HADTUDOMÁNYI SZEMLE
13. évfolyam (2020) 1. szám 27–35. • DOI: 10.32563/hsz.2020.1.2

Dóra Dévai[1]

An Overview of the Development of the Russian Information Warfare Concept Part 1

Az orosz információs hadviselés koncepció fejlődésének áttekintése 1. rész

Abstract

After the infamous cyberattacks against Estonia in 2007 and the Ukrainian conflict in 2014–2015, the Russian military theory, and in particular, Information Warfare (IW) doctrines, have come into the centre 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 first part of this article strives to give an account of the unique nature of the Russian way of IW.

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

[1] Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar – National 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

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 e területek mélyreható vizsgálata szükséges. Az IH rendkívül sajátos szerepet játszik az orosz politikai és katonai elméletben és gyakorlatban, és jelenlegi állapotát a ciklikus megújuláson átesett fejlesztések csúcspontjának tekinthetjük. Jelen tanulmány első része arra irányul, hogy betekintést nyújtson ezen fejlődési folyamat kezdeti szakaszába, amely az orosz IH kialakulásának – és azon belül a kiberműveletek értelmezésének – egyedülálló jellegét adja.

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

Introduction

In the period after the cyberattack against Estonia in 2007 as well as after the Ukrainian conflict in 2014–2015, Russian military theory and *Information Warfare (IW)* doctrines, in particular, have come into the limelight. To gain an in-depth understanding of the Russian military and security policy thinking, analysts have turned to a wide variety of strategic sources. Going beyond the analysis of each primary strategic or doctrinal source separately, strategic theory or *operational art* examines a corpus of sources and contextual factors to identify how the nature and character of warfare[2] is evolving in light of, for example, pervasive technological development, and what kind of strategic, organisational and capability adjustments this requires on the national level. Each nation has its distinctive interpretation. In terms of Russia, Dmitry Adamsky, an Israeli strategic scientist of Russian origin explains this comprehensive approach as *operational art:* "In Russian military science, the term *operational art* is a sphere of military affairs interconnecting strategy and tactics, and it also means the theory and practice of achieving strategic goals through design, organization, and conduct of campaigns, operations, and battles. The theory of operational art explores change and continuity in the current character of war and highlights the most optimal concept of operations, organizational structures, and weaponry for a given historical period."[3]

Similarly, this article also aims to provide a longitudinal overview of the IW related trends and developments in Russian operational art with a focus on the main distinctive elements that determine the peculiar Russian way. As for Western IW thinking, the U.S. has a foundational role, this will be used as a basis of comparison. The analysis is based on primary sources that are strategic and doctrinal documents which abound from 2000 onwards, as the table below shows. The period before 2000, however, lacks publicly available primary sources, namely strategies or doctrines. Therefore,

[2] Baylis, John – Wirtz, James J. – Gray, Colin S.: Strategy in the Contemporary World, Oxford University Press, Oxford, 2018.

[3] Adamsky, Dmitry: Cross-Domain Coercion. The Current Russian Art of Strategy, The Institut Français des Relations Internationales, Paris, 2015. www.ifri.org/sites/default/files/atoms/files/pp54adamsky.pdf (Downloaded: 24.03.2019.)

secondary military literature,[4] i.e. the views of individual military and civilian experts including scholarly analyses will be scrutinised. In the selection of the sources, the main aim was to illustrate certain trends, rather than providing a full spectrum of military sources.

Table 1. *Russian national security and information security documents after 2000.*

2000	National Security Concept of Russia of the Russian Federation
2000	**The (first) Information Security Doctrine of the Russian Federation**
2008	National Security Strategy 2009–2020
2010	Military Doctrine
2011	**Draft Convention on International Information Security**
2011	**Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space**
2013	Concept of the Foreign Policy of the Russian Federation
2013	**Basic Principles for State Policy of the Russian Federation in the Field of International Information Security**
2014	**Concept of Russia's Cyber Security Strategy**
2014	Military Doctrine of the Russian Federation
2015	National Security Strategy of the Russian Federation
2016	Foreign Policy Concept of the Russian Federation
2016	**Information Security Doctrine of the Russian Federation**

Source: Complied by the author

The Intellectual Origins and the Evolution of the Current Russian IW Concept

Even though the conceptualisation and the terminology according to the IW have been undergoing a continuous shift, just like in the U.S., the current version of the IW concept is much more the result of an evolutionary than a revolutionary process. Among others, Dmitry Adamsky points out that the stream of current Russian thinking in the so-called New Generation Warfare is to a large extent the direct outgrowth of the Military Technical Revolution (MTR)/Revolution in Military Affairs (RMA) theorisation in the 1980s. That process was triggered by the rapid evolution and spread of information technology in the 1970s. In the Cold War years, this evolution influenced both Soviet and American leaders, thinkers and commanders. The Soviets conceived

[4] The elite military journal known in Russia as *Voennaia Mysl'* is an organ of the Russian Defence Ministry, the journal's contributors are top military personnel and leading lecturers from Russian military universities and colleges. The English translation of this journal is published under the title *Military Thought*.

radio-electronic warfare as a way to interfere with an adversary's communications channels and nodes, and ultimately his command and control on the battlefield.[5]

These ideas swiftly found validation in the 1991 Persian Gulf War, after which the Pentagon managed the creation of DoD-wide policy to establish responsibilities for the new field of information warfare, first within the Command and Control Warfare framework. Information War was first used by the U.S. Department of Defense in a classified IW directive signed in 1992.[6] Later on, Chairman of the Joint Chiefs Colin Powell implemented the memorandum, but he made changes to it. In the Chairman's memorandum, C2W would be "the military strategy that implements Information Warfare on the battlefield and integrates physical destruction". Moreover, it also added psychological operations and military deception to the list of "principal military actions" supporting command and control warfare.[7]

With time, information war has been softened into *Information Operations* (IO) in *Joint Doctrine for Information Operations* (Joint Publication 3-13), published on October 1998. JP 3-13 sought to avoid a simple re-labelling of terms, and thus depicted IO as a broadening of IW, which now became a wartime tool: "IO conducted *during time of crisis or conflict (including war)* to achieve or promote specific objectives *over a specific adversary or adversaries*".[8] JP 3-13 designated six offensive and eight defensive assigned and supporting capabilities and activities. "These assigned and supporting capabilities and activities include, but are not limited to, *operations security (OPSEC), military deception, psychological operations, electronic warfare (EW), physical attack/destruction, and special information operations (SIO), and may include computer network attack*."[9] The 1998 JP also emphasised the necessity of obtaining and maintaining *information superiority* during IO. Information Superiority is defined as: "The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."[10] In JP 3-13 the set of Information Operations capabilities could include *computer network operations (CNO)*.[11]

In 2003, the U.S. Army released its new and updated version of FM 3-13. It defined information operations as: "The employment of the *core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities,* to affect or defend information and information systems, and to influence decision-making."[12]

---

5 Warner, Michael: Notes on Military Doctrine for Cyberspace Operations in the United States, 1992–2014, *The Cyber Defense Review,* U.S. Army, USA, August 27, 2015. https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1136012/notes-on-military-doctrine-for-cyberspace-operations-in-the-united-states-1992/ (Downloaded: 15.05.2019.)

6 Atwood, Donald J.: Deputy Secretary of Defense, "Information Warfare", Department of Defense Directive, 1992.

7 Warner (2015): *op. cit.*

8 Ibid.

9 Joint Chiefs of Staff: Joint Doctrine for Information Operations, Ministry of Defense, Washington, D.C., 1998. www.c4i.org/jp3_13.pdf (Downloaded: 25.04.2019.)

10 Ibid.

11 In JP 3-13, CNO comprises Computer Network Defense, Computer Network Exploitation and Computer Network Attack, which is defined as operations „to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."

12 Headquarters of the U.S. Army: FM 3-13, Information Operations: Doctrine, Tactics, Techniques, and Procedures, Washington, D.C., 2003. https://fas.org/irp/doddir/army/fm3-13-2003.pdf (Downloaded: 08.03.2019.)

By 2006, the term *cyber operations* were given prime attention and started to gain separate doctrinal documents in the U.S. The National Military Strategy dated 2004, but published in March 2005, recognised cyberspace as a *domain* of conflict. The 2006 edition of the Joint Publication 3-13 Information Operations elevated CNO into the category of core IO capabilities, and in December a distinct, classified Cyber Operations doctrine have been signed. *Cyberspace domain* was defined as: "A domain characterized by the use of electronics and the electromagnetic spectrum to store, modify and exchange data via networked systems and associated physical infrastructures."[13]

In the Soviet Union and Russia, IW and cyber concepts have taken a different developmental curve heavily influenced by longstanding traditions and socio-political conditions. Adamsky pointed out that the Soviet definition given to the science of *cybernetics* ("kibernetika") has also left its mark on the Russian approach. "Seen as a discipline in the intersection of exact, social, and natural sciences, Soviet scientific society defined cybernetics as a science exploring the nature of creation, storage, transformation, utilization, and management of information and knowledge, in complex systems, machines, contiguous living organisms, or societies. In a nutshell, it is a discipline dealing with decision-making management of the highest order."[14]

In Russia, the 1990s have been characterised by the baseline conceptualisation of IW. This is well reflected by the plurality of the terms related to IW. Still, the major defining elements of the Russian approach can be identified. One of the most often quoted experts of Russian strategy, Timothy Thomas gives a good summary of the notion: "In Russian, the *war* part of the term *information war* is translated as either 'informatsionniya voyna, informatsionniya borba', or 'informatsionnoye protivoborstbo'. According to one source, the term 'informatsionniya voyna' is usually used in a wider sense by journalists rather than military professionals. The latter prefer the term 'informatsionnoye protivoborstbo', which also means information warfare [or informational conflict or struggle] and is already in use by some military sources, to include the General Staff Academy. 'Informatsionniya borba' is also used by military professionals, but how it is interpreted from the other two is unknown. It is still too difficult to say specifically which term will find a preference. This is another reason to start discussions with the Russians, to find a common language not only for this term but for many others."[15]

Remaining at Russian terminology and capability categorisation, Russian military experts have divided IW capabilities into two major subdivisions from an early stage. As Timothy Thomas explains: "For example, threats in both Russia's 2000 military doctrine, and in a year 2000 issue of the Russian defense complex journal *Information Security,* were listed as *information-technical* and *information-psychological* aspects of IO. In the latter journal, the information-technical confrontation was divided into *technical intelligence devices, means and measures for protecting the information, super high-frequency weapons, ultrasonic weapons, radio-electronic countermeasures, electromagnetic impulse*

[13] Joint Chiefs of Staff: Cyber Operations Doctrine, Department of Defense, Washington, D.C., 2006.
[14] Adamsky (2015): *op. cit.*
[15] Thomas, Timothy L.: Russian Views on Information-based Warfare, *Airpower Journal,* (1996 Special edition).

weapons, and special software and hardware. Information-psychological aspects included mass media, non-lethal weapons, psychotronic tools, and special pharmaceuticals."[16]

Other examples show the indefinite nature of the components. Captain First Rank (Reserve) R. Bikkenin in 2003 gave a somewhat different grouping: under the information-technical aspects he listed the main targets of attack and defence as electronic assets, especially communications and telecommunications systems and the Internet. Other aspects of the information-technical component of information conflict included disinformation, maskirovka, intelligence, the science of cryptology and steganography. Bikkenin underlined that several new cryptographic algorithms have become widespread, particularly the RSA-algorithm and the El Gamal algorithm.[17]

Adamsky elaborates on the explanation of the roots of these two divisions: "The first source of influence is a Soviet MTR/RMA thesis from the 1980s that envisioned military organizations of the post-industrial era as reconnaissance-strike complexes. Accordingly, one can defeat the adversary not by kinetic destruction, but by disrupting decision-making processes within its system of systems, through electronic warfare (EW) strike on Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) systems. This became a source for the 'digital-technological' impetus of the Russian approach. Second, since informational influence is aimed primarily at an adversary's decision-making, the Russian approach is informed by the tradition of 'active measures' and *maskirovka* – one of the main virtues of the Soviet-Russian intelligence and military art – a repertoire of denial, deception, disinformation, propaganda, camouflage, and concealment. It aims to manipulate the adversary's picture of reality and to produce favourable operational conditions for promoting one's strategic goals. This became a basis for the 'cognitive-psychological' motive."[18]

The information-psychological elements have always been central in the Russian operational art, and in military and intelligence practice, and recently they have become even more emphatic. *Military stratagem* (voennaia khitrost') has been a major component of military art since the Tsarist times and it has complemented, multiplied or substituted the use of force to achieve strategic results in military operations.[19] *Reflexive control* is often mentioned in connection with Russian subterfuge tactics. According to Timothy Thomas, reflexive control is a subject that has been studied in the Soviet Union and Russia for more than 40 years. The strategic centre of gravity is the perception, the consciousness and together with all these, the decision-making of the target. The main aim is to convey to the target specially prepared information to tilt or nudge him to voluntarily make the predetermined decision desired by the initiator of the action.[20] The intent can be to dissuade or to deter the adversary from its intention to attack. Reflexive control can comprise a mix of tactics including

[16] Thomas, Timothy L.: Comparing US, Russian, and Chinese Information Operations Concepts, Foreign Military Studies Office, Fort Leavenworth, 2004a. www.dodccrp.org/events/2004_CCRTS/CD/papers/064.pdf (Downloaded: 05.05.2019.)

[17] Ibid.

[18] Adamsky (2015): *op. cit.*

[19] Ibid.

[20] Thomas, Timothy L.: Russia's Reflexive Control Theory and the Military, *The Journal of Slavic Military Studies,* 17 (2004b/2) 237–256.

maskirovka (disinformation, deception, concealment), lure, threat, IW (including cyber-attacks) among others.

Controlling the target audience by manipulating its perception is applied vis-à-vis the domestic population, as well. By contrast, in the U.S., Title 10 U.S. Code 2241 prohibits the DoD from domestic publicity or propaganda. In case of Russia, this is commonly attributed to the continuation of the ideology and methodology of mass propaganda originating in the early twentieth century Bolshevik era and continuing through the Cold War political war and active measures. In modern times, for example, back in 1996 Timothy Thomas cites an interview with a Ministry of Defence civilian analyst who referred to information war or "Informatsionnoya Voyna" or information noting that: "Both a broad and narrow sense are inherent in the existing concept of information warfare. In the broad sense, information warfare is one of the varieties of the 'cold war' – countermeasures between two states implemented mainly in peacetime with respect not only and not so much to the armed forces as much as to the civilian population and the people's public/social awareness, to state administrative systems, production control systems, scientific control, cultural control, and so forth. It is namely in this sense that the information security of the individual, society, and state is usually understood... In the narrow sense, information warfare is one of the varieties of military activity/operations/actions (or the immediate preparation for them)."[21] Another example from a decade later states that: "The main effort is concentrated on achieving political or diplomatic ends, and influencing the leadership and public opinion of foreign states, as well as international and regional organizations."[22]

Consequently, in Russian operational art, the "information space" ("informatsionnoye prostranstvo") has been treated as a unified strategic environment for a long time. Russian Defence Ministry's document entitled *The Russian Federation Armed Forces' Information Space Activities Concept* (2011) defines "information space" as: "The sphere of activity related to shaping, creating, transmitting, using and storing information, which influences individual and social awareness, as well as the information infrastructure and information in the strict sense."[23] Russian official references to "cyberspace" ("kiberprostranstvo") had long occurred only in translations of foreign texts or references to U.S. cyber strikes. Unlike in the Western concept, where it is treated as a separate domain, the Russian notion of "kiberprostranstvo" is merely a subset of information space and it is inseparable from it. The Western notion of cyberspace, therefore, cannot be used interchangeably in Russian operational art.

However, due to the increasingly important role of cyber issues, the understanding of cyber operations has shifted towards the Western view in the Russian strategic dialogue over the last five–ten years. As a result, more and more Russian strategists believe that Russia must develop a strategy for IW and cyberwar based on both

[21] Thomas (1996): *op. cit.*

[22] Donskov, Col. Yu. E.: The Place and Role of Special Information Operations in Resolving Military Conflicts, *Military Thought,* (2005/6) 30–34. http://militaryarticle.ru/voennaya-mysl/2005-vm/9555-mesto-i-rol-specialnyh-informacionnyh-operacij-pri (Downloaded: 14.03.2019.)

[23] The Russian Ministry of Defence: Kontseptsiya deyatel'nosti Rossiyskoy Federatsii v oblasti informatsionnogo prostranstva [Russian Federation Armed Forces' Information Space Activities Concept], Moscow, 2011. https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle (Downloaded: 24.05.2018.)

Russian and other foreign countries' opinions on the matter. This process appears to be underway, as military journals are full of articles on the development of command and control issues that utilise both Russian and Western concepts.[24]

Conclusion

As a conclusion, it can be inferred that IW development in the Russian operational art might have been inspired by U.S. technological and doctrinal developments, nevertheless, it developed along a different and unique path, and as a result, gained a distinctive character. In the Western military theory and practice, the notion of IW is by far not as central as in the Russian version. In the West, even the terminology has morphed into *Information Operations* implying a more restricted use. In Russian thinking, after the role of kinetic measures has been reduced considerably, IW has turned into the major tool to achieve strategic military and political goals. In that sense, the informational strike is about breaking the internal coherence of the enemy system and not about its integral annihilation.

To relate the Russian capabilities to the Western notion of cyberspace, Russia has focused predominantly on the cognitive or social layer, while the U.S. has prioritised the physical and logical layers.

This peculiar development to a large extent derives from the survival of the underlying Russian strategic traditions adapted to the new realities of the 21st century. In the Russian military and political strategy, the technological and psychological means of IW have developed uninterruptedly and therefore in a much more integrated way. Also, the domestic political and regime security have generated a high degree of alert to threats coming from the information space. Interestingly, the economic and technological asymmetry of Russia did not allow for a developmental path based on technical foundations.

Bibliography

Adamsky, Dmitry: Cross-Domain Coercion. The Current Russian Art of Strategy, The Institut Français des Relations Internationales, Paris, 2015. www.ifri.org/sites/default/files/atoms/files/pp54adamsky.pdf (Downloaded: 24.03.2019.)

Atwood, Donald J.: Deputy Secretary of Defense, "Information Warfare", Department of Defense Directive, 1992.

Baylis, John – Wirtz, James J. – Gray, Colin S.: Strategy in the Contemporary World, Oxford University Press, Oxford, 2018. DOI: https://doi.org/10.1093/hepl/9780198708919.001.0001

Donskov, Col. Yu. E.: The Place and Role of Special Information Operations in Resolving Military Conflicts, *Military Thought,* (2005/6) 30–34. http://militaryarticle.ru/

[24] Thomas, Timothy L.: Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts? *The Journal of Slavic Military Studies,* 27 (2014/1) 101–130.

voennaya-mysl/2005-vm/9555-mesto-i-rol-specialnyh-informacionnyh-operacij-pri (Downloaded: 14.03.2019.)
Headquarters of the U.S. Army: FM 3-13, Information Operations: Doctrine, Tactics, Techniques, and Procedures, Washington, D.C., 2003. https://fas.org/irp/doddir/army/fm3-13-2003.pdf (Downloaded: 08.03.2019.)
Joint Chiefs of Staff: Joint Doctrine for Information Operations, Department of Defense, Washington, D.C., 1998. www.c4i.org/jp3_13.pdf (Downloaded: 25.04.2019.)
Joint Chiefs of Staff: Cyber Operations Doctrine, Department of Defense, Washington, D.C., 2006.
The Russian Ministry of Defence: Kontseptsiya deyatel'nosti Rossiyskoy Federatsii v oblasti informatsionnogo prostranstva [Russian Federation Armed Forces' Information Space Activities Concept], Moscow, 2011. https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle (Downloaded: 24.05.2018.)
Thomas, Timothy L.: Russian Views on Information-based Warfare, *Airpower Journal,* (1996 Special edition) 25–35.
Thomas, Timothy L.: Comparing US, Russian, and Chinese Information Operations Concepts, Foreign Military Studies Office, Fort Leavenworth, 2004a. www.dodccrp.org/events/2004_CCRTS/CD/papers/064.pdf (Downloaded: 05.05.2019.)
Thomas, Timothy L.: Russia's Reflexive Control Theory and the Military, *The Journal of Slavic Military Studies,* 17 (2004b/2) 237–256. DOI: https://doi.org/10.1080/13518040490450529
Thomas, Timothy L.: Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts? The Journal of Slavic Military Studies, 27 (2014/1) 101–130. DOI: http://dx.doi.org/10.1080/13518046.2014.874845
Warner, Michael: Notes on Military Doctrine for Cyberspace Operations in the United States, 1992–2014, *The Cyber Defense Review,* U.S. Army, USA, August 27, 2015. https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1136012/notes-on-military-doctrine-for-cyberspace-operations-in-the-united-states-1992/ (Downloaded: 15.05.2019.)