Download date: 14. Nov. 2026

Danish Institute for International Studies

Russian Hybrid Warfare
A study of disinformation

Hansen, Flemming Splidsboel

Publication date:
2017

Document Version
Publisher's PDF, also known as Version of record

Link to publication

Citation for pulished version (APA):
Hansen, F. S. (2017). *Russian Hybrid Warfare: A study of disinformation*. Danish Institute for International Studies. DIIS Report Vol. 2017 No. 06

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

DIIS REPORT 2017: 06

RUSSIAN HYBRID WARFARE

A study of disinformation

Table of Contents

Introduction 4

Russian hybrid war 7

The Russian media landscape 15

The weaponisation of information 27

Cognitive resilience 33

Notes 38

This report is written by Flemming Splidsboel Hansen and published by DIIS as part of the Defence and Security Studies.

Flemming Splidsboel Hansen is senior researcher and Research Coordinator at DIIS.

DIIS · Danish Institute for International Studies
Østbanegade 117, DK-2100 Copenhagen, Denmark
Tel: +45 32 69 87 87
E-mail: diis@diis.dk
www.diis.dk

Layout: Lone Ravnkilde & Viki Rachlitz
Printed in Denmark by Eurographic

ISBN 978-87-7605-879-1 (print)
ISBN 978-87-7605-880-7 (pdf)

DIIS publications can be downloaded free of charge or ordered from www.diis.dk

© Copenhagen 2017, the author and DIIS

INTRODUCTION

In February 2013 General Valery Gerasimov, Chief of the Russian General Staff, published a short piece on 'the value of science in forecasting', in which he outlined the contours of future warfare. According to Gerasimov some of the key features of this latter will be:

- That it will be undeclared.
- That it will see a broad use of kinetic and non-kinetic tools in close co-ordination.
- That the distinction between the military and civilian domains will become still more blurred.
- That battles will take place in the information space as well as in physical arenas.[1]

Predictions such as these illustrate the so-called hybrid warfare, which has become a household term in the aftermath of the Russian invasion of the Ukrainian peninsula of Crimea in February 2014 and the outbreak of fighting in eastern Ukraine in the spring of 2014.

The label has been redesigned, but the contents are actually familiar. The term 'hybrid warfare' alerts us to the use of both kinetic and non-kinetic tools – this is the hybridity element as defined in this study – and military historians are keen to point out that this of course is not new.[2] For the purposes of this report, kinetic operations relate to 'the motion of material bodies and the forces and energy associated therewith', while non-kinetic operations seek 'to influence a target audience through electronic or print media, computer network operations, electronic warfare… [etc.]'.[3] Strategists and security theorists have been discussing the emergence of 'new wars', together with a host of other associated nomenclature, for a few decades already, and the essence of this discussion has been to highlight the development also pointed to by Gerasimov.[4] It has been abundantly clear for very many years that the wars of the past between, for instance, 'blue' and 'red' troops on a well-defined battle space are exactly that – wars of the past.

These long-term perspectives notwithstanding, however, the pace of the development today is such that some are already abandoning the hybrid warfare term. Alternatives include a return to 'asymmetric warfare' and a move to the newer 'ambiguous warfare', both of which highlight particular aspects of current and future warfare.[5] While the former emphasises the struggle between two or more adversaries with markedly different capabilities, leading the weaker part(s) to attempt to define the nature of the struggle in a way which will minimise the capabilities gap, the latter draws our attention to the 'is it or is it not war?' characteristic of the undeclared war also mentioned by Gerasimov.

It has been abundantly clear for very many years that the wars of the past between, for instance, 'blue' and 'red' troops on a well-defined battle space are exactly that – wars of the past.

In whichever way one views the hybrid warfare term – new or old – what has changed in recent years is the role played by modern information technology. It now serves as a force multiplier on an unprecedented scale and an effective use of the information space may compensate much more today than until very recently for deficiencies in the physical arena. (Russian) information technology, part of the non-kinetic toolbox, its use and the possible defences against it will be the main focus of this report.

RUSSIAN HYBRID WAR

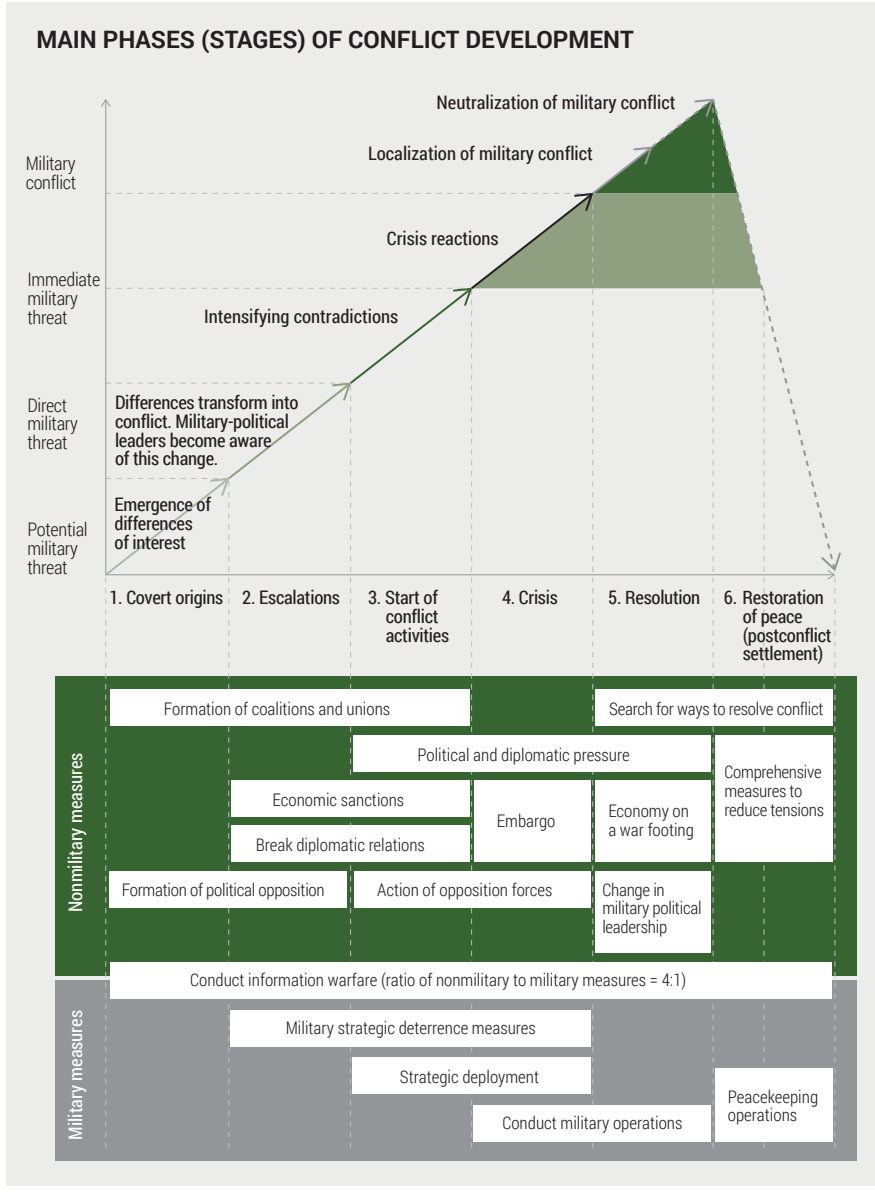
Gerasimov's oft-cited 2013 article has since been condensed by many in the West into the 'Gerasimov Doctrine'. This is slightly misleading, as there is no official doctrine and Gerasimov was, rather, depicting the world which, so he and his colleagues in the General Staff argue, Russia is confronting and has to prepare for. In fact, 'hybrid warfare' in Russian parlance is described as a tool usually employed by Western states and organisations, while the preferred Russian terms are 'non-linear warfare' or 'new generation warfare'. Whichever term is favoured, however, many Western observers see Gerasimov's 2013 article as a semi-official statement on Russia's approach to warfare and as a blueprint for Russia's 2014 occupation and subsequent annexation of Crimea as well as its involvement in the conflict and war in eastern Ukraine. Figure 1 depicts the primary model from Gerasimov's 2013 article[6]

Hybrid warfare basically encompasses any type of action designed intentionally to weaken an opponent, even through, for instance, economic, cultural or environmental policies.

Gerasimov draws several conclusions based on his observations of a number of post-Cold War conflicts and wars, including the 'Arab Spring' and the 2011 Libya intervention. With regard to the latter, he notes how:

> "...asymmetric actions were broadly employed, allowing for a levelling down of the superiority of the adversary in armed fight. [This includes] the use of special operations forces and the domestic opposition for the creation of a permanently operating front across the whole territory of the opposing state as well as influence through information [operations], the form and methods of which are constantly perfected.[7]"

Figure 1: The role of non-military means in the solution of interstate conflicts[8]



Many Russian military thinkers and analysts have since elaborated on the worldview presented by Gerasimov in the 2013 article. Their point of departure is, almost without exception, that Russia is the victim of hybrid warfare waged against it by the West. This theorising does, however, give us a relatively good understanding of the Russian thinking on the issue and we see that the concept is defined very broadly. Hybrid warfare basically encompasses any type of action designed intentionally to weaken an opponent, even through, for instance, economic, cultural or environmental policies.[9]

The essence is often described as 'controlled chaos'. Thus, Russian thinkers often depict a kind of 'chaos button', which may be used to adjust the level of chaos inflicted on a target state (or any other, usually geographically defined, entity).[10] The aim is to cause and feed instability, to weaken the social fabric within a society and to complicate and undermine decision-making. The target state should, ideally, be decisively weakened along the two overall dimensions of legitimacy which serve to define its position on a continuum of strong and weak states. Firstly horizontal legitimacy, defined here as the extent to which the population of a state accept their inclusion in this. And secondly, vertical legitimacy, defined here as the extent to which the population of a state accept the right to rule of those who rule.[11]

It is not surprising that the works of ancient Chinese military strategist Sun Tzu, whose many dictums famously include the advice that 'the greatest victory is that which requires no battle', have become favourite pastime reading and an oft-cited reference in political and military circles in Russia.

The 'chaos button' may be used to adjust the intensity of both kinetic and non-kinetic operations. The former may cover the full spectrum of weapons available, including weapons of mass destruction (WMD), but focus is usually on small-scale and covert operations conducted by special operations forces or by irregular insurgents (in the Russian writing on the issue often referred to as 'partisans') or even terrorist groups supported by the enemy state(s).[12] It follows from the hybridity definition offered here – the conscious thinking about the co-ordinated use of kinetic and non-kinetic tools to maximise effect – that even large-scale physical destruction, or threat of such, is an integral part of the concept. As discussed below, the kinetic tools may already be secondary in importance or even on the verge of losing their role as a necessary component of 'war', but for the purposes of this study, they remain part of the picture.

The deployment of troops is likely to see a combination of uniformed and non-uniformed troops and with a spatial distribution which will make it difficult to identify, in the opening phases of the campaign at least, an unequivocal centre of gravity. Even uniformed troops may appear without insignia in an undeclared war, as seen for instance with the now infamous 'little green men' in Crimea in February and March 2014, which Russian president Vladimir Putin admitted to ordering into Ukrainian territory only two months after the start of 'Operation Return of Crimea'.

In the non-kinetic toolbox information technology, including media, is now central but other important instruments include, for instance, political and financial support for minority groups or system-upsetting political parties seeking to challenge the horizontal and vertical legitimacy of the state, respectively. Ideally, an actor will be able to achieve its objectives without fighting and even without conflict. Long-term and subtle influence operations aimed at the target state are to be preferred. If this proves inadequate, then the 'chaos button' may be pressed harder to apply more pressure on the target state. And if this also proves inadequate, then a policy shift towards a greater emphasis on kinetic operations, including heavier ones, may be initiated. The 2013 article by Gerasimov highlights the non-kinetic aspect of hybrid warfare, noting that the ratio between non-military (non-kinetic) and military (kinetic) operations should be 4:1 (see figure 1). It is not surprising that the works of ancient Chinese military strategist Sun Tzu, whose many dictums famously include the advice that 'the greatest victory is that which requires no battle', have become favourite pastime reading and an oft-cited reference in political and military circles in Russia.[13]

As elsewhere, Russian strategists are also considering the status of cyber in the kinetic-non-kinetic dichotomy.[14] It seems to fall within both domains, depending on its ultimate purpose. It may, firstly, have a destructive character and be intended to render inoperative either military or civilian facilities. Defined here as 'a class of cyber attacks that can cause direct or indirect physical damage, injury or death solely through the exploitation of vulnerable information systems and processes', the so-called kinetic cyber is rapidly attracting more attention, both as a possible cyber weapon to be developed further and as a weapon to be defended against.[15]

The most widely reported incident is that of Stuxnet, a mainly US-developed malicious computer worm designed to inflict physical damage to parts of the nuclear programme of Iran.[16]

Secondly, it may have more of a traditional role as an intelligence-gathering tool. Designed to break into information systems, this non-kinetic cyber tool ultimately should help policy-makers arrive at better decisions by providing them with a fuller picture of the state of affairs. Information obtained in this way may also be used, for instance, to influence public opinion by being spread through mass media or on social media networks. An illustration of this is the alleged Russian hack against the Democratic National Committee, where information was gathered in order to get a better understanding of the thinking, including on Russia, within the Democratic Party, and where eventually part of this information was leaked to the media with the purpose of undermining the legitimacy of presidential candidate Hillary Clinton.[17]

Hybrid warfare in Russian thinking is usually described as non-linear. The political strategist and presidential advisor Vladislav Surkov is rumoured to have penned the scifi novel Bez Neba ('Without the Sky'), in which a number of adversaries fight – each alone against the others – in a World War Five. War is perceived as an ongoing process with no identifiable beginning and with no end. War simply is.[18] This reflects the Russian understanding of hybrid warfare generally and as it is allegedly being waged against Russia specifically.[19] It is a war which is on now, but it is unclear when it was initiated by Russia's adversaries (in the West). What is certain, however, is that it will simply continue. And it will be fought in a non-linear way, that is, not as A → B but rather as A → C → B → X. The temporal and spatial dimensions are diffuse.

Hybrid war – especially when interpreted through the lens of the 'chaos button' – should be seen as opportunistic. The state waging a hybrid war is attempting to identify vulnerabilities in the target state(s), which may be used to further their own interests. As security theory informs us, vulnerabilities represent one side of the insecurity equation, the other side of which is represented by threats.[20] In the words of security theorist Barry Buzan, vulnerabilities and threats 'cannot meaningfully be separated'. The actor under pressure, in this case mainly states, may then choose to focus internally, by reducing vulnerabilities, and/or externally, by lessening threats.[22]

Some of these vulnerabilities may be structural and therefore well-known and the policies against them may be planned well in advance of implementation and then run for an extended time period, while others will appear and be recognised only suddenly, forcing adversaries to think fast if they want to benefit from the opportunity offered. An illustrative analogy may be that of krav maga, a self-defence system described by one practitioner as 'rough, tough, down and dirty', while another explained how 'it employs kicks in the groin, elbows in the jaw and pokes in the eye'.[23] In the world of hybrid warfare, an undefended spot may be vulnerable and therefore the object of an attack.

Another way to conceptualise hybrid warfare is to see it as 'the dark reflection of [the] comprehensive approach', as NATO Secretary General Jens Stoltenberg put it in a 2015 speech.[24] Developed to help stabilise weak states through a combination of kinetic and non-kinetic operations, including, famously, in the cognitive domain ('winning hearts and minds'), the comprehensive approach may be turned on its head and the stabilisation efforts turned into policies of destabilisation.[25] The comprehensive approach seeks to reduce vulnerabilities, while the hybrid warfare approach seeks to increase and exploit them. It is a game of threats and vulnerabilities.[26]

THE RUSSIAN MEDIA LANDSCAPE

'The Putin era has not been a good one for the Russian media'. Such is the opening statement in an article by Jonathan Becker, in which he describes the gradual establishment and mechanics of what is labelled for instance a 'neo-authoritarian' or 'neo-Soviet' media system in Russia.[27] Subsequent developments seem to have only confirmed Becker's assessment, as the Russian media has continued to struggle under Putin's presidencies (2000–2008 and 2012–present) and his premiership (2008–2012). Thus, according to media watchdog Reporters Without Borders, with a score of 49.03, Russia in 2016 ranked 148 out of a total of 180 states surveyed.[28] On a par with states such as Malaysia, Pakistan, Mexico and Tajikistan, Russia finds itself in the category of those with 'bad' media conditions. Reporters Without Borders note that:

What with draconian laws and website blocking, the pressure on independent media has grown steadily since Vladimir Putin's return to the Kremlin in 2012. Leading independent news outlets have either been brought under control or throttled out of existence. While TV channels continue to inundate viewers with propaganda, the climate has become very oppressive for those who question the new patriotic and neo-conservative discourse or just try to maintain quality journalism.[29]

This evaluation is echoed by Freedom House, which assigns a score of 20 to Russia and places the country in the 'not free' category.[30] Freedom House notes of Russia that:

In Russia's authoritarian government, power is concentrated in the hands of President Vladimir Putin. With loyalist security forces, a subservient judiciary, and a legislature dominated by his United Russia party, Putin is able to manipulate elections and inhibit formal opposition. The government also has strong control of the media environment, and has been able to retain domestic support despite an ongoing economic slump and strong international criticism.[31]

This development has been part of a wider process whereby Russia has become increasingly undemocratic and illiberal, leading many experts, such as for instance the Russian researcher Lilia Shevtsova, to apply the authoritarian label to Putinite Russia.[32] Others, such as the British professor Richard Sakwa, question this, noting for instance that '… there remains an extraordinarily active public sphere critical of Putin and all his works', the suggestion of course being that a truly authoritarian regime would not allow this sphere to exist.[33] Among the more well-known critical outlets alluded to by Sakwa are Novaya Gazeta (newspaper) TV Dozhd (television) and Ekho Moskvy (radio) and of course the internet which in principle remains accessible to the Russian public and where as many as an estimated 105 million users may read critical comments about Putin and other Russian politicians as well as about events in Russia and elsewhere.[34]

Given the existence of this independent public sphere, how may the Russian media world be part of an authoritarian system? John Dunn has used the Italian term lottizzazione to describe what is essentially a two-tier system where the most important media outlets, that is, those in the larger tier one, are tightly controlled, whereas the less important ones are allowed a measured degree of freedom in the smaller tier two. We should see this as a politically controlled process, where members of the regime decide the fate of a vast number of media outlets by assigning them to either tier one or two and by subsequently promoting and relegating them according to their public impact: all the influential outlets are found in tier one and have a pro-regime editorial line, whereas the less influential ones are in tier two and enjoy relative editorial freedom.[35]

Under conditions such as these, the regime assigns very different roles to the state-controlled and independent media respectively. While it is the task of the former to present news in a way which will legitimise continued authoritarian rule, the latter is used instrumentally by the regime to demonstrate that its rule is in fact not as repressive as otherwise alleged by its critics.[36] The challenge for the regime is to grant just enough space to independent media activities to allow it to uphold the desired image of political freedom and respect for the rule of law without jeopardising its hold on power. This pattern could be observed, for instance, during the invasion of Crimea, where generally state-controlled media uncritically applauded the actions of the Russian regime, including the operations of the 'little green men', while minor outlets such as Novaya Gazeta could make more critical comments and offer investigative journalism not seen elsewhere in Russia.

This system has become possible as the result of a development under the Putin presidencies, whereby the state in general has regained control of the Russian media. Through a combination of financial muscle and political and legal pressure and even intimidation, the regime has successfully seized the commanding heights of the Russian media world, all in tier one, from where the campaign to shape the

preferences of the public is best waged.[37] The famous oligarchic media rule of the 1990's and early 2000's, where bitter disputes between these tycoons could be followed in the newspapers and magazines and on the radio and television stations which they controlled, has been replaced by state control and, because of the nature of the present Russian state, by a new oligarchic rule. An important difference, however, is that those presently controlling the media understand how to walk in synchrony and in the direction pointed out to them.

Tier one contains, most importantly, television which has become, as elsewhere, the main source of news, entertainment and information for Russian media consumers. State-controlled television is considered one of the most trusted and authoritative institutions in the country and among these various television stations Channel One (Perviy kanal), controlled by the Kremlin through a state majority ownership, has the largest share of viewers and thus possibly the largest impact.[38] To illustrate the relative one-sidedness, in a May 2014 poll an overwhelming 94 per cent of Russians reported to have received their news about the conflict in Crimea, then recently annexed to Russia, from national television mainly, including of course Channel One.[39]

The internet is still in tier two. However, while, as noted, in principle it remains accessible, the Russian authorities have taken measures to deny public access to an increasing number of Internet Protocol [IP] addresses under the pretext of combating 'extremism' as well as measures putting greater pressure on service providers such as social media site Vkontakte to shut down anti-regime fora.[40] In a attempt to control this further, in 2014 the Russian Duma passed a law stipulating that bloggers with more than 3,000 followers need to be registered in the same manner as more traditional media outlets.[41]

The internet is increasingly regarded as a disruptive sphere which allows citizens to circumvent the state-controlled media in tier one.[42] To illustrate, in April 2017 the Russian National Guard announced the establishment of a new cyber-division dedicated to the monitoring of social media with the aim of identifying 'extremist' statements.[43] Part of the reason for this, so it was explained, was a dramatic rise in extremist statements, but it seems reasonable to speculate that this rise is caused more by the catch-all definition of 'extremism' used by the Russian authorities than by the number of statements considered illegal under the previous and more narrow interpretation. It is now considered an act of extremism, for instance, to question the legality of Russia's annexation of Crimea and to reveal information about Russian military losses in Ukraine.[44] Internet surveillance is done primarily through the software known as SORM. In its most recent configuration, SORM-3, it 'gathers information from all communication media, and offers long-term and comprehensive storage of subscriber data'.[45]

What may occasionally happen is that a media outlet situated in tier two may be drawn into tier one, for instance if it is too independent and critical or has too many viewers, listeners or readers. This may done through the introduction of legal restrictions based for instance on claims of tax irregularities, leading to a temporary suspension of all activities of the media outlet in question. It may later resume its activities, only now under new editorial guidelines and possibly even with changes in the staff composition and as a member of tier one.

In July 2016 journalists at the Russian news agency RBC met their new editors, who laid out the contours of the new editorial line at the agency. According to Meduza, a mainly Russian-language online newspaper set up in Riga in 2014 by Russian journalists critical of the media policy of their own state, the editorial changes were forced through by the Russian authorities as a result of a number of investigative reports prepared by RBC.[46] Below is part of the transcript of that first meeting between editors and journalists, illustrating how there is, on the one hand, an acceptable information space and, on the other hand, an unacceptable information space. As the journalists ask about the line between the two spaces, the new editors, Elizaveta Golikova and Igor Trosnikov, resort to a traffic analogy to explain how things now stand at the office.

The existence of the two information spaces and the risks associated with a transgression of the metaphorical solid double line marking their separation means that the Russian media, and in particular the state-controlled media, are currently overwhelmingly unable or unwilling to do the job which they are supposed to do. This includes offering fair and balanced news and reporting on domestic and international affairs.[48] The absence of such journalistic work may be seen in at least three different ways.

Firstly, and most importantly, it may be seen through the spread of disinformation, defined here as information which is known to be untrue or even deliberately fabricated. It is intentionally false. If this information is subsequently spread by someone who is unaware of its false nature, it is reduced to misinformation.[49]

Secondly, it may be seen through omitted facts or untold stories which, if viewed by the standard of traditional editorial guidelines, would definitely have been considered newsworthy. An example would be the lack of reporting in the state-controlled media on the Russian invasion of Crimea in February 2014; it was only when Putin openly acknowledged that the 'little green men' were in fact Russian troops that the solid double line was redrawn and journalists were free to report on the topic. Another example is from the July 2016 meeting at RBC, when a journalist enquired whether earlier reports about an allegedly corrupt scheme surrounding a Moscow building project, the financers of which included Putin's daughter, had crossed the solid double line. To this Trosnikov responded by making clear that 'I am not going to answer a question like that. You want too much', later adding 'for Christ's sake, don't give us this crap about Putin's daughters [sic!]. Let's talk seriously, like adults'.[50]

Thirdly, and related to this second point, the reporting may be so one-sided as to disqualify it. It may not necessarily contain untruths, but it is done less to inform than to leave the news consumer with a certain set of emotions and, ultimately, with certain political preferences. The January 2017 report by the US Intelligence Community on 'Assessing Russian Activities and Intentions in Recent US Elections' pointed to such a case as it made the argument that 'state-owned Russian media made increasingly favourable comments about Donald Trump as the 2016 US general and primary election campaigns progressed while consistently offering negative coverage of Hillary Clinton'.[51] Additionally, the Intelligence Community asserted that RT America had also intensified its 'usually critical coverage of the United States', pointing to what was believed to be a strongly biased (and negative) reporting on US affairs.[52]

In a more recent form of influence spanning all the three spheres just mentioned, the Russian authorities are reported to be operating 'troll factories', where hundreds of state-employed cyber commentators praise the Russian government and criticise its opponents, domestic as well as international. Writing under aliases, these trolls work to spam internet fora, aiming to sway public opinion in a pro-government direction or simply to drown critical comments in a sea of government support.[53] A former employee at a Russian state-run 'troll factory' explained how 'we wrote about 200 comments and 20 news posts for various fake pages each day. At the "factory" there were many different teams writing on different topics and targeting different websites. At the end of 2016 I know for sure that there were departments dedicated to the Ukrainian crisis and the US elections'.[54] The most prestigious assignment is to write in English language internet fora, thereby possibly influencing a truly global audience through what is essentially normative power.[55] The messaging is amplified through the use of automated botnets, which serve to disseminate the comments and posts still further with the aim of overwhelming the debate and achieving maximum reach.[56]

The basic tenet of the Russian disinformation strategy is the claim that all news is constructed and therefore contested. In the best postmodern tradition there is no 'objective news' – only different, rivalling interpretations which purport to show different aspects of what may be called 'reality'.

This short description of the Russian media landscape is important for understanding how the Russian authorities may use the media to further a particular set of interests. In the influential tier one, in general, executive, legislative and judicial voices blend and are echoed by editorial and op-ed sources, expert commentators and voices from the street – all combine to create a well-controlled media space with a minimum of dissonance.[57] One case study of the annexation of Crimea showed, for instance, how the Channel One news coverage brought together voices from the Kremlin and the Duma, editorial opinions, expert analyses and interviews with demonstrators to create a powerful, yet largely uncontested, narrative about events in Kyiv and the peninsula and about the urgent need for military and political action.[58]

This tool is increasingly being aimed at international, and in particular Western, audiences through the internationally directed tier one platforms such as the television channel RT and the news agency Sputnik. Part of the aim, again, is to shape the political preferences of target audiences. RT invites its viewers to 'question more', presents itself as the Russian view on global news and its YouTube audience exceeds that of any other television channel in the world. Sputnik disseminates news in 34 languages (as of May 2017), among which, and this is quite noteworthy, the Danish, Swedish, Norwegian and Finnish languages do not figure. Sputnik started to broadcast in these Nordic languages in 2015, but the services were discontinued in 2016, presumably as the costs exceeded the benefits, that is, the effect on the target populations was unsatisfactory.

It is partly, if not mainly, this development which has made (Russian) 'disinformation' a topic of such urgency in the West in general that states and organisations are now rushing to prepare institutionalised counter-measures. The former category includes for instance the Anti-Disinformation Agency under the Ministry of the Interior of the Czech Republic (operational since January 2017) and the Centre of Excellence for Countering Hybrid Threats in Finland (operational by late 2017 and supported by a number of Western states), while the latter category most famously includes the European Union's East Stratcom Task Force and the (advisory and independent) NATO Strategic Communications Centre of Excellence.

The basic tenet of the Russian disinformation strategy is the claim that all news is constructed and therefore contested.[59] In the best postmodern tradition there is no 'objective news' – only different, rivalling interpretations which purport to show different aspects of what may be called 'reality'. And what the Russian media outlets present are merely possible explanations which serve as alternatives to the stories offered by Western media. It is a strategy which is both cunning and elegant as it preys on the enlightenment tradition and on the vulnerabilities of liberal democratic media. Few researchers working in the social sciences would dare to make the claim that what they offer is 'true' in any definitive sense and this view has sifted through to the media which is keen to offer alternative perspectives and to let readers, listeners and viewers decide for themselves what to believe. It is the post-factual era and it is the exercise of extreme perspectivism.[60]

A prominent example of this approach is the fate of Malaysia Airways Flight MH-17, which was shot down over eastern Ukraine in July 2014. In 2016 the Joint Investigation Team, [JIT], led by the Dutch authorities, drew the firm conclusion that MH-17 was shot down from an area 'controlled by pro-Russian fighters', adding that 'the BUK-TELAR [missile] was brought in from the territory of the Russian Federation and subsequently, after having shot down flight MH-17, was taken back to the Russian Federation'.[61] The Russian state-controlled media, on the other hand, have offered at least nine different versions of what happened to MH-17 and what is particularly noteworthy is that none of these correspond to the conclusion reached by the JIT.[62] Some of these versions – or perspectives on what may have happened – are mutually incompatible but that seems to be of little importance to those engineering the disinformation.[63]

THE WEAPONISATION OF INFORMATION

The term 'the weaponisation of information' is often used to describe this highly instrumental use of the media, including social media, to further particular interests. Slightly dramatic perhaps, within the present context the term alerts us to the fact that the media is incorporated into Russian political thinking not as a constraint but as an asset to be used in the pursuit of various goals. These may range from the tactical or short-term (e.g. 'Artillery shelling by Ukrainian forces killed three children in Donbass') to the strategic or long-term.[64] When appearing in the form of meta-narratives, that is the overarching stories which inform us about the past, present and future, the media stories will usually be impossible to check for authenticity.

A current meta-narrative in Russia may be the claim that 'the West is locked in centuries-old conflict with Russia'.[65] It is reinforced by the heavy focus on military preparedness in Russia, ranging from the emphasis on patriotism to the very public celebration of the country's nuclear arsenal.[66] The claim is put forward at such an abstract level that it is mainly a matter of personal belief. Its dominant use by the Russian media should therefore be regarded as a case of extreme one-sidedness and untold stories, that is, strong media bias. It serves not only as a galvanising force within Russian society, informing the population of the meaning of the notion of 'Russia' today, but also as an interpretative background against which smaller narratives may easily be developed and then spread by the media.[67] The meta-narratives represent the most solid of the solid double lines referred to earlier, as the questioning of these will cast doubt on related smaller narratives also.

The narratives, especially the meta-narratives, may serve as a cognitive filter which affects the interpretation of systemic inputs. This filter may even be employed as a heuristic device, or mental shotgun, allowing its users to quickly connect the dots and to make sense of different events.[68] The spread of disinformation benefits from this heuristic, as it facilitates easy consumer recognition and greater legitimacy. All things being equal, the greater the cognitive resonance – 'to which extent does this piece of news fit what I already know about this particular subject?' – the greater the acceptance by the consumers of what is being presented to them.[69] To illustrate, if consumers accept the meta-narrative saying that 'the West is locked in centuries-old conflict with Russia' as well as a smaller narrative claiming that 'the regime change in Kyiv in February 2014 was a coup instigated by the West', then Russian disinformation about MH-17, blaming for instance the Ukrainian authorities or the West for the shoot-down, are also accepted more easily.

As mentioned earlier, the 2013 Gerasimov article points to a ratio between non-kinetic and kinetic operations of 4:1, indicating that the latter is already considered a secondary aspect of (hybrid) war. In a 2017 article Gerasimov develops this idea further. Work is currently being undertaken within the Russian armed forces to develop a re-conceptualisation of the notion of 'war' and, while it is still uncertain how far Russian military thinkers and politicians will be willing to go, it is already apparent that the conclusions and recommendations will emphasise the non-kinetic elements to an even greater extent.[70] Citing unidentified sources, Gerasimov notes how 'some' are now advancing the idea that 'armed fighting is no longer a necessary attribute [of war]'.[71] There is undoubtedly a political instrumentality to this development as it supports the oft-heard claim by the Russian authorities that the West is waging a (hybrid) war against Russia. If no kinetic operation needs to be executed, or even threatened, for a condition to qualify as 'war', then clearly it is even easier than under the kinetic–non-kinetic hybridity concept to make the argument before the public that 'we are at war'.

A current meta-narrative in Russia may be the claim that 'the West is locked in centuries-old conflict with Russia'. It is reinforced by the heavy focus on military preparedness in Russia, ranging from the emphasis on patriotism to the very public celebration of the country's nuclear arsenal.

The 2017 Gerasimov article may also inform us about the Russian thinking on the topic of 'war' and on the role of the non-kinetic in this. It seems premature to conclude that this thinking sees the possibility of war as an exclusively non-kinetic activity – this at least has not been announced yet – but the development points strongly in this direction. When opening Media-AS 2015, the first staging of what is now an annual event to celebrate those media professionals who make 'a significant contribution to the strengthening of the positive image of the Armed Forces', Russian Minister of Defence Sergei Shoigu expressed the belief that:

The day has come, where we recognise that the word, the camera, the photograph, the internet and information in general have become yet another type of weapon, yet another expression of the Armed Forces. This weapon may be used positively as well as negatively. It is a weapon which has been part of events in our country in different years and in various ways, in defeats as well as in victories.[72]

Rossiiskaya Gazeta, the Russian government newspaper, summed up the message delivered by Shoigu with the telling headline 'words also shoot'.[73] It reflects a recognition of the growing importance of the non-kinetic in general and of information in particular. Further to this, in February 2017, Shoigu announced the establishment of an 'information operations force' as part of the defence structure.[74] The existence of this unit was widely presumed even before Shoigu's February 2017 announcement but the open admission that Russia engages in such activities, including through the use of its military, was noteworthy.

The state-controlled Russian media serves as a force multiplier. It augments other capabilities, kinetic as well as non-kinetic, which the Russian state may employ in its pursuit of political goals. It is difficult to assess how great a force multiplier the media is, but there is no doubt that the greatest effect is felt within the domestic neo-authoritarian media space. Within this setting it serves as a defensive tool mainly, as it is designed to protect and preserve the existing political order. As alternative Russian voices are few and far between and, quite literally, on the periphery, and external voices find it hard to penetrate this media space, there is ample opportunity for the Russian regime to offer its meta-narratives and smaller narratives in a largely uncontested manner.

The effect within the international media space, with its many dissonant voices, is much harder to assess. The media strategy within this setting has an offensive purpose mainly, as it is designed, at the most overall level, to challenge and upset the status quo; it is the activation of the 'chaos button'. The various responses by Western states and organisations mentioned briefly earlier indicate a belief, or at least a grave concern, that the Russian media strategy, in particular of course the use of disinformation, is actually working. Commentaries from very different platforms, making such claims as 'US losing "information war" to Russia', 'Pro-Kremlin disinformation campaign (…) extremely successful' and 'Russia's Hybrid Warfare: A Success in Propaganda' all suggest a destabilising effect of the Russian media strategy on the target audiences in the West.[75]

The state-controlled Russian media serves as a force multiplier. It augments other capabilities, kinetic as well as non-kinetic, which the Russian state may employ in its pursuit of political goals.

Given the comments by Gerasimov and Shoigu, and the intensified future media strategy suggested by them, as well as the close relationship between the Russian state and the media, Western states and organisations should evaluate existing counter-measures and, if necessary, design and implement additional ones. When doing so it is important to separate dissemination from effect. The fact that a piece of disinformation is being cited widely – and perhaps finds its way into both well-established and autonomous media – clearly increases the risk of acceptance by a target audience but it does not follow automatically. Methodologically, it is difficult to measure the effect of a piece of disinformation – or of a whole wave of it – as political preferences may be influenced by many other factors. To illustrate, decreasing support for the EU among the populations of the member states may not be interpreted so as to indicate that the Russian anti-EU narrative is being accepted by these populations.[76] Many alternative reasons, not least those relating to the internal challenges of the EU, offer themselves.[77] It may even be said that relatively high levels of trust in the Russian media in the West may be exactly that – relatively high levels caused more by distrust of the Western media than trust as such in the Russian media.[78]

COGNITIVE RESILIENCE

As mentioned earlier, the Russian media strategy seeks to exploit the vulnerabilities of liberal democratic media. For the EU, for instance, the challenge is how to counteract information spread by internal or external actors, which is deliberately false or is characterised by omitted facts or one-sided analyses and is seeking to undermine support for the fundamental norms – or collective identity – of the Union.[79] Central among these actors is Russia.[80] In response to this challenge the EU has established the East Stratcom Task Force, possibly the most widely recognised, and criticised, anti-disinformation unit set up to handle Russian disinformation.[81] The slogan of the East Stratcom Task Force is 'Question even more', clearly a response to the RT slogan 'Question more'. Several similar agencies, within state structures or organisations, exist, however, and a few of these have been listed above.

It is advisable to focus on vulnerabilities and seek to reduce those rather than to address the threats, which presently seem very difficult for external actors to change.

A 2016 EU Barometer poll conducted within the EU showed greater trust in radio (59%), television (50%) and written media (46%) than in the internet (36%) and online social networks (21%). These figures are positive from the perspective of fighting disinformation, but it should be kept in mind that the latter is spread on all platforms, including of course radio, television and written media.[82] There is great variation across member states. Trust in radio ranges from 82% (Sweden and Finland) to 41% (Malta); trust in television ranges from 78% (Finland) to 23% (Greece); trust in written media ranges from 71% (the Netherlands) to 21% (the United Kingdom); trust in the internet ranges from 50% (the Czech Republic) to 24% (France); and trust in social networks ranges from 36% (Portugal) to 8% (France), whereas distrust in social networks ranges from 75% (Sweden) to 36% (Bulgaria).[83] It should be noted that while public service media may be part of the solution – generating trust – they may also be part of the problem. It depends entirely on their journalistic standards and operational freedom.[84] These figures suggest that some EU member states enjoy better preconditions for fighting disinformation than do others, alerting us to the fact that one standard model will be inadequate.

It is advisable to focus on vulnerabilities and seek to reduce those rather than to address the threats, which presently seem very difficult for external actors to change. In fact, the stream of disinformation, by (state-controlled) well-established media or autonomous media, should be expected to increase only. All states may legitimately ban certain utterances, but it is futile to attempt to prevent disinformation from entering the information space.[85] This is particularly true for the disinformation which is internally generated, but it is also and even true for the disinformation prepared by external actors. To illustrate, the temporary three-month ban against the Russian television channel RTR Planeta imposed by the Lithuanian authorities in February 2017, and approved by the European Commission, may prevent for instance an escalation of conflict between different ethnic groups in Lithuania, but it is highly unlikely to form part of a long-term solution.[86]

The active debunking of disinformation, via a meticulous de-construction of the news items, is advisable in extraordinary circumstances, such as the risk of heightened tension or even outbreak of conflict within a state or between states, as well as for educational purposes.[87] It may alert the public to the fact that disinformation exists and help news consumers distinguish between different forms of information and better identify the false or biased stories. The challenge of disinformation should be viewed as a systemic challenge, however, and the search for possible solutions should therefore focus on systemic responses. The policy of debunking, now done by numerous agencies, is important as it may for instance serve the purposes just mentioned. It is not, however, to be considered a systemic response. For that it is too patchy.

This report suggests to focus on the build-up of greater cognitive resilience, that is, the ability to withstand pressure from various ideas spread, for instance, through disinformation. The term 'resilience' is now widely accepted as a concept relating to the protection of critical functions of society and the 'cognitive resilience' term is very similar, only it plays out in the cognitive domain as opposed to the physical domain. It has to do with world views and interpretative schemata used by the news consumers to make sense of information. In essence, it will allow for the free flow of information, including from Russian state-controlled media, but it will establish a cognitive 'firewall', which prevents the disinformation from taking root and being internalised by members of the target audience. Unless extraordinary circumstances dictate a (temporary) ban directed against specific media outlet(s), and this may be fully legitimate, the flow of information should remain uninterrupted.

Ideally, the cognitive firewall should be installed at both the collective and at the individual level. At the society-wide level the ability to recognise and subsequently reject disinformation and not give it the attention which it demands should be improved. Moreover, as the dominant collective understanding of the media is still shaped by the pre-digital era, it should be understood more explicitly that the digital era offers an almost endless range of possibilities, especially for autonomous news broadcasting, and that this development has built-in risks which we are now beginning to understand. And at the individual level a new media literacy should be developed; a new ideal of Bildung, defined briefly here as an ability to reflect critically on one's practices and on the structures within which one acts, is required which gives members of the target audience the tools with which to distinguish facts from fiction and the information from the disinformation.[88] The Bildung should be established at school, where the teaching of media literacy would be comparable to the teaching of science or computer literacy.

It seems certain that we will see a future characterised by even more contested news arenas and even more disinformation.

The anti-disinformation units mentioned earlier may support this, together with, for instance, media outlets in the target states, by exposing disinformation and alerting the public to the existence of this latter. Several outlets have run informative pieces on how to recognise disinformation and thus to protect oneself from its intentionally false character.[89] Some of the tools suggested or even introduced include disinformation hotlines, where experts will de-construct the news items and raise red flags to warn others that they are entering disinformation territory, the verification of 'real' (as opposed to 'false') websites, a restriction on advertising placed by leading search engines and social media platforms on known disinformation sites as well as the use of advanced algorithms to beat the algorithms which help spread the disinformation.[90] While some of these are systemic responses, for instance the development of anti-disinformation algorithms, others clearly are not.

The contribution of the non-systemic responses should not be underestimated, but the main deficiencies of these relate to time and adaptability. Thus, by the time a piece of disinformation has been debunked, the world of media has moved on, producing a vast number of new items in the process. And as sites are being flagged for disinformation content, new ones will emerge. Producers of disinformation learn as they face obstacles on their way and they will adjust accordingly. The systemic responses will not be able to avoid this challenge of a 'learning race' as the producers of disinformation will attempt to mask their sites and news items so as to pass under the radar of even the media-literate.

It seems certain that we will see a future characterised by even more contested news arenas and even more disinformation. This report has focused on Russia as this state seems to represent the state-of-the-art of disinformation and as it has displayed a high level of media aggression and cynicism. Compare for instance the handling of MH-17 to the downing by the Soviet Air Force in 1983 of Korean Airlines flight KAL-007. While initially the Soviet Union denied any involvement in the incident, the regime soon changed track and allowed news reports in the state-controlled media to explain to the Soviet public that their military commanders had actually given the order to shoot down a civilian airliner. The current Russian regime clearly is unable to perform a similar step with respect to the BUK missile which hit MH-17 and the Russian media not only let it get away with this but even transmitted the counter-narratives designed to cause confusion in the post-modern and perspectivist news space. It is important to note, however, that other actors, state and non-state alike, already engage in and will continue to engage in the spread of disinformation.

There will not be any easy or fix-it-all solutions to this development. Rather, liberal democracies, especially vulnerable as a result of their free media culture, should prepare themselves for a long-term commitment to countering disinformation and to building up cognitive resilience to ensure that the former has minimal effect. It is important to continuously evaluate and adjust, if only for the reason that the producers of disinformation will also do so. The media literacy perspective – Bildung – will not be the silver bullet to kill disinformation but it may provide the necessary foundation on which other strategies may be developed. Together they may eventually make our world safer from disinformation.

NOTES

The author would like to thank an anonymous reviewer for very positive and constructive comments.

1 Valery Gerasimov, "Tsennost nauki v predvidenii", Voenno-promyshlenniy kurer (27 February 2013).

2 See, for instance, John McCuen, "Hybrid Wars", Military Review March–April (2008), pp. 107–113; Ruslan Pukhov, "Mif o 'gibridnoi voine'", Nezavisimaya Gazeta (29 May 2015) and Peter Mansoor, "Hybrid Warfare in History", in Williamson Murray and Peter Mansoor (eds.) Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present (Cambridge: CUP, 2012), pp. 1–17. To illustrate the complexity of the use of terms such as 'hybrid warfare', Peter Mansoor defines it as the combination of 'conventional as well as irregular forces working in tandem'; in "Hybrid Warfare in History", p. 2.

3 In Walter Richter, "The Future of Information Operations", Military Review (January–February) 2009, p. 104. As the non-kinetic is defined as a negative, that is, by what it is not, its meaning is often less clear than that of the kinetic.

4 For an overview and discussion of this debate, see Errol Henderson and J. David Singer, "'New Wars' and Rumors of 'New Wars'", International Interactions 28 (2002), pp. 165-190.

5 See, for instance, House of Commons Defence Committee, Towards the Next Defence and Security Review: Part Two – NATO (London: The Stationary Office, 2014).

6 For an interpretation of the 2013 Gerasimov article, see, for instance, Charles Bartles, "Getting Gerasimov Right", Military Review (January–February) 2016, pp. 30–38.

7 Gerasimov, "Tsennost nauki v predvidenii".

8 The figure is presented by Gerasimov in his 2013 article; this English-language version is from US Army Asymmetric Warfare Group, Ambiguous Threats and External Influences in the Baltic States (Fort Meade, MD: US Army Asymmetric Warfare Group, 2015), p. 4.

9 Aleksandr Bartosh, "Gibridnaya voina v ekonomicheskoi sfere", Nezavisimoe voennoe obozrenie (4 September 2015) and Vadim Koval, "Gibridnaya voina' ot 'Grinpis'", Nezavisimoe voennoe obozrenie (24 October 2014).

10 For illustrations, see Aleksandr Bartosh, "Model upravlyaemogo khaosa – ugroza natsionalnoi bezopasnosti Rossii", Nezavisimoe voennoe obozrenie (12 July 2013), Aleksandr Bartosj, "Tsel i mekhanismi modeli upravlyaemogo khaosa", Nezavisimoe voennoe obozrenie (27 September 2013), Oleg Vladikin, "'Voina upravlyaemogo khaosa': Uroki dlya Rossii. Chast 1", Nezavisimoe voennoe obozrenie (24 October 2014) and Oleg Vladikin, "'Voina upravlyaemogo khaosa': Uroki dlya Rossii. Chast 2", Nezavisimoe voennoe obozrenie (24 October 2014).

11 Kalevi Holsti, The State, War, and the State of War (Cambridge: CUP, 1996).

12 Vladikin, "'Voina upravlyaemogo khaosa': Uroki dlya Rossii. Chast 1", Nezavisimoe voennoe obozrenie (24 October 2014) and "'Voina upravlyaemogo khaosa': Uroki dlya Rossii. Chast 2", Nezavisimoe voennoe obozrenie (24 October 2014).

13 For instance Oleg Sergeev, "Generator strakha", Nezavisimoe voennoe obozrenie (5 June 2015).

14 See, for instance, the debate in the journal Voprosy kiberbezopasnosti (2014 -); it may be accessed at http://cyberleninka.ru/journal/n/voprosy-kiberbezopasnosti.

15 Scott Applegate, "The Dawn of Kinetic Cyber", paper presented at the 5th International Conference on Cyber Conflict (2013); available at https://ccdcoe.org/cycon/2013/proceedings/d2r1s4_applegate.pdf; no page numbers.

16 James Farwell and Rafal Rohozinski, "The New Reality of Cyber War", Survival 54/4 (2012), pp. 107–120.

17 Office of the Director of National Intelligence, Background to "Assessing Russian Activities and Intentions in Recent US Elections: The Analytic process and Cyber Incident Attribution" (6 January 2017).

18 Natan Dubovichkiy (widely seen as the pseudonym of Vladislav Surkov), "Bez neba", Russkiy Pioner (12 March 2014); at http://ruspioner.ru/honest/m/single/4131.

19 Gerasimov, "Tsennost nauki v predvidenii".

20 Barry Buzan, People. States & Fear (Hemel Hempstead: Harvester Wheatsheaf, 1991), pp. 112–116.

21 Ibid., p. 112.

22 Ibid., p. 112.

23 Amelia Hodsdon, "Get your kicks with Israeli tricks", The Guardian (9 February 2005).

24 Keynote speech by NATO Secretary General Jens Stoltenberg at the NATO Transformation Seminar (25 March 2015); at http://www.nato.int/cps/en/natohq/opinions_118435.htm.

25 Flemming Splidsboel Hansen (ed.), The Comprehensive Approach (Copenhagen: The Royal Danish Defence College 2009).

26 Buzan, People. States & Fear, pp. 112–145.

27 Jonathan Becker, "Lessons from Russia: A Neo-Authoritarian Media System", European Journal of Communication 19/2 (2004), p. 139 and John Dunn, "Lottizzazione Russian Style: Russia's Two-Tier Media System", Europe–Asia Studies 66/9 (2014), p. 1431.

28 This is on a scale ranging from 0 (most free) to 100 (least free); see Reporters Without Borders, 2016 World Press Freedom Index; at https://rsf.org/en/ranking.

29 Reporters Without Borders, 2016 World Press Freedom Index – Russia; at https://rsf.org/en/russia.

30 This is on a scale ranging from 0 (least free) to 100 (most free); see Freedom House, Freedom in the World 2017; at https://freedomhouse.org/report/freedom-world/freedom-world-2017.

31 Freedom House, Russia Profile 2017; at https://freedomhouse.org/report/freedom-world/2017/russia.

32 Lilia Shevtsova, "Forward to the Past in Russia", Journal of Democracy 26/2 (2015), pp. 22–36.

33 Richard Sakwa, Putin Redux – Power and contradiction in contemporary Russia (London: Routledge, 2014), p. 8. Sakwa goes on to note that "if Russia is an authoritarian system, it is not a very good one according to the classical concepts of what an authoritarian system should look like"; in ibid. p. 8. For a discussion of authoritarianism, see e.g. Siaroff, Comparing Political Regimes, University of Toronto Press, 2009.

34 United Nations, Internet Users 2015 (no date); at http://data.un.org/Data.aspx?d=WDI&f=Indicator_Code%3AIT.NET.USER.P2; last accessed 1 May 2017.

35 Dunn, "Lottizzazione Russian Style", pp. 1433–1434.

36 For a seminal discussion of the role of the media under authoritarianism, see Fredrick Siebert, "The authoritarian theory of the press", in Frederick Siebert, Theodore Peterson & Wilbur Schramm, (eds.) Four Theories of the Press (Urbana, IL: University of Chicago Press, 1963), pp. 9–38.

37 Scott Gehlbach, "Reflections on Putin and the media", Post-Soviet Affairs 26/1 (2010), pp. 80–81.

38 Jukka Pietiläinen, "Media use in Putin's Russia", Journal of Communist Studies and Transition Politics 24/3 (2008), pp. 365–385; Regyna Smyth and Sarah Oates, "Mind the Gaps: Media Use and Mass Action in Russia", Europea–Asia Studies 67/2 (2015), pp. 285–305; see figures in Ilya Kiriya and Elena Degtereva, "Russian TV market: Between state supervision, commercial logic and simulacrum of public service", Central European Journal of Communication, 3/1 (2010), pp. 37–51; at http://ptks.pl/cejc/wp-content/uploads/2012/07/CEJC_Vol3_No1_Degtereva.pdf; and Flemming Splidsboel Hansen, "Mediatised Warfare in Russia", in Mervi Pantti, (ed.), Media and the Ukraine Crisis: Hybrid Practices and Narratives of Conflict (New York: Peter Lang, 2016), pp. 89–106.

39 Hansen, "Mediatised Warfare in Russia", p. 91.

40 Smyth and Oates, "Mind the Gaps", pp. 291–292.

41 British Broadcasting Corporation [BBC], "Russia enacts 'draconian' law for bloggers and online media" (1 August 2014).

42 Ksenia Ermoshina and Francesca Musiani, "Migrating servers, elusive users: reconfigurations of the Russian internet in the post-Snowden era", Media and Communication 5/1 (2017), p. 42.

43 "Russia's National Guard Creates New Task Force to Monitor Social Media", The Moscow Times (15 April 2017).

44 "Pora postavit deistvenniy zaslon informatsionnoi voine", Kommersant (18 April 2016).

45 Ermoshina and Musiani, “Migrating Servers, Elusive Users”, p. 44.

46 Meduza, “12 newsrooms in 5 years: How the Russian authorities decimated a news industry”, (18 May 2016); at https://meduza.io/en/feature/2016/05/18/12-newsrooms-in-5-years.

47 Meduza, “This is what losing your newsroom looks like in Russia” (12 July 2016); at https://meduza.io/en/feature/2016/07/12/this-is-what-losing-your-newsroom-looks-like-in-russia.

48 See, for instance, the Code of Ethics of the Society of Professional Journalists (6 September 2014); at https://www.spj.org/ethicscode.asp.

49 The term “fake news” seems to include both disinformation and misinformation.

50 Meduza, “This is what losing your newsroom looks like in Russia”. Trosnikov uses the plural, referring to both of Putin’s daughters.

51 Office of the Director of National Intelligence, Assessing Russian Activities and Intentions in Recent US Elections (6 January 2017), p. 3.

52 Ibid. p. 6.

53 BBC, “Ukraine conflict: Inside Russia’s ‘Kremlin troll army’” (19 March 2015); at http://www.bbc.com/news/world-europe-31962644 and Steven Wilson, “The logic of Russian internet censorship”, The Washington Post (16 March 2014); at https://www.washingtonpost.com/blogs/monkey-cage/wp/2014/03/16/the-logic-of-russian-internet-censorship/.

54 In “Revealed: Confessions of a Kremlin Troll”, The Moscow News (18 April 2017). Some of the more well-known work on the ‘troll factories’ has been done by Finnish investigative journalist Jessikka Aro, who later became a target of trolling herself, and whose work has documented some of the mechanics of this type of operations; see, for instance, Yle Kioski Traces the Origins of Russian Social Media Propaganda – Never-before-seen Material from the Troll Factory (20 February 2015); at http://kioski.yle.fi/omat/at-the-origins-of-russian-propaganda.

55 Shaun Walker, “Salutin’ Putin: Inside a Russian troll house”, The Guardian (2 April 2015).

56 Kalev Leetaru, “Did Russia Just Run The World’s Greatest Social Media Campaign?”, Forbes (21 March 2017).

57 Dunn, “Lottizzazione Russian Style”.

58 Flemming Splidsboel Hansen, “Framing yourself into a corner: Russia, Crimea and the minimal action space”, European Security 24/1 (2015), pp. 141–158.

59 Peter Pomerantsev, Nothing is True and Everything is Possible (London: Faber and Faber, 2015).

60 Or ‘weaponised relativism’ for instance; in “The Guardian view on Russian propaganda: The truth is out there”, The Guardian (2 March 2015).

61 The Public Prosecution Service of the Netherlands, Presentation preliminary results criminal investigation MH17 28-09-2016 [sic!] (28 September 2016); at https://www.om.nl/onderwerpen/mh17-vliegramp/presentaties/presentation-joint/.

62 East Stratcom Task Force, Disinformation Digest (30 September 2016).

63 BBC, “Flight MH17: Russia and its changing story” (16 October 2015).

64 See, for instance, BBC, “Girl killed in Ukraine never existed’” (8 April 2015); at https://www.youtube.com/watch?v=HW-4a0P8sjs. It will often be difficult, even impossible, to clearly separate the different levels and a false story such as this one may of course have strategic implications also.

65 Flemming Splidsboel Hansen, “Russia’s relations with the West: Ontological security through conflict”, Contemporary Politics 22/3 (2016), pp. 349–375.

66 See, e.g., the various contributions in Tamara Guzenkova (ed.) Patriotizm kak ideologiya vozrozhdeniya Rossii (Moscow: Rossiiskiy Institut Strategicheskikh Issledovanii, 2014).

67 Hansen, “Mediatised Warfare in Russia”.

68 Leonard Mlodinow, The Drunkard’s Walk: How Randomness Rules Our Lives (London: Penguin 2009), p. 174

69 See, e.g., Flemming Splidsboel Hansen, “Mediatized Warfare in Russia: Framing the Annexation of Crimea”, in Mervi Pantti, (ed.) Media, Communication Power and the Ukraine Conflict (Frankfurt am: Peter Lang, 2016), pp. 89–106.

70 Valery Gerasimov, “Mir na granyakh voiny”, Voenno-promyshlenniy kurer (15 March 2017).

71 Ibid.

72 “Slovo tozhe strelyaet”, Rossiiskaya gazeta (30 March 2015). For information on Media-AS, see Polozhenie o vserossiiskom festivale pressy “Media-AS-2015”; at http://mil.ru/files/morf/Media-ace.pdf and Itogi finalnogo etapa vserossiiskogo festivalya pressy “Media-AS-2017”; at http://мультимедиа.минобороны.рф/multimedia/infographics/parad/media-ace-2017.htm.

73 “Slovo tozhe strelyaet”, Rossiiskaya gazeta (30 March 2015).

74 “The Secrets of Russia’s Propaganda War, Revealed”, The Moscow News (1 March 2017).

75 In Warren Strobel, “US losing ‘information war’ to Russia, other rivals – study”, CNBC (25 March 2015), “Commentary: Means, goals and consequences of the pro-Kremlin disinformation campaign“, EU East Stratcom Disinformation Review (19 January 2017) and Keir Giles, “Russia’s Hybrid Warfare: A Success in Propaganda”, Arbeitspapier Sicherheitspolitik 1 (2015), pp. 1–5.

76 See, for instance, EU East Stratcom Disinformation Review, various issues, and Kremlin Influence Index 2017 (Kyiv: Detector Media 2017).

77 See, for instance, “Central Europe under the fire of propaganda: Public opinion polls in the Czech Republic, Hungary and Slovakia”, GLOBSEC Trends (2016). These challenges could include the Euro, migration and Brexit; see, for instance, Wolfgang Münchau, “A history of errors behind Europe’s many crises”, Financial Times (29 March 2016).

78 For figures, see European Commission, Standard Eurobarometer – Media use in the European Union 86 (2016).

79 Ulrich Sedelmeier, “Collective Identity”, in Walter Carlsnaes, Helene Sjursen & Brian White (eds.) Contemporary European Foreign Policy (London: Sage, 2004), pp. 123–140.

80 See, for instance, European Parliament, EU strategic communication to counteract anti-EU propaganda by third parties (23 November 2016).

81 See https://euvsdisinfo.eu/.

82 European Commission, Standard Eurobarometer – Media use in the European Union 86 (2016), QA8a.

83 Ibid., Q8Aa1 – Q8Aa5. The figures for Denmark are: Radio (76%), television (71%), written media (57%), the internet (38%) and social networks (17%); the level of distrust of social networds stands at 63% among Danish respondents.

84 Unidentified speakers at the conference on “Media Freedom and Pluralism in Europe – Threats and Responses”, University of Copenhagen (2 December 2016).

85 See, for instance, European Parliament, EU strategic communication to counteract anti-EU propaganda by third parties, Article 35

86 “EU allows Lithuania to ban Russian tv channel”, EU Observer (17 February 2017).

87 “Lithuania looking for source of false accusation of rape by German troops”, Reuters (17 February 2017).

88 Anders Odenstedt, “Hegel and Gadamer on Bildung”, The Southern Journal of Philosophy 46/4 (2008), pp. 559–580.

89 See, for instance, BBC, “Solutions that can stop fake news spreading” (30 January 2017) and “How to avoid falling for lies and fake news” (11 February 2017).

90 BBC, “Solutions that can stop fake news spreading”.

Photos
Coverphoto, Page 7-8: Scanpix, Denmark
Page 14-15, 27-28: Polfoto, RIA-News
Page 32-33: Polfoto, AP, Alexander Zemlianichenko

DIIS · Danish Institute for International Studies

The Danish Institute for International Studies is a leading public institute for independent research and analysis of international affairs. We conduct and communicate multidisciplinary research on globalisation, security, development and foreign policy. DIIS aims to use our research results to influence the agenda in research, policy and public debate, and we put great effort into informing policymakers and the public of our results and their possible applications.

Defence and Security Studies at DIIS

This publication is part of the Defence and Security Studies at DIIS. The aim of these studies is to provide multidisciplinary in-depth knowledge on topics that are central for Danish defence and security policy, both current and in the long term. The design and the conclusions of the research under the Defence and Security Studies is entirely independent. Conclusions do not reflect the views of the ministries or any other government agency involved, nor do they constitute an official DIIS position. Additional information about DIIS and our Defence and Security Studies can be found at www.diis.dk

DIIS · DANISH INSTITUTE FOR INTERNATIONAL STUDIES
Østbanegade 117 | DK-2100 Copenhagen | Denmark | www.diis.dk