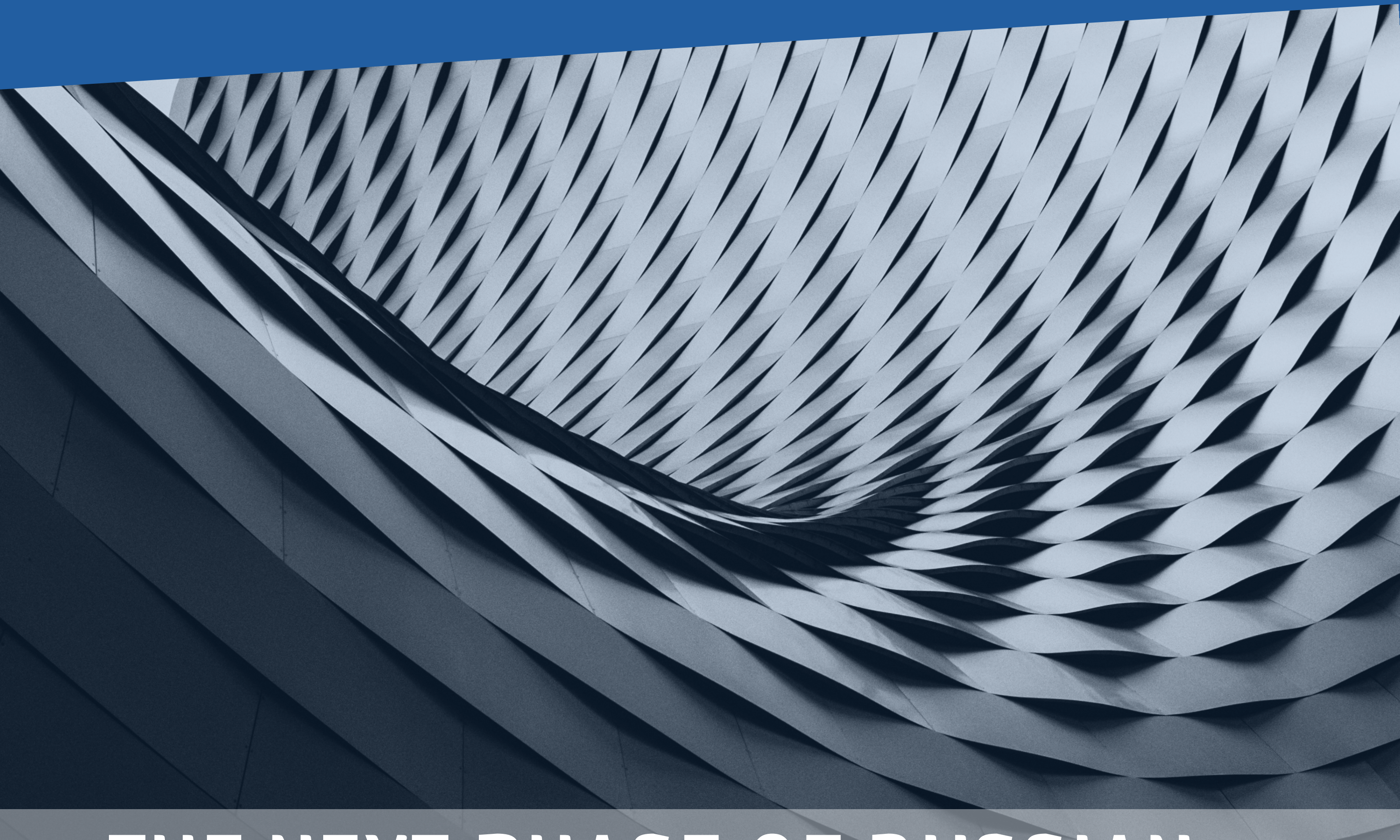

THE NEXT PHASE OF RUSSIAN INFORMATION WARFARE

AUTHOR: KEIR GILES

PREPARED BY THE
NATO STRATEGIC COMMUNICATIONS
CENTRE OF EXCELLENCE

In the 18 months since Russia's seizure of Crimea, Western understanding of Russian information warfare techniques has developed beyond all recognition. From the preserve of a few isolated specialists, study of Russia's use of the information tool has become mainstream. A number of excellent investigative reports have examined in detail the ideological grounding and conceptual basis for Russia's approach to information warfare.[1] And a substantial body of research has emerged describing in detail the operational measures used by Russia.[2]

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on the basis of current studies, and are responding by preparing for currently visible threats and capabilities, are out of date and will be surprised once again by what happens next.

This paper therefore examines not only some of the conceptual underpinnings of the Russian approach to information warfare, but also new developments which to date have not been widely covered in open sources, and their potential implications for the next wave of information confrontation with Russia.

PRECURSORS

It is now much more widely understood that information warfare in the Russian conception should not be measured against more recent Western concepts of information operations, or information activities. 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 - all-encompassing, and not limited to wartime - and the Western one - limited, tactical information operations carried out during hostilities.[3] In some Western military definitions, these risk being effectively limited to deception, providing an adversary military commander with false operational information on which to base his decision.[4] 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 and more to carry out cyber-enhanced disinformation campaigns with much wider objectives.

Nevertheless many aspects of the current debate over the nature of information warfare - and its relationship with "pure" cyber - have been known for decades among

[1] Including in particular by Ulrik Franke in "War by non-military means: Understanding Russian information warfare", FOI report FOI-R--4065--SE, March 2015.

[2] To take a number of recent examples: Pavel 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; Ben 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; Jolanta Darczewska, "The Devil Is In The Details: Information Warfare In The Light Of Russia's Military Doctrine", Point of View No. 50, Ośrodek Studiów Wschodnich, May 2015.

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

[4] The wide range of caveats and disclaimers applied by individual countries to NATO doctrine on information operations indicates the controversial nature of the issue. See NATO publication AJP-3.10, "Allied Joint Doctrine For Information Operations".

the specialist community in the West.[5] As put over a decade ago by the eminent scholar of Russian ways of thinking Timothy L. Thomas:

> What is really different [in Russia] is the conceptual understanding of an information operation from a cultural, ideological, historical, scientific and philosophical viewpoint. 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.[6]

And long before the rise of Islamic State, dealing with Islamic extremism provided object lessons in how subversive information activities can leverage the modern media environment and the hyperconnectivity of the internet, with strategic objectives: in the words of Osama bin Laden, “*It is obvious that the media war in this century is one of the strongest methods; in fact, its ratio may reach 90 percent of the total preparation for the battles*.”[7] In particular, in the previous decade, countering Islamic extremism online provided experience of “*a multi-tiered online media operation in which a number of production units... produce content consistent with the core... message*”[8] - a phenomenon now repeated on a vastly greater scale by Russia. And in language which only a decade later seems curiously archaic, a U.S. study from 2006 explored the potential of “the world of blogs, bloggers and their interconnections” for carrying out information operations; but in doing so raised a number of specific considerations which continue to be relevant to Russian exploitation of social media today.[9]

More recently, there had already been publicly released studies of the use of social media for political influence purposes, up to and including regime change (although even during the Arab Spring, in the West this received attention only from a narrow circle of specialists).[10] But recent recognition of the successes of information campaigns by both Russia and Islamic State have provoked a much broader shift in the conceptual framework of information threat by Western media, leadership and society. In a substantially new information threat environment, recognition is developing that the online challenge is not just a “cyber” one; and that hostile information in the form of content, as well as code, brings with it problems and challenges.

[5] To take a number of recent examples: Pavel Koshkin, “The See for instance the wide-ranging collection of essays in Alan D. Campen and Douglas H. Dearth (eds.), “Cyberwar 2.0: Myths, Mysteries and Reality”, AFCEA International Press, Fairfax, Virginia 1998. The fact that as long ago as 1998 informed experts were already referring to “Cyberwar 2.0” is indicative.

[6] Timothy L. 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.

[7] Osama bin Laden, quoted in Jack Barclay, “Subverting Al-Qaeda's Online Sales Pitch – Opportunities for Strategic Messaging on the Internet”, Defence Academy of the United Kingdom unpublished paper from 2010.

[8] “Violent Islamist Extremism, The Internet, and the Homegrown Terrorist Threat”, United States Senate Committee on Homeland Security and Governmental Affairs, 8 May 2008, http://www.hsgac.senate.gov//imo/media/doc/IslamistReport.pdf

[9] Jim Kinniburgh and Dorothy Denning, “Blogs and Military Information Strategy”, IOSphere, Summer 2006, available via http://calhoun.nps.edu/bitstream/handle/10945/37156/Blogs-IOSphere-Summer06-2.pdf?sequence=1

[10] As, for example, Scott Railton, “Revolutionary Risk-Cyber Technology and Threats in the 2011 Libyan Revolution”, US Naval War College, 2013.

WAR AND PEACE

The Ukraine conflict provides a clear demonstration of how Russia sees cyber activity as a subset, and sometimes facilitator, of the much broader domain of information warfare.[11] In fact, the techniques visible in and around Ukraine 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.[12] For all their innovative use of social media, current Russian approaches have deep roots in long-standing Soviet practice.[13] As pointed out by Jolanta Darcewska, in a detailed review of coverage of information warfare in Russia's new Military Doctrine, "*doctrinal assumptions about information warfare demonstrate not so much a change in the theory of its conduct... but rather a clinging to old methods (sabotage, diversionary tactics, disinformation, state terror, manipulation, aggressive propaganda, exploiting the potential for protest among the local population).*"[14]

The basic principles of the Russian approach to information security and information threats have been consistently clear from Russian declaratory policy,[15] and the development of their implementation can be traced through a wealth of official Russian documents laying out the approach to information security.[16] Public military discussion of the integration and utilisation of cyberspace to facilitate compromise of adversary decision-making channels, as well as command and control networks, has a prehistory in Russia dating back to the early 1990s if not before.[17] But as with Russia's military transformation, this evolution accelerated following the war with Georgia in 2008, when limited performance in the information domain was one of the many criticisms aimed at the Russian Armed Forces. The proposal within Russia at that time was to establish dedicated "Information Troops", whose purpose "*would be the creation of an information domain that makes international reality responsive to Russia's interests*."[18] By the beginning of 2014, before the Russian move on Crimea, it was clear that "*information operations, which may encompass broad, socio-psychological manipulation... are comfortably in the mainstream of Russian military thought*".[19]

One of the most striking elements of this evolution has been in the Russian approach to the relationship between information warfare and a traditional state of war. The erosion of the distinction between war and peace, and the emergence of a grey zone, is noted repeatedly throughout recent Russian military writing on the nature of warfare – including, but not limited to, the presentation by Chief of General Staff Valeriy Gerasimov widely referred to in the West as the "Gerasimov doctrine".[20] Actions in cyberspace had already been identified as making hostilities possible outside formal war.

[11] 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.

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

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

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

[15] For example "Basic Principles for State Policy of the Russian Federation in the held of International Information Security to 2020, Approved by the President of the Russian Federation July 24, 2013."

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

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

[18] "Russia is underestimating information resources and losing out to the West", unattributed article, Novyy Region, 29 October 2008

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

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

According to one 2011 analysis, "*Dividing lines between war and peace can be eroded conveniently in cyberspace. Damage (whatever its nature) can actually be done to an adversary without overstepping formally the line between war and peace.*"[21]

And an exceptional study of Russian views on information operations and information warfare (IW) by Sweden's FOI defence research agency noted in the previous year that:

> "
>
> Regarding network and computer operations in peacetime IW, viruses and other malware are important in order to compromise the information assets of the engineering systems of the enemy. Other aspects of IW are accumulating (stealing) information on the enemy, by intelligence gathering, while developing and testing one's own IW weapons.[22]

But this is a radical departure from previous Russian views of the status of information warfare. In the mid-1990s, leading experts Timothy L. Thomas and Lester Grau were able to write that:

> "
>
> ...from a military point, the view of Information Warfare against Russia or its armed forces will categorically not be considered a non-military phase of a conflict whether it will be causalities or not... considering the possible catastrophic use of information warfare means by an enemy, whether on economic or state command and control systems, or on the combat potential of the armed forces... Russia retains the right to use nuclear weapons first against the means and forces of information warfare, and then against the aggressor state itself.[23]

This and similar new developments in Russian information warfare thinking[23] laid the groundwork for the creative approach to achieving information dominance which was demonstrated in Crimea - to be examined further below.

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

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

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

[24] As examined on the eve of the Ukraine conflict by Tim Thomas in "Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?", The Journal of Slavic Military Studies, 10 March 2014, pp. 101-130.

RUSSIAN OBJECTIVES

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

This is a principle that has to be borne in mind at all times when considering Russian aims to extract, exfiltrate, manipulate, distort, or insert information, or just isolate a target from sources of information other than Russian ones. The channels available for doing this are as diverse as fake or real news media for planting disinformation; troll campaigns; official government statements; speeches at rallies or demonstrations; defamatory YouTube videos; direct messages by SMS, or even just walking up to somebody on the street and telling them something. Recent Russian campaigning provides examples of all of the above.

It follows that it is essential to be able to place apparently isolated incidents and trends within the overall framework of Russian information doctrine: in other words, to attempt to see the big picture as seen from Moscow, rather than from Washington or from Brussels.

One key element of this is an objective assessment of whether Russian information campaigns as currently deployed are succeeding in their objectives or failing.

Western views on this specific issue often place emphasis on countering Russian disinformation with "truth". In part this approach is based on a widespread assumption that Russian disinformation fails through lack of plausibility[25]: that Russian fabrications and denials are ineffective because they were so obvious that they do not confuse senior, or intelligent, individuals in the West. It is true that by these standards, a significant proportion of Russian disinformation appears clumsy, counter-productive, obvious, and easily debunked.[26]

But excessive focus on easily detected disinformation not only overlooks the many other aspects of concurrent Russian campaigning, it also disregards the fact that credibility is not always a metric of success for Russian information warfare campaigns.

Unlike in Soviet times, disinformation from Moscow is primarily not selling Russia as an idea, or the Russian model as one to emulate. In addition, it is often not even seeking to be believed. Instead, it has as one aim undermining the notion of objective truth and reporting being possible at all. In some respects this emulates Soviet campaigns that had no direct target other than destabilisation and weakening the target society.[27] But the new vulnerability that current Russian campaigning can exploit is, in the words of veteran scholar of Russia Leon Aron, Western societies' "weakened moral immunity to propaganda", and "weakness of confidence in sources of knowledge".[28]

[25] As for instance Professor Lawrence Freedman: "efforts at deception were by and large ineffectual, as the Russian role became progressively transparent." Lawrence Freedman, "Ukraine and the Art of Limited War", Survival: Global Politics and Strategy, 56:6, 7-38 (2014).

[26] Mark Galeotti, 'The west is too paranoid about Russia's information war', The Guardian, 7 July 2015, http://www.theguardian.com/world/2015/jul/07/russia-propaganda-europe-america

[27] See for example the description of the activities of the KGB First Chief Directorate's Service A, in Christopher Andrew, Vasili Mitrokhin, "The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB", London: Basic Books, 1999.
Also "Soviet Influence Activities: A Report on Active Measures and Propaganda, 1986-87", U.S. Department of State, August 1987.

[28] Speaking at the Lennart Meri Conference, Tallinn 24 April 2015.

Consequently, media and information warfare expert Ben O’Loughlin explains,

> It is not simply that Russia’s ‘hybrid war’ model might be destabilizing audiences’ sense of certainty about what is happening in world affairs. It is that such a strategy undermines the very fundamentals of information and credibility that informed debate are supposed to rest upon.[29]

Statements by Western government officials that use of the internet to search for information on the Ukraine conflict will a priori produce false results is one indicator of the effectiveness of this approach.[30]

Within this framework of erosion of “truth”, Russia’s elastic targeting of different audiences with different implausible and mutually contradictory narratives has other objectives than to be believed.[31] Among many examples, one is provided by the nonsensical conspiracy theories promoted by Russia surrounding the shooting down of Malaysia Airlines flight MH17. Over a year after the event, Russian media released a recording of individuals apparently conspiring to place a bomb on board the aircraft. These individuals were described as CIA operatives, regardless of the fact that their poor grasp of English immediately made the suggestion laughable.[32] And informed listeners did indeed laugh and mock the attempt, including in Russia.[33] But the disinformation that has been planted lives on indefinitely thanks to the internet, and can be brought up and reproduced indefinitely. As with many other aspects of Russian campaigning, this achieves multiple objectives.

First, it exploits an obvious asymmetry. Planting and disseminating a lie is exceptionally easy, especially when leveraging the power of the internet. Countering this information, in the manner currently suggested by many western responses – rebutting disinformation directly and repeating the truth – is time and labour intensive on an entirely different scale. It requires effort, both tracking hostile disinformation, and establishing the extent to which is untrue, and then attempting to spread the message to the same audiences.

It also requires institutional memory. There are numerous examples from Soviet times of how persistent narratives can become so deeply established that they cause Western interlocutors to question themselves. One specific example concerns Soviet media treatment of the Katyn massacres in 1940.[34]

[29] Ben O’Loughlin, “The permanent campaign”, Media, War & Conflict 2015, Vol. 8(2) pp. 169–171.

[30] ”Say a school student is assigned to write a small essay on the Ukrainian crisis. This teenager does like everybody else nowadays, and starts with Google, searching for information using a search engine. So most of what he receives has nothing to do with the truth.” Finnish Director of Government Communications Markku Mantila, quoted in “Suomi vastaa informaatiosotaan – kouluttaa sata virkamiestä tunnistustoimiin”, Yle news, 15 October 2015, http://yle.fi/uutiset/suomi_vastaa_informaatiosotaan__kouluttaa_sata_virkamiesta_tunnistustoimiin/8385264

[31] Simas Čelutka, “Russia’s challenge to the Western mind”, Kyiv Post, 24 August 2015, http://www.kyivpost.com/opinion/op-ed/simas-celutka-russias-challenge-to-the-western-mind-396407.html

[32] “Крушение “Боинга”. Записи разговоров двух агентов ЦРУ [Эксклюзив]”, Комсомольская Правда via YouTube, 11 August 2015, https://www.youtube.com/watch?v=4BhJifVhqFU

[33] See the wide range of acerbic comments added to the above video by viewers in Russia.

[34] A substantial number of primary sources relating to the mass murder of Polish troops by Soviet security forces in 1940 is available at “Records Relating to the Katyn Forest Massacre at the National Archives”, U.S. National Archives, undated, https://www.archives.gov/research/foreign-policy/katyn-massacre/

> **When Western audiences were not armed with this prior awareness, and as a result began to question in their own minds whether they had their facts straight, Russian disinformation objectives were achieved.**

An effective Soviet countermeasure to widespread awareness of this atrocity was to focus instead on German war crimes carried out in the similar sounding village of Khatyn. Whenever Katyn was mentioned, deliberate confusion with Khatyn was an effective tactic for delaying and stalling the debate, or indeed shutting it down altogether.[35] Countering this tactic required not only painstaking rebuttal on each and every occasion, but also prior awareness that it would be adopted. And on the first occasion when Western audiences were not armed with this prior awareness, and as a result began to question in their own minds whether they had their facts straight, Russian disinformation objectives were achieved.

Second, the most obvious and laughable Russian disinformation distracts from more subtle campaigns and narratives, and from tactical victories, where Russian messages and narratives have achieved successful penetration from the public opinion space into the decision-making space of its targets. Again, numerous examples are available - at the time of writing, one of the most striking is the concept that the best way to respond to Russian aggressive posturing with tactical nuclear weapons (TNWs) is to withdraw the last remaining Western TNWs from Europe altogether.[36]

PLACING DISINFORMATION

By comparison with the pre-internet era, the effective seeding of disinformation is vastly simpler. Noisy and unsubtle exploits like hacking the Twitter feed of a major news agency to plant false information[37] have taken place, but even these are entirely unnecessary when stories can be introduced into media by other, seemingly natural and legitimate, means. Major commercial news media outlets in Western nations have made substantial cuts in reporting staff as advertising revenue has bled away to other media, and few of the numerous amateur blogs and forums which have sprung up have the capacity for serious source validation on their own. Consequently, sock puppet websites which appear to provide or aggregate news can achieve substantial reach and penetration.[38] Once the disinformation placed there has been fed into the mainstream news flow at one or more points, and is picked up and reported by reputable traditional media whose editors and reporters are not aware that it is spurious, others will follow: even in the new climate of awareness, major news media do not wish to be left behind on a story which has made it to the news agenda.

These activities are facilitated by the ubiquitous activities of pro-Russian trolls and bots, which exploit specific features of the relationship between traditional and social media in order to both plant, disseminate and lend credibility to disinformation.[39] Interacting directly with readerships in a range of fora including online discussion boards, Twitter and more, these continue to act as a force multiplier for driving

[35] See Louis Fitzgibbon, “Katyn vs ‘Khatyn’: Another Soviet Hoax”, The Journal of Historical Review, Fall 1980 (Vol. 1, No. 3), pp. 230-233, available at http://www.ihr.org/jhr/v01/v01p230_FitzGibbon.html

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

[37] “AP Twitter hack causes panic on Wall Street and sends Dow plunging”, The Guardian, 23 April 2013, http://www.theguardian.com/business/2013/apr/23/ap-tweet-hack-wall-street-freefall

[38] “How To Project A Fringe Website Onto ‘American Media’”, RFE/RL, 20 July 2015, http://www.rferl.org/content/ukraineunspun-fringe-website-american-media/25415775.html

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

> “ Major news media do not wish to be left behind on a story which has made it to the news agenda. Pro-Russian trolls and bots, which exploit specific features of the relationship between traditional and social media in order to both plant, disseminate and lend credibility to disinformation, acting as a force multiplier for driving home the Russian message.

home the Russian message - especially by diverting or suppressing any debate which points out the inconsistencies or implausibilities of the Russian version of events.[40]

A substantial body of research on Russian troll campaigns has developed in the West since early 2014[41], to add to the Russian-language reporting available previously, and their key features are well documented[42] and will not be repeated here. Nevertheless, awareness of the different tactics and techniques used by the troll armies is not universal. Even in May 2015, one exceptionally well-informed individual was wondering at *“hundreds of Twitter messages saying the same thing, as if they are coordinated.”*[43] And 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 remain oblivious to their intent and their effect.[44]

In addition, the Western mass media coverage of this phenomenon provides another example of superficial aspects of the Russian information campaign distracting from more substantive issues. In Western reporting, attention has been focused exclusively on a single “troll farm” in St Petersburg.[45] Despite the fact that the existence and activities of this organisation have been documented for over a year at the time of writing, thanks to on-the-spot reporting by local Russian media[46] later followed up by Finnish and other investigative journalism[47], it continues to feature repeatedly in Western media - assisted by former employees giving

[40] Ksenia Kirillova, “Российские тролли терроризируют Запад”, Novyy region 2, 20 October 2015, http://nr2.com.ua/blogs/Ksenija_Kirillova/Rossiyskie-trolli-terroriziruyut-Zapad-109046.html

[41] For an early example, see detailed research by Saara Jantunen, specialist in strategic communications at the Finnish Defence Research Agency. James Mashiri, “Trolliarmeija, eli Venäjän informaatio-psykologinen sodankäynti”, Random thoughts blog, 18 September 2014, https://fmashiri.wordpress.com/2014/09/18/trolliarmeija-eli-venajan-informaatio-psykologinen-sodankaynti/.

[42] For a useful summary, see Wikipedia entry on “Web brigades”, https://en.wikipedia.org/wiki/Web_brigades For a more detailed view, see Peter Pomerantsev & Michael Weiss: The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money. The Institute of Modern Russia, New York 2014; “Russian trolls spread government propaganda”, Al-Jazeera, 11 August 2015, http://www.aljazeera.com/news/2015/08/russian-trolls-internet-government-propaganda-150811205218686.html; “This is How Pro-Russia Trolls Manipulate Finns Online – Check the List of Forums Favored by Propagandists”, Stopfake.org, 13 July 2015, http://www.stopfake.org/en/this-is-how-pro-russia-trolls-manipulate-finns-online-check-the-list-of-forums-favored-by-propagandists/

[43] Michael McFaul, former U.S. Ambassador to Russia, in “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

[44] A senior correspondent for a respected British national newspaper was still saying in April 2015 that the large numbers of e-mails and comments and responses through social media that were in support of Russian policy indicated a real groundswell of opinion among the readership. And in September 2015, the author was interviewed on BBC radio following an extended feature on one of these former employees. During the interview, the presenter reported receiving a large number of messages backing Russian policy and claiming that the UK also engages in similar opinion manipulation. The presenter was shocked at the suggestion that not all those messages might have been genuine, despite having just listened to a detailed report on how Russia pays large numbers of individuals to generate them.

[45] For example, most recently at the time of writing, in Alec Luhn, “Game of trolls: the hip digi-kids helping Putin’s fight for online supremacy”, The Guardian, 18 August 2015, http://www.theguardian.com/world/2015/aug/18/trolls-putin-russia-savchuk

[46] Anton Butsenko, “Тролли из Ольгино переехали в новый четырехэтажный офис на Савушкина”, Delovoy Peterburg dp.ru, 28 October 2014, http://www.dp.ru/103iph/

[47] Jessikka Aro, “Yle Kioski Traces the Origins of Russian Social Media Propaganda – Never-before-seen Material from the Troll Factory”, Yle, 20 February 2015, http://kioski.yle.fi/omat/at-the-origins-of-russian-propaganda.

repeated interviews.[48] The Russian authorities appear content to leave this location in the foreign media spotlight, as it serves as an effective distraction from the wider network of troll farms, or the organisation behind them.[49] This single-minded focus on the easiest target prevents deeper investigation, and as such, it is entirely acceptable to Russia - as suggested by the fact that the Petersburg troll farm remains in visible operation, and at least one intricate entrapment operation has been mounted against Western journalists attempting belatedly to follow up the story.[50]

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.

A second wave of trolling, augmented by bot resources, is now well developed, and appears to include more tailored and sophisticated features to increase its effectiveness. To take one example of the customisation of troll types for specific targets, the "bikini trolls" described by researcher Mārtiņš Daugulis at the NATO Strategic Communications Centre of Excellence feature scantily clad young ladies in their profile pictures, with enticing descriptions, and "*target an especially vulnerable social group, men over the age of 45*".[51] But a key feature of this approach is that these profiles attract followers and interaction from their targets - and thus defeat some of the tools for troll and bot analysis which were effective at detecting and exposing more straightforward and generic troll profiles.[52] In this way they are able to build up a degree of apparent legitimacy, while remaining dormant until required for their primary purpose.

Russia has also taken opportunities to hijack already existing authoritative social media accounts in order to spread disinformation. A case in point is the Swedish TV4 television channels, whose Twitter accounts started broadcasting Russian information to their followers.[53] 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 be put into use at the appropriate moment.

It has been argued that the use of trolls and bots in this manner can also be explained by marketing exercises, as well as state-sponsored disinformation. But this argument overlooks the fact that in exactly the same way as 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.[54]

[48] Most prominently Marat Burkhardt� and Lyudmila Savchuk. Among many examples of sustained media coverage, see "One Professional Russian Troll Tells All", Radio Free Europe / Radio Liberty, 25 March 2015, http://www.rferl.org/articleprintview/26919999.html, and Tom Parfitt, "My life as a pro-Putin propagandist in Russia's secret 'troll factory'", Daily Telegraph, 24 June 2015, http://www.telegraph.co.uk/news/worldnews/europe/russia/11656043/My-life-as-a-pro-Putin-propagandist-in-Russias-secret-troll-factory.html.

[49] "Blogger uncovers evidence using Google Trends of several new pro-Kremlin 'troll factories'", Meduza, 19 August 2015, https://meduza.io/en/news/2015/08/19/blogger-uncovers-evidence-using-google-trends-of-several-new-pro-kremlin-troll-factories. Catherine Fitzpatrick, "Russian Blogger Finds ProKremlin 'Troll Factories'", The Daily Beast, 20 August 2015, http://www.thedailybeast.com/articles/2015/08/20/russian-blogger-finds-pro-kremlin-troll-factories.html.

[50] James Hill, "The Agency", New York Times, 7 June 2015, http://mobile.nytimes.com/2015/06/07/magazine/the-agency.html.

[51] Mārtiņš Daugulis, speaking at the NATO Strategic Communications Centre of Excellence inaugural conference, 20 August 2015. See also "Internet Trolling as a hybrid warfare tool: the case of Latvia", NATO Strategic Communications Centre of Excellence, undated summary, http://www.stratcomcoe.org/internet-trolling-hybrid-warfare-tool-case-latvia

[52] As described in Lawrence Alexander, "A Response to the KremlinBot Skeptics", Global Voices, 24 April 2015, http://globalvoicesonline.org/2015/04/24/a-response-to-the-kremlin-bot-skeptics/print/

[53] Patrik Oksanen, "TV4:s twitter blev ryskt", helahälsingland.se, 3 February 2015, http://www.helahalsingland.se/opinion/ledare/tv4-s-twitter-blev-ryskt

[54] 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.

> Russia has also taken opportunities to hijack already existing authoritative social media accounts in order to spread disinformation.

Examples are already available of how the transfer between one domain and another is seamless.[55] Observers of cyber campaigning during the conflict in Ukraine noted how malware which was intended to generate revenue by simulating clicks was diverted to promote pro-Russian videos on YouTube.[56] And Twitter accounts can follow the same pattern. The authoritative–sounding Finnish language accounts @Vaalit, @Eurovaalit, @ Eduskuntavaalit (Elections, European Elections, Parliamentary Elections) and a range of other associated accounts were originally set up to generate revenue as click bait, but are now repeating Russian disinformation, with profiles providing links to RT.[57]

In each case, the underlying reason for the change is unclear. It is possible that distributing Russian disinformation is more profitable than selling clicks; an alternative explanation is that the owners of the accounts really do hold an altruistic ideological conviction that Russia must be supported. In any case, the net effect is precisely the same. Overall, the pattern is of Russia amassing abilities on social media, ready to be deployed when needed.

INTERNET INFRASTRUCTURE

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

Intensified Russian interest in civilian internet communications infrastructure is one possible indicator of future plans. After a long prehistory in the classified domain, Russian investigation of subsea communications cables is now of a sufficiently high profile that it has reached substantial public reporting in the West. Highly visible commentary in, for example, the New York Times[58] has been accompanied by more detailed investigations in Finnish[59] and Polish[60] media. This is an indication that the subsea activity which is the subject of recent media attention is not just limited to the area around the continental United States, but also extends to the Baltic Sea and elsewhere.[61] The technologies for accessing data from subsea cables are well established.[62] Targeting them would meet a wide range of Russian objectives; according to former SACEUR Jim Stavridis, these would include “a rich trove of

[55] 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

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

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

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

[59] Laura Halminen, “Venäjä nuuskii nyt lännen tietoliikennettä – Krimillä liikennekaapelit vain tärveltiin”, Helsingin Sanomat, 7 November 2015, http://www.hs.fi/ulkomaat/a1446879570779

[60] ”Kable, bez których stanie świat”, TVN24, 9 November 2015, http://www.tvn24.pl/weekend/tvn24-na-weekend,12/kable-bez-ktorych-stanie-swiat,237

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

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

intelligence, a potential major disruption to an enemy's economy and a symbolic chest thump for the Russian Navy."[63]

Unsurprisingly, nations have been reticent about revealing exactly what is known about Russian subsea activity in their immediate environment. The precise capabilities available to Western nations for detecting what is happening in the subsea environment are classified, just as the Russian activities there are. In the case of Finland, the only official statement as to the nature of the underwater intruder which was detected in April 2015 was that it was "not a submarine" – leading to speculation that it was a remotely operated vehicle.

But sophisticated subsea technologies may not be necessary in all cases. Finland in particular has seen media reporting of alarm at the apparently systematic acquisition by Russian interests of land and properties in key locations near strategically important facilities, including "locations related to telecommunication links".[64] The Turku archipelago, in the narrowest stretch of water between southern Finland and Sweden, is highlighted as a key location where communications cables and energy interconnectors are vulnerable.[65]

Potentially hostile activity by Russian assets in space, however, is greatly more visible, thanks to the involvement of commercial companies in space operations, and to amateurs reporting on what they observe. The unusual manoeuvres carried out by Russian space vehicles in the vicinity of communications satellites has a number of possible explanations. At worst, this could be practice for attack runs for deploying antisatellite weapons in order to degrade Western communications at a critical moment. At the other extreme, the most charitable explanation is that this provides an opportunity for close observation and investigation of Western communication satellites.[66] In either case, this is a further example of intensified Russian interest in communications infrastructure.[67]

The reason for this interest may well lie in the Russian experience of success in achieving information dominance in Crimea during the operation there in March 2014. In addition to control over broadcast and print media, Russia also successfully achieved control over telecommunications including the notionally independent internet, and thus successfully isolated Crimea from independent news from the outside world.[68] The result was public perception in Crimea of events in the rest of Ukraine being determined exclusively by Russia, which greatly facilitated the Russian seizure of the peninsula and subsequent attempts at its legitimation.

Significantly for the nature of possible future Russian information operations, the method used to achieve this was simply taking physical control of the internet and telecoms infrastructure[69], and selectively disrupting

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

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

[65] "Suomen vesiväylät "motissa" venäläisfirma osti maat", Iltalehti, 19 January 2015, http://www.iltalehti.fi/uutiset/2015011919044524_uu.shtml, and "Maakauppoja strategisissa kohteissa", Iltalehti, 12 March 2015, http://www.iltalehti.fi/uutiset/2015031119338528_uu.shtml

[66] 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

[67] Capabilities both discussed further in Mike Gruss, "Space Surveillance Sats Pressed into Early Service", SpaceNews, 18 September 2015, http://spacenews.com/space-surveillance-sats-pressed-into-early-service/.

[68] Shane Harris, "Hack Attack. Russia's first targets in Ukraine: its cell phones and Internet lines", Foreign Policy, 3 March 2014, http://foreignpolicy.com/2014/03/03/hack-attack/

[69] "В АР Крим невідомими у військовій формі повторно заблоковано декілька вузлів зв'язку", Ukrtelekom, 1 March 2014, http://www.ukrtelecom.ua/presscenter/news/official?id=120389

cable connections to the mainland.[70]

This argues that suitable telecoms expertise was available to the Russian special forces involved in the operation, and points to an entirely new interface between cyber, information, and kinetic operations, and one which Western planners should study closely. This combining of capabilities has been demonstrated further in ongoing operations in eastern Ukraine. According to Maj-Gen Stephen Fogarty, head of the U.S. Army's Cyber Center of Excellence:

> “
>
> Russian activities in Ukraine... really are a case study in the potential for CEMA, cyber-electromagnetic activities... It's not just cyber, it's not just electronic warfare, it's not just intelligence, but it's really effective integration of all these capabilities with kinetic measures to actually create the effect that their commanders [want] to achieve. [71]

Meanwhile, by contrast, the U.S. Army itself is reported to be only at an early stage of working toward this effective integration.[72]

As has been noted elsewhere, the very distinctive nature of Crimean Internet geography means that replicating this success in information dominance elsewhere would by no means be as straightforward for Russia. Even Crimea itself is now directly connected to the Russian internet, removing one of its key vulnerabilities of a single point of failure for internet connections.[73]

But the close Russian interest increasingly displayed in communications infrastructure in other areas of the world can have a range of hostile implications. Investigating vulnerabilities of this infrastructure can facilitate espionage operations, isolation, or means of planting disinformation - or a combination of all of these. In addition, information interdiction of the kind demonstrated in Crimea should also be thought of in a broader context. Capabilities displayed in eastern Ukraine include a much enhanced electronic warfare (EW) capability, including for GPS jamming,[74] which unofficial reports suggest has already been directed from Russia at U.S. and NATO military units visiting border regions of the Baltic states.

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

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

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

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

[74] 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/.

TARGETING PERSONNEL

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

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

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

> “For Russia, cyber activities in the broad sense are critical to offensive disinformation campaigns.

Examples of the results are already available, as with the mass telephoning of Polish military personnel in November 2015.[75] Other instances of selecting and then simultaneously contacting a large number of specific individuals include government messaging to Russian internet users who accessed a mail service from Egypt[76], and a well-documented instance of intimidatory SMS messages to individuals taking part in the Maidan protests in Kiev in January 2014.

The messages, including “Dear subscriber, you are registered as a participant in a mass disturbance”, appeared to be from the individuals’ local phone service provider but was apparently accomplished without the providers’ involvement.[77]

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

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

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

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

POLICY IMPLICATIONS

Russia's current preparations for a possible new information offensive therefore encompass a number of aspects which were not visible in the early stages of the campaigning around Ukraine. The ongoing information preparation of the battle space includes testing procedures, as well as gathering information on how to reach military as well as civilian populations, and on the vulnerabilities of civilian Internet infrastructure. This provides a menu of different different capabilities which might be employed to mount a fundamentally new information threat to Western nations.

This is consistent not only with long-standing Russian information warfare aspirations, but also with Russian discussion of a capability gap with the West, and the consequent need to adopt asymmetric measures. Norwegian analyst Tor Bukkvoll wrote in 2011 that "*The idea of developing an asymmetric technological response – popular in many nations with more or less strained relations with the West – has become a truism among the Russian traditionalists. The main reason is the realization that the Western lead is too great to catch up with.*"[78] And, indeed, according to Vladimir Putin, Russia's approaches to conflict "*are to be based on intellectual superiority. They will be asymmetrical, and less costly*".[79]

In this context, as noted by Latvian analyst Jānis Bērziņš, Russian information operations "*have reached a point where they can take on strategic tasks*".[80]

> "
>
> In other words, the West may be well prepared for "pure" cyber challenges, but events in Ukraine show that it also needs to be prepared for information war when these are seamlessly melded with cyber, kinetic and EW operations.

There are a number of direct and obvious policy implications for Western nations.

For Russia, cyber activities in the broad sense are critical to offensive disinformation campaigns which can have strategic effect even if the cyber component of these campaigns is very limited. In other words, the problem of propaganda and disinformation - as subsets of the much broader Russian information campaign overall - is at least as important as the traditional (if often misguided) "cyber Pearl Harbor" notion of crippling cyber attacks on critical national infrastructure. By contrast, the Western approach to cyber threats has typically focused on technical responses to technical threats, largely disregarding the interface with information warfare in the broad sense. This approach is entirely apt for some persistent or background threats, but not always sufficient for a broader-based approach like the one adopted by Russia.[81] In other words, the West may be well prepared for "pure" cyber challenges, but events in Ukraine show that it also needs to be prepared for information war when these are seamlessly melded with cyber, kinetic and EW operations.

[78] Tor Bukkvoll, "Iron Cannot Fight- The Role of Technology in Current Russian Military Theory", Journal of Strategic Studies, 2011, Vol.34, No.5, pp. 681-706

[79] Vladimir Putin, "Poslaniye Federal'nomu Sobraniyu Rossiyskoy Federatsii" (Address to the Federal Assembly of the Russian Federation), as transcribed in Krasnaya Zvezda, No.89, 11 May 2006.

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

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

Since a primary target for Russian information and disinformation campaigns is mass consciousness, greater public involvement is essential. This poses a strategic communications challenge for Western governments. Despite the focus on regenerating communications strategies to address the Russian public, it is also critical to involve domestic audiences and explain the challenge they are facing. In some Western nations, explicit ministerial or even presidential acknowledgement of the information warfare problem has been highly effective in raising awareness.[82] In others, there has been effectively no visible public debate: and this critically undermines those societies' resilience to information attack.

The well-founded calls for more effective intelligence sharing among Western nations to enhance responses to the Russian challenge should also extend to the pooling and sharing of unclassified expertise. Experience dictates that substantial achievements can be made in predicting Russian actions and responses without recourse to classified sources; there is scope for much more effective interaction between those centres of expertise in various nations that engage in this activity.

Finally, as well as giving depth and context to understanding of current events by immediately highlighting shifts in Russian policy and tactics,[83] Russian information approaches can be analysed to draw conclusions on future trends. In their advance work to prepare public opinion, Russian and Russian-backed media, metamedia and social media behaviours provide indicators of future activity which can be interpreted successfully,[84] with appropriate investment in combined data mining and Russia studies expertise.

NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE

The NATO StratCom Centre of Excellence, based in Latvia, is a multinational, cross-sector organization which provides comprehensive analyses, advice and practical support to the alliance and allied nations.

[82] As, for example, by Finnish President Sauli Niinistö: "Presidentti Niinistö infosodasta: Me kaikki olemme maanpuolustajia", Yle news, 17 October 2015, http://yle.fi/uutiset/presidentti_niinisto_infosodasta_me_kaikki_olemme_maanpuolustajia/8388624.
According to Finnish Director of Government Communications Markku Mantila, "the fact that in Finland we have discussed this issue openly is very good. The general public is alert to information influence." See "Suomi vastaa informaatiosotaan – kouluttaa sata virkamiestä tunnistustoimiin", Yle news, 15 October 2015, http://yle.fi/uutiset/suomi_vastaa_informaatiosotaan__kouluttaa_sata_virkamiesta_tunnistustoimiin/8385264

[83] As for example with the change in rhetoric on Ukraine at the time of Russia's initial military intervention in Syria. See Vladimir Varfolomeyev, "Киевская "хунта" полностью исчезла из российских теленовостей (Первый, Россия, НТВ, ТВЦ, РЕН, Пятый)- "Медиалогия"", Twitter post, 14 September 2015, https://twitter.com/Varfolomeev/status/511017948614782976/photo/1