PECULIARITIES OF RUSSIAN INFORMATION OPERATIONS

Uku Arold

For an academic researcher it is not an easy task to define the information influence activities of the current Putin regime in a parsimonious way. Some of the obstacles are similar to the challenges that NATO and its nations face in adapting foreign policy, the military, and intelligence organisations in today's era of globalised information. Other obstacles are uniquely Russian, derived from aspects of a worldview and codes of conduct dating back to Soviet Socialist and even to Czarist times, or spring from the peculiarities of a regnant regime. In this introductory article overview of the phenomenon of Russian information operations, the reasoning for a taxonomy referring to NATO terminology is provided in order to help readers categorise the findings of the following study papers in this volume. Methodological and empirical considerations specific for research on this partly amorphous subject area are discussed as well.

What are information operations?

Patrick D. Allen has highlighted the five most popular misconceptions of our own information operations in Western understanding.[1] In the light of these insights I provide an overview of the activities that are carried out under the umbrella term 'information operations'.

1. IO Is Not Just Slowing Down an Enemy's "OODA Loop"

   Allen explains: *While slowing the enemy's OODA loop is one way to use IO, there are other ways to use IO that don't delay the enemy's OODA loop, or that make the enemy's OODA loop irrelevant to the friendly objective. For example, if the friendly side has successfully convinced the enemy that a friendly deception plan is the real plan, then the friendly*

[1] **Allen, P. D**. 2007. Information Operations Planning. Boston, London: Artech House, pp. 14–18. [**Allen** 2007]

side does not want to delay the enemy walking into that trap. As Napoleon stated, "Never interrupt your enemy when he is making a mistake."[2]

Penetrating the adversary's decision-making processes is central to Military Deception (MILDEC) and Command and Control Warfare (C2W). However, the concept of information operations goes further. Modern military conflicts are not limited to two or more warring state actors. The primary aim for all parties is to gain legitimacy in the eyes of the civilian population and international public. Different actors have varying motivations and degrees of confrontation. As additional target audiences crucial to the success of the overall campaign emerge, no clear-cut line can be drawn between friends, neutrals, and enemies. In this globalised information era the battlespaces are just much more complex.

2. IO Is Not Just Influence Operations

Allen explains: *The phrase "IO is the name, influence is the game" is false (by being too limiting), but has appeared frequently in the psychological operations (PSYOP) community. /// But influence operations ignore the technical aspects of IO that act against opposing information and information systems and help protect friendly information and information systems.*[3]

This misguided approach has been common both in NATO policy circles and among military staffs. Although, according to the agreed concept for NATO, strategic psychological operations exist. In practice, policies and decisions aiming to influence foreign targets on a strategic scale have not usually been called by that name. In US case, 'military information support', 'global engagement', 'public diplomacy' and 'strategic communications' have been preferred approaches instead of the disputable term PSYOP. With raising awareness about the hazards of adversary propaganda, for want of a better term, 'information operations' was borrowed from the defence community and became popular.

---

[2] *Ibid*.

[3] **Allen** 2007.

3. IO Is Not Just Special Technical Operations (STO)

   Allen explains: *The community that is focused on the technical aspects of information storage, flows, and processing tends to forget that the ultimate aim of affecting information is to affect enemy decisions. /// This leads to another aspect of IO – you can't guarantee that the enemy will decide and act as you desire. Even if you have the perfect deception plan and have spoofed all of their information systems, the enemy may still make a decision that is contrary to where you have been trying to lead him.*[4]

   This point addresses the contemporary debate about cyber warfare in a more general way. In meaningful information operations, it is not bits and bytes that do things with other bits and bytes. These don't matter much. Information and communication technology (ICT) is just a vehicle to transport influence. Only if clever use of ICT (and not just in dystopian scenarios) can really have a significant impact on adversary Command and Control, or can change the behaviour of important social groups in a planned way, can we say that it matters. We should not invest in computers fighting heroically with other computers but should focus where the required influence could be attained. These targets are in the wider information environment – actual key people, logistic supply systems, relevant social groups and norms – and not in technology itself. As early as 1998, Robert L. Leonard declared the attack-defend approach to information warfare through the ICT and information systems lens 'totally useless' as, by its inherently symmetrical definition, it does not encompass the quintessential laws of war.[5]

4. IO Is Not Just Electronic Warfare (EW)

   Allen explains: *EW claim to the full EM spectrum appears to be an effort to control CNO and possibly the OPSEC core capabilities as well. However, there is much more to computer network operations than simply operating in the EM spectrum. First, for example, social engineering – non-electronic ways to gain access to computer networks – is completely separate from the EM spectrum. Second, focusing on the EM spectrum*

---

[4] *Ibid.*

[5] **Leonhard, R. R**. 2007. Sõjapidamisprintsiibid infoajastul [The Principles of War for the Information Age]. Tallinn: Eesti Entsüklopeediakirjastus, lk 215.

misses the longer time frames involved in CNO and IO. For example, placing a Trojan Horse virus for later access, or setting up for time-delayed launching of software or physical actions, does not benefit from focusing on just the EM spectrum. Third, physical access to, or interference with, a computer network is part of the CNO charter, yet that also lies beyond the EM spectrum. Fourth, although parts of military deception can be performed in the EM spectrum, many other parts cannot. Lastly, only a very small portion of PSYOP and other influence operations involve the EM spectrum.[6]

This approach has been popular in forces where people from Electronic Warfare branches have been tasked with developing concepts and doctrines for information operations. It does provide a holistic framework that is connected with hard physics. Metaphors from physics have always been tempting for military theorists: mass, energy, center of gravity, power, balance, etc. EW sub-disciplines are important players in many situations where information operations are the answer, but they do not help much in the battles of narratives.

5. IO Is Not Just Information Assurance

Allen explains: *The existing overlap among definitions of IO and IA are recognized by DoD's new IO definition. IO, by definition, involves an adversarial situation, where humans or manmade systems are designed to attack and defend, or compete against each other in the realm of influence. IA, however, is designed to ensure the confidentiality, integrity, and availability (CIA) of information regardless of the source of the threat to that information.*[7]

This approach is reflected in a number of study papers by different Western think tanks dealing with Russian disinformation. We have to safeguard our computers and secrets better and, in public, help to repair truth that is broken by the Russian 'war on information'. These are notions that should never be underestimated, but they still address only a fraction of Russian information operations.

---

[6] **Allen** 2007, pp. 14–18.

[7] *Ibid*.

Russian terminology

In Russian academic literature and normative documents regarding national security the term 'information operations' (*информационные операции*) is used mainly as a reference point to NATO or its member states' antiparallel doctrines and staffs. The terms 'Information-psychological operations' and 'information-technical operations' are used to signify a set of influence operations and a set of electronic warfare and cyber measures, respectively. The preferred umbrella term for both cerebral and wired aspects, as well as for offensive and defensive measures in information operations, is 'information confrontation' (*информационное противоборство*). The legacy of this concept is borrowed from the early US concept of 'information warfare' (now deceased) that has been adopted in Russia as 'information confrontation', 'information war(fare)' (*информационная война*) and 'information struggle' (*информационная борьба*). As the struggle has become considered officially permanent by Russia[8], the term 'information confrontation' has found its way into national security documents, "banning" information warfare has made it into Russian initiatives on 'international informational security', and this remains the name of central academic subject matter journal by the Russian Academy of Sciences and the Russian Military Academy[9]. The use of 'information struggle' sometimes refers to the tasks of units engaged in 'information confrontation' and is used as a more easily quotable but outdated synonym for 'information confrontation'.[10] [11] [12]

---

[8] **Герасимов, В**. 2013. Ценность науки в предвидении. [The Value of Science in Anticipation]. – Военно-промышленный Курьер, № 8 (476). 27.02–5.03.2013, стр. 1–3. <http://vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf> (accessed 10.05.2016).

[9] Journal ***Informatsionnye Voiny***. Scientific-practical interdisciplinary (military theory, philosophy, psychology, sociology, politics, economy, history, applied mathematics) journal. Issued since April 2007, 4 volumes in year, circulation: 1000. Principle editor is Moscow University Higher School of Contemporary Social Sciences department head, formerly Deputy Director FSB Vladimir Leopoldovich Schultz.

[10] **СМИ: Медведев поручил создать центр подготовки специалистов по информационным войнам** 2009. [Media: Medvedev ordered establisment of centre for preparation of information warfare specialists]. –Корреспондент.net, 8 октября 2009, 12:18. <http://korrespondent.net/world/russia/992318-smi-medvedev-poruchil-sozdat-centr-podgotovki-specialistov-po-informacionnym-vojnam> (accessed 10.09.2016).

[11] **Армия России впервые отработала информационное противоборство на учениях «Кавказ-2016»** 2016. [Russian Army for the first time worked on information confrontation during "Caucasus-2016" exercises]. – ТВ Звезда. 14 сентября 2016, 12:21 <http://tvzvezda.ru/news/vstrane_i_mire/content/201609141221-va0s.htm> (accessed 17.10.2016)

[12] **Interfax newswire** 14:02 14/09/2016. Information warfare group formed during Caucasus 2016 exercises.

Maj. Gen. I. N. Dylevsky *et al*. published an article in the institutional journal of Russian Ministry of Defence *Voyennaya Mysl* "On dialectics of deterrence and the prevention of military conflicts in the information age" where the renewed overall military doctrine is elaborated.[13] The Russian military doctrine of 2010 was renewed in 2014. Its main amendments were clearly connected with lessons identified from operations in and around Ukraine 2013–2014. Dylevsky *et al.* explain why in the 2010 revision, and much more in the 2014 revision, preparing units and facilities for information confrontation has such a high priority. It appears that by careful wording the authors balance providing an exhaustive overview for insiders while maintaining operational security from curious external eyes.

> *By means of information confrontation might consider: facilities of technical intelligence, specially designed or existing informational means, psychotronic means, means of special program-technical influence, means of information protection*.[14]

The military encyclopedic lexicon published on the Ministry of Defence webpage, originating from the 2007 print edition, gives a taxonomy of information confrontation means ('information weapons') as depicted in figure 1.

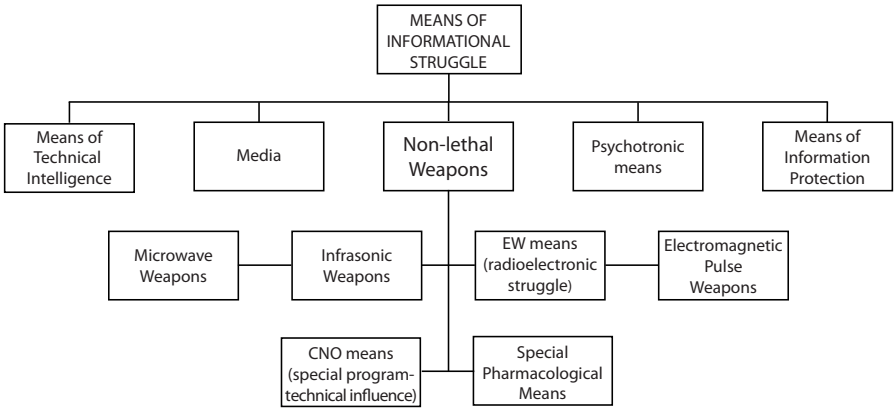

Figure 1. Means of informational struggle in 2007 – old view[15]

[13] **Дылевский, И. Н.; Запивахин, В. О.; Комов, С. А.; Коротков, С. В.; Кривченко, А. А**. 2016. О диалектике сдерживания и предотвращения военных конфликтов в информационную эру. – Военная Мысль, № 7/2016.

[14] *Ibid.*

[15] **Средства информационной борьбы** («Информационное оружие»). – Военный энциклопедический словарь. <http://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=14342@morfDictionary> (accessed 10.10.2016).

Former chief of the 5th Directorate of Operational HQ, Russian General Staff, Dylevsky indicates that most non-lethal weaponry, once fancy, have found their way out of the information confrontation paradigm for now. Tools and techniques that potentially have strategic impact have persisted in the sphere of favoured military thought, i.e., information confrontation. Intelligence, media, and information protection have fallen under the supervision of the national security council; information security and daily media management are guided from the presidential administration. There are indications that the psychotronic weapons programme (the Russian version of "Men staring at goats") has a prominent role in the upper echelons of national security circles. EW proved its efficacy during the Cold War and is now struggling for a larger role in information confrontation where cyber-people already claim major victories.

The most notorious of these is one of the first state-sponsored cyber espionage campaigns code-named by the targets as "The Cuckoo Egg", and most recently the accomplishments of APT-28 and APT-29 in hacking, manipulating and exposing the Democratic National Congress files. With considerable confidence, APT-28 aka Fancy Bear is attributed to the Russian internal security service FSB, and APT-29 to Russian military intelligence GRU. [16] [17] [18] Hence, the proven will and capability to engage in manipulating elections of the arch-enemy is something hard for EW (REB) forces to compete with.

There is a presidential grant recently awarded that motivates rationalisations on the subject of information confrontation.

One of the exemplary audits was made by the director of C2/engineering faculty, institute No. 37 of the Military Science Academy, Dmitri Sirotkin, and Alexandr Tyrtyshny, aspirant from the faculty of law, institute civic sciences, New Russian University[19]. Whereas authors focus on the defence

---

[16] **Alperovitch, D**. 2016. Bears in the Midst: Intrusion into the Democratic National Committee. – Crowdstrike Blog. June 15, 2016. <https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/> (accessed 18.10.2016).

[17] **Rid, T**. 2016. All Signs Point to Russia Being Behind the DNC Hack. – Vice News. Motherboard. July 25, 2016 // 08:55 AM. <http://motherboard.vice.com/read/all-signs-point-to-russia-being-behind-the-dnc-hack> (accessed 18.10.2016).

[18] **FireEye** 2014. APT28: A Window Into Russia's Cyber Espionage Operations? <https://www2.fireeye.com/rs/fireye/images/rpt-apt28.pdf> (accessed 18.10.2016).

[19] **Сироткин Д. В.; Тыртышный А. А**. 2016. Модель организации взаимодействия между федеральными органами исполнительной власти в области информационного противоборства. [Organisational cooperation model for federal organs of executive power in information confrontation]. – Информационные Войны, № 3/2016. [**Сироткин, Тыртышный** 2016]

activities of information confrontation, in the context of Russian newspeak it provides rather good insight into the existing legal framework of information confrontation defence capabilities corresponding to recent developments in the organisational national security setup. It does exclude the judicial branch of power as it is not graspable by the analysis of legal documents. The legislative branch is represented by status quo legislative acts as it does not have any independent legal agency. The internal work of the Presidential Administration can be identified just from its leading agenda of mass media and coercive measures by the presidential security organisation (Block 4) as, traditionally, its inner dynamics are not meant for legal consideration. The steering role of the military in information confrontation has considerably increased during the Russian-Ukrainian War, in a practical sense.

Among Russian power elites, belief in an almighty information confrontation has, qualitatively, an even bigger role than belief-in-spin among British political journalists. There is probably no trick used in Western political communication campaigns or in Defence information operations (or situations that are believed to be information operations) that Russia has not tried to emulate in its own context afterwards.

For Russia, *information confrontation* is the term that applies to tactical, operational, strategic and even grand strategic level. For NATO, *information operations* is a predominantly military activity on operational and tactical levels. Communications is brought to the heart of strategy under the umbrella term of Strategic Communications. Imperatives for strategic communications differ from those of information operations on several important points. For instance, democratic nations stress the obligation of national governments and of NATO to communicate policies and activities openly, honestly, and encourage dialogue. For people trained in the traditions of Soviet and contemporary Russian strategic thought, public statements are a smokescreen. Colonel V. Olevski, a frequent reviewer of NATO political and military transformations for Russian military journals, consistently translates NATO Strategic Communications to Russian in a blunt manner as 'strategic propaganda' (*стратегическая пропаганда*).[20] [21]

[20] **Олевский, В**. 2016. Доктрина психологических операций НАТО. [NATO psychological operations doctrine]. – Зарубежное военное обозрение, № 6/2016, стр. 28–36.

[21] **Олевский, В**. 2014. Концепция «Стратегической пропаганды» НАТО, ч. 1. [NATO concept of „strategic propaganda", part 1]. – Зарубежное военное обозрение, № 9/2014, стр. 9–16.

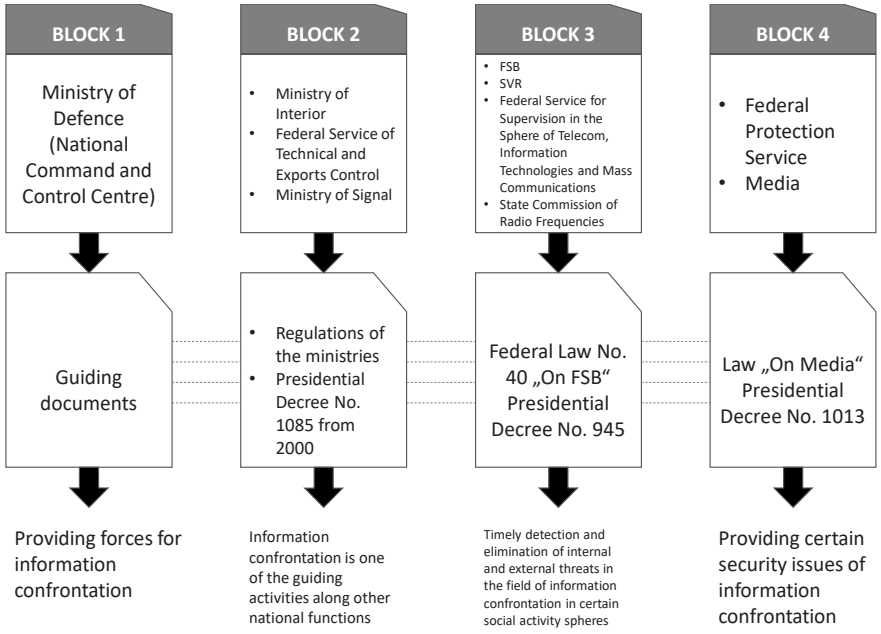

Figure 2. Organisational co-operation model for federal organs of executive power in information confrontation[22]

The term 'propaganda' does not have negative connotations in the vocabulary of Russian leaders. In December 2013 when Russia performed a major reshuffle among state controlled media in the wake of the Ukrainian campaign, Putin's press chief Dmitry Peskov stated: "*The tool of propaganda is an integral part of any state. It is everywhere. And Russia should use it as well. Propaganda in the good sense of the word*."[23] In the Soviet Army the function of psychological operations used to be called 'special propaganda' (*спецпропаганда*). In the Communist Party hierarchy and in important public organisations there were specific subunits for 'propaganda'. Guidelines were regularly printed for "agitators and propagandists" on how to explain current issues in working collectives.

This approach sits in high contrast to protestant cultures. Calling something 'propaganda' has been derogatory since its introduction in a Papal

[22] **Сироткин, Тыртышный** 2016.

[23] **The Moscow Times** 2013. Russia Needs More Propaganda, Putin Spokesman Says. December 20, 2013. <https://themoscowtimes.com/articles/russia-needs-more-propaganda-putin-spokesman-says-30646> (accessed 15.10.2016).

bull in 1622 on the establishment of counter-reformatory organisations.[24] [25] Communication theorist Denis McQuail draws attention to a common hypocrisy regarding use of the P-word: "*Generally, propaganda is conducted by an 'enemy' whereas 'our own' transfer information, proofs and arguments*."[26]

Russian approach to the internet

Russian information operations have become best known for their internet trolling campaigns. The phenomenon is not new in Russian internal politics where 'the commissars of the internet' or 'the brigadniki' have been generally acknowledged as players of the FSB and the Ministry of Interior's K Department since the 1990s. The primary purpose of said erstwhile trolls was to intimidate liberal voices into silence by publicly posting personal data and blunt personal insults against the intelligentsia.[27] An analogous US program that was revealed was called Operation Earnest Voice whereby an attempt was made in Muslim political internet forums to pacify militant sentiment using sockpuppet accounts. According to Russian schoolbooks on its own information operation officials, Op Earnest Voice is believed to have gone underground and been redirected to Putin, and the UK GCHQ JISTR programme is believed to target the Russian political system on a constant basis.[28] Generally, the use of MID talking points and Russian underworld jargon have caught the attention of trolls, making their impact weak. However, in some countries the business model of online journalism still encourages provocative anonymous comments "below the line", the lifeblood of normalizing covertly popularized Russian ideas among particular electorates.

---

[24] **Jowett, G. S.; O´Donnell, V**. 2006. Propaganda and Persuasion. (4th ed.). London-New Delhi: SAGE Publications, p. 72.

[25] **Taylor, P. M**. 2003. Munitions of the Mind: A history of propaganda from the ancient world to the present era. (3rd ed.). Manchester-New York: Manchester University Press, p. 111.

[26] **McQuail, D**. 2003. McQuaili massikommunikatsiooni teooria. [McQuail Mass Communication Theory]. Tartu: TÜ Kirjastus, lk 400.

[27] **Полянская, А.; Кривов, А. Ломко, И**. 2002. Комиссары Интернета. [Commissars of the internet]. <http://ipvnews.org/bench_article19112010.php> (accessed 20.10.2016).

[28] **Володенков, С. В**. 2015. Информационное противоборство как составляющая современных «гибридных войн»: роль и особенности. – «Гибридные войны» в хаотизирующемся мире XXI века. [Information confrontation as part of contemporary "hybrid wars" – its role and features" in compendium "Hybrid Wars" in Chaotic World of the XXI Century]. Москва: Издательство Московского университета, стр. 189–209.

The Putin regime has been always very careful about uncontrollable information flows. Putin himself called the internet "a CIA project" after claims about the NATO-made-Maidan and US-made Arab Spring.[29] For several years Russia has promoted a new area of international law, international information security, whereby information warfare and the development of information weaponry would be internationally banned. At the same time, all signatory parties would agree to a partitioning of the internet to nationally sovereign territories where the sovereigns are urged to track and capture any extremist.[30] Russia has proposed this package of proposals on several fora, most prominently to the 2011 UN General Assembly in connection with public protests against bribery, thievery and rigging elections. In 2015 Russia managed to gain the support of one additional oppressive state and proposed a national code of conduct for the internet once again.[31]

Public diplomacy

Russia could claim success in its approaches to information operations where it is more consistent with its 'nature'. In this sense, even the official documents that used to flirt with human liberties and democracy (in some circles referred as the Constitution of the Russian Federation) tend to downplay its importance in national security policy papers and laws. We witness more and more newspeak instead of clumsy doublespeak concerning restrictions to international law and human rights.

Russian documents explaining soft power in the sense in which Joseph Nye introduced it – 'power by attraction' as opposed to hard power or 'power by coercion' – remain relatively dead. On the other hand, publications about the use of non-military coercion under the terms 'humanitarian dimension of foreign policy' or 'Russian energy soft power' are vividly discussed by

[29] **MacAskill, E**. 2014. Putin calls internet a 'CIA project' renewing fears of web breakup. – The Guardian, 24 April 2014 22.09. <https://www.theguardian.com/world/2014/apr/24/vladimir-putin-web-breakup-internet-cia> (accessed 18.10.2016).

[30] **МИД РФ** 2011. Convention on International Information Security (Concept). – Webpage of Russian Ministry of Foreign Affairs. <http://archive.mid.ru//bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/7b17ead7244e2064c3257925003bcbcc!OpenDocument> (accessed 5.10.2016).

[31] **UNGA** 2015. Developments in the field of information and telecommunications in the context of international security Report of the Secretary-General. 22 July 2015. – Webpage of United Nation General Assembly.
<http://www.un.org/ga/search/view_doc.asp?symbol=A/70/172> (accessed 5.10.2016).

prominent members of the political elite; policies employing the former approach can be witnessed in national (supposedly unofficial) decisions.

The most prominent Russian public diplomacy organisation is The Alexander Gorchakov Public Diplomacy Fund[32]. Alexander Gorchakov was a XIX century Russian foreign minister who made important innovations in the tactics of manipulating internal and foreign public opinion.[33] He was also a promoter of Russian-Prussian relations against France (*Dreikeiserbund*).[34] Gorchakov was one of the few public officials of Czarist Russia who was adored by the official Soviet Union in Stalin's era during the first third of World War II when Russia and Germany were allies. [35]

A draft information security doctrine from 2015 which was meant to substitute the previous version from the first year of Vladimir Putin's presidency is quite revealing on the *modus operandi* of NGO participation in international co-operation; they are basically good old front organisations in the subversion business abroad.

Sometimes official Russia has shown the clear understanding that it is not very effective at moulding public opinion in foreign cultures, therefore experts have been hired from the target society. Western PR companies have been used to try to bolster the image of Russia prior to the G8 meeting in St. Petersburg, softening the image of Josif Stalin who is generally considered to be a prime example of a criminal against humanity. The epic fail of using PR companies to get the Russian point of view across came in the form of Vladimir Putin's article in the New York Times which was edited by the author at the last moment to underline that Americans as a nation have no reason to feel exceptional (i.e., to make the harshest possible cultural insult against US national identity). However, supposedly thanks to Ketchum, Vladimir Putin made Time Magazine man of the year. Although, this very accolade was also given in the past to figures like Ayatollah Khomeini and Adolf Hitler, so it could not be considered a clear-cut victory either.

The Putin regime is much more effective at arts that have been perpetrated on the domestic population for centuries.

---

[32] **Gorchakov Fund webpage**. <http://gorchakovfund.ru/> (accessed 14.10.2016).

[33] **Gecse, Géza** 2012. Bütsantsist Bütsantsini. Suurvene mõttelaadi olemus. [From Byzantium to Byzantium. Essence of the Russian Imperialist Thought]. Tallinn. Ajakirjade Kirjastus, lk 104–108.

[34] **Alexander Gorchakov** 2016. Wikipedia article.
<https://en.wikipedia.org/wiki/Alexander_Gorchakov> (accessed 17.10.2016).

[35] **Ragsdale, H.; Ponomarev, V. N**. 1993. Imperial Russian Foreign Policy. Cambridge: Cambridge University Press, p. 369.

Disinformation

In academic research about current Russian information operation practices there is lot of fuzziness about how much actual truth is contained in Russian information campaigns. Overwhelmingly, these attempts at categorization originate from the receivers' end of the communication model.

Marcel van Herpen from the Cicero Institution, who has exhaustively researched policy as practised by the current Putin regime, compares it to National Socialist propaganda research findings. He says that, besides lies, the Putin regime operates with different kinds of truths: from the outright lie, to the half truth, to the truth out of context. He noted that the latter two played a major role in Moscow's aggression in Ukraine.[36]

Alan Yuhas from the Guardian US newspaper describes the Russian info campaign as the following: "*Skewed facts, half-truths, misinformation and rumors all work in the propagandist's favor.*"[37]

Dalibor Rohac from Foreign Policy makes a list of Russian messaging as: propaganda, lies, half-truths, conspiracy theories.[38]

Ben Nimmo from CEPA provides a more systematic description and a mnemonic hint to characterize the aims of Russian disinformation: Dismiss, Distort, Distract, Dismay.

Consequently, it is hard to say from these accounts where it is more a matter of rhetorical flourish for journalistic clarity and where this categorisation attempts to reflect the actual planned aims and doctrine of the perpetrator.

First, there is a need to distinguish misinformation from disinformation. Misinformation is information that is believed, does not reflect reality, but is not deliberately disseminated to mislead.[39] Misinformation is often a result

---

[36] **Herpen, M. van** 2016. Putin's Propaganda Machine. Soft Power and Russian Foreign Policy. Lanham: Rowman & Littlefield, p. 1.

[37] **Yuhas, A**. 2014. Russian propaganda over Crimea and the Ukraine: how does it work? – The Guardian, 17 March 2014. <https://www.theguardian.com/world/2014/mar/17/crimea-crisis-russia-propaganda-media> (accessed 17.10.2016).

[38] **Rohac, D**. 2015. 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/?utm_source=Sailthru&utm_medium=email&utm_term=*Democracy%20Lab&utm_campaign=2014_Democracy_Lab> (accessed 18.10.2016).

[39] **Kuklinski, J. H.; Quirk, P. J.; Jerit, J.; Schwieder, D.; Rich, R. F**. 2000. Misinformation and the Currency of Democratic Citizenship. – The Journal of Politics, Vol. 62, No. 3. (August 2000), pp. 790–816. <http://www.jstor.org/stable/2647960?seq=1#page_scan_tab_contents> (accessed 18.10.2016).

of interfering noise in the communication process or speculation that rushes in to fill an information vacuum.

Disinformation, on the other hand, is a deliberately misleading piece of information. In the Russian context, disinformation (*дезинформация*) is the predecessor of active measures (*активные мероприятия*), currently a subdivision according to the new term *support measures*/*assistance operations* (*мероприятия содействие*).[40] [41] Department D [D for Disinformation] was created in the KGB First Directorate (Foreign Intelligence) in 1959. During reorganisation in 1968 the expanded department became Department A [A for active measures].[42]

The official definition of KGB active measures was "*agent-operational measures aimed at exerting useful influence on aspects of the political life of a target country which are of interest, its foreign policy, the solution of international problems, misleading the adversary, undermining and weakening his positions, the disruption of his hostile plans, and the achievement of other aims*[43]".

Basically, a very wide array of activities to exert influence on a strategic level. Everything that is planned as active measures is active measures according to this definition. The only distinctive characteristic is the perpetrator – the special service. In practice, Western services tend to expand this definition to encompass all overt and covert influence activities, whether they were carried out by the KGB, the military, the Communist Party or the Soviet press.[44]

As FSB spokesman 1994–1996 Alexander Mikhaylov admitted to Russian intelligence journalist Andrei Soldatov in an interview in March 2002:

---

[40] **Estonian Internal Security Service** 2014. KAPO Annual Review 2014. <https://www.kapo.ee/sites/default/files/public/content_page/Annual%20Review%202014.pdf> (accessed 15.10.2016).

[41] **Soldatov, A., Borogan, I**. 2010. The New Nobelity. The Restoration of Russia's Security State and the Eduring Legacy of the KGB. New York: PublicAffairs, p. 108. [**Soldatov, Borogan** 2010]

[42] **Barron, J**. 1974. KGB: The Secret Work of Soviet Secret Agents. London: Hodder & Stoughton, pp. 420–423.

[43] **Mitrokhin, V**. 2013. KGB Lexicon. The Soviet Intelligence Officers Handbook. Abingdon: Routledge, p. 13. [**Mitrokhin** 2013]

[44] **Schoen, F.; Lamb, C. J**. 2012. Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference. National Defense University Press. Washington, D.C. <http://ndupress.ndu.edu/Portals/68/Documents/stratperspective/inss/Strategic-Perspectives-11.pdf> (accessed 15.10.2016).

> *Disinformation involves having a direct impact on the enemy, not on society as a whole. And if we're talking about enemies – well, yes, assistance operations are operations which have an impact on the enemy*.[45]

For the Russian Federation foreign intelligence is mostly about influence activities. The definition of intelligence that is currently valid according to the Estonian Internal Security Service Annual Review 2014 is

> *a secret form of political struggle that uses means and methods of a concealed character to gather classified information and implement active measures in order to influence the opponents and weaken their political, economic, scientific, technical and military positions*.[46]

This purpose is reflected in Russian federal law "On foreign intelligence" Article 2 Intelligence activities which explains this two-fold approach to intelligence: information gathering and covert operations.[47]

The classic rationale behind covert action is that policy makers need a third option between doing nothing (the first option) in a situation in which vital interests may be threatened and sending in a military force (the second option), which raises a host of difficult political issues. For Western intelligence, propaganda and paramilitary options are main types of covert action.[48] It is a hotly debated issue if there should be an option for democratic leaders to claim plausible deniability of covert action and whether intelligence agencies should occasionally be tasked with propaganda activities.[49] Having claimed media as type of weapon and by defining intelligence as form of political struggle, this could be considered default practice for Russian federal agencies conducting covert action on the information field and using agents of influence. Going much further than just being publicly creative with the truth is rather standard procedure for Russian political leaders as well.

---

[45] **Soldatov, Borogan** 2010, p. 266, note 19.

[46] **Estonian Internal Security Service** 2014. KAPO Annual Review 2014. <https://www.kapo.ee/sites/default/files/public/content_page/Annual%20Review%202014.pdf> (accessed 15.10.2016).

[47] **Федеральный закон «О внешней разведке»** 10 января 1996 года, № 5-ФЗ. – SVR webpage. <http://svr.gov.ru/svr_today/doc02.htm> (accessed 10.06.2016).

[48] **Lowenthal, M. M**. 2005. Intelligence. From Secrets to policy. 3rd Edition. CQ Press, pp. 157–158, 162–165.

[49] **Shulsky, A.; Schmitt, G. J**. 2002. Varjatud sõda [Silent Warfare]. Tallinn: Eesti Ajalehed, lk 169–177.

It is worthwhile to remember that, for NATO operations, Military Committee policy on psychological operations expressly forbids the use of unattributed or falsely attributed messaging and the dissemination of untruth.[50]

Russian information confrontation principles

There are two distinct sets of Russian information confrontation principles that are widely referred to by Russian information warfare researchers. The first set originates from a Russian Ministry of Defence 2011 document "Russian Federation Armed Forces' Information Space Activities Concept" (*Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве*).[51] This document was published on the Russian Ministry of Defence webpage first in Russian and later in English[52]. It is often referred to by think tanks in NATO countries as Russian cyber war doctrine or Russian information war principles. However, the content of this document is rather uninformative. It lists principles for capability planning and administrative work: legitimacy, priority, complexity, interaction, cooperation, innovation. These are not principles of war in the Jominian sense, but headlines for paragraphs declaring everything the Russian military does in infospace as proportional and justified. Wordings and dissimilarities between Russian language and English language official versions hint that this document might have been developed as a part of international information security initiatives for diplomatic use. Praise of this document as the first official reference to the military use of information space does not stand up either because military doctrines from 2000[53] and 2010[54] revisions, approved by the presidents of Russian

[50] **Military Decision on MC 402/2** – NATO Military Policy on Psychological Operations.

[51] **Минобороны России** 2011. Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве. <http://function.mil.ru/news_page/country/more.htm?id=10845074@cmsArticle> (accessed 8.10.2016).

[52] **Russian Ministry of Defence** 2011. Russian Federation Armed Forces' Information Space Activities Concept. <http://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle> (accessed 8.10.2016).

[53] **Военная доктрина Российской Федерации** 2000 [Military Doctrine of the Russian Federation], утв. Указом Президента РФ от 21 апреля 2000 года, № 706. – Система ГАРАНТ. <http://base.garant.ru/181993/#block_1000> (accessed 8.10.2016).

[54] **Военная доктрина Российской Федерации** 2010. [Military Doctrine of the Russian Federation]. Russian Security Council webpage.
<http://www.scrf.gov.ru/documents/33.html> (accessed 8.10.2016).

Federation, both include the utilisation of informational instruments of power for the advancement of national interests in comprehensive military planning.

The second set of principles is evolving in books and articles by various Russian scholars of information confrontation and information security. Slightly different versions of this list could be observed in schoolbooks for degree education and the vocational training of information confrontation researchers and operators. The following list is taken from a version of the classic encyclopedia "Information-psychological Warfare Operations. Concise encyclopedic lexicon. 2nd edition" from 2011 by Vladimir Vepernitsev, Andrei Manoilo, Anatoly Petrenko, and Dmitriy Frolov[55]. These principles are illustrated by a draft Russian Federation Information Security Doctrine from 2015[56].

1. **Asymmetry**

   Comments:

   a) Rhetorical negations have cognitively similar value with endorsement due to metaphorical framing – repetition of same associations strengthens neural links between them.
   b) Computer network defence is always one step behind the attacker, by symmetric responses to attacks gaining strategic initiative not being feasible.

   Doctrine: A main national information security provision area is "development of information confrontation resources and means" and "countering the information influence exercised on the public", especially on youth spiritual (i.e., orthodox clerical) and patriotic traditions. Russia would essentially counter "the use of information confrontation means and methods" by foreign security services.

[55] **Вепринцев В. Б.; Манойло А. В.; Петренко А. И.; Фролов Д. Б**. 2011. Операции информационно-психологической войны. краткий энциклопедический словарь-справочник. Горячая Линия-Телеком, стр. 318–319.

[56] **Доктрина информационной безопасности Российской Федерации** (проект) 2015. [Russian Federation information security doctrine (draft)]. – Russian Security Council webpage. <http://www.scrf.gov.ru/documents/6/135.html> (accessed 8.10.2016).

2. Domination

Comments:

a) For superiority in information space increasing the number of media outlets and opinion-formers (agents of influence[57] and "useful idiots"[58]) affecting the target is the first option.
b) To disrupt competitive messages, Denial-Of-Service attacks and Electronic Attacks are used as standard against the adversary's official information channels and against a mass media sympathetic to the adversary's cause.
c) Competitors' arguments would be void when senders are discredited by specific, genuine or manipulated mass personal data exposure that contributes to character assassination.
d) In an unfavourable cultural context information overload could be attained by inserting a large number of internally conflicting emotional theories and claims into the information space.

Doctrine: Threats are:

– "Increase in the amount of content in foreign mass media containing biased and prejudiced information" about Russian policies.
– "Russian mass media outlets are often subjected to blatant discrimination abroad."
– The ability for citizens to bypass the internal total surveillance system SORM and remain anonymous or undetected in their activities would hamper the state organ's capability to prosecute them.

3. Clandestine

Comment:

a) To maintain credibility, proxies are preferred for disseminating factually untrue information.
b) Expendable sources are set up for first claims in order to provide a point of reference for official spokespeople and politicians.

---

[57] Agent of influence – "*An agent operating under intelligence instructions who uses his official or public position, and other means, to exert influence on policy, public opinion, the course of particular events, the activity of political organisations and state agencies in target countries.*" (**Mitrokhin** 2013, p. 3).

[58] **Useful Idiot** 2016. Wikipedia article. "*In political jargon, useful idioot is a term for people perceived as propagandists for a cause whose goals they are not fully aware of, and who are used cynically by the leaders of the cause*." Exemplary use of term has been about Western left-leaning intellectuals, who being illusioned about the Soviet Union were promoting its causes. <https://en.wikipedia.org/wiki/Useful_idiot> (accessed 19.10.2016).

c) If no time to set up proxies or temporary sources, unattributed information would be disseminated by trolls and later claimed as representation of public opinion.

Doctrine: Threats are other security services and "externally controlled non-governmental organisations" that, through communication, are able to undermine the sovereign power of the Putin regime. Religious, ethnic, and civil rights groups are warned about specifically.

4. Surprise

Comment:

a) As in any conflict, the upper hand is gained by misleading about the place, time, historical patterns or the vector of attack.
b) Levers of influence (economic, diplomatic, informational, legal, etc.) are changed frequently to dispel attention and raise false hopes.

Doctrine: domestic advancement to ICT originated from Russia to avoid backdoor attacks.

5. Aiming balance of powers

Comment:

a) This principle reflects the Putin regime aspiration for a multipolar world security setup in which Russia, through its superb manipulation skills, could become the actual "administrator of international affairs".
b) To contain competing alliances using all levers of national power.
c) To create and empower information institutions with global reach.

Doctrine: Whereas Russia sees "militarisation of the global information space" and "information arms race", national interests are declared:

– to gain the provision of "national sovereignty in the global information space" and "shaping of an international legal order aimed at countering the threat to strategic stability".
– to secure the dissemination of favourable information to the Russian public and international community incl. "official position of the Russian leadership on events of social significance in Russia and the world".
– to build internal psychological resistance with features of soft power around "the preservation and strengthening of the cultural, historical, moral and spiritual (i.e., Russian Orthodox Christian) values of the multi-ethnic people of the Russian Federation" and "support for spreading the spiritual and cultural values of the people of Russia worldwide."

6. Lack of international binding regulations

a) Clear distinctions of war and peace, and between warring parties and others, no longer apply to contemporary conflicts.

b) Professionals of information confrontation are encouraged to be creative and not to bother about legal boundaries while commissioned to perform subversive activities in another state in peacetime.

Doctrine: Russia would fight against use of ICT for propagating terrorist ideology and "spreading ideas of extremism" (in Russia, a legally vague but exhaustive punitive definition). Russia's state policy is to build a network of government-controlled NGOs to support Russian foreign policy abroad and target similarly-labelled nodes of foreign societies, to task ethnic Russians in foreign NGOs abroad with projecting Russian national interests into the information sphere.

7. Long term impact

a) Measures of information confrontation have been considered weapons of mass destruction among Russian legal and security circles since at least the 1990s.

b) Desisting from informational hostilities does not cure affected societies momentarily.

c) Information confrontation means providing a window of opportunity to set frozen conflicts that need relatively little effort to perpetuate for future leverage.

Doctrine: For domestic security, the protection of national interests in the infosphere would be provided by consolidating the efforts of government institutions, NGOs and citizens to achieve national priorities. (Citizens' needs would be "balanced" by "necessary restrictions". Citizens would have the right to search, receive, convey, process and disseminate information by any legal means.)

8. Allies and adversaries combine

a) Plausible enough cover of perpetrators (separatists, extremists, activist media, anonymous trolls, hacktivists) provides a venue for the continuation of official co-operation on pragmatic issues.

b) *Divide et empera* by corruption or extortion.

c) Exploiting splits and national vulnerabilities to disrupt alliances.

Doctrine: The first area for the provision of information security is "information support" for the state policy, which is based on:

- countering negative foreign information influences on Russian public life "through the imposition of moral values not traditional to Russia" (i.e., liberalism, democracy, pluralism, etc.).
- "strengthening the Russian mass media, including through the expansion of their capabilities to increase their audience and promptly disseminate objective information to the citizens". For that: enhance the drilling of journalists.
- "pursuing a single coordinated information policy of Russian state-owned mass media and the information resources of the state organisation in cooperation with mass media".

In order to control this exhaustive task list and maintain regime stability, the doctrine underlines the cultivation of an autocratic approach by "*strengthening the vertical and centralizing the control of resources and means for providing information security of the Russian Federation*" on all levels and by definition throughout the entire society and down to every individual and any foreign resident connected to Russia somehow. The scope of professional academic literature provides a peek into the range of information confrontation activities: from organising work in public libraries according to ideological ends, to the provision of support to the strategic use of weapons of mass destruction. As Russia considers itself permanently at war, for media at home and abroad the words of prominent Soviet World War II propagandist Ilya Ehrenberg echo loudly between the lines of the doctrine: "*In wartime, every objective reporter should be shot*."[59]

Practical considerations on researching Russian information operations

1. Paranoia

A CEPA report from January 2013 concluded:

> *Russia's strategic culture is profoundly paranoid and likely to remain so. As a result Russia behaves in ways that threaten or subvert other countries and obstruct Western diplomacy. The right response to this is not to appease Russia, but to contain it and to mitigate the effects of its actions*.[60]

[59] **Miner, S. M**. 2003. Stalin's Holy War: Religion, Nationalism, and Alliance Politics, 1941–1945. Chapel Hill and London: University of North Carolina Press, p. 290.

[60] **Lucas, E**. 2013. Report No. 34: Rethinking Russia: The Paradox of Paranoia. – Center for European Policy Analysis. <http://cepa.org/sites/default/files/documents/CEPA%20Report%20No.%2034,%20Rethinking%20Russia.pdf> (accessed 8.10.2016).

It is Russian history (see cultural awareness) and the personal background of the power elite (see criminality) that reinforces this approach. Near-total control over national broadcasting and intelligence, spoiled with the high probability rate of meeting the sponsor's inner requests, feed the paranoia further. This is reflected in national doctrines in a sordid manner, and in information confrontation literature in most exaggerated ways. In peer-reviewed academic Russian journals it would not be a surprise to read articles where civil emergencies are attributed to US geodetic weapons, or crime waves to some foreign electromagnetic system. The totality of propaganda of the current regime, accompanied by an atmosphere of fear, makes empirical research on the Russian population challenging; there is a need for good testing methodologies to evaluate if a researcher is really measuring attitudes about grievances or is just chronicling socially desirable responses. Russian public literature, academic included, is not as a rule of thumb suitable for diagnosing other countries because of the high impact of pervasive information confrontation measures and the inner cultural paranoia of writers. Russian politicians and political researchers tend to overestimate the ability of their own and their real and imaginary adversaries to control situations and to program societies.

2. Operational security obstacles

Russia considers information security one of its key priorities. Developments on this area are considered essential elements of friendy information (EEFI) that should be protected against curious eyes by the classification of data, by law, by desinformation and by active defense. Since 2014 many elaborative current publications on information confrontation are not therefore legally available abroad. The same goes for online resources as well. Outside the .ru domain a considerable part of runet is inaccessible. "Free VPN" on the other side is never completely free. Special care should be taken when researching through internet sources; attempts to plant malware on sites dealing (or claiming to deal) with ideological developments and methodologies of information confrontation are not rare. In social media indicative pieces of information have been set up to mislead researchers about the organisation and setup of Russian information confrontation forces and regulations. While in Russia, a researcher in this field of interest should consider him/herself pinpointed for a variety of 'support measures'. In this case, faith in the Russian judicial system does not help. Doing research safely from your home country could easily mark you out for character assassination if you have reached too far.

3. Cultural awareness

The evolution of Russian philosophy and doctrines is not isolated from strategic thought in the West. Russia has absorbed several ideas from military disputes in larger NATO countries as well as from China, usually a decade or more after these ideas were popular in their respective countries. However, analysing Russian thought and might needs in-depth understanding of its phenomenal culture, or some even call it distinct civilization. Dogmatic thinking about the predetermined historical role in world affairs spoils Russian academic analysis in a similar way to how, in Western predominant understanding, the virtues of an individual's desires have been raised as a central theme in economic and political research. In Russia, the latter is not the case not only for the power elite but for common countrymen as well.

It is important to keep in mind that Russian reflection of our theories when translated back after doctrine development in Russian academic security circles could end up considerably different from the original purpose of the security or military approach, to the extent of becoming incomparable.

4. Information overload

If a researcher does not limit his or her interests only to popular publications available in English, the amount of Russian language information on information confrontation would be overwhelming. Some of it is created as a smokescreen. For example, in order to mask state-controlled cyber activities, popular hacktivism and trolling is encouraged during campaigns. The first filter would be to leave out all literature dealing with psychotronic weaponry. Though fancy, research on this area is highly classified and to keep such classification much deliberate disinformation is spread. "Victims" into whose heads thoughts have been inserted are common and the researcher does not have the authority to check if these recollections are genuine or something to do with a set of personal positive diagnostics from ICD-10 chapters F20-F29.[61] When discarding such sources so widely there is always the risk of missing important parts of clairvoyant data that could have been used for strategic decision-making,

[61] **WHO** 2016. International Statistical Classification of Diseases and Related Health Problems 10th Revision (ICD-10)-WHO Version for 2016. Schizophrenia, schizotypal and delusional disorders (F20-F29).
<http://apps.who.int/classifications/icd10/browse/2016/en#/F20-F29> (accessed 8.10.2016).

or missing the opportunity of solving the Nooscope mystery[62], but parsimony in this field would not garner much information anyway.

5. *Führerprinzip*

Empirically, there is little significance in researching official statements in isolation. Information confrontation is about combining and adjusting the levers. Unfortunately, both practical propagandists and academic social and humanitarian science researchers have undergone a relapse back to totalitarian times in large numbers. Instead of formal logic, peer-reviewed magazines provide articles containing "conclusive proof" that the Great Leader has occasionally, in one context or another, supported one of the hypotheses. Along with these masterpieces, all analytical products copying Russian foreign policy talking points should be considered not as reliable sources for direct insight but rather as deliberate disinformation pieces to be analysed separately with critical rhetorical devices. However, current official curricula in higher military and security academia does include elaboration of the evergreen subject "Russian idea" which has the compulsory defining component "Putin".[63]

Figure 3. Training of future Russian generals on 4 P's. "The unifying idea: Patriotism, Professionalism, Ascetism, Putin".

[62] **Ivshina, O**. 2016. Nooscope mystery: The strange device of Putin's new man Anton Vaino. – BBC Russian Service. 19 August 2016.
<http://www.bbc.com/news/world-europe-37109169> (accessed 8.10.2016).

[63] **Аксенов, П**. 2016. Академия генштаба: дело может кончиться большой войной. [General Staff Academy: The case could result in a major war]. – BBC Russian Service. 8 September 2016. <http://www.bbc.com/russian/vert-fut-37302945> (accessed 8.10.2016).

6. **False positives**
   It is important not to overestimate Russian information confrontation capabilities and sophistication. Due to the Russian strategic culture and political choices of the Putin regime, almost any official or semi-official statement about international affairs or our particular homeland could be perceived as irritating. Irritating effects *per se* in most cases do not necessarily reflect deliberate information operations. Many things said in Russia are said because those who say them genuinely think so. They think so because the cultural background and inner defence mechanisms of information confrontation have already worked their magic on the sender. The risk of false positives when dealing with Russian propaganda is currently very high because several institutes are currently discovering Russia and its information activities but have no experience in how to analyse this strange information flow coming from Russia or from the respiratory organs of 'useful idiots' in West.

Papers in the current compendium are really worth being studied by anyone interested in Russian information operations. Many reports here are fresh, first-hand, systematized accounts from different frontlines where the Putin regime gambles in order to survive. These pieces of research touch upon many different perspectives of the phenomenon that is here to stay. The interdisciplinary approach to Russian information operations (information confrontation) that the Estonian National Defence College excels at, among many other studies, is well worth continuing in more in-depth research and conferences.

References

Alexander Gorchakov 2016. Wikipedia article. <https://en.wikipedia.org/wiki/Alexander_Gorchakov> (accessed 17.10.2016).

Allen, P. D. 2007. Information Operations Planning. Boston, London: Artech House.

Alperovitch, D. 2016. Bears in the Midst: Intrusion into the Democratic National Committee. – Crowdstrike Blog. June 15, 2016. <https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/> (accessed 18.10.2016).

Barron, J. 1974. KGB: The Secret Work of Soviet Secret Agents. London: Hodder & Stoughton.

Estonian Internal Security Service 2014. KAPO Annual Review 2014. <https://www.kapo.ee/sites/default/files/public/content_page/Annual%20Review%202014.pdf> (accessed 15.10.2016).

Estonian Internal Security Service 2014. KAPO Annual Review 2014. <https://www.kapo.ee/sites/default/files/public/content_page/Annual%20Review%202014.pdf> (accessed 15.10.2016).

FireEye 2014. APT28: A Window Into Russia's Cyber Espionage Operations? <https://www2.fireeye.com/rs/fireye/images/rpt-apt28.pdf> (accessed 18.10.2016).

Gecse, Géza 2012. Bütsantsist Bütsantsini. Suurvene mõttelaadi olemus. [From Bynzantium to Byzantium. Essence of the Russian Imperialist Thought]. Tallinn. Ajakirjade Kirjastus.

Gorchakov Fund webpage. <http://gorchakovfund.ru/> (accessed 14.10.2016).

Herpen, M. van 2016. Putin's Propaganda Machine.Soft Power and Russian Foreign Policy. Lanham: Rowman & Littlefield.

Interfax newswire 14:02 14/09/2016. Information warfare group formed during Caucasus 2016 exercises.

Ivshina, O. 2016. Nooscope mystery: The strange device of Putin's new man Anton Vaino. – BBC Russian Service. 19 August 2016. <http://www.bbc.com/news/world-europe-37109169> (accessed 8.10.2016).

Jowett, G. S.; O´Donnell, V. 2006. Propaganda and Persuasion. (4th ed.). London-New Delhi: SAGE Publications.

Kuklinski, J. H.; Quirk, P. J.; Jerit, J.; Schwieder, D.; Rich, R. F. 2000. Misinformation and the Currency of Democratic Citizenship. – The Journal of Politics, Vol. 62, No. 3. (August 2000). <http://www.jstor.org/stable/2647960?seq=1#page_scan_tab_contents> (accessed 18.10.2016).

Leonhard, R. R. 2007. Sõjapidamisprintsiibid infoajastul [The Principles of War for the Information Age]. Tallinn: Eesti Entsüklopeediakirjastus.

Lowenthal, M. M. 2005. Intelligence. From Secrets to policy. 3rd Edition. CQ Press.

Lucas, E. 2013. Report No. 34: Rethinking Russia: The Paradox of Paranoia. – Center for European Policy Analysis. <http://cepa.org/sites/default/files/documents/CEPA%20Report%20No.%2034,%20Rethinking%20Russia.pdf> (accessed 8.10.2016).

MacAskill, E. 2014. Putin calls internet a 'CIA project' renewing fears of web breakup. – The Guardian, 24 April 2014 22.09. <https://www.theguardian.com/world/2014/apr/24/vladimir-putin-web-breakup-internet-cia> (accessed 18.10.2016).

McQuail, D. 2003. McQuaili massikommunikatsiooni teooria. [McQuail Mass Communication Theory]. Tartu: TÜ Kirjastus.

Military Decision on MC 402/2 – NATO Military Policy on Psychological Operations.

Miner, S. M. 2003. Stalin's Holy War: Religion, Nationalism, and Alliance Politics, 1941–1945. Chapel Hill and London: University of North Carolina Press.

Mitrokhin, V. 2013. KGB Lexicon. The Soviet Intelligence Officers Handbook. Abingdon: Routledge.

Ragsdale, H.; Ponomarev, V. N. 1993. Imperial Russian Foreign Policy. Cambridge: Cambridge University Press.

Rid, T. 2016. All Signs Point to Russia Being Behind the DNC Hack. – Vice News. Motherboard. July 25, 2016 // 08:55 AM. <http://motherboard.vice.com/read/all-signs-point-to-russia-being-behind-the-dnc-hack> (accessed 18.10.2016).

Rohac, D. 2015. 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/?utm_source=Sailthru&utm_medium=email&utm_term=*Democracy%20Lab&utm_campaign=2014_Democracy_Lab> (accessed 18.10.2016).

Russian Ministry of Defence 2011. Russian Federation Armed Forces' Information Space Activities Concept. <http://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle> (accessed 8.10.2016).

Schoen, F.; Lamb, C. J. 2012. Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference. National Defense University Press. Washington, D.C. <http://ndupress.ndu.edu/Portals/68/Documents/stratperspective/inss/Strategic-Perspectives-11.pdf> (accessed 15.10.2016).

Shulsky, A.; Schmitt, G. J. 2002. Varjatud sõda [Silent Warfare]. Tallinn: Eesti Ajalehed.

Soldatov, A., Borogan, I. 2010. The New Nobelity. The Restoration of Russia's Security State and the Eduring Legacy of the KGB. New York: PublicAffairs.

Taylor, P. M. 2003. Munitions of the Mind: A history of propaganda from the ancient world to the present era. (3rd ed.). Manchester-New York: Manchester University Press.

The Moscow Times 2013. Russia Needs More Propaganda, Putin Spokesman Says. December 20, 2013. <https://themoscowtimes.com/articles/russia-needs-more-propaganda-putin-spokesman-says-30646> (accessed 15.10.2016).

UNGA 2015. Developments in the field of information and telecommunications in the context of international security Report of the Secretary-General. 22 July 2015. – Webpage of United Nation General Assembly. <http://www.un.org/ga/search/view_doc.asp?symbol=A/70/172> (accessed 5.10.2016).

Useful Idiot 2016. Wikipedia article. <https://en.wikipedia.org/wiki/Useful_idiot> (accessed 19.10.2016).

WHO 2016. International Statistical Classification of Diseases and Related Health Problems 10th Revision (ICD-10)-WHO Version for 2016. Schizophrenia, schizotypal and delusional disorders (F20-F29). <http://apps.who.int/classifications/icd10/browse/2016/en#/F20-F29> (accessed 8.10.2016).

Yuhas, A. 2014. Russian propaganda over Crimea and the Ukraine: how does it work? – The Guardian, 17 March 2014. <https://www.theguardian.com/world/2014/mar/17/crimea-crisis-russia-propaganda-media> (accessed 17.10.2016).

Аксенов, П. 2016. Академия генштаба: дело может кончиться большой войной. [General Staff Academy: The case could result in a major war]. – BBC Russian Service. 8 September 2016. <http://www.bbc.com/russian/vert-fut-37302945> (accessed 8.10.2016).

Армия России впервые отработала информационное противоборство на учениях «Кавказ-2016» 2016. [Russian Army for the first time worked on information confrontation during "Caucasus-2016" exercises]. – ТВ Звезда. 14 сентября 2016, 12:21 <http://tvzvezda.ru/news/vstrane_i_mire/content/201609141221-va0s.htm> (accessed 17.10.2016)

Вепринцев В. Б.; Манойло А. В.; Петренко А. И.; Фролов Д. Б. 2011. Операции информационно-психологической войны. краткий энциклопедический словарь-справочник. Горячая Линия-Телеком.

Военная доктрина Российской Федерации 2000 [Military Doctrine of the Russian Federation], утв. Указом Президента РФ от 21 апреля 2000 года, № 706. – Система ГАРАНТ. <http://base.garant.ru/181993/#block_1000> (accessed 8.10.2016).

Военная доктрина Российской Федерации 2010. [Military Doctrine of the Russian Federation]. Russian Security Council webpage. <http://www.scrf.gov.ru/documents/33.html> (accessed 8.10.2016).

Володенков, С. В. 2015. Информационное противоборство как составляющая современных «гибридных войн»: роль и особенности. – «Гибридные войны» в хаотизирующемся мире XXI века. [Information confrontation as part of contemporary "hybrid wars" – its role and features" in compendium "Hybrid Wars" in Chaotic World of the XXI Century]. Москва: Издательство Московского университета.

Герасимов, В. 2013. Ценность науки в предвидении. [The Value of Science in Anticipation]. – Военно-промышленный Курьер, № 8 (476). 27.02–5.03.2013. <http://vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf> (accessed 10.05.2016).

Доктрина информационной безопасности Российской Федерации (проект) 2015. [Russian Federation information security doctrine (draft)]. – Russian Security Council webpage. <http://www.scrf.gov.ru/documents/6/135.html> (accessed 8.10.2016).

Дылевский, И. Н.; Запивахин, В. О.; Комов, С. А.; Коротков, С. В.; Кривченко, А. А. 2016. О диалектике сдерживания и предотвращения военных конфликтов в информационную эру. – Военная Мысль, № 7/2016.

МИД РФ 2011. Convention on International Information Security (Concept). – Webpage of Russian Ministry of Foreign Affairs. <http://archive.mid.ru//bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/7b17ead7244e2064c3257925003bcbcc!OpenDocument> (accessed 5.10.2016).

Минобороны России 2011. Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве. <http://function.mil.ru/news_page/country/more.htm?id=10845074@cmsArticle> (accessed 8.10.2016).

Олевский, В. 2016. Доктрина психологических операций НАТО. [NATO psychological operations doctrine]. – Зарубежное военное обозрение, № 6/2016.

Олевский, В. 2014. Концепция «Стратегической пропаганды» НАТО, ч. 1. [NATO concept of „strategic propaganda", part 1]. – Зарубежное военное обозрение, № 9/2014.

Полянская, А.; Кривов, А. Ломко, И. 2002. Комиссары Интернета. [Commissars of the internet]. <http://ipvnews.org/bench_article19112010.php> (accessed 20.10.2016).

Сироткин Д. В.; Тыртышный А. А. 2016. Модель организации взаимодействия между федеральными органами исполнительной власти в области информационного противоборства. [Organisational cooperation model for federal organs of executive power in information confrontation]. – Информационные Войны, № 3/2016. [**Сироткин, Тыртышный** 2016]

СМИ: Медведев поручил создать центр подготовки специалистов по информационным войнам 2009. [Media: Medvedev ordered establisment of centre for preparation of information warfare specialists]. – Корреспондент.net, 8 октября 2009, 12:18. <http://korrespondent.net/world/russia/992318-smi-medvedev-poruchil-sozdat-centr-podgotovki-specialistov-po-informacionnym-vojnam> (accessed 10.09.2016).

Средства информационной борьбы («Информационное оружие»). – Военный энциклопедический словарь. <http://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=14342@morfDictionary> (accessed 10.10.2016).

Федеральный закон «О внешней разведке» 10 января 1996 года, № 5-ФЗ. – SVR webpage. <http://svr.gov.ru/svr_today/doc02.htm> (accessed 10.06.2016).

Maj. **UKU AROLD**, Deputy Chief of the Strategic Communication Department, Headquarters of the Estonian Defence Forces