RECORD VERSION

STATEMENT BY

MR. TIMOTHY L. THOMAS
SENIOR ANALYST, FOREIGN MILITARY STUDIES OFFICE
FORT LEAVENWORTH, KS

BEFORE THE

HOUSE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON EMERGING THREATS and CAPABILITIES

FIRST SESSION, 115TH CONGRESS

ON RUSSIA'S INFORMATION WAR CONCEPTS

MARCH 15, 2017

NOT FOR PUBLICATION UNTIL RELEASED BY THE

COMMITTEE ON ARMED SERVICES

STATEMENT BY MR. TIMOTHY L. THOMAS

SENIOR ANALYST, FOREIGN MILITARY STUDIES OFFICE
FORT LEAVENWORTH, KS

RUSSIA'S VIEWS ON MODERN WARFARE AND USE OF INFORMATION OPERATIONS: THE INTEGRATION OF ROLES

Views on Modern Warfare

During the past three or four years Western analysts have tried to decipher Russian military actions and find a term to describe them. Two concepts in particular have dominated these discussions. The first is the issue of hybrid operations. Western analysts have not only labeled Russian actions as hybrid but also state that this is the wording Russia's military uses to describe their operations.[1] However, Russia states that it is the West who is using hybrid operations against Russia. Second, after 2013 the West added another descriptor to their assessment of Russian military actions, labeling Russia's operations to be examples of new-generation wars (NGW). As opposed to the hybrid label, for which there was no hard evidence, the NGW label is based on wording used by Russian military authors to describe future methods of conducting warfare. In 2013 Russian military officers on several occasions referred to NGW, with two authors in particular using the term as the title of their joint article. However, ever since 2013, the Russian military has gone silent on the topic of NGW and for the past two years the Russian military has been using the term new-type wars (NTW).

Hybrid Thought

In 2014 and 2015 many Westerners increasingly referred to Russian actions in Ukraine as part of a hybrid war that included the use of hard and soft tactics to achieve the goals of Russian President Vladimir Putin and the military. However, Russia's military makes the opposite assertion, that the West is using hybrid tactics against Russia. For example, with regard to hybrid war, a *Military Thought* article in 2015 by two Russian authors stated the following:

> 'Hybrid warfare (gibridnaya voyna),' then, is not exactly the right term and is slightly at odds with the glossary used in this country's military science. Essentially, these actions can be regarded as a form of confrontation between countries or, in a narrow sense, as a form in which forces and capabilities are used to assure national security.[2]

---

[1] See, for example, Dovydas Pancerovas, "Russia's Sixth Column in Lithuania is a Sign Russia is Already Conducting Hybrid War in Our Country, Too," *15min.lt,* 23 September 2014.

[2] V. B. Andrianov and V. V. Loyko, "Questions Regarding the Use of the Armed Forces of the Russian Federation in Crisis Situations in Peacetime," *Voennaya Mysl'* (*Military Thought),* No. 1 2015, p. 68.

If you template your own thought process, such as hybrid thought, onto another nations, you might totally miss their key assessment and decision-making criteria, follow a wrong path, or make unforced errors. Thinking your opponent is using your thought process is mirror-imaging.

New-Generation War

In 2013 several articles appeared that mentioned the NGW concept. A full explanation of the concept was first provided in a 2013 article titled, "The Nature and Content of a New-Generation War." The authors, S. A. Chekinov and S. G. Bogdanov, who had earlier discussed indirect and asymmetric operations in detail, described the "way" in which a future war might be fought.[3] Initially Chekinov and Bogdanov described NGW as based on nonmilitary options, mobile joint forces, and new information technologies. They offered seven points for consideration.

First, the aggressive side would use nonmilitary actions as it plans to attack its victim in a NGW.[4] **Second**, decisive battles will rage in the information environment, where the attacker manipulates the "intelligent machines" at a distance. A quantum computer may turn into a tool of destruction in this sense, as new-generation "blitz" wars will be created, operating in the nanosecond range. **Third**, the aggressor may use nonlethal, new-generation, genetically engineered biological weapons that affect the human psyche and moods, which intensify propaganda effects and thereby help to drag the target country into chaos and disobedience among the population.[5] (Russian authors appear to fear this happening inside their country. They write often on the fear of so-called "color revolutions" occurring.)

Fourth, the start of the military phase will be preceded by large-scale reconnaissance and subversive missions conducted under the guise of information operations. These operations will be used to target important objectives vital to the country's sustainability.[6] **Fifth**, the attack will probably begin with an aerospace operation lasting several days. The goal will be to damage an opponent's key military and industrial capabilities, communication hubs, and military control centers.[7] **Sixth**, the defender must anticipate an attack by military robots in conjunction with the aerospace attack. This implies the extended use of UAVs first of all, as well as robot-controlled systems capable of engaging in combat activities independently.[8] **Seventh,** the authors relate that the opening period of a NGW will be pivotal, breaking it down into several phases, to include targeted information operations, electronic warfare operations, aerospace operations, and the use of precision weaponry, long-range artillery, and weapons based on new physical

[3] S. G. Chekinov and S. A. Bogdanov, "The Nature and Content of a New–Generation War," *Voennaya Mysl'* (*Military Thought)*, No. 10 2013, pp. 13-25.
[4] Ibid., p. 19.
[5] Ibid., 21.
[6] Ibid.
[7] Ibid.
[8] Ibid., 22.

principles. In the closing period of war attackers will roll over any remaining points of resistance and destroy surviving enemy units with special operations.[9]

The authors concluded by stating that "a country preaching a defensive doctrine may get the short end of the deal in the face of a surprise attack by an aggressor."[10] Information superiority and anticipatory operations will be the main ingredients for success in NGWs.[11] For the past 1500 days, however, the term NGW has not appeared in Russia's military press to the best of my knowledge.

New-Type Warfare

In early 2015, in the *Bulletin of the Academy of Military Science* of Russia, General-Lieutenant A. V. Kartapalov, then the Chief of the Main Operations Directorate of the General Staff of Russia (in late 2015 he was named as the head of the Western Military District), wrote a lengthy article on the recent lessons of military conflicts and what they had taught Russia. The article examines changes in the nature of armed struggle and what is described as "new warfare" or "war of a new type."[12]

Kartapolov noted that increasingly the U.S. is using hybrid operations, which include military and non-military measures. These measures are accompanied by dynamic information-psychological effects against the population and leadership of victim states; by the use of armed internal opposition detachments; and by the use of special operations forces [author: which mimic almost perfectly Russian actions in Ukraine]. Russia calls such actions "indirect." They differ from "direct" operations, since the latter must be especially dynamic and not passive in any form according to Kartapalov.[13]

The potential capabilities of the U.S. military were especially underscored by Kartapalov. He stated that America's basing systems abroad, its global missile defense architecture and instantaneous global strike concept (which presupposes strategic and non-nuclear precision weapons), and its precision electronic information strikes and technical development of a reconnaissance-strike system have all been created or improved. These actions in Kartapalov's opinion can undermine global stability, disrupt the correlation of forces in the nuclear missile sphere, and create a real threat in the mid-term to the security of the Russian Federation.[14]

To balance the technological superiority of countries, such as the U.S., nonstandard forms and methods are being developed. Russia's new-type warfare includes "asymmetric" methods for confronting an enemy. Measures include the use of Special Forces operations, foreign agents, various forms of information effects, and other

[9] Ibid., 23.
[10] Ibid., p. 23.
[11] Ibid.
[12] A. V. Kartapalov, "Lessons of Military Conflicts and Prospects for the Development of Means and Methods of Conducting Them, Direct and Indirect Actions in Contemporary International Conflicts," *Vestnik Akademii Voennykh Nauk (Bulletin of the Academy of Military Science)*, No. 2 2015, pp. 26-36.
[13] Ibid., p. 29.
[14] Ibid., p. 35.

nonmilitary forms of effects. For each conflict a different set of asymmetric operations will be created. Such actions must be timely and coordinated with respect to targets, location, and time in regard to various departments of government organizations.[15] Kartapalov notes that asymmetric operations "are inherent to a conflict situation in which by means of actions of an economic, diplomatic, informational, and indirect military nature a weaker enemy uses an asymmetric strategy (tactics) to conduct an armed struggle in accordance with his available limited resources to level the stronger side's military-technological superiority."[16]

As a result, indirect and asymmetric actions must be included in the appropriate regulations and provisions, and they must be introduced into the operational training of forces in military schools and institutes.[17] Kartapalov noted that asymmetric actions are conducted with the aim of eliminating (neutralizing) advantages the enemy has and delivering against him (subjecting him to) damage using minimal expenditures, to include: covertness of preparation for the conduct of operations; persuasion of the weak side to use prohibited means to conduct military operations; concentration of efforts against the enemy's most vulnerable locations (targets); searching for and expose the enemy's weak points; imposing on the enemy one's own variant (one's own will) for the course of the conflict; and expending low resources with respect to enemy actions. The goal is to achieve superiority or parity with results.[18] The diagram below is the only template Russia's military has offered on distinct phases of a modern war, termed a new-type war, to which Russia subscribes, according to Kartapolov:

[15] Ibid., p. 36.
[16] Ibid., p. 35.
[17] Ibid., p. 36.
[18] Ibid., p. 35.

Russia's Indirect/Asymmetric Plans

General of the Army Makhmut Gareev, the President of the Academy of Military Science, introduced the concept of strategic deterrence. He defined this asymmetric approach as part of a set of interrelated political, diplomatic, information, economic, military, and other measures that deter, reduce, or avert threats and aggressive actions by any state or coalition of states with threats of unacceptable consequences as a result of retaliatory actions.[19] He offered the asymmetrical method of destroying an opponent's unified information space, sources of intelligence, navigation and guidance systems, and communications and command and control systems instead of fighting with ground forces."[20]

[19] M. A. Gareev, "Strategic Deterrence: Problems and Solutions," *Krasnaya Zvezda (Red Star)*, No. 183, 8 October 2008, p. 8, as downloaded from Eastview.com on 17 March, 2010.
[20] Ibid.

With regard to indirect actions, Gareev stated one must understand"the correlation of direct and indirect actions in strategy. Indirect actions are tied to political, economic, and psychological influences on the enemy and to methods of feeding him disinformation and destroying him from within…We are talking about a greater flexibility in military art…including nonmilitary and nontraditional ones."[21]

S. G. Chekinov and S. A. Bogdanov, the NGW authors, stated that the re-division of territory and markets is now being 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. States that cannot secure their information security risk losing their political sovereignty, economic independence, and cannot aspire to be even regional leaders. This may require studying more closely the foreign experience in information operations.[22] Asymmetrical approaches feature a combination of forms and methods of using forces and means to exploit areas where adversaries have an unequal combat potential as compared to Russia. The use of such means allows for the avoidance of a direct confrontation.[23]

Deterrence: An Indirect/Asymmetric Vector?

It appears that Russia is utilizing a series of deterrent concepts intended to prevent the use of armed force against Russia, and to protect its sovereignty and territorial integrity.[24] Russia has two terms for deterrence, *sderzhivanie* and *ustrashenie.* The military uses the former much more often than the latter. S*derzhivanie* is defined as the deterrence of containment. It is used to limit the development of weapons or the use of military actions. U*strashit'* is defined as deterrence through intimidation. It is used to frighten someone via fear. In effect, the terms seem to be complimentary. Frightening someone can result in their containment. Containing someone can result in their being frightened. Two examples are provided here, namely information and space deterrence:

Information: In November 2015, Russian TV carried images of supposed "top secret" schematics of a Russian naval torpedo, the Status-6. The torpedo allegedly carries nuclear warheads and supposedly can travel up to 10,000 kilometers, making it capable of striking the western shores of the US and creating a tsunami in the process. The Russian press labeled this action as "deliberate stove piping," that is, an attempt to scare analysts with a deliberate release of information. The torpedo would be impossible for

[21] M.A. Gareev: "Lessons and Conclusions Drawn From the Experience of the Great Patriotic War for Building Up and Training the Armed Forces," *Voennaya Mysl'* (*Military Thought*), No. 5 2010, p. 20.
[22] S. G. Chekinov and S. A. Bogdanov, "The Strategy of the Indirect Approach: Its Impact on Modern Warfare," *Voennaya Mysl'* (*Military Thought),* No. 6 2011, pp. 3-13.
[23] Ibid.
[24] *On the Russian Federation's National Security Strategy*, *President of Russia's Website*, 31 December 2015.

either Prompt Global Strike or a Global ABM to detect or intercept. Of interest is that the torpedo's development may not even be complete, [25] but just the suggestion of such a capability can help to deter an opponent, who is uncertain as to the validity of the claim. A month later Russia stated that it's "Rus" deep-diving submersible, part of the secret Defense Ministry's Main Directorate for Deep-Sea Research, had transmitted information from NATO's underwater intercontinental communications cables. The Rus can descend to 6,000 meters with a crew of three hydronauts, where it can carry out technical, emergency rescue, photography, video filming, or scientific research operations.[26]

Space Maneuvering: A Russian satellite "parked itself between two Intelsat satellites in geosynchronous orbit for five months this year" and maneuvered at times to within ten kilometers of these vehicles.[27] Roscosmos declined to comment on the matter, and the Russian Defense Ministry said it would "look into the situation."[28] This maneuvering was designed to imply capabilities to offset the Prompt Global Strike and Global ABM concepts that are seen as direct threats to Russia. In addition, Strategic Missile Force commander Karakayev noted that plans envisage fundamentally new means and techniques for penetrating any missile defense system.[29]

Information Operations

As Defense Minister Shoygu stated, words, cameras, photos, the Internet, and other types of information can become weapons on their own. These weapons can serve, in the hands of an investigator, prosecutor, or judge, he notes, as elements that change the course of history. Indeed, this appears to be what Russia is attempting to accomplish with its vast propaganda/information net that has spread out across Europe and offers its brand of objective reality (consider, for example, Russia's numerous failed attempts to explain, via various scenarios, how MH 17 was shot down; to them, reality is negotiable) instead of truths.

The Red Web

In 2015 two Russian authors, Andrei Soldatov and Irina Borogan, wrote a book titled *The Red Web: The Struggle between Russia's Digital Dictators and the New Online Revolutionaries*. It offers an excellent summary and background on the development of Russian information and cyber issues over the past century. The authors, who have their own website (Agentura.ru), note that the book is an investigation into what happened in their country when two forces, surveillance and control on one side and freedom on the

[25] Sivkov.
[26] No author listed, "Secret 'Rus' Surfaces Successfully," *Argumenty Nedeli Online (Weekly Arguments Online)*, 17 December 2015.
[27] *Interfax* (in English), 12 October 2015.
[28] Ibid.
[29] *Interfax-AVN Online*, 16 December 2015.

other, collided over digital issues.[30] *The Red Web* demonstrates how a combination of surveillance, control, mobilization, information, and manipulation are integrated to the benefit of the Kremlin.

On Control

In 1998 Russia's Federal Security Service (FSB) produced a draft document that made Russia's Internet Service Providers (ISP's) install black boxes on their lines, thereby connecting the ISP with the FSB. The black box system, which furthered control over information, was known as SORM (System of Operative Search Measures) and it became a technical means to investigate electronic networks, or to conduct eavesdropping on the Internet. It was not even mandatory for the FSB to show a warrant to anyone when it made inspections. The ISP owners were forced to pay for the black box and its installation yet they had no access to it.[31] There reportedly have been three levels of SORM over time. Soviet KGB telephone tapping was dubbed SORM-1. Internet tapping, to include Skype, was dubbed SORM-2, while SORM-3 included all telecommunications.[32]

On June 7, 2012, the Russian State Duma introduced legislation for a nationwide system of filtering on the Internet, including a single register of banned sites, i.e., a blacklist.[33] The blacklist would block Internet protocol addresses, sets of numbers, URLs, or domain names the FSB described as harmful. The Federal Agency for Supervision of Communications (Roskomnadzor) maintained the blacklist.[34] By March 2014 Russia had four official blacklists of banned websites and pages: those deemed extremist; those that included child pornography and suicide or banned drug discussions; copyright problems; and sites blocked because they called for demonstrations not approved by the authorities (and conducted without a court order). An unofficial fifth blacklist was for those sites or groups deemed to be uncooperative.[35] Putin wanted to ensure that the West would never be able to start an uprising like Arab Spring in Russia. In April 2014, he declared that the Internet was a CIA project.[36] Authorities clearly feared the Internet might be used to interfere in internal affairs, or undermine sovereignty, national security, territorial integrity, public safety, or be used to divulge information of a sensitive nature.[37]

A Template to Understand Russia's Media Control

[30] Andrei Soldatov and Irina Borogan, *The Red Web: The Struggle between Russia's Digital Dictators and the New Online Revolutionaries*, Public Affairs, New York, 2015, p. x.
[31] Ibid., p. 68.
[32] Ibid., p. 70.
[33] Ibid., p. 166.
[34] Ibid., p. 196.
[35] Ibid., p. 263.
[36] Ibid., p. 238.
[37] Ibid., p. 233.

Soldatov and Borogan developed a template through which to understand the Kremlin's approach to media control:

- Parliament produces a flow of repressive legislation that exploits cracks in previously published rules and regulations;
- Hacktivists and trolls attack and harass liberals online, posing as someone other than a Kremlin supporter;
- Roskomnadzor is granted the power to censor and filter the Internet;
- Kremlin-affiliated oligarchs bankroll and take over media companies;
- Specific manufacturers are selected to provide surveillance equipment;
- Putin's paranoia of enemies ties these actions together, resulting in threats and intimidation.

Putin's system is effective as long as people are certain the Kremlin is in control. This dynamic can be transformed when a crisis occurs and message are shared in real time.[38] Thus, in the end, the digital directors of the Kremlin have gotten what they wanted: a reenergized populace sympathetic to Putin's actions and convinced of Western conspiracies to neuter Russia, resulting in his exceptionally high popularity rating.

Case Study: Ukraine

There have been several countries that have allegedly been attacked by Russian hackers in the past six months that have openly discussed the incidents, with Lithuania, Latvia, and Estonia some of the most prominent. Only Ukraine is discussed here.

Before addressing several late 2015 attacks, it is important to return to the Presidential elections in Kiev in May 2014, for the necessary background. Just 72 hours before the election that potentially would offer a mandate to Ukraine's population to develop a legitimate pro-Western government, the election headquarters were hacked by a pro-Moscow group known as CyberBerkut. Fortunately operations were restored in time for the elections. CyberBerkut has also attached government documents on its website, and it has hacked the Ministry of Foreign Affairs then the Ministry of Defense, among others. CyberBerkut is allegedly an independent Ukrainian organization. Ukrainian officials, however, strongly suspect Russian involvement with the group. There is little surprise in Ukraine's weak cyber security system, since it has much Russian technology in its inventory, is infested with Russian supporters, lacks security updates, and hosts much of its e-mail on servers located in Russia. The hacker tools being used against Ukraine are sophisticated, further indicating nation-state sponsorship.[39] But there is no proof. And that is the same scenario that seems to be repeating itself in 2015.

In January and February 2015 there were Ukrainian reports that Russian special services had launched campaigns to disrupt Ukraine's mobilization effort. There were social

[38] Ibid., pp. 313-314.
[39] Margaret Coker and Paul Sonne, "Cyberwar's Hottest Front," *The Wall Street Journal*, 10 November 2015, pp. A1, A12.

network videos that told people to reject mobilization. Ukraine's Security Service noted that this is a campaign to force people to doubt the need for protecting their "motherland" and that it is an information and psychological operation. Their sources say that two groups of the General Staff's Main Intelligence Directorate are behind the disruption campaign. Phase one is to persuade people of a logical link between poor command, oligarch actions, and frontline problems. Sample applications were provided to help people avoid mobilization on, as the application noted, legal grounds. Phase two may involve organized protests by so-called soldier's mothers and reports about soldier funerals and torture.[40]

Thus Russia has been a bit trickier with its use of cyber against Ukraine. One Kiev report noted that there was a scheme to bribe voters with Internet technologies. As the report noted

> The cyber technology to remotely bribe voters has for the first time been used at these elections (on 25 October and mayoral runoffs in several big Ukrainian cities on 15 November). It includes several stages. At the first one, people are enticed by having their mobile phones topped up by 50 hryvnyas (about two dollars). Then those who respond are paid 400 hryvnyas for a photo of a ballot paper with a tick next to the name of an elected candidate.[41]

A member of the Interior Ministry of Ukraine stated that the funding came from Moscow. Law enforcement officials stated that 10,000 people sold their votes at the 25 October election.[42]

In December a report from iSight Partners claimed that it had gotten the malicious code that caused a massive blackout in the Ivano-Frankivsk region of Ukraine leaving hundreds of thousands of homes without power. The size of the blackout was viewed as a milestone in hacking, since in the past such attacks, which are commonplace, never caused such an incident. The country's energy minister blamed Russia for the attack on the power grid and security firm ESET agrees, since malware known as BlackEnergy caused the outage and it is a Trojan that has been used by Russia in previous attacks against Ukrainian targets.[43] Another report noted that US security agencies were studying malware from the 23 December blackout affecting nearly 700,000 homes for several hours. They had not decided if the hackers acted on behalf of Russia's government or with its implied consent.[44]

---

[40] Kiev 1+1 Television, 25 January 2015.
[41] Kiev 1+1 Television, 13 November 2015.
[42] Ibid.
[43] See http://www.cnet.com/news/cyberattack-causes-widespread-power-blackout-in-ukraine
[44] See http://thedailybeast.com/articles/2016/01/06/exclusive-cia-eyes-russian-hackers-in-blackout-attack.html

Several examples of Russia's use of reflexive control (get someone to do something for themselves that they are actually doing for you) in Ukraine (use of analogies, deception, etc.).

Russia's Intelligence Oversight Apparatus

To implement many of the arrangements above, eight agencies are reportedly permitted to conduct investigative activities in Russia: the Ministry of Internal Affairs (MVD), the Federal Security Service (FSB), Federal Protective Service, Foreign Intelligence Service (SVR, which of course investigates activities outside Russia), Customs, the Federal Drug Control Service, the Federal Corrections Service, and the MOD's Intelligence Directorate (GRU). Several of these organizations have expanded their surveillance activities as of 2012. For example, the Federal Corrections Service purchased the System of Operational and Investigative Measures (SORM) equipment, which are packages enabling one to intercept phone and Internet traffic. The law was expanded to include areas where people did community service for crimes instead of being incarcerated. It is nearly possible to wiretap an entire city.[45] Earlier the Supreme Court had upheld the Right of the FSB to wiretap oppositionists on the ground of engaging in protest activity.[46] Overall it appears that the goal of increased agency and FSB surveillance of the Internet is designed to highlight pro-Kremlin messaging and limit domestic opposition messaging and thus movements.

Military-Related Cyber/Information Reforms

During the past two years there have been several very interesting cyber developments for the MOD. In January 2014 the Chief of the General Staff's Eighth Directorate stated that Russia will create a special structure to protect critically important facilities against computer attacks.[47] In April it was reported that Roselektronika will design a supercomputer which will help testing, along with simulations. The supercomputer's processing capacity is 1.2 petaflops.[48] On May 12, 2014, an article noted that the creation of Information Operations Troops would be stopped, since it was too expensive.[49] However, only two weeks later an article described the army's creation of cyber subunits. Missions included both defense and mounting attacks. In addition to programmers, the table of organization and equipment would include highly skilled mathematicians, engineers, cryptographers, communications personnel, translators, and other supplementary specialists. This will require a center for cyber defense inside the General Staff and a cyber-defense center for each military district and fleet.[50] To date, however, no corroborating evidence has supported this contention in open source documents, other

[45] Andrey Soldatov and Irina Borogan, "Why Are We Now Being Monitored More?" *Yezhednevnyy Zhurnal (Daily Journal)*, 20 December 2012.
[46] Ibid., and Soldatov and Borogan in *The Red Web*.
[47] *RIA Novosti Online (RIA News Online)*, 30 January 2014.
[48] *RIA Novosti (RIA News)*, 9 April 2014. FLOPS (floating point operations per second) is a measure of a computer's processing speed. A petaflop is the equivalent of one quadrillion FLOPS.
[49] *RIA Novosti Online (RIA News Online)*, 12 May 2014.
[50] Aleksandr Stepanov, "Battle of the Computers," *Versiya (Version)*, 26 May 2014.

than the creation of a science company in Tambov dealing with cyber issues; and the desire to create two science companies of programmers.

At the Tambov science company, a military organization designed to recruit talented young programmers, students will be taught how to wage computer wars, erect barriers against Internet attacks, prevent attacks on classified networks, and impede an adversary's troop command and control and weapon use.[51] Another report on the science company stated that the new subunit will make it possible to boost the efficacy of applied-science research, testing in the EW sphere, and training of specialists, and will help in developing data protection methods.[52] In 2013 Shoygu had supported the development of a cyber-command authority,[53] but it wasn't until 2017 that the unit was officially announced.

Conceptual Views

In 2011 the MOD proposed a document known as the *Conceptual Views on the Activities of the Armed Forces of the Russian Federation in Information Space*. This document defined terms that included information warfare and information weapons, among others. *Conceptual Vie*ws also offered principles (legality, priority, integration, interaction, cooperation, and innovation) to guide the activities of the Russian Federation's Armed Forces (RFAF) in information space.[54] The paper proposed several definitions of terms. One of the most interesting was the concept of information war, which the paper defined in the following way:

> Conflict between two or more States in information space with the goal of inflicting damage to information systems, processes, and resources, as well as to critically important structures and other structures; undermining political, economic, and social systems; carrying out mass psychological campaigns against the population of a State in order to destabilize society and the government; as well as forcing a State to make decisions in the interests of their opponents.[55]

Of interest is that this last line is nothing more than the definition of reflexive control (RC), which the Russians use to deceive decision-makers into making decisions that Russia desires. RC was defined in 1995 by Colonel S. Leonenko, who stated that RC "consists of transmitting motives and grounds from the controlling entity to the controlled system that stimulate the desired decision. The goal of RC is to prompt the enemy to make a

---

[51] Aleksandr Stepanov, "Defense Ministry Announces Recruitment for Science Troop. Students Will be Put under Cyber Arms," *MK Online (Moscow Komsomol Online)*, 6 April 2015.
[52] Anton Valagin, "The Ninth Company Will Become an Electronic One," *Rossiyskaya Gazeta Online (Russian News Online)*, 26 January 2015.
[53] Aleksey Mikhaylov and Dmitriy Balburov, "Shoygu Returns to Rogozin's Idea of Creating a Cyber Command Authority. The Defense Ministry is Preparing for a Full-Scale War in Cyber Space," *Izvestiya Online (News Online)*, 12 February 2013.
[54] "Conceptual Views on the Activities of the Armed Forces of the Russian Federation in Information Space," *Ministry of Defense of the Russian Federation*, 2011.
[55] Ibid.

decision unfavorable to himself."[56] Reflexive control can be used at the strategic or tactical level to influence decision-makers or individual citizens. It must be studied closely.

2013-Information Confrontation and Future War (Major-General Vladimir Slipchenko, whose article was published posthumously)

In the 1990s and into the first decade of 2000, Major-General Vladimir Slipchenko was one of the most prolific and creative military writers in Russia. His two most impressive works were books, those being *Future War* and *Sixth-Generation War*. His importance should not be underestimated, since after his death a leading ground force journal, *Army Journal*, published one of his articles. He noted there that information superiority includes (1) domination in space and reconnaissance systems, and in warning, navigation, meteorological, command and control, and communication assets (2) advantages in numbers of recce-strike systems and precision missiles (3) speed of introducing new programs, systems, and capabilities and (4) reliable information protection of assets.[57] Slipchenko wrote that man should expect the development of a set of various forces and means capable of disrupting the normal functioning of the planet's information domain and information assets as well as the means of life support for Earth's inhabitants. Next-generation warfare may not be focused at the operational or strategic level but at the planetary level, provoking technogenic catastrophes in large economic regions or those with information networks and assets. He wrote that after 2050 ecological weapons may also be developed for directed effects against countries' mineral and biological resources, local areas of a biosphere (atmosphere, hydrosphere, lithosphere), and climate resources.[58]

2015 Directive on a Russian Federation/People's Republic of China Agreement on International Information Security

Directive No. 788-d was dated 30 April 2015 and contained a synthesis of a Chinese-Russian cyber agreement. It contained ten articles and an annex. The articles were fundamental concepts, principal threats to information security, principal areas of cooperation, general principles of cooperation, principal forms and mechanisms of cooperation, information protection, financing, relationships to other treaties, dispute resolution, and concluding provisions. The annex defined ten terms.[59] They are: information security, infrastructure, area, resources, and protection; critical information infrastructure facilities; computer attack; illegal utilization of information resources; unsanctioned interference with information resources; and threats to information security.[60] The directive discussed threats to critical information infrastructure facilities,

---

[56] S. Leonenko, "On Reflexive Control of the Enemy," *Armeyskiy sbornik* (*Army Digest*), No. 8 1995, p. 28.

[57] V. Slipchenko, "Information Resources and Information Confrontation: their Evolution, Role, and Place in Future War," *Armeyskiy Sbornik (Army Journal)*, No. 10 2013, p. 52.
[58] Ibid., p. 53.
[59] "Directive on an Agreement between the Governments of the Russian Federation and the People's Republic of China on International Information Security," *Government of the Russian Federation Website*, 13 May 2015.
[60] Ibid.

such as networks, finance, power, and so on; and it discussed the importance of illegally influencing the creation or processing of information.

Two terms that were defined are worth highlighting, information area and computer attack. An information area is "the sphere of activity associated with information creation, transformation, transmission, utilization, and storage exerting an influence on, *inter alia*, individual and social consciousness, information infrastructure [defined as the aggregate of technical facilities and systems for information creation, etc.], and information proper."[61] Thus an information area concerns itself with both information-technical (infrastructure, transmission, etc.) and information-psychological (individual and social consciousness).

An information attack is "the deliberate use of software (software and hardware) tools to target information systems, information and telecommunications networks, electrical communications networks, and industrial process automated control systems carried out for the purposes of disrupting (halting) their operation and (or) breaching the security of the information being processed by them."[62] Thus an information attack appears focused more on systems than people, although it can, of course, impact them depending on the type of messages transmitted.

Article Two considered information security threats to be constituted by the utilization of information and communications technologies for carrying out acts of aggression aimed at violating state's sovereignty, security, and territorial integrity; for inflicting economic and other harm, such as exerting a destructive impact on information infrastructure facilities; for terrorist purposes (to include the propaganda of terrorism); and for perpetrating infringement of the law and crimes, such as illegal access to computer information. Threats included the use of technologies to interfere in states' internal affairs, violate public order, inflame interethnic, interracial, and interfaith enemies, propagandize racist and xenophobic ideas and theories giving rise to hatred and discrimination and inciting violence and instability, and also to destabilize the internal political and socioeconomic situation and disrupt the governance of a state…[63]

Of special interest was that each state "shall not carry out such actions against the other Party and shall assist the other Party in the realization of the said right."[64] "Such actions" include the right to protect the states information resources against illegal utilization and unsanctioned interference, including computer attacks on them.

Conclusions

Russia is motivated by dangers and threats to its information space, whether they be political, economic, military, diplomatic, or others. Software writers and their teams, along with a thriving hacker and troll community, continue to cause problems for the West. Russia's military aims to further enhance reform by introducing high-tech equipment into

[61] Ibid.
[62] Ibid.
[63] Ibid.
[64] Ibid.

the military. As Defense Minister Shoygu stated, words, cameras, photos, the Internet, and other types of information can become weapons on their own. These weapons can serve, in the hands of an investigator, prosecutor, or judge, Shoygu notes, as elements that change the course of history.

Meanwhile, the FSB and other intelligence services will continue to control the population's online activities; to engage the international community in developing a cyber-code of conduct or to influence events abroad; and to prevent "color revolutions" from breaking out in Russia. Suspicion of the West will, it appears, continue to dominate security thinking.