a threat, remained relatively unaffected. Russia's continuity of thought was facilitated by a continuity of leadership. From the turn of the century onward, with alumni of the former KGB running the country, the KGB's approach to information security once again became dominant. This is most perceptible of all in Russia's approach to the free circulation of information as a threat to its own security and stability.

Russia's Threat Perception

A key and consistent element throughout this development process

88 S. Kozlov and E. Groysman, "Спецназ зарубежья: Невидимый фронт психологической войны: американский опыт" (Special Forces abroad. Invisible front in psychological warfare: US experience), *Bratishka,* http://bratishka.ru/archiv/2009/3/2009_3_12.php (accessed 21 July 2016).

has been Russia's perception of the information warfare threat to itself, which also informs the country's defensive and protective measures against undesirable information from abroad outlined above.

The perceived threat is an existential one. The received wisdom in Russia is that "information confrontation campaigns" are developed by the West to compromise Russia's national sovereignty and facilitate regime change.

In historical terms, this view does have some justification. To the extent that Mikhail Gorbachev's declaration of *glasnost'*, or freedom of expression, triggered processes that led to state collapse in the form of the end of the Soviet Union, this freedom can be viewed as a direct challenge to Russian statehood.

Russia's emphasis on *information* as a whole as the contested space, and the disinclination to treat activities in electronic media as any different from any other sphere of information processing, results in part from the unbroken descent of current Russian information security principles from the Soviet approach to restricting and controlling information. The position on the merits and dangers of information held by the KGB and its successor organisations has been consistent since before the end of the Soviet Union. The uncontrolled distribution and reproduction of information online has from its very beginning been seen as just as much of a threat to Russia as was, previously, the invention of the photocopier.[89]

This attitude gave rise to early strong resistance by the Russian state security bodies to adoption of the internet. At parliamentary hearings in late 1996 entitled "Russia and the Internet: The Choice of a Future," a senior information security official characterised the internet as a whole as a threat to Russian national security.[90] Also in the mid-1990s, leading

89 As has been colourfully described in A. Soldatov and I. Borogan, *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries*, London, PublicAffairs, 2015.

90 State Duma proceedings, 17 December 1996. See also A. Soldatov, "Фапси—общественности: 'меньше знаешь—крепче спишь'" (FAPSI to the public: The less you know, the sounder you sleep, *Segodnya*, 12 December 1999.

Russian thinkers on information warfare were describing information weapons as "more dangerous than nuclear ones," and warned against joining the inherently insecure internet:

> *"Russia's participation in international telecommunications and information exchange systems is impossible without the comprehensive resolution of the problems of information security."*[91]

The anomaly in Russian practice was that adoption of the internet took place at a time when the security structures were in relative terms weaker, and not able to prevent the process being driven by commercial entities. But more recently, and in particular in the period from 2013 onwards, their hold on online activity has been applied and reinforced with direct support from President Putin. Measures of control over online content and its distribution were consistently aspired to by the FSB, but have only been noticeably implemented in the course of the last three years.

Nevertheless this does give rise to incongruities, and tension between concepts of information security that were developed for print, television and radio, and the realities of the internet as a medium for data transmission which by default has no respect for borders or "national information space." There is a direct conflict between the Western concept of the internet insisting on the free, unrestricted and ungoverned flow of information, and the consensus espoused by Russia and like-minded states, that places important caveats on the flow of information and insists on the principle of national sovereignty in cyberspace.

In effect, Russia sees a threat from online content as well as code; from hostile information carried via the internet as well as hostile software. Russian media officials have consistently committed to "restrictions of rights and freedoms only in the interests of security;"[92] but the balance

91 G. Smolyan, V. Tsygichko, and D. Chereshkin, "Оружие, которое может быть опаснее ядерного. Реалии информационной войны" (A Weapon That May Be More Dangerous Than a Nuclear Weapon: The Realities of Information Warfare), *Nezavisimoye voyennoye obozreniye* , 18 November 1995.

92 "Щеголев: цензуры Интернета в России не допустят" (Shchegolev: Internet censorship will not be allowed in Russia), *Interfax*, 20 January 2012, http://www.interfax.ru/print.asp?sec=1448&id=226823 (accessed 13 July 2016).

point between these two conflicting interests is at variance with the normal range in the West. An indicative example is the use of the SORM system for monitoring internet usage by private citizens in Russia. Far from being a secret programme, this is an openly avowed feature of internet usage, and one which has since its inception been accepted without visible thought or question by the vast majority of users.

But in addition to information from abroad, the apps and software used to communicate via the internet are also subject to suspicion. Russian government statements and orders have repeatedly highlighted "the dangers of using foreign-made software and foreign commercial internet services, such as instant messengers, by Russian civil servants... this [has] allowed criminals and foreign intelligence specialists to access both Russian state secrets in economic and defense sphere and the personal data of Russian citizens."[93] Here, too, there may be some justification for this security concern. The relative lack of visible hostile cyber activity during the conflict between Russia and Ukraine has been attributed, among many other factors, to widespread use of Russian mail servers by Ukrainian officials – so there is no need for Russia to hack e-mail accounts that they already have access to by default. It is not unreasonable to assume that foreign governments might be able to induce service providers to do the same to Russia.

At the same time, confirmation bias does reinforce Russian perception of unrelated new developments as part of a consistent hostile campaign. Apparently unable to conceptualise spontaneous public expressions of mass civic dissent, the Russian authorities considered that protests over the State Duma election results in December 2011 were provoked by a U.S. cyber/information warfare campaign against Russia.[94] In 2016, Russian

93 "Foreign special services step up online operations targeting Russia - top security official," *RT*, 15 June 2016, https://www.rt.com/politics/346772-foreign-special-services-step-up/ (accessed 4 July 2016).

94 Although the election protests were the most widely reported outside Russia, a trend of greater readiness to engage in civic protest – facilitated by social media – had been noted over the preceding years. See Susan de Nîmes (editor), *Potential Challenges to Public Order and Social Stability in the Russian Federation,* Conflict Studies Research Centre, August 2011, http://conflictstudies.org.uk/files/20110810_CSRC_Russia_Social.pdf (accessed 23 June 2016).

Minister of Culture Vladimir Medinskiy explained that the Netflix video streaming service is financed by the U.S. government as a method of "entering the minds of every inhabitant of the Earth."[95] Even Pokémon Go (a virtual reality game widely, but perhaps briefly, popular at the time of writing) has been described in official Russian sources as a component of Western information warfare,[96] with Minister of Communications and Mass Media Nikolay Nikirofov suggesting it was "created with the help of certain intelligence agencies, who are collecting video information from territories all over the world."[97] The difference between this argument and measures to restrict Pokémon Go in the United States is indicative. In the US, the game has been prohibited inside Department of Defense facilities because it would broadcast the movements of users inside those locations, including indicating the location of secure facilities where connected devices are not permitted.[98] In Russia, by contrast, the concern over its use in public spaces is reminiscent of Soviet times, when for example photographing everyday locations like bridges or railway stations was prohibited because it would provide useful intelligence to the enemy on transport capacity in the event of war.

Whether based on a realistic current threat appreciation or not, Russia's perception is that information campaigns in the broadest sense pose a serious and growing threat to the country, implemented and perfected by the United States and the West in the course of a series of regime change operations over decades. The 2007 conference of the Academy

95 "Мединский обвинил власти США в попытке «залезть в каждый телевизор» через Netflix" (Medinskiy accuses US authorities of trying to "infiltrate every television" through Netflix), RNS, 22 June 2016, https://rns.online/internet/Medinskii-obvinil-vlasti-SSHa-v-popitke-zalezt-v-kazhdii-televizor-cherez-Netflix--2016-06-22/ (accessed 24 June 2016). English-language reporting available at http://www.rferl.org/content/russia-netflix-culture-minister-us-mind-control/27814138.html

96 James Mashiri, "An Absurd Signal: Pokémon Confirms Russia's War Footing," Image, 19 July 2016, http://blogit.image.fi/somesotilas/an-absurd-signal-pokemon-confirms-russias-war-footing/ (accessed 20 July 2016).

97 "'The Devil has arrived through this mechanism' The Russian authorities weigh in on Pokémon Go. Five quotes," Meduza, 18 July 2016, https://meduza.io/en/feature/2016/07/18/the-devil-has-arrived-through-this-mechanism (accessed 20 July 2016).

98 B. Gertz, "Pentagon bans Pokemon Go over spying fears," *The Washington Times*, 11 August 2016, http://www.washingtontimes.com/news/2016/aug/11/pentagon-bans-pokemon-go-over-spying-fears/ (accessed 15 September 2016).

of Military Sciences (AVN) highlighted the emergence of "non-military threats." According to then Chief of General Staff Yuriy Baluyevsky:

> *"Based on the experience of the collapse of the Soviet Union and of Yugoslavia, and on the examples of the colour revolutions in Georgia, Ukraine, Kyrgyzstan, and elsewhere, one can clearly see that major threats do objectively exist and are implemented not only by military means, but primarily by covert and overt methods of political and diplomatic, economic, and information influence, various subversive actions and interference in the internal affairs of other countries. In this regard, Russian security interests require not only to assess these threats but also to determine appropriate measures to respond to them."*[99]

The conference recommended that this new threat assessment be reflected in the next edition of Russia's Military Doctrine; it did not in the end appear in the 2010 version,[100] and had to wait till 2014 – after the start of the Ukraine crisis – to be highlighted.[101]

The Arab Spring and Libya

In the intervening period, strategic shocks in the Middle East and North Africa appeared to confirm Russian perceptions of a consistent Western campaign to remove regimes of which the United States disapproved – and of the use of information as the primary tool to do so. In early 2011, AVN President Army Gen Makhmut Gareyev pointed to "subversive information technologies of the West" being the root cause of

99 For a detailed investigation of Russian threat assessments during this period, see S. Blank, "'No Need to Threaten Us, We Are Frightened of Ourselves,'" Russia's Blueprint for a Police State, The New Security Strategy," in S. Blank and R. Weitz (eds.), The Russian Military Today And Tomorrow: Essays In Memory Of Mary Fitzgerald, US Army War College Strategic Studies Institute, July 2010, http://www.strategicstudiesinstitute.army.mil/pdffiles/pub997.pdf (accessed 23 June 2016).

100 K. Giles, "The Military Doctrine of the Russian Federation 2010," Research Review, NATO Defense College, February 2010, http://www.ndc.nato.int/download/downloads.php?icode=170 (accessed 21 June 2016).

101 A review of the 2014 Doctrine is available in P. Sinovets and B. Renz, "Russia's 2014 Military Doctrine and beyond: threat perceptions, capabilities and ambitions," Research Paper 117, NATO Defense College, 10 July 2015, http://www.ndc.nato.int/news/news.php?icode=830 (accessed 23 June 2016).

the disorder that came to be known as the Arab Spring:

> *"Internet networks were implanted in Egypt, Tunisia and Libya over a two-year period. It started with systematic training for communication checks, without direct calls for unlawful actions. At the right moment, a centralized order was issued across all networks for people to take to the streets."*[102]

Comments by then-president Dmitriy Medvedev in 2011 are regularly quoted, but nonetheless indicative of Russian apprehension at the West's eventual objectives:

> *"Look at the situation that has unfolded in the Middle East and the Arab world. It is extremely bad. There are major difficulties ahead... We need to look the truth in the eyes.* ***This is the kind of scenario that they were preparing for us, and now they will be trying even harder to bring it about****."*[103]

Intervention by Western powers in the resulting civil war in Libya precisely matched the pattern for "modern warfare" described by then Chief of General Staff Nikolay Makarov in published articles, including one the previous year: "use of political, economic and information pressure and subversive actions, followed by the unleashing of armed conflicts or local wars, actions that result in relatively little bloodshed" in order to achieve the aggressor's intent.[104] And the disastrous longer-term consequences of destabilisation following Western interventions in Libya and elsewhere bear out Russian arguments that Western powers consistently failed to appreciate the second- and third-order effects of

---

102 Interfax news agency, 26 March 2011.

103 "Дмитрий Медведев провел во Владикавказе заседание Националного антитеррористического комитета" (Dmitriy Medvedev held a meeting of the National Anti-Terrorism Committee in Vladikavkaz), Russian presidential website, 22 February 2011, http://www.kremlin.ru/transcripts/10408 (accessed 19 July 2016, emphasis added).

104 N. Makarov, "Характер вооруженной борьбы будущего, актуальные проблемы строительства и боевого применения Вооруженных Сил РФ в современных условиях" (The Character of future armed conflict, and current problems of organisational development and combat application of the Armed Forces of the Russian Federation under contemporary conditions)," *Vestnik Akademii Voyennykh Nauk* (Bulletin of the Academy of Military Science), No. 2, March 2010.

their actions.

Events in the Middle East and North Africa also confirmed Russian perceptions of social media as a dangerous and destabilising tool of Russia's enemies.

There had already been publicly released studies of the use of social media for political influence purposes; but even during the Arab Spring, assessments of their utility for facilitating regime change appeared to receive attention only from a narrow circle of specialists in the West.[105] Russian attention, however, must have been drawn to public statements by NATO regarding use of social media posts from within Libya to contribute to actionable intelligence, including targeting information.[106]

And once again, the fact that the majority of social media platforms were foreign-owned contributed to their classification as an instrument for exploitation by Western governments:

> *"The security and intelligence services [spetssluzhby] of the Arab states were not able to prevent the distribution of [social media] messages because they did not have access to the controlling servers of the social networks, which are located on the territory of the United States security and intelligence services."*[107]

Social media in fact present multiple challenges to Russia, even beyond threats to the homeland itself. The experience of Russian servicemen posting to social media from eastern Ukraine – where they are officially not supposed to be – provides a clear demonstration that in the absence of strictly enforced operational security disciplines, incautious social media usage makes available valuable operational intelligence for harvesting by

105 As, for example, S. Railton, *Revolutionary Risk - Cyber Technology and Threats in the 2011 Libyan Revolution*, US Naval War College, 2013.

106 R. Norton-Taylor and N. Hopkins, "Libya air strikes: Nato uses Twitter to help gather targets," *The Guardian*, 15 June 2011, https://www.theguardian.com/world/2011/jun/15/libya-nato-gathers-targets-twitter (accessed 19 July 2016).

107 Yu. Kuleshov et al., "Информационно-психологическое противоборство в современных условиях: теория и практика" (Information-Psychological Warfare In Modern Conditions), *op. cit.*, p. 107.

an adversary.[108]

Taken together, the obvious problems presented by unrestrained and unregulated use of social media exacerbate Russian perceptions of the internet as a whole as both a tool for exercising influence abroad, and a direct vulnerability for Russia itself. Finally, virtually unrestricted freedom of expression on social media must in itself compound the impression that greater control is long overdue. In 2012, President Putin described the experience of listening to an independently-minded Russian radio station as "having diarrhoea poured over him day and night."[109] Putin and those who think like him are now presented with social media disseminating widely online criticism of Russia, including prolific and highly-skilled satire exercised via Twitter. It can reasonably be assumed that their reaction to this is even more emphatic.

Further Reading

In English

- A. Soldatov and I. Borogan, *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries*, London, PublicAffairs, 2015.

- M. Snegovaya, "Putin's Information War in Ukraine: Soviet Origins of Russia's Hybrid Warfare," *Institute for the Study of War*, Russia Report 1, September 2015, http://understandingwar.org/sites/default/files/Russian%20Report%201%20Putin's%20Information%20Warfare%20in%20Ukraine-%20Soviet%20Origins%20of%20Russias%20Hybrid%20Warfare.pdf (accessed 15 July 2016).

108 Patrick M. Gillen, *Real-Time Detection of Operational Military Information in Social Media*, Naval Postgraduate School, September 2015, http://calhoun.nps.edu/handle/10945/47261 (accessed 23 June 2016).

109 "'Я не обижаюсь на вас, когда вы поливаете меня поносом': Путин пообщался с руководителями СМИ" ("I don't get upset with you when you pour diarrhoea on me": Putin chats with media leaders), *Gorod novostey*, 19 January 2012, http://www.city-n.ru/view/296196.html (accessed 13 July 2016).

- K. Giles, "Can Russia switch off the net?" *The World Today*, October-November 2014.

- K. Giles, "'Information Troops' - A Russian Cyber Command?," in Czosseck, Tyugu and Wingfield (eds.), *Third International Conference on Cyber Conflict*, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), June 2011, http://conflictstudies.org.uk/files/Russian_Cyber_Command.pdf (accessed 23 June 2016).

In Russian

- Igor Panarin, "Система информационного противоборства" (A system of information confrontation), *Voyenno-promyshlennyy kuryer*, 15 October 2008, http://vpk-news.ru/articles/3672 (accessed 18 July 2016).

- V. Sulimov and P. Muraveyko, "Ретроспектива развития способов ведения информационного противоборства в военных конфликтах" (Retrospective on the development of information-warfare methods in military conflicts), *Nauka i Voyennaya Bezopasnost*, No. 4, 2008, pp. 3-10.

5. Implementation

Russian information campaigning can serve multiple concurrent objectives at any given time. As described by Mark Laity, Chief Strategic Communications at SHAPE:

> *"If you look at what they [Russia] did when they annexed Crimea and invaded eastern Ukraine, the information line of effort was fundamental, not just to give them a strategic narrative to try to justify what they did, but [also] to use information to deceive, delay and disrupt, like a smokescreen."*[110]

More recently, analysts have observed different elements in the same toolkit used to facilitate operations in Syria.[111]

This blending of different disciplines and approaches inherent in Russian concepts of information warfare is reflected in grey zones of overlap between activities that are often considered separate and distinct in Western thought. Some techniques for disseminating disinformation are indistinguishable from marketing; some cyber attacks use the same exploits as cyber crime; some information operations are dependent on a kinetic attack as a facilitator.

RT (formerly Russia Today) and Sputnik are usually the first to be named in discussions of Russian information campaigns via the mass media. But they are only the most visible elements in a very wide range of different outlets, both those which are avowed and those which conceal their elements, tailoring their output to the expectations of their intended readers and viewers. The media effort is thus able to adopt a different approach for different forums, ranging from simple fabrication, through

110 "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.

111 S. Blank, "Russia's information wars in Syria and Ukraine," European Geostrategy, 21 June 2016, http://www.europeangeostrategy.org/2016/06/russias-information-wars-in-syria-and-ukraine/ (accessed 27 June 2016).

confusion with half-truths, to sophisticated argument.

Even those parts of Russian information campaigns that are visible to audiences in any one language are only part of a broad multilingual front, including not only state-backed media and trolling, but also fake media – sock puppet websites set up to resemble genuine news outlets, but seeding their news feeds with false or contentious reporting that ties in with Russian narratives.[112] The nature of the internet means that the effective placing of disinformation in reputable news outlets is vastly cheaper, simpler, and more permanent than in previous decades when the primary medium was newspapers.

A study of information dominance published in an authoritative Russian military source lists the main principles of media campaigns as follows:

> *"The primary methods of manipulating information used by the mass media in the interests of information-psychological confrontation objectives are:*
>
> - *Direct lies for the purpose of disinformation both of the domestic population and foreign societies;*
> - *Concealing critically important information;*
> - *Burying valuable information in a mass of information dross;*
> - *Simplification, confirmation and repetition (inculcation);*
> - *Terminological substitution: use of concepts and terms whose meaning is unclear or has undergone qualitative change, which makes it harder to form a true picture of events;*
> - *Introducing taboos on specific forms of information or categories of news;*

112 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/.

- *Image recognition: known politicians or celebrities can take part in political actions to order, thus exerting influence on the world view of their followers;*
- *Providing negative information, which is more readily accepted by the audience than positive."*[113]

But influence on mass consciousness in adversary societies involves activity against a much broader range of targets than the media. According to senior scholar of Russia John Lough, the instruments to carry this out include "other agents of the Russian state who are looking to influence the opinion of security specialists, people in think-tanks, academics and maybe even some journalists."[114] This extends, naturally enough, to direct influence on politicians and decision-makers. Multiple studies have investigated Russian links to European politicians; one Hungarian institute has produced reports focusing on these links with both the right wing[115] and the left.[116]

There are even broader implications. Principles of subversion and weakening the adversary outlined in Russia include targeting a broad range of areas which the West does not traditionally think of as vulnerabilities:

> *"The types of actions to deprive the enemy of its ability to fight... seek directly to affect not only the enemy's military potential proper but also its political, economic, information, scientific-and-technical, moral, culturological, demographic and environmental potentials...*

113 Yu. Kuleshov et al., "Информационно-психологическое противоборство в современных условиях: теория и практика" (Information-Psychological Warfare In Modern Conditions, *op. cit.*, p. 107.

114 Oral evidence: Russia: Implications for UK defence and security, House of Commons Defence Committee, UK Parliament, 19 April 2016, http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/defence-committee/russia-implications-for-uk-defence-and-security/oral/32126.html (accessed 4 July 2016).

115 The Russian Connection: The spread of pro-Russian policies on the European far right, Political Capital Institute, March 2014, http://www.riskandforecast.com/useruploads/files/pc_flash_report_russian_connection.pdf (accessed 24 June 2016).

116 Péter Krekó-Lóránt Győri, Russia and the European Far Left, Political Capital Institute, undated, http://www.statecraft.org.uk/sites/default/files/documents/Peter%20Kreko%20Far%20Left%20definitive.pdf (accessed 24 June 2016).

> *Here, culturological warfare means coercive action or counteraction with regressive or progressive goals in the sphere of science, education, pastoral care, the arts, the national language, religion and traditional ways of life."*[117]

In this respect, Russia is not unique. Other hostile actors including Islamic State have identified and exploited the same attack vectors. As noted in 2015, "Both Russian and ISIS information campaigns astutely target inherent weaknesses in Western liberal democratic societies, and exploit a range of self-inflicted vulnerabilities which are fundamental to those societies' views of themselves and their values."[118]

Cyber, Kinetic and Information Operations

Recent practice indicates that the broad nature of the Russian information warfare concept can include real-world operations designed to create information effects as well as the reverse, and a seamless integration of "cyber" concepts and operations throughout.

Russian capabilities to exploit cyber vulnerabilities for damaging physical effect are widely discussed in open sources.[119] But for the purposes of information warfare, expensive one-shot cyber weapons, or noisy and unpopular DDoS attacks, are entirely unnecessary if you can gain physical control of internet infrastructure – as was demonstrated at an early stage during the seizure of Crimea. Occupation of the Simferopol Internet Exchange Point and disruption of cable connections to the mainland contributed to total information dominance on the peninsula for Russia, greatly facilitating further operations.[120]

---

117 V. Kvachkov, Спецназ России (Russia's Special Purpose Forces), *op. cit.*

118 K. Giles, "Осознание Западом серьезности информационного противоборства" (The West Wakes Up To Information Warfare), Ninth International Forum "Partnership of state, business and civil society for international information security," *Moscow State University*, 2015, pp. 294-308.

119 O. Matthews, "Russia's Greatest Weapon May Be Its Hackers," *Newsweek*, 5 July 2015, http://www.newsweek.com/2015/05/15/russias-greatest-weapon-may-be-its-hackers-328864.html (accessed 15 July 2016).

120 Shane Harris, "Hack Attack. Russia's first targets in Ukraine: its cell phones and Internet lines," Foreign

The prehistory of this kind of operation includes the traditional seizure or destruction of civilian broadcast facilities at the first stage of any attempt at regime change, whether imposed from abroad or the result of a domestic coup. Extension of the principle into targeting internet infrastructure is a relatively new development, but one which had been flagged in Russian conceptual writing on information warfare. A much-quoted analysis of the new capabilities required by Russia following the armed conflict in Georgia in 2008 noted that:

> *"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."*[121]

And the Russian Armed Forces' 2011 cyber proto-doctrine included provision for "deploying forces and resources to provide for information security on the territories of other states."[122] Parsed through Russian doctrinal language, this innocent-sounding formulation was interpreted as also referring to setting up units that would target adversary communications facilities.[123]

Commentary at the time speculated whimsically on "commandos parachuting into server centres, iPads in hand"; but events in Crimea, indicating the embedding of telecommunications network expertise within Russian SOF, show that this picture was in fact not far from the truth.

Policy, 3 March 2014, http://foreignpolicy.com/2014/03/03/hack-attack/ (accessed 15 May 2016).

121 BBC Monitoring: "Russia is underestimating information resources and losing out to the West," *Novyy Region*, 29 October 2008 (emphasis added).

122 "Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве" (Conceptual Views on the Activity of the Russian Federation Armed Forces in Information Space), Russian Ministry of Defence, 22 December 2011, http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle (accessed 13 July 2016).

123 K. Giles, "Russia's Public Stance on Cyberspace Issues," in C. Czosseck et al (eds.), 2012 4th International Conference on Cyber Conflict, NATO CCDCOE, Tallinn, 2012, https://ccdcoe.org/publications/2012proceedings/2_1_Giles_RussiasPublicStanceOnCyberInformationWarfare.pdf (accessed 13 July 2016).

Even within cyberspace itself, with an overlap of tactics, techniques and procedures (TTPs) between cyber crime, cyber activism, and cyber attack, from a Russian perspective the synergies between the different forms of hostile CNOs are clear. According to Austrian researcher Alex Klimburg:

> *"The differences between these categories of cyber activity are often razor thin, or only in the eye of the beholder. From the perspective of a cyber warrior, cyber crime can offer the technical basis (software tools and logistic support) and cyber terrorism the social basis (personal networks and motivation) with which to execute attacks on the computer networks of enemy groups or nations."*[124]

This overlap means there is little practical obstacle to using criminal networks to further state aims in cyberspace while limiting attribution risk to government.[125]

Furthermore, "cyber" attacks can be used as a facilitator for information campaigns whether or not they cause significant impact – or, indeed, when they have not even taken place. According to one unpublished analysis, facilitators can include "demonstrative actions in cyberspace that inflict no substantial economic or other damage to the target state [but only] cause panic among the population and, as a result, distrust in the authorities." At the time of writing, it is suggested that this is one possible explanation for a chain of unexplained disruptive incidents crossing the boundaries between cyber and physical effects in Sweden, during a period of intensified hostile messaging from Russia over the possibility of Swedish membership in NATO.[126]

---

124 A. Klimburg. "Mobilising Cyber Power," Survival: Global Politics and Strategy, vol. 53, no. 1, February-March 2011, pp. 41-60.

125 Highlighted in "M-Trends 2015: A View from the Front Lines," Mandiant, undated, https://www2.fireeye.com/rs/fireye/images/rpt-m-trends-2015.pdf (accessed 15 July 2016).

126 For an overview, see Edward Lucas, "Cyber in Tallinn," Center for European Policy Analysis, 6 June 2016, http://cepa.org/Cyber-in-Tallinn (accessed 21 July 2016). See also M. Piotrowski, "The Swedish Counter-Intelligence Report on Hostile Russian Activities in the Region in a Comparative Context," Polish Institute of International Affairs (PISM), Bulletin No. 25 (875), 24 March 2016, https://www.pism.pl/files/?id_plik=21575 (accessed 21 July 2016).

Russian disinformation campaigns routinely involve the use of forged documents,[127] in a tradition that dates back to Soviet active measures and beyond.[128] In some cases, these are provided to media outlets with the claim that they have been obtained by hacking activities. In many cases, it appears likely that these documents were produced and obtained by other routes altogether. But the effect of the "cyber attack" story is twofold: it creates the impression that Russian–backed hackers are far more effective than they may necessarily be; and it also entices Western media editors to publish the contents of the documents before establishing their reliability or provenance, since they have the added spice of having been apparently obtained by a sexy and exciting means.[129]

The threat, as opposed to the use, of military force is another key ingredient of Russian information campaigns. A repeated feature of Russian rhetoric toward NATO and the West both before and after the seizure of Crimea has been emphasis on military preparations for conflict, up to and including discussion of the use of nuclear weapons.[130] Subsets of this narrative include provoking air and sea incidents which can be misrepresented in order to portray legitimate activities by the United States or other NATO allies as dangerous and provocative,[131] and repeated

127 See for example J. L. Feder and V. Stepanov, "The U.S. Embassy In Russia Just Exposed A Forgery In The Best Way Ever," Buzzfeed, 18 November 2015, https://www.buzzfeed.com/lesterfeder/snark-diplomacy (accessed 21 July 2016).

128 "Soviet Active Measures: Forgery, Disinformation, Political Operations," United States Department of State Special Report No. 88, October 1981, http://insidethecoldwar.org/sites/default/files/documents/Soviet%20Active%20Measures%20Forgery,%20Disinformation,%20Political%20Operations%20October%201981.pdf. See also Mikhail Agursky, "Soviet Disinformation And Forgeries," International Journal on World Peace, Vol. 6 No. 1 (January-March 1989), pp. 13-30, https://www.jstor.org/stable/20751319 (both accessed 21 July 2016).

129 See for example J. Smith, "Pro-Russian Hackers Expose U.S. Military Contractor Activity in Ukraine," Observer, 3 February 2015, http://observer.com/2015/03/pro-russian-hackers-expose-u-s-military-contractor-activity-in-ukraine/

130 For a detailed exploration of Russian nuclear messaging, see Karl-Heinz Kamp, "Nuclear Implications of the Russian-Ukrainian Conflict," NATO Defense College Research Report, April 2015, http://www.ndc.nato.int/news/news.php?icode=789 (accessed 15 July 2016).

131 "Shouldering Incident Reminiscent of Sea of Japan Bumpings," Naval Historical Foundation, 30 June 2016, http://www.navyhistory.org/2016/06/shouldering-incident-reminiscent-of-sea-of-japan-bumpings/ (accessed 6 July 2016), Keir Giles, "Russian High Seas Brinkmanship Echoes Cold War," Chatham House, 15 April 2016, https://www.chathamhouse.org/expert/comment/russian-high-seas-brinkmanship-echoes-cold-

declarations of intent to deploy Iskander-M missiles (or, previously, advanced air defence missile systems) in Kaliningrad in response to any development in Europe of which Russia disapproves.[132]

It is the nuclear threats in particular that create an impression of Russia as an unpredictable and irresponsible security actor, and cause bewilderment and concern in the West. But this is precisely their intent, since threats like this are an integral part of Russia's "asymmetric response" to perceived security challenges:

> *"Asymmetrical actions in the military field may include:* ***measures making the opponent apprehensive*** *of the Russian Federation's intentions and responses;* ***demonstration of the readiness and potentialities*** *of the Russian Federation's groups of troops (forces) in a strategic area to repel an invasion with consequences unacceptable to the aggressor; actions by the troops (forces) to deter a potential enemy by* ***guaranteed destruction of his most vulnerable*** *military and other strategically important and* ***potentially dangerous targets*** *in order to persuade him that his attack is a hopeless case."*[133]

Furthermore:

> *"Any forms and methods will do to* ***deter*** *the aggressor* ***by force****, such as… an ultimatum with a caution that Russia would (in the event of war) use nuclear weapons immediately and exercise no restraint in employing high-precision weapons to destroy strategically vital objectives on the aggressor's territory; and planning and conduct of an information campaign to mislead the adversary about Russia's readiness*

war (accessed 6 July 2016).

132 This is a perennial feature of Russian messaging, despite the deployments proceeding according to a long-planned schedule. For two recent examples of this schedule being treated as news, see Andrew Osborn, "Russia seen putting new nuclear-capable missiles along NATO border by 2019," *Reuters*, 23 June 2016, http://www.reuters.com/article/us-russia-europe-shield-idUSKCN0Z90WT (accessed 24 June 2016). and "Iskander-M missile systems to be deployed in Kaliningrad region till 2018" [sic], *TASS*, 16 May 2015, http://tass.ru/en/russia/795113 (accessed 24 June 2016).

133 S. G. Chekinov and S. A. Bogdanov, "Асимметричные действия по обеспечению военной безопасности России" (Asymmetric actions to provide for the military security of Russia), *Voennaya Mysl'* (Military Thought), No. 3 2010, p. 10. Emphasis as in original.

to beat off aggression."[134]

Troll Farms and Botnets

One of the most prominent aspects of Russian information campaigning in Western public consciousness is the ubiquitous activities of trolls (online personae run by humans) and bots (run by automated processes), interacting directly with readerships in a range of media.[135] A substantial body of research on Russian troll campaigns has developed in the West since early 2014, some of which is listed in "Further Reading" below.

These false accounts can pose as authoritative information sources, redistributing disinformation from sock puppet media outlets. But in addition to this use of trolling as a direct injection method, the effect can also on occasion be subtle and indirect, and contribute to the aim described above of establishing a permissive environment. This can be achieved by diverting or suppressing any debate that runs counter to the Russian version of events, and thus creating an atmosphere and an impression of consensus, rather than pushing specific disinformation or narratives.[136] In addition, on occasion the intent of online trolling can be indistinguishable from the original (internet) meaning of the word – simply provoking argument and confusion. As described in one Ukrainian study, "it is important to keep in mind that arguments with a troll are not really discussions with a real person but with a virtual image created specifically to sow discord."[137] This remains true whether the troll

134 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. Emphasis as in original.

135 Lawrence Alexander, "Social Network Analysis Reveals Full Scale of Kremlin's Twitter Bot Campaign," 2 April 2015, http://globalvoicesonline.org/2015/04/02/analyzing-kremlin-twitter-bots/ (accessed 27 June 2016).

136 As described for example in R. Read, "Poland Is Under Assault From Russia's Cyber Troll Propaganda Army," The Daily Caller, 23 June 2016, http://dailycaller.com/2016/06/23/poland-is-under-assault-from-russias-cyber-troll-propaganda-army/ (accessed 27 June 2016).

137 Yuriy Savytskyi, "Kremlin trolls are engaged in massive anti-Ukrainian propaganda in Poland," EuroMaidan Press, 21 June 2016, http://euromaidanpress.com/2016/06/21/kremlin-trolls-are-engaged-in-massive-anti-ukrainian-propaganda-in-poland/ (accessed 27 June 2016).

is acting on behalf of Moscow or not.

Factors like these leave mainstream media unsure as to whether the sway of opinion reflected in their correspondence or comments pages is genuine and should be publicised, reported or reflected in editorial lines. Despite widespread experience of the hostile attentions of the Russian social media armies over the course of more than a year, some sections of the Western media require constant reminders of their intent and their effect.[138]

This persistent amnesia also augments the effectiveness of troll and bot intimidation of journalists, researchers and authors who are critical of Moscow. Once their work is considered sufficiently important or influential to pose a risk of discrediting Russia, they are subjected to a broad campaign of harassment and intimidation of which troll and bots constitute an integral part. The result is that writing about Russia entails either compromise, or a significant degree of personal, reputational, financial and social risk. While there are individuals who take this risk, suffer the consequences and continue to write, others entirely blamelessly decide that too much is at stake and retreat. This chilling effect represents a victory for Russian information campaigning.[139]

The origins of what is casually referred to as the "Kremlin Troll Army" can be traced to prototypes like the short-lived "Kremlin School of Bloggers" in the last decade, which pre-dated today's broad uptake

138 When commenting on Russian issues in live media interviews, the author has repeatedly had to explain to presenters and interviewers why their programmes were being suddenly deluged with e-mails and tweets in support of Russia and critical of Western policy.

139 For indicative examples, see E. Nakashima, "Russian hackers harassed journalists who were investigating Malaysia Airlines plane crash," Washington Post, 28 September 2016, https://www.washingtonpost.com/world/national-security/russian-hackers-harass-researchers-who-documented-russian-involvement-in-shootdown-of-malaysian-jetliner-over-ukraine-in-2014/2016/09/28/d086c8bc-84f7-11e6-ac72-a29979381495_story.html (accessed 28 September 2016), and S. Oksanen, "What It's Like To Write About Russia," 14 June 2016, UpNorth, http://upnorth.eu/sofi-oksanen-what-its-like-to-write-about-russia/ (accessed 15 September 2016). See also P. Tucker, "Exclusive: Russia-Backed DNC Hackers Strike Washington Think Tanks," Defense One, 29 August 2016, http://www.defenseone.com/threats/2016/08/exclusive-russia-backed-dnc-hackers-strike-washington-think-tanks/131104/ (accessed 15 September 2016).

of social media in Russia.[140] But the sophistication of the tools and processes in use is constantly developing, and the stereotype described in mainstream media or academic research tends to be consistently out of date and oversimplistic.

The nature of the trolls and bots themselves provides another example of how an oversimplified notion of Russian capabilities and assets may leave the targets of disinformation open to surprise.[141] Paid trolls are joined by misguided individuals in the target countries who support their activities for a wide range of personal reasons.[142]

This reflects a key principle described across information warfare theory, of exploiting already existing vulnerabilities and divisions in the target society:

> *"The vast majority of the population of the victim country does not even suspect that it is being subjected to information-psychological influence. This leads in turn to a paradox: the aggressor achieves his military and political aims with the active support of the population of the country that is being subjected to influence. Control over strategically important state resources is handed over voluntarily, since this is seen not as the result of aggression, but as a progressive movement toward democracy and freedom."*[143]

It is also normal for troll operators to take over previously established online personae with established authority in their respective media for authority, such as senior members of discussion boards or well-established Twitter accounts. These, and deliberate measures outlined in "Future

140 Nathan Hodges, "Kremlin Launches 'School of Bloggers,'" Wired, 27 May 2009, https://www.wired.com/2009/05/kremlin-launches-school-of-bloggers/ (accessed 23 June 2016).

141 See D. Herrick, "The Social Side of 'Cyber Power'? Social Media and Cyber 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 (accessed 20 June 2016).

142 "Portrait of a troll," Organized Crime and Corruption Reporting Project (OCCRP), 19 June 2016, https://www.occrp.org/en/other/5369-portrait-of-a-troll (accessed 21 June 2016).

143 Yu. Kuleshov et al., "Информационно-психологическое противоборство в современных условиях: теория и практика" (Information-Psychological Warfare In Modern Conditions, *op. cit.*, p. 108.

Prospects" below, mean that there is no easy method of determining the line between an orchestrated troll campaign and the expression of genuinely held, even if misguided, opinion. They also mean that the potential future impact of more sophisticated campaigns on social media – going far beyond influencing media coverage or public opinion - is at present underestimated.

Plausibility

Identifying and rebutting falsehood in Russian information campaigns has been a focus of Western overt counter-disinformation efforts. It is commonly suggested that the most effective response is "establishing an effective counter-narrative which calls a lie a lie," and learning "offensive stratcom that tells people the truth."[144]

But this may not be the most effective way of addressing the challenge overall, since plausibility or lack of it is not always a measure of Russia's success or failure in meeting its objectives.[145] While it is true that in the Russian view, "falsifying events and imposing restrictions on the activity of the mass media are among the most effective asymmetric means of warfare,"[146] this does not necessarily mean that this falsification is intended to be credible or persuasive. A RAND study from 2016 notes that this aspect of Russian campaigning directly contradicts accepted principles of successful information campaigns in the West - but this counter-intuitive nature makes it even harder to devise effective countermeasures.[147]

144 As described in J. Lindley-French, "Conference Report: 'NATO and New Ways of Warfare: Defeating Hybrid Threats'," NATO Defense College, 19 May 2015, http://www.ndc.nato.int/news/news.php?icode=814 (accessed 20 July 2016).

145 See for example N. MacFarquhar, "A Powerful Russian Weapon: The Spread of False Stories," The New York Times, 28 August 2016, http://www.nytimes.com/2016/08/29/world/europe/russia-sweden-disinformation.html (accessed 29 September 2016).

146 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 (accessed 22 June 2016).

147 C. Paul, M. Matthews, "The Russian 'Firehose of Falsehood' Propaganda Model: Why It Might Work and Options to Counter It," RAND, 2016, http://www.rand.org/pubs/perspectives/PE198.html (accessed 15 September 2016).

There is no shortage of examples of statements by Russian media and official figures which are so remote from reality that they are not even expected to be believed by the listeners. At the time of writing, a recent prominent example is the threatening, but evidently nonsensical, language to Finland used by President Putin on a visit to the country in early July 2016. According to Putin, in the event of Finland joining NATO, Russia would reverse the current situation where "we have pulled back our troops from the border between Finland and Russia to a distance of 1,500 kilometres" – which if true, would mean most of European Russia was demilitarised.[148]

Multiple untruths, not necessarily consistent, are in part designed to undermine trust in the existence of objective truth, whether from media or from official sources. This contributes to eroding the comparative advantages of liberal democratic societies when seeking to counter disinformation, by neutralizing the advantages associated with credibility.[149] Even the existence of mutually contradictory Russian narratives is not an inherent disadvantage as described in some Western analysis. As described in a Finnish study:

> *"As the main objective of these measures is to dazzle and disorient Western public [sic], running several parallel narratives is not a deficiency, but an asset and important feature of Russian strategic deception."*[150]

In addition, countering every single piece of Russian disinformation is labour-intensive out of all proportion to the result. According to US

148 A. Vinokurov, "Путин рассказал финнам о войне с НАТО" (Putin tells the Finns about war with NATO), Gazeta.ru, 1 July 2016, https://www.gazeta.ru/politics/2016/07/01_a_8353601.shtml (accessed 28 September 2016). See also English-language explanation at "Putin's comment about location of Russian troops baffles" [sic], Yle News, 2 July 2016, http://yle.fi/uutiset/putins_comment_about_location_of_russian_troops_baffles/9000152 (accessed 20 July 2016).

149 See Maria Przełomiec, 'Is the West able to effectively fight back against Russia's information war?', Polish Institute of International Affairs, 27 February 2015, https://blog.pism.pl/blog/?p=1&id_blog=36&lang_id=12&id_post=512.

150 K. Pynnöniemi and A. Rácz (eds.), Fog of Falsehood: Russian Strategy of Deception and the Conflict in Ukraine, FIIA Report No. 45, 10 May 2016, p. 18.

ambassador to Ukraine Geoffrey Pyatt:

> *"Everyone knows the Kremlin seeks to use information to deny, deceive, and confuse… You could spend every hour of every day trying to bat down every lie, to the point where you don't achieve anything else. And that's exactly what the Kremlin wants."*[151]

But over and above tactical questions, the evolving nature of political life in the West itself poses a more fundamental challenge to a model for information confrontation that relies on "truth." Recent Euro-Atlantic political phenomena such as the popularity of Donald Trump as a presidential candidate in the United States, and the obscuring of fact by speculation and fantasy in the UK's debate over leaving the EU,[152] have highlighted the trend towards what has been described as a "post-fact" or "post-truth" political environments.[153]

In this context, when Russia seeks to undermine trust in authority figures, much of its work has already been done. Challenging Russian false narratives needs to overcome the basic obstacle of prominent Western politicians also relying on falsehoods to achieve political resolutions, and the proliferation of unchallenged false and spurious arguments that ensues from the resulting lack of trust.[154]

"Nothing Is True and Everything Is Possible" was the title of a book published in late 2014 by journalist Peter Pomerantsev, which did much to bring the Russian use and abuse of information to greater notice. But its title could equally well be applied to the attitude of those sections of

151 'Interview: U.S. Ambassador Geoffrey Pyatt on Euromaidan, Ukrainian reforms and Kremlin trolls', *Business Ukraine*, 5 December 2015, http://bunews.com.ua/interviews/item/interview-us-ambassador-geoffrey-pyatt-on-euromaidan-ukrainian-reforms-and-kremlin-trolls.

152 "'Glaring deficiencies' in EU debate, Electoral Reform Society says," BBC News, 1 September 2016, http://www.bbc.com/news/uk-politics-37238641 (accessed 15 September 2016).

153 For discussion and detail, see "Art of the lie: Politicians have always lied. Does it matter if they leave the truth behind entirely?" The Economist, 10 September 2016, http://www.economist.com/news/leaders/21706525-politicians-have-always-lied-does-it-matter-if-they-leave-truth-behind-entirely-art (accessed 15 September 2016).

154 Such as, to take an example popular in Russia, the deception practiced by then Prime Minister Tony Blair to lead the United Kingdom into war with Iraq during 2002-3.

Western societies which instinctively distrust authority.[155] In this manner, Russia today is reaping unexpected benefits from Soviet campaigns targeting previous generations. An intellectual heritage permeated by postmodernist and relativist attitudes has now laid down fertile ground for disinformation and deception campaigns not only among Western historians, academics and even left-wing politicians, but among wide sectors of society not sufficiently well informed or motivated to sift evidence for themselves. Just as with overt and covert information activities in former decades, so in the current environment in some cases Russia does not instigate social or intellectual trends, merely exploits them for perceived strategic advantage.

It follows that effective answers to Russian information campaigning lie elsewhere than in simple rebuttals. But they are also dependent on the future, not current shape of information warfare capabilities. These are evolving rapidly, and will be discussed in the next section.

Further Reading

In English

The Ukraine Campaign

- K Geers (ed.) *Cyber War in Perspective: Russian Aggression against Ukraine,* NATO CCD COE, Tallinn, December 2015, https://ccdcoe.org/multimedia/cyber-war-perspective-russian-aggression-against-ukraine.html (accessed 13 July 2016).

- T. Maurer and S. Janz, "The Russia-Ukraine Conflict: Cyber and Information Warfare in a Regional Context," *The International Relations and Security*

155 An unintentionally revealing comment by an instructor on a BBC journalism course attended by this author in the mid 1990s was: "Don't trust any government officials. They may be wearing a suit, but it doesn't mean they're stupid."

Network, October 17, 2014, http://www.isn.ethz.ch/Digital-Library/Articles/Detail/?id=184345

- K. Pynnöniemi and A. Rácz (eds.), Fog of Falsehood: Russian Strategy of Deception and the Conflict in Ukraine, FIIA Report No. 45, 10 May 2016.

- M. Jaitner and P.A. Mattsson, "Russian Information Warfare of 2014," in M. Maybaum et al. (eds.), *2015 7th International Conference on Cyber Conflict*, NATO CCDCOE, Tallinn, 2015, https://ccdcoe.org/cycon/2015/proceedings/03_jaitner_mattsson.pdf (accessed 13 July 2016).

  (An overview of information operations in the early stages of the Ukraine crisis.)

- J. Darczewska, "The anatomy of Russian information warfare: the Crimean operation, a case study," *Point of View* No. 42, OSW, May 2014, http://www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_information_warfare.pdf (accessed 13 July 2016).

  (A survey of the ideological background to planning and implementation of information operations in Crimea.)

- R Szwed, *Framing of the Ukraine–Russia conflict in online and social media*, NATO Strategic Communications Centre of Excellence, May 2016, http://www.stratcomcoe.org/framing-ukraine-russia-conflict-online-and-social-media (accessed 20 June 2016).

- *Analysis of Russia's information campaign against Ukraine*, NATO Strategic Communications Centre of Excellence, July 2015, http://www.stratcomcoe.org/analysis-russias-information-campaign-against-ukraine-1 (accessed 20 June 2016).

- A. Rácz, *Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist*, Finnish Institute of International Affairs, Report No. 43, Helsinki, 2016, http://www.fiia.fi/en/publication/514/russia_s_hybrid_war_in_ukraine/ (accessed 13 July 2016).

Social Media, Trolls and Bots

- T. E. Nissen, "#TheWeaponizationOfSocialMedia @Characteristics_of_Contemporary_Conflicts" [sic], Royal Danish Defence College, March 2015.

- Wikipedia entry on "Web brigades," https://en.wikipedia.org/wiki/Web_brigades

- "What's it like to be hated by the Russian internet?" *The Guardian*, 26 May 2015, http://www.theguardian.com/world/2015/may/26/russia-internet-hated

Broader Russian Influence and Approaches

- P. Pomerantsev & M. Weiss: *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*. The Institute of Modern Russia, New York 2014.

- Kovalev, "Life after facts: how Russian state media defines itself through negation," Open Democracy, 13 June 2016, https://www.opendemocracy.net/od-russia/alexey-kovalev/life-after-facts-how-russian-state-media-defines-itself-through-negation (accessed 19 July 2016).

  (An enlightening exploration of the reasons for acceptance of propaganda and obvious fabrications by Russian audiences.)

- Antczak-Barzan, "Russian phobia or a real threat? Propaganda-based elements of Russian hybrid warfare and their implications for NATO," NATO Defense College, forthcoming publication.

- M. Winnerstig (ed.), "Tools of Destabilization: Russian Soft Power and Non-military Influence in the Baltic States," FOI report FOI-R--3990--SE, December 2014.

- R. Skaskiw, "Nine Lessons of Russian Propaganda," *Small Wars Journal*, 27 March 2016, http://smallwarsjournal.com/jrnl/art/nine-lessons-of-russian-propaganda (accessed 19 July 2016).

- "Written evidence submitted by Ben Nimmo and Dr Jonathan Eyal: Russia's information warfare - airbrushing reality," *House of Commons Select Committee on Defence*, UK Parliament, 14 March 2016, http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/defence-committee/russia-implications-for-uk-defence-and-security/written/30408.html (accessed 19 June 2016).

  (Focusing more closely on Russian influence exerted in and on the UK during the Brexit referendum campaign.)

- B. Nimmo, "Anatomy of an Info-War: How Russia's Propaganda Machine Works, and How to Counter It," *Stopfake.org*, 19 May 2015, http://www.stopfake.org/en/anatomy-of-an-info-war-how-russia-s-propaganda-machine-works-and-how-to-counter-it/ (accessed 27 June 2016).

- M. Van Herpen, *Putin's Propaganda Machine. Soft Power and Russian Foreign Policy*. Rowman & Littlefield, Lanham, Maryland, USA, 2016.

In Russian

- 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* No. 1 (46), 2014, pp. 104-110.

6. Future Prospects

Russia's concepts of operations are in constant development, and future campaigns will not resemble the ones seen to date. The process of rotating as broad a range of personnel as possible through operational deployments to the Ukrainian border and to Syria is mirrored by an intensive programme of applying lessons learned in both theatres.

The US assessment is that eastern Ukraine presents "an emerging laboratory for future 21st-century warfare."[156] Here, Russia and Russian-backed militias have made use of their access to highly sophisticated and effective electronic attack technology, including GPS spoofing to defeat navigational and guidance systems.[157] Meanwhile, Russian descriptions of operations in Syria emphasise how military force is no longer the primary determinant of effect and can take second place to other elements of state power. As expressed by Chief of General Staff Valeriy Gerasimov, in contemporary conflict, "the emphasis on the methods of fighting moves toward the complex application of political, economic, information, and other nonmilitary means, carried out *with the support of military force*."[158]

Gerasimov also explains that Russian experience of campaigning in Syria has confirmed the advantages of:

> *"achieving political goals with the minimum armed impact on an adversary. Predominantly by undermining his military and economic potential, by applying informational and psychological pressure, and by*

156 G. Warwick, "Assisting The Human Central to Pentagon's Third Offset," *Aviation Week*, 4 January 2016, http://aviationweek.com/defense/assisting-human-central-pentagon-s-third-offset (accessed 15 July 2016).

157 P. Tucker, "In Ukraine, Tomorrow's Drone War Is Alive Today," Defence One, 9 March 2015, http://www.defenseone.com/technology/2015/03/ukraine-tomorrows-drone-war-alive-today/107085/ (accessed 15 July 2016); "Russia overtaking US in cyber-warfare capabilities," SCMagazine.com, 30 October 2015, http://www.scmagazine.com/russia-overtaking-us-in-cyber-warfare-capabilities/article/450518/ (accessed 15 July 2016).

158 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 (accessed 22 June 2016, emphasis added).

active support for internal opposition and for insurgency and subversive methods."[159]

This confirms the trend noted from Russian operations in Ukraine; a shift of emphasis reducing the relative weight of forms of intervention which are overt, as was seen in Russian operations in Georgia in 2008, and increasing that of those that are covert, deniable (plausible or otherwise), and completed before open hostilities are declared or begun. Overall:

"Informational and psychological operations in future wars will have to comply with the basic principles of new type (hybrid) warfare - they must be timely, unexpected, and clandestine."[160]

Internet Infrastructure

Nevertheless, current activities do provide pointers to the possible shape of future Russian operations. Intensified investigation of foreign civilian internet communications infrastructure is likely to be an indicator of planning options under consideration.

In multiple domains, Russia appears to be showing an increased sense of urgency in this task, with the result that previously discreet activities are now widely reported. A prime example is investigation of subsea communications cables. This is believed to be one of the tasks of Russia's Main Directorate for Deep-Water Research (GUGI), a previously highly secretive organisation which is now receiving public attention due to the greatly increased tempo and prominence of its operations.[161]

Meanwhile in space, unusual manoeuvres carried out by Russian

159 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 (accessed 22 June 2016).

160 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.

161 See "Main Directorate of Deep-Sea [sic] Research (Military Unit 40056)," Globalsecurity.org, undated, http://www.globalsecurity.org/intell/world/russia/gugi.htm (accessed 20 July 2016).

vehicles in the vicinity of communications satellites[162] combine with an intensive programme of test launches of anti-satellite weapons[163] in an alarming pattern of rehearsal for hostile action. Disruption of adversary satellite communications would be considered a key enabling factor of information dominance providing important advantages in conventional warfare:

> *"Modern leading states manage communications, navigation, reconnaissance, the whole command of strategic nuclear forces and aerospace defence, and high-precision conventional weapons through space. Disrupting this entire system through radio-electronic and other asymmetric means could greatly reduce this advantage of the adversary."*[164]

The reason for this interest may well lie in the Russian experience of effective interference with civilian telecommunications infrastructure leading to information dominance in Crimea in March 2014, but these are not the only implications. Investigating and exploiting vulnerabilities of internet infrastructure can facilitate espionage operations, isolation, or means of planting disinformation - or a combination of all of these. In addition, information interdiction should also be thought of in a broader context. Capabilities displayed by Russia in eastern Ukraine include a much enhanced electronic warfare (EW) capability, including for GPS jamming.[165] Even where physical access to facilities is not available, a role is described for Russia's EW forces in suppressing civilian traditional and online media:

> *"The EW forces will take on a new mission in this operation [the*

162 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

163 Bill Gertz, "Russia Flight Tests Anti-Satellite Missile," Washington Free Beacon, 27 May 2016, http://freebeacon.com/national-security/russia-flight-tests-anti-satellite-missile/ (accessed 19 July 2016).

164 Army General Mahmut Gareyev, cited in "Как развивать современную армию?" (How to develop a modern army?), Krasnaya Zvezda, 10 March 2016, http://www.redstar.ru/index.php/syria/item/28017-kak-razvivat-sovremennuyu-armiyu (accessed 22 June 2016).

165 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/.

initial phase of conflict] - blocking radio and television signals, and signal traffic in social networks to shut out propaganda disinformation pouring into the ears of the population and Armed Forces personnel."[166]

The sense of urgency appears to extend into CNO. As put in February 2016 by US Director of National Intelligence James Clapper, "Russia is assuming a more assertive cyber posture based on its willingness to conduct operations even when detected and under increased public scrutiny."[167]

As a consequence, NATO "should be prepared to operate despite the loss or disruption of cyber infrastructure and hardware, including loss of space assets, network servers, undersea cables, radio communications, and power generation."[168] In other words, in time of conflict NATO states may find that access to internet resources may be degraded or entirely absent – including for the purposes of communicating with their own civilian populations or Armed Forces personnel outside hardened and discrete networks. 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. Assessments voiced by senior NATO officers in open debate include the suggestion that at the outset of hostilities, Russian EW assets deployed in Kaliningrad could shut down communications over large areas of the region's NATO neighbours.

Russia may already have undertaken steps to prepare for this kind of operating environment. According to a well-informed Russian general speaking in 2012, Russia had detected that its military officers were

166 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.

167 J. R. Clapper, US Director of National Intelligence, Worldwide Threat Assessment of the US Intelligence Community, Senate Armed Services Committee Statement for the Record, 9 February 2016, https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf (accessed 1 July 2016).

168 "Framework for Future Alliance Operations," North Atlantic Treaty Organisation, August 2015, available at http://www.act.nato.int/images/stories/media/doclibrary/ffao-2015.pdf, p. 41 (accessed 28 June 2016).

losing the skills of "low tech war," and consequently required additional "training to face an opponent with total information superiority." In particular the Kavkaz-2012 exercise had shown that officers were losing the ability to work without information systems – "so when information support and command and control systems are switched off, there are problems." The answer was "how to teach officers to work with paper maps again, not electronic ones."[169] And as noted above, the Russian Security Council is reported to have investigated the implications of the country operating without internet access at all.

Convergence

The requirement to think of cyber and information vulnerabilities in the physical domain as well is a symptom of what Martin Libicki refers to as "convergence," the integration of capabilities cutting across disciplines which the West has traditionally thought of as disconnected. Close observers of Russian operations in Ukraine have noted that these operations make use of "not just cyber, not just electronic warfare, not just intelligence, but […] really effective integration of all these capabilities with kinetic measures to actually create the effect that their commanders [want] to achieve."[170] As assessed by a study of the new dimension of commercial UAV warfare in Ukraine, "experience of current combat operations shows that the dividing lines between these different kinds of warfare are becoming increasingly blurred and irrelevant."[171]

But this is to apply a Western perspective to Russian planning, which

169 Lt-Gen Andrei Tretyak, former head of Main Operations Directorate, speaking at NATO Defense College, 27 November 2012.

170 S. J. Freedberg, "Army Fights Culture Gap Between Cyber & Ops: 'Dolphin Speak'," BreakingDefense.com, 10 November 2015, http://breakingdefense.com/2015/11/army-fights-culture-gap-between-cyber-ops-dolphin-speak/ (accessed 15 July 2016)

171 K. Hartmann and K. Giles, "UAV Exploitation: A New Domain for Cyber Power," in N. Pissanidis et. al (eds.), Cyber Power: 8th International Conference on Cyber Conflict, NATO CCDCOE, Tallinn, 2016, https://www.academia.edu/25921967/UAV_Exploitation_A_New_Domain_for_Cyber_Power (accessed 4 July 2016).

as always risks fundamental misinterpretation. Russian military planners do not need to grapple with the problem of convergence in the same way as their Western counterparts, because – thanks to the holistic and integrated approach to information warfare – they never went through a process of divergence in the first place.

Characteristic in this integrated information warfare spectrum is the prominent role of Russian EW capabilities, the subject of belated concern in Western militaries. According to a Russian assessment in 2010, "in the near future fundamental changes in the development of EW means and materiel should allow it to develop into a specific main form of combat action, which in many ways will determine the course and outcome of armed conflict," since "the effect of the actions of EW means are comparable with the use of modern high-precision weaponry."[172]

Furthermore,

> *"Future wars will be launched by electronic warfare (EW) forces, which will protect friendly forces, block foreign propaganda disinformation, and strike at enemy EW forces and assets, blending with strategic and aerospace operations, with the latter augmented by cruise missiles and reconnaissance assets (UAVs, robots) delivering strikes and fires."*[173]

Beyond this application of EW effects to targets which lie outside the Western conceptual framework, there is a further significant implication for NATO force planners. After the experiences of Iraq and Afghanistan, rather than return to a structure and posture for conventional warfare as it was conceived in previous decades, NATO should be prepared to defend itself in an entirely new operating environment and under entirely new conditions.

---

172 "Состояние сил РЭБ: интервью с начальником войск РЭБ ВС РФ О. Ивановым" (The condition of the EW Troops: interview with commander of the RF EW Troops O. Ivanov), *Krasnaya Zvezda*, 15 April 2010.

173 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.

Social Media Preparations

A process of building up of capabilities on social media is visible, in particular in the form of accumulation of trusted social media accounts with large networks and numbers of followers. These accounts are at the present moment not used for any overtly hostile process, but engaged in establishing their credibility, and developing tactics for defeating analytical methods used to identify false personae. In particular these tactics include tailored and sophisticated features which generate followers and interaction from genuine accounts.

It has been argued that as well as state-sponsored disinformation, the use of trolls and bots in this manner can also be explained by marketing exercises. But this argument overlooks the fact that in exactly the same way that the tactics, techniques and procedures for cybercrime are the same as those used for cyber espionage, so marketing on the one hand, and maximising the visibility of disinformation on the other, also use exactly the same techniques.[174]

Examples are already available of how the transfer between one domain and another is seamless.[175] Twitter accounts can follow this pattern, with examples of accounts that were originally set up to generate revenue as click bait now repeating Russian disinformation, with profiles providing links to RT.[176] Russia has also taken opportunities to hijack already existing authoritative social media accounts.[177] In addition to those instances already visible, it can be assumed that other high profile accounts are also under Russian or Russian-backed control, and ready to

174 This overlap is discussed, inter alia, in Jeffrey L Caton, "Distinguishing Acts Of War In Cyberspace: Assessment Criteria, Policy Considerations, And Response Implications," U.S. Army War College Strategic Studies Institute, October 2014.

175 For further analysis, see Kenneth Geers, "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 (accessed 29 June 2016).

176 Private correspondence with Joonas Vilenius, CIO of WG Consulting, a social media intelligence consultancy.

177 Patrik Oksanen, "TV4:s twitter blev ryskt," helahälsingland.se, 3 February 2015, http://www.helahalsingland.se/opinion/ledare/tv4-s-twitter-blev-ryskt (accessed 21 July 2016).

be put into use at the appropriate moment.

Targeting Personnel

Another campaign for which Russia appears to be developing, testing and accumulating capabilities is the targeting of personnel, *en masse* but on a personalised basis. NATO should be prepared for false messaging on a mass scale, directed to named individuals, which appears to come from trusted sources personally known to those individuals.

Painstaking individual collection of data on targets need not be undertaken when identities and credentials are broadcast by smartphones, and therefore easily harvested and processed on an industrial scale by anyone with the capability to pretend to be a legitimate ISP – over and above the personal information that is volunteered online by even the most discreet users of social media. Russia deploys equipment in eastern Ukraine and elsewhere which not only filters the information available to internet users, blocking access to a range of websites and replacing them with Russian sources, but also collects data from personal electronic devices.[178] In addition Russia watches which individuals from the militaries of NATO nations are posted within its easy reach, and has practised exploiting their vulnerabilities.[179]

These vulnerabilities continue to be offered for exploitation. Visitors to the Olympic Games in Sochi in 2014 received clear advice that "communications while at the Games should not be considered private," and that "travelers [sic] may want to consider leaving personal electronic devices (e.g. laptops, smartphones, tablets) at home."[180] But this was

178 "Army busts internet provider blocking access to Ukrainian websites, TV in east," Interfax-Ukraine, 6 January 2016. "Ukrainian troops find jamming device in Luhansk Region," InterfaxUkraine, 2 January 2016. See also Keir Giles, 'The Next Phase in Russian Information Warfare', NATO Strategic Communications Centre of Excellence, November 2015.

179 *Ibid*.

180 "Security Tip (ST14-001): Sochi 2014 Olympic Games," US-CERT, 4 February 2014, https://www.us-cert.gov/ncas/tips/ST14-001. See also R. Oliphant, "Russia planning 'near-total surveillance' of visitors, athletes at Sochi Winter Olympics," Daily Telegraph, 6 October 2013, http://www.telegraph.co.uk/news/

an isolated example of bringing attention to the dangers inherent in using connected devices in Russia. At the time of writing, behaviour by servicemen and officials from NATO nations in information security environments controlled by Russia continues to indicate a widespread lack of threat awareness.

The December 2015 cyber attacks on Ukrainian energy networks, with the accompanying mass telephone campaign preventing energy consumers from contacting their providers, was an aberration from the relative lack of visible cyber activity that characterized the remainder of the Ukraine conflict.[181] At the time of writing, speculation in open sources is continuing as to the attack's motivations and intended result. But while diverging from the general pattern of limited visible cyber attacks in the context of the Ukrainian conflict, the accompanying telephone campaign – in effect a mass denial of service attack suppressing information distribution and hampering recovery operations - tied in with the trend of testing and exploiting new methods of information conflict involving mass targeted communications. Other examples include the mass simultaneous telephoning of Polish military personnel from Russia, and precisely geographically targeted intimidatory text messages in Ukraine.[182]

The most dangerous feature of this targeting is information that appears to come from a trusted source, whether via text message, social media, or email. One possible scenario is for this capability to be used to spread mass and persuasive disinformation or false instructions at a critical moment in a crisis involving confrontation with Russia.

Exploitation

Multiple examples above demonstrate how activity in the information

worldnews/europe/russia/10359587/Russia-planning-near-total-surveillance-of-visitors-athletes-at-Sochi-Winter-Olympics.html (both accessed 21 July 2016).

181 P. Maldre, "The Many Variants of Russian Cyber Espionage," *op. cit.*

182 Detailed, together with other incidents, in K. Giles, The Next Phase of Russian Information Warfare, *op. cit.*

domain is used by Russia as a precursor or preparation for hostile action in other domains. It follows that Russia's focus on information as an enabler before and during conflict provides opportunities to gather indicators and warnings.

According to one authoritative Russian analysis, overt information campaigns in the approach to conflict should include

> *"a package of measures, including broadcasts of information on various communication channels about intensive and wide-ranging preparation of the Russian economy and public for war, mobilization of reservists in many age brackets, relocation of army units on high alert, and deployment of reserves from the heartland. This information must be backed up by false activities to be captured by adversary reconnaissance. A broad campaign is to be launched simultaneously to inform the public about the adversary's destructive motivations and intentions."*[183]

But in addition to observing these clear indicators and being fed "false activities," defensive intelligence preparations should include close monitoring of shifts and trends in Russian information campaigning, including on social media. At the level of theory, NATO has already recognised the need for investment in collection and analysis to exploit early signals in order to provide pointers to imminent Russian activity:

> *"It will be important for the Alliance to monitor and analyse adversarial messaging and narratives in order to contribute to the early network of indications and warning to help recognise, characterise and attribute an emerging hybrid threat. An adversary's message may be sophisticated and nuanced to address the target audience in each respective nation, or organization but by rapidly assessing an adversary's narrative, NATO may be able to get ahead and take the initiative."*[184]

183 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.

184 "Framework for Future Alliance Operations," North Atlantic Treaty Organisation, August 2015, available at http://www.act.nato.int/images/stories/media/doclibrary/ffao-2015.pdf, p.23 (accessed 28 June 2016).

One specific element of Russian capability which is strikingly understudied in open sources is the analysis function which must necessarily precede information campaigns. It is unlikely that Russia embarks on information operations without prior research and collection of operational intelligence, societal data and personal information to ensure their effectiveness. Russia itself appears to have arrived at the same conclusion with regard to the notional threat from the West. In July 2016, a law sponsored by former KGB officer Andrey Lugovoy was passed by the State Duma criminalising research into Russian television audiences by foreign organisations.[185] Shortly afterwards, the highly-regarded and independent Levada-Center polling organisation was given "foreign agent" status, effectively curtailing its activities.[186]

This move was widely interpreted in the West as an indication of weakness or nervousness by the Russian leadership over domestic public opinion.[187] Instead, it suggests that suggests that target audience analysis is viewed as a critical enabler of information warfare, and Russia has moved to close off this vulnerability. It follows that similar audience research activities conducted or commissioned by Russia within NATO member states should be assessed as probing for vulnerabilities, and part of the process of Russia determining its key measure of the correlation of forces and means (COFM) with regard to information warfare. Consequently, this too would contribute to indicators and warnings of the future direction of Russian effort.[188]

185 Chris Dziadul, "Major blow for TNS in Russia," Broadband TV News, 23 June 2016, http://www.broadbandtvnews.com/2016/06/23/major-blow-for-tns-in-russia/ (accessed 21 July 2016).

186 "Поддержка Левада-Центра" (Support for Levada-Center), *Levada-Center*, 12 September 2016, http://www.levada.ru/2016/09/12/podderzhka-levada-tsentra/ (accessed 29 September 2016).

187 "'Strongman' Putin is so fragile, he's cracking down on polling," *The Washington Post*, 13 September 2016, https://www.washingtonpost.com/opinions/global-opinions/strongman-putin-is-so-fragile-hes-cracking-down-on-polling/2016/09/13/354f4374-7917-11e6-bd86-b7bbd53d2b5d_story.html (accessed 15 September 2016).

188 COFM in Russian usage is a tool to reveal Russian advantages and adversarial disadvantages, and hence identify opportunities to project force, whether military or nonmilitary. In the past this has involved intensive programmes of assigning numerical values to threats and capabilities in order to calculate the balance of power, with the assumption that imbalance in the adversary's favour was inherently unstable and threatening, regardless of their intent. See Thomas, "Thinking Like A Russian Officer," op. cit., and interview with Vladimir Pavlovich Kravchenko, former head of the KGB First Main Directorate Foreign Intelligence

Further Reading

- K. Giles, "The Next Phase of Russian Information Warfare," *NATO Strategic Communications Centre of Excellence*, November 2015, http://www.stratcomcoe.org/next-phase-russian-information-warfare-keir-giles (accessed 20 June 2016).

- "Internet Trolling as a hybrid warfare tool: the case of Latvia," *NATO Strategic Communications Centre of Excellence*, undated, http://www.stratcomcoe.org/internet-trolling-hybrid-warfare-tool-case-latvia-0 (accessed 20 June 2016).

- For a case study of the preparatory information campaign ahead of the Russian intervention in Syria, see M. Czuperski et al., "Distract Deceive Destroy: Putin at War in Syria," *Atlantic Council*, undated, http://publications.atlanticcouncil.org/distract-deceive-destroy/ (accessed 27 June 2016).

- K. Hartmann and K. Giles, "UAV Exploitation: A New Domain for Cyber Power," in N. Pissanidis et al. (eds.), *8th International Conference on Cyber Conflict: Cyber Power,* NATO Cooperative Cyber Defence Centre of Excellence, https://ccdcoe.org/sites/default/files/multimedia/pdf/CyCon_2016_book.pdf (accessed 22 June 2016), pp. 205-222.

Information Systems Scientific Research Institute (НИИ информационных систем внешней разведки Первого Главного Управления КГБ СССР), *Alfa-Resurs*, undated, http://www.specnaz.ru/article/?1261 (accessed 1 July 2016).

7. Conclusion

Five final points deserve to be emphasised.

NATO and Western policymakers cannot afford to underestimate the extent to which Russian concepts and approaches in information activities differ from what they may take for granted. Options for action at all levels, strategic, operational and tactical, which appear rational in NATO capitals should not be taken as a guide to what appears sensible or practical in Moscow.

This includes the specific question of when, or whether, hostile action in information space or cyberspace constitutes an act or state of war.[189] As noted above, an overt state of conflict with Russia need not necessarily exist in order for Russian capabilities to be deployed. But this also means that in information space, as elsewhere, activities by NATO nations which appear to them to be entirely innocent and unprovocative can be assessed from Moscow as immediately hostile, and provoke a reaction which once again takes NATO by surprise.

The Russian challenge in the information domain is not static, but constantly and rapidly evolving. This includes absorbing and adapting lessons both from foreign military experience, and from Russia's own current operations in Ukraine and Syria. It follows that NATO and its member states must remain agile and adaptable even simply to track the current state of Russian theory and capabilities, let alone to devise plausible countermeasures.

At the same time, Russian information activities take place against a background noise of similar processes. Distinguishing hostile information operations commissioned abroad from home-grown legitimate dissent is challenging, but vital.

189 As detailed in K. Giles and A. Monaghan, Legality in Cyberspace: An Adversary View, U.S. Army War College Strategic Studies Institute, March 2014, http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=1193 (accessed 23 June 2016).

Finally, in information warfare, there are no rear areas. According to Russian CGS Valeriy Gerasimov, a key feature of modern warfare is "simultaneous effects to the entire depth of enemy territory, in all physical media and in the information domain."[190] If and when information warfare with Russia moves to an overt phase, it is not just NATO servicemen that will be the targets; but their families, their communities, their societies and their homelands, no matter how safely far away from Russia they may presently consider themselves to be.

190 V. V. Gerasimov, "Роль Генерального штаба в организации обороны страны в соответствии с новым Положением о Генеральном штабе, утвержденным Президентом Российской Федерации" (The Role of the General Staff in the Organization of the Country's Defense in Accordance with the New Statue on the General Staff, Approved by the President of the Russian Federation*), Vestnik Akademii Voennykh Nauk* (Bulletin of the Academy of Military Science), No. 1 2014, pp. 14-22.

NATO Defense College, Via G. Pelosi, 00143 Roma, Italy