Hadtudományi Szemle
13. évfolyam (2020) 2. szám 5–12. • DOI: 10.32563/hsz.2020.2.1

Dóra Dévai[1]

An Overview of the Development of the Russian Information Warfare Concept
Part 2.

Az orosz Információs Hadviselés koncepció fejlődésének áttekintése
2. rész

Abstract

After the infamous cyber attacks against Estonia in 2007 and the Ukrainian conflict in 2014–15, the Russian military theory, and in particular, Information Warfare (IW) doctrines, have come into the center of attention. IW has played a very peculiar role in the Russian political and military theory and practice, and its current state can be regarded as a climax in its evolution. To gain an in-depth understanding of the Russian strategic thinking, the second part of this article strives to give an overview of the current phase of the process.

Keywords: *Information Warfare, operational art, information space, reflexive control*

Absztrakt

Az Észtország elleni hírhedt számítógépes támadásokat követően, és különösen az ukrajnai konfliktus után az orosz katonai elmélet és az Információs Hadviselés (IH) a figyelem középpontjába került. Az orosz katonai és stratégiai gondolkodás megértéséhez ezen területek mélyreható vizsgálata szükséges. Az IH rendkívül sajátos szerepet játszik az orosz politikai és katonai elméletben és gyakorlatban, és jelenlegi állapotát a ciklikus

[1] Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar – University of Public Service, Faculty of Military Sciences and Officer Training, e-mail: Devai.Dora@uni-nke.hu, ORCID: https://orcid.org/0000-0003-1024-4474

megújuláson átesett fejlesztések csúcspontjának tekinthetjük. Jelen tanulmány arra irányul, hogy betekintést nyújtson ezen fejlődési folyamat legutóbbi szakaszába, amely az orosz IH-fejlődés – és azon belül a kiberműveletek értelmezésének – egyedülálló jellegét adja.

Kulcsszavak: *információs háború, stratégiai művészet, információs tér, reflexív kontrol*

1. Capability development

The Russian military has been studying *virus or software warfare* since the 1970s as one of the most important aspects of future information warfare. *Cyber warfare* in Russian sources, however, has for a long time only appeared in reference to the Western computer attacks against Russian systems. While computer attacks have been an integral part of IW capabilities, they constitute just one of the many other elements and possess much less prominence than in the US.[2] In contrast to the US Cyber Command, the actual cyber capabilities development has been rather cryptic both in terms of organisation and capabilities. Part of the scarce publicly available information is that within the military *the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU)* has a major share in *information warfare operations including cyber capabilities.* Russian Defence Minister Sergei Shoigu made a passing reference in his speech at the Duma referring to the so-called information troops (voiska informatsionnykh operatsii) having been operational for four years. Shoigu also stated that propaganda needs to be clever, smart and efficient.[3] In addition, the indictment of the US Department of Justice pertaining to cyber attacks refers to specific GRU units in Moscow: military units 26165 and 74455, also known as 6th Directorate and the Advanced Persistent (APT)28 group responsible for Sofacy and Fancy Bear attacks.[4] Beyond that, very little can be retrieved from authentic Russian sources. What also seems to be another major form of organisation in terms of cyber capabilities is a range of so-called *scientific companies* (nauchnyye kompanii) in the

[2] M. C. Fitzgerald, 'Russian Views on IW, EW, and Command and Control: Implications for the 21st Century.' Hudson Insitute, Washington DC, 1999. Available: www.dodccrp.org/events/1999_CCRTS/pdf_files/track_5/089fitzg.pdf (02. 05. 2019.); Th. Thomas, *Russia. Military Strategy.* Foreign Military Studies Office. Fort Leavenworth, 2015. Available: https://info.publicintelligence.net/FMSO-RussianMilitaryStrategy.pdf (02. 04. 2019.); Dmitry Adamsky, 'Cross-Domain Coercion. The Current Russian Art of Strategy.' The Institut Français des Relations Internationales, Paris, 2015. Available: www.ifri.org/sites/default/files/atoms/files/pp54adamsky.pdf. (24. 03. 2019.)

[3] Viktor Khamrayev, 'My ne dolzhny militarizirovat' stranu beskonechno.' *Kommersant*, 22. 02. 2019. Available: www.kommersant.ru/doc/3226991? (05. 04. 2019.)

[4] Sasha Baranovskaya, 'Moscow's cyber-defense. How the Russian government plans to protect the country from the coming cyberwar.' *Meduza*, 19. 07. 2019. Available: https://meduza.io/en/feature/2017/07/19/moscow-s-cyber-defense. (05. 05. 2019.); 'U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations.' US Department of Justice, 04. 10. 2018. Available: www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and. (05. 05. 2019.)

military, which was invented and formed by Defence Minister Sergei Shoigu in 2012, for example, the 9th scientific company stationed in Tambov.[5]

The Russian understanding of *the army's role in the information space* is much wider than in the Western model. In the Western thinking, 'cyberspace' is the key notion, which is more appropriate to the military context. The Russian operational art, however, uses the notion of 'information space', which they put in the context of social, political and civilisational threats. This shift helps to justify the Kremlin's domestic and foreign policies. By emphasising the 'informational' nature of the Russian army's activities and not their 'cybernetic' nature, the strategists focus on information, as well as the political agitation and mobilisation it engenders, which is in line with the mission entrusted to the armed forces of neutralising the influence of information on their own personnel and the civilian population. The army's involvement in government propaganda is thus justified via a separate, military module of the propaganda apparatus, of which the Krasnaya Zvezda media holding and its associated traditional and electronic media are part.[6]

Since the Soviet times, another factor that has weighted heavily on Russian strategists' mind is the fact that Russia has always acutely sensed and thus sought to counterbalance its technical and economic inferiority by systematically exploring and integrating *asymmetric strategies* in its operational art. In the Russian threat perception, US influence operations and attacks coming from and through the information space loom large. Most strategists underline that in the Russian IW concept the masterful combination of both the technical and the psychological capabilities are subordinated to the strategic goal to outmaneuver and to try to give an upper hand over, or to deter from, the attack by the adversary, the US. Right after the end of the Cold War, Russia's first official military doctrine in 1993 unmistakably reflects the ongoing civil-military consensus on the nature and requirements of the new RMA. The document states that R&D efforts should be focused above all on the development of the new deep-strike weapons and advanced C4ISR/*electronic warfare (EW)* assets. Nevertheless, lacking the sufficient resources the current strategy of selective investment coupled with careful analysis of U.S. vulnerabilities could enable Russia to compete with and even surpass US forces in specific *operational niches* – such as information/electronic warfare – long before the RMA is generalised throughout the Russian military. The Russian military has argued that EW has become a form of offence against precision weapons and advanced C4ISR systems.[7] EW, as opposed to the Western bias for cyber capabilities, thus has become one of the preeminent components of the information-technical means of warfare.[8]

[5] Sergey Sukhankin, 'Russia Beefs up its Offensive Cyber Capabilities.' Eurasia Daily Monitor, Jamestown Foundation, Washington DC, 30. 05. 2016. Available: https://jamestown.org/program/russia-beefs-offensive-cyber-capabilities/ (06. 04. 2019.); Vladimir Isachenkov, 'V Minoborony RF sozdali voyska informatsionnykh operatsiy / In the Ministry of Defense of the Russian Federation created the troops information operations.' Interfax.ru, 22. 02. 2017. Available: www.interfax.ru/russia/551054. (02. 05. 2018.)

[6] Jolanta Darczewska, 'Russia's Armed Forces on the Information War Front, Strategic documents.' OSW Studies (Center for Eastern Studies), No. 57, Warsaw, June 2016. Available: www.stratcomcoe.org/j-darczewska-russias-armed-forces-information-war-front-strategic-documents (02. 10. 2020.)

[7] Fitzgerald, 'Russian Views.'

[8] Roger N McDermott, *Russia's Electronic Warfare Capabilities to 2025*. International Center for Security, Tallin, 2017. Available: https://icds.ee/wp-content/uploads/2018/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf. (18. 04. 2019.)

Overall, the technological capability development, especially EW, has been in the forefront of the comprehensive Russian military transformation that began in 2008. The IW capability upgrade gained a new momentum in 2012 when Vladimir Putin became the new Commander-in-Chief, the Russian military received a new Minister of Defence, Sergey Shoygu, and a new Chief of General Staff, Valeriy Gerasimov, and also a new Defense Plan in January 2013.[9]

2. The Stage of Maturity

As part of the operational art, Russian military strategists have analysed past and current conflicts in order to discern ways and means of improvement. Russian specialists sought to integrate what they learned from the conflicts they fought throughout the 1990s and 2000s. Through this trial and error method, the Information Warfare conceptualisation and capability development has achieved a more mature stage by 2010. The strategic documents and the expert literature of the subsequent period mirror to what extent IW has been embedded into Russian operational art and also into strategic (domestic and foreign) political thinking. Furthermore, Crimean and Ukrainian conflicts, just like the US mid-term election meddling later on, provided ample evidence of how effectively the IW principle has been aligned with political goals, and thus has been put into operational practice.

In 2008 the former General of the Army Makhmut Gareev, the president of the Academy of Military Science, stated that Russia must confront threats with *asymmetric measures united by a common goal and concept of actions.* For this aim Gareev introduced the concept of *strategic deterrence*.[10] He defined this asymmetric approach as part of a set of interrelated political, diplomatic, information, economic, military, and other measures. A year later, S. G. Chekinov and S. A. Bogdanov discussed the indirect approach. They envisioned that the re-division of territory and markets is now achieved through the indirect approach and the employment of *nonmilitary means.* The indirect approach strategy uses various forms and methods of indirect military and nonmilitary actions and means, to include information, noncontact confrontation, electronic, fire-based, land-sea and aerospace attacks. Nonmilitary means include political, legal, economic standards, spiritual values, general-purpose information, and technological systems used by the state to influence internal and external relations.[11]

The first comprehensive official definition of IW was also published around this time. The *Russian Federation Armed Forces' Information Space Activities Concept* issued by the Ministry of Defence in 2011 stated that:

[9] Giles Keir and Andrew Monaghan, 'Russian Military Transformation. Goal in Sight?' Strategic Studies Institute, Carlisle, 2014. Available: https://ssi.armywarcollege.edu/pdffiles/PUB1196.pdf. (23. 04. 2018.)

[10] M. A. Gareev, Strategicheskoye sderzhivaniye. Problemy i resheniya [Strategic Deterrence. Problems and Solutions]. Krasnaya Zvezda, no. 183, 08. 02. 2008. Available: https://regnum.ru/news/1065985.html. (24. 05. 2018.)

[11] Thomas, *Military Strategy.*

> 'Information War is the *confrontation* [Informatsionnaya voyna] between two or more states in the *information space* with the purpose of inflicting damage to information systems, processes and resources, critical and other structures, *undermining the political, economic and social systems, a massive psychological manipulation of the population to destabilise the state and society, as well as coercion of the state to take decisions for the benefit of the opposing force*.'[12]

For these reasons, this period has been evaluated as a climax of the evolution in Russian operational art, collecting a corpus of ideas under the idea of *New Generation War (NGW)*. On 24th March 2013, addressing the plenary session of the Academy of Military Sciences at the General Staff Academy, Chief of the Russian General Staff (CGS) and Army General Valery Gerasimov delineated current thinking on future warfare. The overarching theme was that Russia's military is becoming more high-tech and continues to develop non-nuclear deterrence capabilities. According the NGW logic the ratio of military and non-military means should be 4:1. *Information conflict,* in particular, opens up '*extensive asymmetric capabilities for the reduction of an enemy's combat potential*.'[13] In NGW, it is impossible to prevail without achieving *informational superiority* over the adversary.[14] The different stages of a conflict are:

'1. *peacetime groups of forces start military action (without war declaration or preparatory deployment);*
2. *highly maneuverable stand-off combat actions conducted by combined-arms forces;*
3. *degradation of the adversary's military-economic potential by swift destruction of military and state critical infrastructure;*
4. *massive employment of Precision-Guided Munitions (PGMs), special operations, unmanned weapon systems, weapons based on new physical principles, and involvement of »military-civilian component« (armed civilians) in combat activities;*
5. *simultaneous strike on enemy forces and other targets in the entire territorial depth;*
6. *simultaneous military action in all physical domains and in the informational space;*
7. *employment of asymmetric and indirect methods;*
8. *managing troops and means in a unified informational sphere*.'[15]

[12] 'Kontseptsiya deyatel'nosti Rossiyskoy Federatsii v oblasti informatsionnogo prostranstva / Russian Federation Armed Forces' Information Space Activities Concept,' The Russian Ministry of Defence, 2011. Available: https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle. (24. 05. 2018.)

[13] Valerij Gerasimov, 'Tsennost' Nauki v Predvidinii / The Value of Science is in Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying Out Combat Operations.' *Voyenno-Promyshlennyy Kuryer Online* (Military-Industrial Courier Online), Febr. 2013. Available: https://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20160228_art008.pdf. (11. 05. 2019.)

[14] Yuriy Gorbachev, 'Kibervoina uzhe idet' [Cyberwar is already underway]. *Nezavisimoye Voyennoye Obozreniye,* no. 13, 12. 04. 2013. Available: http://nvo.ng.ru/armament/2013-04-12/1_cyberwar.html. (01. 04. 2019.)

[15] Gerasimov, 'Tsennost.'

Later on, in 2015 the *National Security Strategy* consolidated the *strategic deterrence* idea: *'Interrelated political, military, military-technical, diplomatic, economic, informational, and other measures are being developed and implemented in order to ensure strategic deterrence and the prevention of armed conflicts. These measures are intended to prevent the use of armed force against Russia, and to protect its sovereignty and territorial integrity*.'[16] This interrelated mix of tactics has been labelled as *cross-domain* deterrence by Western analysts, referring to the integration of all five military domains, but also the regional and global dimensions, as well as to the kinetic and non-kinetic, and the soft and hard measures. What transpires is that IW, and cyber attacks as a part of it, form an important part of both the cross-domain deterrence concept (as *informational deterrence*) and the NGW. IW is to be carried out in all domains, and both in peacetime and throughout the whole conflict cycle.

Adamsky also emphasises the overarching role played by IW in the Russian operational art. Unlike in the Western military thinking, 'informational struggle' *is not a codified concept of operations, but rather an amalgam or a corpus of ideas* that have an overarching role in modern warfare and political strategy. According to Adamsky it works as a 'systemic integrator': 'it knits together all operational efforts, serving as a kind of DNA that choreographs coercion activities across non-military and military (nuclear and non-nuclear) domains.'[17] He gives a good summary of the predominant characteristics:

> 'First, Russia's approach to informational struggle is *holistic* (kompleksnyi podhod), that is, it merges digital-technological and cognitive-psychological attacks. While digital sabotage aims to disorganize, disrupt, and destroy a state's managerial capacity, psychological subversion aims to deceive the victim, discredit the leadership, and disorient and demoralize the population and the armed forces. Second, it is *unified* (edinstvo usilii), in that it synchronizes informational struggle warfare with kinetic and non-kinetic military means and with effects from other sources of power; and it is unified in terms of co-opting and coordinating a spectrum of government and non-government actors – military, paramilitary, and non-military. Finally, the informational campaign is an *uninterrupted* (bezpriryvnost') strategic effort. It is waged during 'peacetime' and wartime, simultaneously in domestic, the adversary's, and international media domains and in all spheres of new media. The on-line 'troll' armies wage battles on several fronts: informational, psychological, and, probably, digital-technological. This enables the creation of managed stability-instability across all theaters of operations.'[18]

3. Conclusion

So far, two main phases can be distinguished after the end of the Cold War. First, the period of the 1990s up to the end of the 2010s, which has been about pathfinding

[16] National Security Strategy (Russia, 2015), art. 36.
[17] Adamsky, 'Cross-Domain Coercion.'
[18] Ibid.

and coming to terms with the new geopolitical, technological, economic and strategic realities after the collapse of the Soviet Union and a series of conflicts in the so-called Russian 'near abroad'. The second period has applied the lessons learnt, and also benefited greatly from the positive effects of the surge in the oil prices that boosted the long pending military transformation. Putin has also transformed the institutional ecosystem to achieve a higher level of centralisation. The theoretical, conceptual and strategic landscape as well as the actual operations have achieved a high level of maturity.

Moreover, taking note of the ever-growing military cyber capabilities of the Western nations, the status of cyber capabilities is undergoing reconsideration and enhancement in Russian strategic thinking too. As a result, Russia is better capable of reaping the benefits and making strategic use of the information space, and can be expected to use cyber strikes increasingly and in a more overt manner, rather than only as a covert intelligence tool.

In contrast to this intensely integrative, holistic and incessant approach, in the US the strategic theory and practice is still somewhat contradicting. Cyber capabilities are only partly developed and integrated into Information Operations, and at the same time, they are also built parallelly along a separate path.[19] Along cyber security and information security, Western nations should take into account to a much larger extent the cognitive layer of cyberspace and the manifold threats initiated by Russia.

Bibliography

Adamsky, Dmitry: 'Cross-Domain Coercion. The Current Russian Art of Strategy.' The Institut Français des Relations Internationales, Paris, 2015. Available: www.ifri.org/sites/default/files/atoms/files/pp54adamsky.pdf. (24. 03. 2019.)

Baranovskaya, Sasha: 'Moscow's cyber-defense. How the Russian government plans to protect the country from the coming cyberwar.' *Meduza*, 19. 07. 2019. Available: https://meduza.io/en/feature/2017/07/19/moscow-s-cyber-defense. (05. 05. 2019.)

Darczewska, Jolanta: 'Russia's Armed Forces on the Information War Front, Strategic documents.' OSW Studies (Center for Eastern Studies), No. 57, Warsaw, June 2016. Available: www.stratcomcoe.org/j-darczewska-russias-armed-forces-in-formation-war-front-strategic-documents (02. 10. 2020.)

Fitzgerald, M. C.: 'Russian Views on IW, EW, and Command and Control: Implications for the 21st Century.' Hudson Insitute, Washington DC, 1999. Available: www.dodccrp.org/events/1999_CCRTS/pdf_files/track_5/089fitzg.pdf. (02. 05. 2019.)

Gareev, M. A.: 'Strategicheskoye sderzhivaniye. Problemy i resheniya' [Strategic Deterrence. Problems and Solutions]. *Krasnaya Zvezda*, no. 183, 08. 02. 2008. Available: https://regnum.ru/news/1065985.html (24. 05. 2018.)

Gerasimov, Valerij: 'Tsennost' Nauki v Predvidinii / The Value of Science is in Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying Out Combat Operations.' *Voyenno-Promyshlennyy Kuryer Online* (Military-Industrial Courier

[19] E.g.: Cyberspace Operations, JP 3-12, 2018.

Online), Febr. 2013. Available: https://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20160228_art008.pdf. (11. 05. 2019.)
Gorbachev, Yuriy: 'Kibervoina uzhe idet' [Cyberwar is already underway]. *Nezavisimoye Voyennoye Obozreniye,* no. 13, 12. 04. 2013. Available: http://nvo.ng.ru/armament/2013-04-12/1_cyberwar.html. (01. 04. 2019.)
Isachenkov, Vladimir: 'V Minoborony RF sozdali voyska informatsionnykh operatsiy / In the Ministry of Defense of the Russian Federation created the troops information operations.' Interfax.ru, 22. 02. 2017. Available: www.interfax.ru/russia/551054. (02. 05. 2018.)
Keir, Giles – Monaghan, Andrew: 'Russian Military Transformation. Goal in Sight?' Strategic Studies Institute, Carlisle, 2014 Available: https://ssi.armywarcollege.edu/pdffiles/PUB1196.pdf. (23. 04. 2018.)
Khamrayev, Viktor: 'My ne dolzhny militarizirovat' stranu beskonechno.' *Kommersant*, 22. 02. 2019. Available: www.kommersant.ru/doc/3226991? (05. 04. 2019.)
'Kontseptsiya deyatel'nosti Rossiyskoy Federatsii v oblasti informatsionnogo prostranstva / Russian Federation Armed Forces' Information Space Activities Concept.' The Russian Ministry of Defence, 2011. Available: https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle. (24. 05. 2018.)
McDermott, Roger N.: *Russia's Electronic Warfare Capabilities to 2025.* International Center for Security, Tallin, 2017. Available: https://icds.ee/wp-content/uploads/2018/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf. (18. 04. 2019.)
Sukhankin, Sergey: 'Russia Beefs up its Offensive Cyber Capabilities.' Eurasia Daily Monitor, Jamestown Foundation, Washington DC, 30. 05. 2016. Available: https://jamestown.org/program/russia-beefs-offensive-cyber-capabilities/. (06. 04. 2019.)
Thomas, T.: *Russia. Military Strategy.* Foreign Military Studies Office. Fort Leavenworth, 2015. Available: https://info.publicintelligence.net/FMSO-RussianMilitaryStrategy.pdf. (02. 04. 2019.)
'U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations.' US Department of Justice, 04. 10. 2018. Available: www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and. (05. 05. 2019.)