REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
05/01/2019	Technical Report	

4. TITLE AND SUBTITLE
Electrons, Underwater Cables, Satellites, and Creative Thought: The Russian Military's Invisible Information Environment

5a. CONTRACT NUMBER
W56KGU-18-D-0004/0001/S120

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Timothy L Thomas

5d. PROJECT NUMBER
0719S120J3

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
The MITRE Corporation
7515 Colshire Drive
McLean, VA 22102

8. PERFORMING ORGANIZATION REPORT NUMBER
PRS-19-0314

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
United States Army (ACC-APG)

10. SPONSOR/MONITOR'S ACRONYM(S)
ACC-APG

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
The following discussion offers one assessment of things not visible, focusing on the multi-dimensional information environment. It is a difficult one to assess. During the Cold War, we all knew the intent of a tank and who the potential enemies were. In the information age, ascertaining the intent of an electron and where it originated (an adversary or surrogate) present much more difficult challenges in assessing who really may or may not have attacked whom. It is also difficult to observe items that are out of sight (electronic networks, satellites, and underwater cables, all key sources of information and communications) and whether they are being inspected or manipulated by foreign entities.

15. SUBJECT TERMS
Military Intelligence; Military Planning; digital deterrence; Russia; communications; cyber operations; reconnaissance; information systems; military strategy

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE		39	Susan Carpenito
					19b. TELEPHONE NUMBER *(Include area code)* 781-271-7646

MITRE

Sponsor: USEUCOM
Contract No.: W56KGU-18-D-0004/0001/S120
Project No.: 0719S120

Electrons, Underwater Cables, Satellites, and Creative Thought: The Russian Military's Invisible Information Environment

Author: Timothy Thomas

May 2019

Introduction

A few months ago, a U.S. Army general sat behind a table and looked at a map of Russia. He said he could visualize where the Russian brigades might be located in each military district on this purely cartographic representation. What he didn't know, and what he asked about, was "what can't I see."

The following discussion offers one assessment of things not visible, focusing on the multi-dimensional information environment. It is a difficult one to assess. During the Cold War, we all knew the intent of a tank and who the potential enemies were. In the information age, ascertaining the intent of an electron and where it originated (an adversary or surrogate) present much more difficult challenges in assessing who really may or may not have attacked whom. It is also difficult to observe items that are out of sight (electronic networks, satellites, and underwater cables, all key sources of information and communications) and whether they are being inspected or manipulated by foreign entities.

Overview

Russia's military has stepped quickly into the information age, developing information troops and information science companies along with a vast array of new precision weaponry and reconnaissance means (unmanned aerial vehicles, satellites, etc.). The military is cooperating with numerous domestic information and computer assets (Kaspersky, Dr. Web, etc.). These forces, along with the aerospace and electronic warfare branches, are developing ways to watch or manipulate adversaries by learning to disorganize command and control entities; inspect or neutralize satellites; tap into underwater cables; develop information, space, and ocean theaters of military operations (TVDs) from which actions spring; make advance preparations for an initial period of war; forecast the impact of the information age on war's conduct; and other related activities.

The vast majority of this paper's content addresses Russia's current approach to acquire and control new operational capabilities. The newer strategies and conduct of operations are listed first below, as they utilize new scientific discoveries to uncover innovative ways to use reconnaissance assets, precision weaponry, military art, or deterrence theories. Perhaps more important is how Russian theorists have expanded their vision for employing such assets to the entire planet. Two components of Russia's breakout of information warfare's components that have also been present since the 1990s, information-technical and information-psychological developments, are also discussed.

Near the end of the paper the international strategies that have been used for years are discussed. Two more contemporary documents (2011 *Conceptual Views* and 2014 *Military Doctrine*) demonstrate the carry-over of specific goals from the 1990s into the contemporary era that Russia still hopes to achieve. These documents are centered around rules, regulations, and terminology for the use of information resources. Early United Nation presentations by Russian experts focused on defining information weapons and other terms. Such goals are still sought after today, as the documents clearly indicate. An April 2018 presentation by Russian General Major

Igor Dylevskiy, an information warfare expert, demonstrates the contemporary application of the same process.

Russia's military approach to the information age is thus clearly multi-dimensional and requires continuous study. The following outline represents the order in which topics are presented in this paper:

- Information assets and strategies;
- Information's role in the initial period of war;
- Strategic operation for the destruction of critically important targets (SODCIT);
- Forms and methods of information use;
- Information and digital deterrence;
- Information troops;
- Information-technical and information-psychological capabilities;
- Reinstating political-military officers in the force;
- The military's 2011 *Conceptual Views* and 2014 *Military Doctrine*;
- General Major Igor Dylevskiy's 2018 presentation at the 6th Moscow conference on international security.

Each topic is highlighted in **bold** below so that readers can quickly find sections in which they may be more interested.

NEWER DEVELOPMENTS

Information strategies

There are three key points to analyze when considering Russian information strategies. First is the scale of such operations. Russian analysts indicate that information's capabilities, not surprisingly, have expanded from specific territories to a planetary scale. It is now possible to hit targets with either missiles or electrons anywhere on the planet. Perhaps Russia's discussion of an information theater of military operations (TVD) is where the focus of a planetary concept of operations can be found. A second point is that for an information strategy to be successful, information superiority must be attained, and that involves the capability to interrupt, if necessary, an adversary's information flows. In this regard Russia is focusing on the carriers of information, namely underwater cables, satellites, and electronic warfare means, as issues to control if it is to thwart the command and control capabilities of a foreign force. Third, there remains the ability to construct information flows, not interrupt them, and deceive an opponent with information specially developed for their consumption. Such capabilities are referred to in Russia as the reflexive control of an opponent. All of these points are explained in greater detail below.

Writing in 2010, Russia analyst S. G. Chekinov noted that "Orbiting weapons capable of hitting key military targets at any point of the planet would give a global dimension to armed struggle."[1] His reference to the global dimension of armed struggle has been restated by others and indicates a theoretical move from considering warfare on a strategic scale to a planetary one.

[1] S. G. Chekinov, "Predicting Trends in Military Art at the Start of the 21st Century," *Voennaya Mysl'* (*Military Thought)*, No. 7 2010, pp. 19-33.

Information strategies involving the global information space use information and digital assets to influence situations and decision-makers. In 2013 Russia's *Army Journal* published an article by General-Major Vladimir Slipchenko, who was known for his creative thought. Slipchenko wrote that superiority over an opponent was only possible after superiority in information, mobility, and rapidity of reaction were assured. Precise fire and information effects against economic structures and military objectives were required. Slipchenko referred to this mode of conduct as noncontact war. Most important of all he stressed that, in such war, information confrontations would be continuous and would leave the operational and strategic levels and acquire a planetary scale. However, such confrontation's principal goal remains to be the maintenance of one's own information security and the lowering of a potential enemy's security.[2] Chekinov and Slipchenko are not alone in thinking about planetary concepts of influence.

Concepts such as information strategies and wars on a planetary scale are developed in the bowels of the General Staff in Moscow. Russian General Staff Chief Valery Gerasimov, quoting Soviet military theorist Alexander Svechin in regard to strategy, has noted on occasion that each situation has a logic all its own. That is, strategy's makeup is not fixed but entirely flexible. It depends on creative thought to best utilize the circumstances under consideration, and choices will remain hidden until utilized. With an array of missiles, satellites, underwater cables, and electronic networks before it, strategies are dependent on the creativity and innovation of commanders to exploit the situation at hand.

Underwater cables and satellites play huge roles as assets whose locations may be known but their location so widespread (planetary) that they can only be watched intermittently, perhaps when a warning sounds. It is not only their location, but also their function that may be invisible. Until such equipment's function is discussed openly or is actually utilized (or is inspected by a foreign entity), its function remains a secret. The same doubts apply to the application of military art. How forces will be used remains a secret until they are deployed.

With regard to underwater cables, a 2014 Russian report stated that the oceanographic research ship Yantar can submerse to a depth of over 6,000 meters. The range of tasks it can resolve is broad and interesting, such as "the retrieval of information from the NATO counties' underwater intercontinental communications cables along which our 'partner's' most secret and sensitive information is transmitted."[3] A 2017 British report noted that Russia could use not only the Yantar but also underwater drones to attack network cables carrying Internet and telephone communications around the world.[4] Another 2017 report of Russian origin noted that the Yantar is a "unique floating dock for mini-submarines and unmanned submersibles" and that they are cable of connecting to information cables on the bottom of the sea.[5] A 2018 Russian report stated that the U.S. was particularly concerned about protecting underwater communications and that

[2] V. Slipchenko, "Information Assets and Information Confrontation," *Armeyskiy Sbornik (Army Journal)*, No. 10 2013, 52-53, 55. The author would like to thank Dr. Harold Orenstein for his translation of this article.
[3] Unattributed report, "Secret 'Rus' Surfaces Successfully," *Argumenty Nedeli Online*, 17 December 2015.
[4] David Brown and Tom Parfitt, "Russian Navy Ship Yantar Can Sever Internet Cables, *The Times* (Electronic Edition), 17 December 2017.
[5] Andrey Riskin, "Which Secrets is the Russian Intelligence Ships Yantar Seeking on the Bottom of the Mediterranean Sea?" *Nezavismaya Gazeta Online*, 10 October 2017.

their damage could cause wide-scale disorganization in communications.[6] Obviously the Russians are aware of the sensitivity associated with these cables.

Information flows can also be disturbed by anti-satellite (ASAT) weaponry. Satellite observation or destruction topics have been under discussion in Russia for over 60 years. While there are several types of satellite disruptions, the first for discussion is the Tirada-2S, because it is designed to interfere with information flows. The system is supposedly capable of radio-electronic suppression or jamming of communication satellites, to include the complete disabling of the satellites.[7] The Tirada is ground based, suppresses an adversary's electronic apparatus by means of an impulse, and likely receives target designation from Russia's Missile Attack Warning System. The new Russian combat laser, the Peresvet system, blinds satellites[8] and may have a similar function, among others, as the Tirada.

There are other satellite types in the Russian inventory that, while not directly affecting information flows, will perform such activities simply due to the consequences of their other functions. In 2017 Russia announced it had developed both "killer satellites" and maneuvering inspection satellites that approach and inspect other satellites. As one military expert noted:

> In the event of a global conflict it is extremely important to destroy the enemy's group of satellites in order to derive him of communications, navigation, and the capability to conduct reconnaissance. Thus, the idea of creating such interceptors appears. In the USSR, for example, tests were conducted during which one satellite approached another and exploded, striking the target with fragments.[9]

The inspection could, utilizing the visible, infrared, and ultraviolet bands, collet data and transmit it to a control center.[10] If the data indicates the satellite is conducting communications, the control center could send a message to the Tirada to disable it. The inspector satellite could also be equipped with electronic intelligence collection or accommodate attack weapons, "whether it be an energy gun, micro-missiles, or simply a bag of nails."[11] A late 2018 report noted that there are various kinds of ASAT weaponry in Russia's inventory. The ASAT Kontakt missile can be launched from a MiG-31 aircraft; the S-500 Prometey air defense missile system is designed to intercept orbital vehicles; and the Nudol space missile is part of the A-235 missile defense system, capable of interceptions at ranges up to 1500 kilometers.[12]

---

[6] Aleksey Ivanov, "Russian Navy May Deprive United States of Communications," *Rossiyskaya Gazeta Online*, 22 June 2018.
[7] *Interfax* (in English), 9 January 2019. No author or title provided.
[8] Aleksey Abaturov, "Russian 'Sweepers' of Near-Earth Space: Tirada, Nudol, and Kontakt," *Yezhenedelnik Zvezda*, 20 November 2018.
[9] S. Valchenko, N. Surov, and A. Ramm, "Russia Sends Inspector into Orbit: Military Test Operations of Maneuvering Identification and Intercept Satellite," *Izvestiya Online*, 26 October 2017.
[10] Vladimir Tuchkov, "Russia's Killers: Who Already Finds Themselves in the Sights: Moscow is Creating a Grouping of Orbital Spacecraft Called Killer Satellites," *Svobodnaya Pressa*, 30 March 2018.
[11] Ibid.
[12] Abaturov, "Russian 'Sweepers'…"

Radio-electronic warfare (REB) capabilities are another way to interrupt information flows. Referring again to Chekinov's explanation of 21st century military trends, he noted the following:

> Electronic warfare devices are, therefore, placed side by side with nuclear and conventional weapons and electronic warfare itself turns from a kind of operations (combat) support into one of the key elements of combat operations. In the light of past experience, the share of electronic suppression in disorganizing the enemy's control system and undercutting his combat potential accounts for about a third. In the longer run, it may rise and have a more significant impact on the efficiency of air force attacks and strikes by other weapons.[13]

REB has become a major method to deny communications and information flows to opponents and to disorganize them. REB Chief General-Lieutenant Yuriy Lastochkin, for example, mentioned REB's ability to disorganize adversary troops and weapons eight times in a 2017 article.[14] He and two other authors described how operational art is developing in conjunction with improvements in weaponry and ways to conduct combat. Capabilities, it was noted, have always determined methods. Weapon improvements have resulted in new operational tasks for REB and allowed the force to both disorganize adversary troops and weapons and repulse aerospace attacks.[15] Destroying circuitry, distorting or destroying information, or simple electronic suppression all contribute to the command and control (C2) disorganization effort.[16] REB methods will be a main way to cause chaos in an adversary's C2.

While these methods of cables, satellites, and REB all interrupt information flows, Russia is also expert at producing its own information flows that are designed to deceive an adversary. One of the methods for doing so is referred to reflexive control (RC) theory. It is an element of an information strategy. RC theory attempts to cause an opponent to do something for themselves (make decisions in line with the situation) that they are actually doing for Russian forces (who have fed their opponent with information about the situation that caused the opponent to react in a way favorable to Russia). One source noted that RC is essentially information and psychological effects against persons on the opposing side who are making decisions. It is "a set of measures, interconnected with respect to goal, place, and time, aimed at…forcing the enemy to reject his initial plan and accept knowingly a decision that is disadvantageous for him…"[17] Another source stated that "An important feature of such a war [information] is the extensive use of enemy resources. Influencing his information systems on the basis of the principles of reflexive control, one can achieve desirable actions from opposite sides, that in real practice are often referred to as a provocation."[18]

---

[13] Chekinov, "Predicting Trends…"
[14] Yu. Lastochkin, Yu. Koziratsky, Yu Donskov, and A. Mororescu, "Combat Employment of EW Forces as an Element of Ground Forces Operations," *Voennaya Mysl'* (*Military Thought)*, No. 9 2017, pp. 18-25.
[15] Ibid.
[16] Ibid., p. 24.
[17] Stanislav Ermak and Aleksandr Raskin, "Are All Methods Good in Battle? On Some Aspects of Reflexive Control of the Enemy," *Armeyskiy Sbornik* [*Army Journal*], No. 7 2002, p. 44. The author would like to thank Dr. Harold Orenstein for his translation of this article from Russian to English.
[18] Nikolay Khorunzhyy, "Does Russia Need a Cyber Command?" *Kovrov VPK.name*, 23 August 2013.

RC has space, and therefore planetary, implications as well. In 2002, authors Stanislav Ermak and Aleksandr Raskin discussed RC methods as they apply to space. Coercive pressure, transmitting false information, and influencing an opponent's decision-making algorithm were discussed. They then noted that a special role in RC was provided to space information resources for enemy control. Two ways to do so are using resources based on new physical principles and incapacitating on-board complexes on spacecraft.[19] Today, as noted above, Russia's space troops have developed an "inspection satellite" that can inspect other orbiting satellites for their function.[20] As a result, they can be used for RC measures (such as deterrence) by indicating that an adversary satellite's value or use has been discovered (when perhaps it has not) and therefore neutered to a degree.

The most probable areas where command and control and RC can be combined are in the process of decision-making in general and in the planning of combat operations. To reflexively control the enemy, a specially designated force and means should be developed, the Russians note, to include a specific Table of Organization and Equipment (TO&E)[21] with information-psychological confrontation qualifications. These forces would develop and transmit recommendations to the commander on how to use RC measures together with command and control actions.[22] These forces would be expected to accomplish the following:

> Here the implementation of the RC method at stages of immediate preparation for and execution of the combat mission is carried out by means of sending the appropriate information packets to the enemy. It should be recalled that an information packet within the framework of a RC method is implemented through the totality of simulacra, which are embodied in both a nonrepresentational form (simulation) and a representational form (concealment). Information packets are sent to the enemy with the goal of creating favorable conditions for executing a combat mission .[23]

Information packets are designed to provide specific information that conceals existing combat situations or describes a nonexistent situation.[24] Such situations are subject to two sets of reflection, information and actual operations. Information reflection is how the enemy views friendly forces and their condition based on their system of intelligence and the enemy's assessment of an opponent's potential. Operational reflection is the principles and features of an enemy's decision-making within the information he has about the condition of his opponent's force and combat operations plans. Combat experience also counts when such decision-making is conducted.[25] Such packets of information could be utilized to influence operations on a strategic or even planetary scale.

---

[19] Ermak and Raskin, pp. 44-46.
[20] S. Valchenko, N. Surov, and A. Ramm, "Russia Sends Inspector into Orbit: Military Test Operations of Maneuvering Identification and Intercept Satellite," *Izvestiya Online* [*News Online*], 26 October 2017.
[21] Ibid., p. 39.
[22] Ibid., p. 41.
[23] Ibid., p. 40.
[24] Ibid.
[25] Ibid.

Russian theorists understand that the ability to interrupt information flows or to use information to deceive an opponent are methods that must be developed and prepared in peacetime. It requires mapping an opponent's information network and, if possible, collecting intelligence on such systems in order to be able to disrupt or influence them at a moment's notice. Such access allows Russian forces to prepare to gain the initiative in what they term as the initial period of war.

Information's Role in the Initial Period of War (IPW)

An 11 January 2018 *Wall Street Journal* article discussed Russian hacking successes against the U.S. power grid. Robert Silvers, former assistant secretary for cyber policy at Homeland Security, noted that "what Russia has done is prepare the battlefield without pulling the trigger."[26] There is hardly a better description of Russia's IPW concept.

Being prepared for the initial period of any war has been a constant focus for the Soviet Union and now Russia. Most likely this is a direct result of lessons learned from the Soviet experience in WWII, when the nation was not properly prepared to go to war with Germany and experienced early setbacks. Now in the age of information, where information superiority is so crucial to success, the IPW has taken on added important.

An important discussion of information and the IPW was conducted on the pages of *Voennaya Mysl'* (*Military Thought)*. The IPW was defined as when warring states conduct operations before the start of war to achieve objectives or to create favorable conditions for committing their main forces.[27] Outer space, information warfare, and new weapon capabilities all help inform the shape needed for the IPW. These weapons enable sides before the start of operations to conceal the status and intent of their armed forces and the nature of any planned attacks. More importantly "In all likelihood, the aggressor country is to be expected, still in peacetime, to launch a wide-scale targeted information operation and intense reconnaissance activities, including a set of related and closely coordinated actions."[28]

It was noted that the IPW of new-generation wars will be decisive for the outcome of a future war. Such wars will include the launching of information operations, to include technical and psychological attacks along with electronic operations. Information operations and electronic and fire strikes disorganize government systems, demoralize populations, and prevent leaders from rallying forces to repel aggression.[29] The attainment of information superiority is required in areas such as the mass media in order to stir up chaos and confusion in an adversary's government and military management. The main effort in the information struggle is to be directed against an adversary's government and military control systems, while providing protection to national

[26] Rebecca Smith and Rob Barry, "Russian Hack Exposes Weakness in U.S. Power Grid," *The Wall Street Journal*, 11 January 2018, pp. A1, A9.
[27] S. G. Chekinov and S. A. Bogdanov, "Initial Periods of War and their Impact on a Country's Preparations for Future War," *Voennaya Mysl'* (*Military Thought)*, No. 11 2012, p. 16.
[28] Ibid., p. 24.
[29] Ibid., p. 25.

information resources from adversary influences.[30] Russian IPW preparations include broadcasts to prepare the economy and public for war; the mobilization of reserves; the relocation of military units; the broadcast of false information to deceive adversary reconnaissance; and a campaign to inform the public about the adversary's motivations and intentions.[31]

Perhaps due to concern for the US's cyber security in the IPW, the US Federal Bureau of Investigation (and earlier, the government of Ukraine) decided to no longer tolerate the sale of the Russian-produced Kaspersky anti-virus solutions, a product sold in stores and advertised on prominent radio stations in the US. A recent *Wall Street Journal* article noted that the Kaspersky anti-virus solution has been on a Defense Department watch list of potential problems since 2004. In 2013 the Defense Intelligence Agency issued a Pentagon-wide threat assessment about the company. US officials note that the firm's products were used as a tool for spying on systems in the US.[32]

Proper IPW preparation includes planning for the immediate implementation, whether preemptively or after conflict erupts, of strategic operations to destroy critically important targets. These plans help Russian forces ensure it can attain the initiative in future confrontations.

Strategic Operations to Destroy Critically Important Targets (SODCIT)

Russia's military doctrine of 2014 noted that information can impose an effect on the enemy to the full depth of his territory in global information space. This makes the U.S national military objective of deterring "state adversaries from threatening the U.S. homeland and U.S. interests while assuring the security of allies"[33] take special note.

Cyber operations, which seemingly are without borders, are most likely one aspect of Russia's SODCIT concept, as it allows Russia to affect an enemy to the full depth of his territory in global information space. The SODCIT concept implies deep reach into an opponent's rear area and threats there to political, economic, military, and information infrastructures and targets of strategic significance. There is very little in the open military literature about this concept, but it has apparently been discussed in Russia for several years and, due to its strategic implications, is extremely important yet close hold.

In 2010, a *Red Star* article noted that changes in the nature of wars would be reflected in the various forms in which the Armed Forces are used. The article's author, Marina Yeliseyeva, wrote that "The **strategic operation to destroy critically important facilities** has been developed."[34] Retired Colonel General Viktor Barynkin added "it has become expedient to combine strategic defensive and offensive operations and strategic operations in the ocean theater

[30] Ibid., p. 27.
[31] Ibid., p. 26.
[32] Paul Sonne, "Russian Firm Was Long Seen as Threat," *The Wall Street Journal*, November 18-19, 2017, p. A2.
[33] C. M. Scaparrotti, *United States European Command: Theater Strategy*, 2016, p.6.
[34] Marina Yeliseyeva, "Lessons for All Time," *Krasnaya Zvezda (Red Star) Online*, 27 October 2010.

of hostilities into a single strategic operation."[35] This appears to border on a planetary and not a strategic operation.

In 2013 the journal *Air-Space Defense* published an article on forms and methods of combat in space. It added "space" to Barynkin's strategic operation noted above, stating:

> It is possible to use various space systems in support of each of these operations. Thus, supporting a **strategic operation to destroy critically important enemy targets** necessitates the use of space-based means of reconnoitering these targets; electronic intelligence assets; meteorological reconnaissance assets in the interests of a proper selection of attack weapons and their combat employment methods; and space-based navigation, communications, relay, and strike evaluation systems.[36]

A 2014 article that mentioned the SODCIT concept was found in *Military Thought*. It stated that determining combat missions, mixes, methods, and variations of long-range precision-guided munitions (PGMs, which are supported by an information infrastructure) employment in operations can be presented according to a priority-ranked subprocess:

- Determination of parameters of the concept of organizing the planning and conduct of demonstration strikes by long-range PGM;
- Substantiation of variations of the concept of limited strikes for deescalating the military conflict and compelling the enemy to cease armed confrontation;
- Development of the concept of the **strategic operation to destroy critically important enemy facilities**.[37]

The authors added that in the makeup of the special mathematical and software support (SMPO) for employing long-range PGM forces, a central place must be set aside for use against systems of complex-structure targets. Calculations must be oriented toward correlating the combat capabilities of long-range PGM groupings with weapon targets; and optimization problems can be used to solve operational issues, to include:

- Determination of the mix of long-range PGM forces (weapons) for performing missions of destroying key facilities in RF Armed Forces general-purpose force operations;
- Determination of the mix of long-range PGMs for participation in a **strategic operation to destroy critically important facilities [strategicheskaya operatsiya po porazheniyu kriticheski vazhnykh obyektov] (SOKVO).**[38]

---

[35] Ibid.
[36] Vasiliy Y. Dolgov,and Yuriy D. Podgornykh, "Space As a Theater of Military Operations: On Possible Forms and Methods of Combat Employment of Space Command Forces and Assets," *Vozdushno-Kosmicheskaya Oborona Online*, 10 April 2013.
[37] A.A. Protasov, V.A. Sobolevskiy, and V. V. Sukhorutchenko, "Planning the Use of Strategic Weapons," *Voennaya Mysl'* (*Military Thought)*, No. 7 2014, pp. 9-27.
[38] Ibid.

Finally, in 2015 the Aerospace Forces (VKS) noted that its missions were to do the following: reconnoiter the aerospace situation; uncover the beginning of an aerospace air and missile attack; notify state and military command and control entities about it; repel aggression in the aerospace sphere; protect command and control facilities of top echelons of state and military command and control, administrative-political centers, industrial and economic areas, and important facilities of the country and troop groupings against attacks from space and from the air; **destroy critically important enemy facilities** and troops by employing conventional and nuclear weapons (the term "strategic operation" was missing but by adding the term "nuclear," strategic operations seem to be implied); provide air support and support to combat operations of troops of Armed Forces branches and combat arms; and support launches of spacecraft (MBR [ICBM] launches) and their control in orbital flight.[39]

Thus, while the term is used sparingly, it has been observed in specific places. It's use in conjunction with aerospace forces or precision-guided munitions is significant, since they both possess long-reach capabilities to the depth of an adversary's territory anywhere on the globe. Russian planetary warfare theorists must find such concepts intoxicating.

Forms and Methods[40] of Information's Use

A consistent element of a Russian planners thought process is to examine the forms and methods of a capability's use. This element applies to information topics as well, as demonstrated by S. A. Komov who a few years ago wrote an article "On the Methods and Forms for the Conduct of Information War" and by the many authors after him who covered similar ground. In a recent Russian military article on the army's military-political instructional plan for 2019, forms and methods were mentioned prominently in several categories.[41]

A definition of a form and a method along with their use in an information sense is listed below:

> A "form" is an organization, which in regard to information warfare could include international media elements such as *Russia Today or Sputnik* or military developments, such as the creation of cyber and electronic warfare "science companies;" a cyber corps, which was announced in 2013 but for which no further information has been provided; information operation forces, announced in 2017; and the Advanced Research Foundation, Russia's equivalent to the US's Defense Advanced Research Projects Agency. These forms or organizations implement methods.

---

[39] Viktor Bondarev interview by V. Kutishchev, "Russian Aerospace Forces," *Armeyskiy Sbornik (Army Journal)*, No. 3 2017, pp. 33-34.
[40] For a discussion of Russia's forms and methods of operations, see Timothy Thomas, "Russia's Forms and Methods of Military Operations: The Implementors of Concepts," *Military Review*, May-June 2018, pp. 30-37.
[41] No author provided, "Instructional Plan for the Military-Political Preparation of the Armed Forces of the Russian Federation in 2019," *Armeyskiy Sbornik (Army Journal0*, No. 11 2018, pp. 91-101, as downloaded from https://dlib.eastview.com on 16 January 2018.

> "Methods" are broken into two parts, weaponry and military art. Weaponry includes hackers, reflexive control techniques, trolls, disinformation, deterrence capabilities, killer satellites, and other agents of destruction or influence. Military art includes the use of indirect and asymmetric capabilities to achieve specific goals, such as the exploitation of the West's free press or an indirect attack on the cyber infrastructure of another nation. Russia's excellent contingent of algorithm writers ensures that the nation will be strong for years to come in writing software as weapons that can eavesdrop, persuade, or destroy.[42]

It is important to continue to study information forms and methods of conflict. They can be some of the most subliminal or deceptive forms of manipulation and are always being updated in Russian information warfare circles.

Information and Digital Deterrence

In both 2015 and 2016 Ukraine's power was turned off due to a cyber-attack that, to Ukrainian experts, originated in Moscow. The so-called "Black Energy" malware causing the events has also been spotted on the US grid, according to a 2017 *Wired* article. The author summed up the events in the following manner:

> By turning the lights out in Kiev—and by showing that it's capable of penetrating the American grid—Moscow sends a message, warning the US not to try a Stuxnet-style attack on Russia or its allies like Syrian dictator Bashar al-Assad. In that view, it's all a game of deterrence.[43]

It is important to know how Russia both defines and employs its deterrence concepts, so that issues don't escalate out of control simply due to a misunderstanding of terminology or practice. Russian and US understandings of terms like nuclear deterrence, nonnuclear deterrence, and information deterrence may differ—or not exist in both nations. It is well-known that a key component of EUCOM's theater strategy is to deter conflict.

There have been several Russian military or civilian ways to define deterrence in the past decade. In 2008 retired General of the Army Makhmut Gareev, the President of the Academy of Military Science, defined strategic deterrence as an asymmetric approach and 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.[44] In the Russian Defense Ministry's 2011 *Conceptual Views on the Activities of the Armed Forces of the Russian Federation in*

---

[42] Statement by Mr. Timothy L. Thomas, at the time Senior Analyst, Foreign Military Studies Office, Fort Leavenworth, Kansas 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.
[43] Andy Greenberg, "Lights Out," *Wired*, July 2017, p. 61.
[44] 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.

Information Space, deterrence was seen to exist as a conflict prevention asset in information space in the following way:

> Deterrence and conflict prevention: develop an information security system for the Russian Federation's Armed Forces that can deter and resolve military conflicts in information space; remain in a constant state of readiness; expand the group of partner states; conclude, under UN auspices, a treaty on international information security; establish control over the escalation of conflict; take priority steps to counter the development and spread of a conflict; neutralize factors leading to the conflict's spread; and shape public opinion means to limit the ability of instigators to further escalate the conflict.[45]

In 2012, in *Military Thought*, two authors noted that deterrence types are those involving the threat of force or those that are nonmilitary and indirect (asymmetrical). A force can be either offensive or a powerful defensive task force; it could be an ultimatum; or it could be the use of an information campaign to mislead an adversary about Russia's ability to confront aggression and thereby deter him from acting.[46] In 2015 Russia's *National Security Strategy* defined strategic deterrence as the result of interrelated political, military, military-technical, diplomatic, economic, information, and other measures, to include maintaining the capacity for nuclear deterrence.[47]

To deter or counter threats (which appear to include the US's Prompt Global Strike concept; a global ABM system; color revolutions; cyber-attacks; and an ISIS threat to the south) to Russia, Putin's staff is employing some old methods and developing new ones. Naturally nuclear deterrence remains at the top of the list of ways to counter threats from the US. Russia has two terms for deterrence, *sderzhivanie* and *ustrashenie.* The military uses the former much more often than the latter and defines it as containment, used to limit the development of weapons or the use of military activities. The latter is defined as deterrence through intimidation or fear. In effect, the terms seem to be complimentary. Frightening someone can result in their containment. Containing someone can result in their being frightened.

A 2016 discussion of deterrence in the information age appeared in the journal *Military Thought*. It was written by several Russian information specialists, with recommendations as to how to avoid information age conflict. On the one hand, the authors note, deterrence is based on the build-up of a state's military capabilities, while on the other hand, preventing military conflicts is often based on the proportional reduction of military potentials. It appears that the joint functioning of these two items are required to stabilize the international situation.[48] However, new means for deterring conflict are evolving. While the Cold War primarily witnessed nuclear

---

[45] "Conceptual Views on the Activities of the Armed Forces of the Russian Federation in Information Space," *Ministry of Defense of the Russian Federation*, 2011.
[46] S. G. Chekinov and S. A. Bogdanov, "Initial Periods of War and their Impact on a Country's Preparations for Future War," *Voennaya Mysl'* (*Military Thought)*, No. 11 2012, p. 26.
[47] "The Russian Federation's National Security Strategy," *President of Russia Website*, 31 December 2015.
[48] I. N. Dylevskiy, V. O. Zapivakhiyn, S. A. Komov, S. V. Korotkov, and A. A. Krivchenko, "On the Dialectic of Deterrence and the Prevention of Military Conflicts in the Information Age," *Voennaya Mysl'* (*Military Thought)*, No. 7 2016, p. 5. The author thanks Dr. Harold Orenstein for his translation of this article from Russian into English.

deterrence, a period of nonnuclear deterrence has followed with an emphasis on precision weaponry. A potential new deterrent trend that has appeared is "hostile information" (information-technical, information-psychological) activities that can violate state sovereignty or interfere in a state's internal affairs.[49] The authors made a reference to the 2014 edition of Russia's *Military Doctrine* under the section titled "organization and conduct of the information struggle," where a task of the Armed Forces was stated to be the development of forces and means of information confrontation which can deter opponents. "Means" of information confrontation (struggle) the authors listed include the following:

- Technical reconnaissance resources (used to obtain information by allocating parameters of various types of physical fields);
- Information resources (information used to influence knowledge, moral values, motives, and behavior stereotypes of individuals, collectives, and the public consciousness in order to form certain behaviors);
- Psychotronic resources (make it possible to covertly control consciousness, psychological processes, and the behavior of people);
- Special hardware and software effects (computer viruses, worms, and Trojan programs used to steal, destroy, and/or modify information of databases, block their access, or breach computer functions);
- And resources for protecting information (technical, cryptographic, and software resources designed to limit the acquisition of information due to leakage).[50]

New means of strategic deterrence now include information weapons, the authors note. There must be a method for selecting targets according to a "cost effectiveness" criteria. The effect of attacks on the economy, financial systems, and the information infrastructure must be monitored. Since information weapons can be employed in conjunction with precision guided weapons, one must determine the necessary quantity of resources for nonnuclear (precision and information) deterrence. Finally, the thoughts of an adversary's leadership must be considered, that is, a nonnuclear attack could cause an adversary to resort to nuclear or nonnuclear means.[51]

Russia has employed other forms of information deterrence. In November 2015, Russian TV used information as a deterrent when it 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" to deliver an information bomb. The torpedo would be impossible for either Prompt Global Strike or a Global ABM to detect or intercept. Of interest is that the torpedo's development

[49] Ibid., p. 6.
[50] Ibid., p. 8.
[51] Ibid., pp. 8-9.

may not even be complete, [52] but just the suggestion of such a capability can help to deter an opponent, who is uncertain as to the validity of the claim.

In 2017 Russian military expert Valery Mukhin noted that the use of inspector satellites can serve as a serious deterrent. This is because with the system, Russia can check on whether the stated functions of a satellite are true or not. Such a satellite can maneuver between orbits and is effective in peacetime.[53]

A lack of information can serve as a deterrent as well. 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.[54] Roscosmos declined to comment on the matter, and the Russian Defense Ministry said it would "look into the situation."[55] This maneuvering's lack of specific information as to the satellite's goals "implied" (that is, it lacked information) capabilities (attack, reconnaissance, inspection?) that could not be ascertained. Thus, the absence of information can serve as a deterrent just as much as its presence.

With regard to legal deterrence, Russia is using the UN to support its legal claims to areas it says are within the nation's proclaimed "national interests." This applies to the Arctic, where Russia has spent much time and money mapping the Arctic Sea. If Russian representatives can prove their case with images or numbers, based on digital mapping of the area, it may be able to reserve for itself exclusive access to the region's oil and gas riches. Russia would, in effect, deter other nations from the region through the use of digital (information) assets.

Perhaps more importantly, Russia wants a United Nations resolution on specifics of the information sphere. This includes criteria for types of information effects and acts of aggression; a way to regulate the identification and authentication of sources of information effects; and standards for investigating information effects to include a method for collecting evidence.[56]

A conclusion to be reached here is that Russia has noticed that technological progress is changing the means and parameters by which to deter an opponent. Russia's leaders appear to believe that by exposing weapon capabilities, as Putin did in his March address to the nation describing new weaponry and as Russia had done earlier with its Status-6 torpedo, that the threat can be neutered through what might be termed information deterrence, that is, stating again and again that no analogous systems exist in the world to counter Russian equipment. The nature of international relations is changing as well, as we are now much more connected globally than ever before—by the media, satellites, and optical fiber. Russia is working to create a system of strategic deterrence that takes advantage of these changes, both nuclear and nonnuclear, to contain and intimidate its neighbors and their partners.

---

[52] Konstantin Sivkov, "Essential and Sufficient: Status-6 System Leaves an Adversary No Choice," *Voyenno-Promyshlennyy Kuryer Online (Military-Industrial Courier Online)*, 2 December-8 December 2015.
[53] S. Valchenko, N. Surov, and A. Ramm, "Russia Sends Inspector into Orbit: Military Test Operations of Maneuvering Identification and Intercept Satellite," *Izvestiya Online*, 26 October 2017.
[54] *Interfax* (in English), 12 October 2015. No author or title provided.
[55] Ibid.
[56] "On the Dialectic of Deterrence…," p. 10.

One final consideration for the future is whether artificial intelligence or quantum computer discoveries will add an unexpected type of deterrence, that being deterrence based on a capability to gaze into any adversary's cyber system. The military has invested in a host of new technologies that will enable Russia to influence events in directions they desire on the battlefield. Rostelecom will test a data transmission network using quantum technologies in early 2019, according to one report.[57]

The military has been writing about artificial intelligence since 1996, when they published such an article in *Armeyskiy Sbornik (Army Journal*). President Putin's official website noted that the main goal of a new park titled Era Technopolis is to create military artificial intelligence systems and supporting technologies. This will be a place for young scientists of technical capabilities to work.[58] Worries abound, of course, of the consequences of using artificial intelligence. For example, Russia's Deputy Speaker of the Duma stated that the speedy preparation of laws concerning artificial intelligence are needed soon. There are ethical issues to consider as well as ways to compensate for robotic mistakes or how to handle copyright laws. There will also be increased social tensions as jobs are lost to robots.[59]

The military, however, doesn't see these issues as too constraining. Deputy Defense Minister Yuriy Borisov noted that "artificial intelligence technologies will help to provide effective countermeasures in information space." "Whoever can control this [information space], whoever organizes countermeasures in the right way, is the victor."[60] As weapons and the nature of conflicts change, he notes, high-speed, high-precision, and high-performance is needed, and artificial intelligence helps provide these attributes.[61]

In September 2018 there was an added discussion of the Advanced Research Foundation and its work on artificial intelligence. The Deputy General Director of the foundation, Sergey Garbuk, said he understands artificial intelligence to be "technologies that allow for accomplishing a number of applied tasks that man accomplishes well owing to his natural intellectual capabilities."[62] Intellectual tasks are identifying shapes, processing human speech, separating objects against complex backgrounds, and predicting the behavior of complex systems. Competitions organized by the foundation so far have been dedicated to converting complex Russian speech to text, facial recognition in complex conditions, creating aerospace imagery interpretation technologies for identifying concealed structures, and technologies for the automated smart monitoring of an operator's manual operations to spot deviation from established technique routines.[63]

Information Troops

[57] *Interfax* (in English), 17 October 2018. No title or author was provided.
[58] *Official Website of the Russian Federation President* (in English), at http://en.kremlin.ru, 23 February 2018.
[59] *Interfax* (in English), 10 January 2018. No title or author was provided.
[60] No author listed, "Development of Artificial Intelligence is Essential to Conduct Cyberwarfare Successfully," *Ministry of Defense of the Russian Federation*, 14 March 2018.
[61] Ibid.
[62] Interview conducted by Igor Yermachenkov with Sergey Garbuk, no title offered, *Advanced Research Foundation*, 26 September 2018.
[63] Ibid.

Russian military expert Aleksandr Perendzhiyev, working for the Association of Military Political Scientists, noted that victory is now forged in virtual space as much as on the battlefield. Former Soviet KGB Analysis Directorate Chief Vladimir Rubanov noted that "information space realistically is becoming a sphere of military activity on an equal basis with theaters of military operations on land, at sea, and in aerospace."[64] As a result the development of information operation troops became another priority, especially since Russia felt it was lacking specific forces on the modern battlefield, where information space was playing an ever larger role.

In February 2017 this shortcoming was rectified when Defense Minister Sergey Shoygu stated that information operation troops had been created. They are, he noted, more effective and stronger than the old directorate known as counterpropaganda. Further, an information conflict class is now reportedly taught at the General Staff Academy. Shoygu stated that the troops must distinguish themselves through offensive actions, and that cyberspace is an area of responsibility for information troops. Stating that he does not intend to call hackers to arms, he still sees advanced specialists in cyber technology as "indispensable," and he also sees a mission for propaganda specialists.[65] Currently three prominent specialists have carried much of the propaganda work load for the nation, and they must be supplemented with new support mechanisms. They are, in the Foreign Ministry Information and Press Department, Mariya Zakharova; in the Defense Ministry Press Service and Information Directorate, Major General Igor Konashenkov; and in the Presidential Press Secretary, Dmitriy Peskov.[66]

Control over the activities of troops online is another area of interest to Russian military policy. The most recent law "On the Status of Servicemen" states that army personnel are forbidden to disclose on the Internet or in the mass media any information "about themselves and their colleagues which could reveal their official assignment, the details of their official activities, or their basing location."[67] Photographs, videos, and geotags on social networks were specifically mentioned. Odnoklassniki (classmates), VKontakte (in contact), and Facebook were websites and social networks particularly mentioned as those not to use. The ban does not extend to citizens who have been discharged from the Armed Forces.[68] Monitoring will also be conducted on the online activities of students at military institutes. The InfoWatch Traffic and the Device Monitor programs reportedly can detect confidential files in a stream of data as well as disloyal employees, according to Yekaterinburg-based website Znak.com.[69]

In addition to correcting these internal issues, the military's intelligence service, the GRU, has been involved in a host of influence operations abroad and there appears to be no restriction on their activities. A January 2017 edition of *Moscow Defense Brief*, titled "Russian Information and Cyber Operations," stated that the GRU's 12th Main Directorate may be responsible for

[64] Mariya Latsinskaya, Aleksandr Braterskiy, and Ignat Kalinin, "Russia Sent Troops onto the Internet: Shamanov Explained Why Information Operations Troops Are Necessary," *Gazeta.ru*, 22 February 2017.
[65] Oleg Odnokolenko, "Shoygu Orders Information Troops to Take Offensive. Military Propaganda Body Comes into Operation in the Defense Ministry," *Nezavisimaya Gazeta Online*, 27 February 2017.
[66] Ibid.
[67] Marina Yurshina, Tatyana Berseneva, and Aleksandr Kruglov, "The Secret Selfie: Military Banned from Writing about Themselves on Social Networks," *Izvestiya Online*, 23 October 2018.
[68] Ibid.
[69] No author or title listed, *Znak.com*, 23 October 2018.

information warfare and cyber operations. The same report noted that in 2012 Russia's Defense Ministry established a Cyber Command, that is, five years before Shoygu announced the development of information troops. The command's objectives were stated to be global and large-scale information operations, targeting both individual provinces and entire countries or continents.[70]

One important accusation of GRU activity was a report in *The Daily Beast* that stated Guccifer 2.0, an alleged hacker who provided WikiLeaks with stolen emails from the Democratic National Committee, was a GRU operative. Attempting to appear as a lone Romanian hacker, Guccifer on one occasion failed to "activate the VPN client before logging on. As a result, he left a real, Moscow-based Internet Protocol address in the server logs of an American social media company."[71] The IP address allowed U.S. investigators to identify Guccifer 2.0 as a GRU officer and the address (Grizodubovoy Street in Moscow, GRU Headquarters) where he worked.[72]

Information-Technical and Information-Psychological Capabilities

For at least the past 25 years, Russia has broken its information war theory into information-technical and information-psychological categories. Today, the two aspects are more integrated than ever before. For example, an information-technical cyber-attack against another nation's banking industry exposes or manipulates data about the banking industry that causes fear or even information-psychological panic in the general population. Or consider how the exposure of an information-technical achievement such as the Status-6 torpedo (now known as Poseidon), which can be nuclear armed, could have an enormous impact on the information-psychological stability of a US coastal region that could be a target of such a torpedo. They work together.

In 2015 retired Russian officers S. G. Chekinov and S. A. Bogdanov stated that, for future war goals to be successful, an information strategy is required that secures information superiority over an adversary. This can be accomplished in the media realm by stirring up chaos and confusion in a country and instilling ideas of violence, treachery, and immorality to demoralize the public.[73] Such information-psychological attacks require, from Russia's perspective, that all mass media be placed under government control and direct the main efforts in the information struggle against a probable aggressors' government and military control systems. Information superiority can even create conditions for a government to achieve its political objectives in peacetime.[74] In regard to information-technical attacks, chaos can be increased when attacks are launched against the hardware and software of an adversary's information and telecommunication environment in order to damage it.[75]

---

[70] Aleksey Ramm, "Russian Information and Cyber Operations," *Moscow Defense Brief*, No. 1 2017, pp. 16-17.
[71] Spencer Ackerman, "Exclusive: 'Lone DNC Hacker' Guccifer 2.0 Slipped Up and Revealed He Was a Russian Intelligence Officer," *The Daily Beast*, 26 September 2017.
[72] Ibid.
[73] S. G. Chekinov and S. A. Bogdanov, "The Initial Periods of Wars and their Impact on a Country's Preparations for Future War," *Voennaya Mysl'* (*Military Thought)*, No. 11 2012, pp. 26-27.
[74] Ibid., p. 27.
[75] Ibid., p. 25.

A 2017 article in the *Journal of the Academy of Military Science* in Moscow stated that hiding from the powers of influence is difficult, since they are developing both conscious and subconscious influences on people.[76] Technologies of influence are now capable of producing information-psychological and information-technical effects that outdo the effects of armament systems and hardware. The goal of information action is to redirect forces from destroying an adversary to unconditionally subjugating him. Some influence actions are equivalent to the use of military force.

Modern power, the authors add, rests on an inventory of the following means (or strategy) to wage information war realistically. They are arranged here in three groups: primary information warfare means, information support means, and the regular armed forces. All play different information-technical and information-psychological deterrent roles:

A. Primary: training groups to plan and wage information war; developing information warfare theory and a record of waging it; legal frameworks that allow for information warfare to be waged in peacetime and wartime; development of organized structures for waging information warfare; and the use of world-renowned academics.
B. Support: technical intelligence; specialized intelligence service; navigation aids; electronic warfare capabilities; information-telecommunications network development; high-speed computers and complex software; worldwide internal media centers; human rights organizations; and a movie industry, audiovisual industry, and computer (virtual) games industry.
C. Regular: strategic nuclear forces; ballistic missile defense systems; precision-guided munitions; naval forces; and special forces.[77]

Information warfare is now a preferred method of attack, since it can be used liberally while nuclear weapons cannot. New forms and methods of information's use will be applied based on 21st century technological breakthroughs. The basis for long term success will be preparing key groups of personnel for waging information warfare. Future information power will be based on preparing young people to compete in information warfare studies, specifically mathematics and physics in high schools. These topics will increase in the number of hours taught by two hours each week.[78]

The terms information-technical and information-psychological are still used widely today by officers as prominent as General Staff Chief Valeriy Gerasimov. In Gerasimov's 2018 presentation to the Academy of Military Science, for example, he noted that the roles of both information-technical and information-psychological actions are expanding.[79] At other times,

[76] V. K. Novikov and S. V. Golubhikov, "Analysis of Information War in the Last Quarter of a Century," *Vestnik Akademii Voennykh Nauk (Journal of the Academy of Military Science)*, No. 3 2017, p. 10.
[77] Ibid., p. 14.
[78] Ibid., p. 16.
[79] Valeriy Gerasimov, "The Influence of the Contemporary Nature of Armed Struggle on the Focus of the Construction and Development of the Armed Forces of the Russian Federation. Priority Tasks of Military Science in Safeguarding the Country's Defense," *Vestnik Akademii Voennykh Nauk (The Journal of the Academy of Military Science)*, No. 2 2018, p. 18.

these two aspects of information warfare are often implied but not directly stated. For example, in the 2011 document titled *Conceptual Views on the Activities of the Armed Forces of the Russian Federation in Information Space*, discussed above, the authors subdivided the definition of information war into four parts. The relationship of the parts to the information-technical and information-psychological components is obvious. The first part was confrontation designed to cause damage to information systems processes and resources, and to critically important structures (information-technical). The second was confrontation with the objective of undermining the political, economic, and social systems of Russia (could include active measures, information-technical, or information-psychological measures). The third objective was to carry out massive psychological manipulation of the population to destabilize it and the state (information-psychological). Finally, the objective of the confrontation was to compel a state to make decisions that are in the interests of its adversary (which is a reference to a component of disinformation, namely reflexive control).[80] Some recent information-technical and information-psychological observations follow.

Information-technical

The information-technical aspect of Russia's information war theory has been well covered regarding weaponry. Most weaponry today possesses some degree of information-technical quality and relies heavily on algorithm use. Such developments include cyber forces, precision-guided weaponry, satellite functions, electronic warfare equipment, radars, and numerous other pieces of equipment that employ digital components. Covered here are the information-technical systems that drive information security issues for the Defense Ministry.

There were several technological issues that help Russia ensure the acquisition of information superiority for its internal systems. In 2016, the military completed a "closed data transfer segment" communication system that is independent from the Internet. It is accessible only on special licensed computers using a Defense Ministry dedicated operating system.[81] In May 2018 it was noted that either this project or one very similar to it had "received a boost" in the form of a budget item to "provide for the creation of an integrated communications network for the needs of national defense, national security, and law enforcement."[82] Russian Communications and Mass Media Minister Nikolai Nikiforov stated in the article that it was possible to create a backup Internet infrastructure element in Russia.[83]

Other technical issues were under discussion as well. First, the Defense Ministry reported it no longer trusts the Windows operating system, relying instead on the Russian Astra Linux operating system. The Russian Federation's National Defense Operations Center is based on this system. It is envisioned that one day the system will be loaded on special smartphones and tablets. The security system includes Russian-made Elbrus, Baykal-T1, and Komdiv processors, the heart of a generation of supercomputers. It was further noted about Astra Linux that:

[80] "Conceptual Views on the Activities of the Armed Forces of the Russian Federation in Information Space," *Ministry of Defense of the Russian Federation*, 2011, p. 5.
[81] *RT Online* (in English), 13 February 2018. No author or title provided.
[82] *Interfax* (in English), 11 May 2018. No author or title provided.
[83] Ibid.

> The operating system kit includes the office application LibreOffice. The Pergament electronic document management system is used for secure communications. It is possible to install the Panorama geoinformation application to create and edit digital maps and city plans. The operating system is compatible with such popular Russian software products as the 1S accounting system and the Kaspersky and Dr. Web anti-virus programs.[84]

Second, Russia is making progress in the development of quantum cryptology systems and post-quantum cryptographic systems. They are essential for protecting information, such as future attacks generated by an adversary's quantum computers.[85] One recent report noted that Russia expects its first quantum computer to appear in the fall of 2021. It will have not less than 50 qubits, and be capable of creating more accurate weather forecasts, have the ability to crack codes and set up complex passwords, and improve predictions of new material science, engineering problems, and the properties of pharmacological drugs.[86]

Third, a park-complex known as the Era Technopolis is under construction. Its objectives include developing innovative technology, helping to reduce the time required to build arms and special equipment, and educating highly skilled personnel for military research institutes. The Technopolis is stated to work for the "Russian army elite" and is designed to ensure the nation's lead in the military-technical sphere. It is organized into three clusters, scientific-research, scientific-educational, and scientific-production. The Era Technopolis is another step on the way to reinstate central research institutes and applied research in military institutions.[87]

Russia has developed 12 different science companies, one of which is dedicated to information security. These companies include specially selected young draftees out of a university who are allowed to perform their military duty alongside experts in the field from the military-industrial complex, enabling them to learn from skilled scientists. The information security company has been working for three years. The company has several functions: it helps perform research and along with mathematicians helps validate the use of various cryptographic protocols and devices; conducts research in special communications and various kinds of electronic equipment; and conducts research along with systems programmers working in the information security field. The company allows young people to become involved in a military science environment, expand their cooperation with defense enterprises, and improve the quality of scientific work and protect state secrets.[88]

Finally, Russia's Defense Ministry had developed a closed-access "military Internet" (the term "Intranet" was not used in the article describing the system). As computerized processes have

---

[84] Aleksandr Kruglov and Aleksey Ramm, "Military Says Goodbye to Windows: Defense Ministry Will Put Russian-Produced Operating System on Service Computers," *Izvestiya Online*, 9 January 2018.
[85] No author provided, "Ministry of Defense Ponders Development of Quantum Cryptology Machines," *RIA Novosti*, 1 February 2018.
[86] Mariya Nedyuk, "A Quantum Computer Will Appear in Russia Three Years from Now. It Was Previously Anticipated that this Would Take Five Years," *Izvestiya Online*, 7 May 2018.
[87] Inna Sidorkova, "Military Skolkovo: Why Shoygu is Building a Technopolis in Anapa," *RBK Online*, 13 March 2018.
[88] Yevgeniy Miroshnichenko, "Company of Creative Thought; This Scientific Unit Has Trained Effective Personnel in the Field of Information Security for Three Years," *Krasnaya Zvezda (Red Star) Online*, 20 September 2017.

risen along with the number of information sources, such a system helps shape a safe information and telecommunication infrastructure using technology based on domestic developments.[89] The first indication of this system came in 2016, in a *Red Star Online* report:

> The deployment by the Armed Forces of Russia of a military Internet, a communications system officially named 'Classified Data Transmission Segment' (ZSPD), has been completed. The military network is not connected to the global Internet, and all computers connected to it have protections against connections to uncertified flash drives and external hard discs.[90]

Military personnel reportedly have their own electronic mail service, and the military Internet has its own websites. The networks home page is accessed at the "mil.zs" address. Access is available on certified computers, which work on the Armed Forces Mobile System. It is the State Secrets Protective Service, also known as the Eighth Directorate of the General Staff, that performs the certifications. The American example, the authors note, had many holes with different protocols and networks under different management. So many connections to the Internet allowed someone like Edward Snowden to do serious damage to the US. The Russian article stated that it is the hope of the military to avoid such damage.[91]

Later it was announced that the Russian military-industrial complex will get their own secret Internet, designated as the "Protected Communication System" (Sistema Zashchishchennykh Svyazey or SZS). Work on the system was to have been completed at the end of 2017. Both defense enterprises and science companies will use the system and be able to transmit data with at least 10 Mbps of bandwidth. Only special Astra Linux operating systems using the Armed Forces Mobile System will work on the network.[92]

Information-psychological

Information-psychological measures are discussed often in Russian military journals. These discussions rarely make front page news in the West, but they are vitally important to understanding an authoritarian regime. Military officers consider information-psychological aspects of information warfare to no longer be "add-ons" but rather as key components of waging war. The articles do not discuss what Russia is doing but rather what they believe the West is doing to Russia.

The discussion below begins with a 2015 article from the journal *Military Thought*, followed by four articles from the *Journal of the Academy of Military Science* (AMS) (one from 2014 and three from 2017), and two 2018 articles from *Army Journal*. The articles describe what Russia believes are Western attempts to destabilize Russian society's values and incite a color

[89] *Interfax* (in English), 18 September 2018. No author or title provided.
[90] Vladimir Zykov and Aleksey Ramm, "A Military Internet has Appeared in Russia: The Classified Data Transmission Segment Allows Ministry of Defense Components to Safely Exchange Secret Information," *Krasnaya Zvezda (Red Star) Online*, 19 October 2016.
[91] Ibid.
[92] Vladimir Zykov and Aleksey Ramm, "Defense Enterprises to Get Their Own Internet—Secret Technical Information to be Shared on the Protected Network," *Izvestiya Online*, 31 October 2016.

revolution there. Westerners would consider the list of methods that Russia authors state the former is using against the latter to be just what the latter is doing to the former!

A 2015 article in the journal *Military Thought* discussed the information-psychological aspect of information warfare. The authors described information as a strategic national resource that penetrates all spheres of life, making it problematic to collectively protect the security of individuals, society, the state, and its institutions. The authors defined information warfare (IW) in ways that they believe an adversary would use the concept against Russia. These ways included the use of technologies to create deliberately false information or distort existing information. Such IW use is designed to influence the civilians and servicemen of other states through the spread of information; and to damage information-related processes and systems of an adversary to achieve information superiority.[93] An information impact is achieved, they note, by distorting facts or imposing emotional perceptions favorable to the influencing side. The use of information vacuums and alien ideas are practiced, and there are attempts to involve Russia in unwanted conflicts, to induce public hatred among Russians toward their own state, or to stage a color revolution. An image of Russia is thereby produced that is tyrannical, backward, and aggressive.[94] The use of misinformation or slanted information helps promote a defeatist mood. The downing of the Malaysian airliner in July 2014 is indicative of this type of activity.[95] [Note: again, this is how Russia is interpreting events for their soldiers. As is well known, an international forum has condemned the Russian version of events and directly blamed Russia or the insurgents for the tragedy, but Russian theorists refuse to accept this proven view.].

The rest of the article was more general, describing the power behind today's use of information technology. Information's spread through the Internet and social media can destroy values, culture, and language on the one hand; or be used in systems to precisely control advanced weaponry. The authors note that the center of gravity is shifting. It no longer lies with the use of power alone but is shifting to information methods and means using covert and other subtle capabilities. War in general is becoming super technological where informatization and automated systems are now crucial to victory. Information parameters are determining the efficiency of modern weapons, especially those involved in electronic warfare.[96] Information confrontation has become so great that the period between war and peace is being obliterated. Cold Wars are gaining in scale and political effect. Information infrastructures are under constant threat of major disasters. An opposing force can now cause accidents, disorganize state governance and the functioning of financial systems, and cause defeat by merely actuating specific information or cyber components via computer networks.[97]

In the 2014 *AMS* article, three authors from Belarus described the information-psychological confrontation that was unfolding. They believe the West was victorious in the information-psychological war (portrayed as an economic and information war) in the early 1990s. They termed this to be a "new-generation" war since the confrontation rejected actual weapons. They stated that information-psychological warfare had become an acknowledged form of military

[93] I. V. Puzenkin and V. V. Mikhailov, "The Role of Information and Psychological Means to Ensure the Country's Defense Capability," *Voennaya Mysl'* (*Military Thought)*, No. 7 2015, p. 11.
[94] Ibid., p. 12.
[95] Ibid., p. 13.
[96] Ibid., p. 14.
[97] Ibid., p. 15.

art.[98] That is, they believe information can be used in indirect and asymmetric ways in strategic, operational, and tactical vectors.

The authors discussed the goals, trends, and information measures of such confrontations. First, they listed 13 ways to achieve the goals of information-psychological confrontation. Second, they listed five trends that will determine the nature of information-psychological confrontations in the next decade. Finally, when planning and implementing measures for information-psychological confrontations, they listed five principles that should guide actions.[99] The goals will be discussed further, along with trends.

The authors note that the principal goals of an information-psychological confrontation are regime change, an increase in the time to make decisions, and the means to control people. These goals are achieved via the following methods:

- changing the citizen's moral values;
- creating a lack of spirituality;
- destroying traditions and cultivating a negative attitude toward cultural legacy;
- manipulating the social consciousness;
- disorganizing systems and creating obstacles;
- destabilizing political relations;
- exacerbating political struggles and provoking repression;
- reducing information support;
- misinforming, undermining, and discrediting administrative organs;
- provoking social, political, national, and religious conflicts;
- mobilizing protests and strikes;
- undermining authority;
- and damaging interests of a state.[100]

Trends that determine the nature of information-psychological confrontations are: shifting aggression from the military-geographic domain to the information-psychological field; the role of television in initiating conflict; the influence of Western ideology on society's values; the absence of direct invasion and destruction; and the irreversibility of a confrontation's consequences.[101] The mass media's methods of manipulating TV were: blatant lies; concealing important information; immersion of information in a morass of garbage; replacement of terminology and use of unclear concepts and terms; introduction of taboos into certain sections of news; acknowledgement of the importance of images (use of well-known personalities with impact); and transmitting negative information that is perceived as better than positive news by the listener.[102] While the source of this information is from a Belarus perspective and not a Russian one, it still offers important insights into considerations of the contemporary value of information (and the article was prominently placed in the Russian Academy's flagship publication). These

[98] Iu. E. Kuleshov, B. B. Zhutdiev, and D. A. Fedorov, "Information-Psychological Confrontation under Contemporary Conditions: Theory and Practice," *Vestnik Akademii Voennykh Nauk (The Journal of the Academy of Military Science)*, No. 1 2014, pp. 104-106. Dr. Harold Orenstein translated this article into English.
[99] Ibid., pp. 106-109.
[100] Ibid., p. 106.
[101] Ibid., pp. 107-108.
[102] Ibid., p. 107.

methods also sound hauntingly similar to Western accusations about Russian media techniques, especially reports coming from the Baltics.

In the first 2017 *AMS* article, it was stated that technological enslavement had replaced military colonization as the primary method to acquire territory.[103] Manipulating people involves the creation of information and images, where the image becomes more important than the content itself. Recoding the consciousness of a population is a major aspect of the information revolution, and the object of such influence is the subconscious.[104] Here the power of narratives and meanings play a large role. Social technologies are a set of forces and means interconnected by smaller goals (psychological, informational, and ideological) aimed at achieving the stated larger goal, regardless of the interests and aims of the society and the population being acted upon.[105] Using these technologies to destroy statehood involves destroying traditions, religious norms, common ethno-cultural characteristics, networks that integrate central and regional relations, and the education system. This is accomplished with the use of hidden subversive technologies and tools for destroying internal bonds of statehood; and ensuring the absolute geopolitical domination of the aggressor state over the attacked country's state system and depriving it of economic and resource-based self-sufficiency, among other issues.[106] The author described how a color revolution, a term applied to the methods used to create regime change (in Ukraine it was called the orange revolution and in Georgia the rose revolution), is initiated:

- The socio-political and economic system of a country is destabilized, plunging it into a state of "controlled chaos."
- Conditions are created for "managed chaos" within the transformed state system to attract an opposition center.
- The aggressor focuses efforts on creating a new state system.
- Finally, the aggressor resolves that task of strengthening state institutions of the country under its control by forming, training, and equipping the power and administrative structures of the once-attacked state.[107]

In the second *AMS* article from 2017, the authors stated that the age of information warfare has become an objective reality for all nations. Information's "technological mode" stimulates diverse capabilities for information-psychological influence on people, to include the ability to move the behavior of society's consciousness in a needed direction.[108] Revolutionary situations are created in target states, which then permit regime change. The goal of information actions is to redirect the interests of the population toward unconditional subjugation. This is a multi-directional approach of a non-military character, and it can be equivalent in results to the direct use of military force.[109]

---

[103] V. N. Remarchuk, "The Destruction of the Modern State System by Means of 'Social Technologies,'" *Vestnik Akademii Voennykh Nauk (Journal of the Academy of Military Science)*, No. 2 2017, p. 46. The author would like to thank Stephen Hunnewell for his help with this translation.
[104] Ibid., p. 47.
[105] Ibid., p. 48.
[106] Ibid., p. 49.
[107] Ibid., p. 50.
[108] V. K. Novikov and S. V. Golubhikiv, "Analysis of Information War in the Last Quarter of a Century," *Journal of the Academy of Military Science*, No. 3 2017, p. 10. Dr. Harold Orenstein translated this article into English.
[109] Ibid.

More importantly, the authors list an inventory of 21 capabilities (both information-technical and information-psychological) that modern powers require in order to wage information warfare without regard for the United Nations and other world states. The inventory initially listed several branches of service but then listed several IW means: technical intelligence; specialized intelligence services; navigation aids; electronic warfare capabilities; global communication systems; and high-speed computers and complex software. Specific IW components were:

- international media centers;
- military bases abroad;
- numerous human rights organizations and human rights activities abroad;
- a movie industry and an industry to produces computer (virtual) games;
- private military companies;
- systematic training for how to plan and wage information warfare;
- a theory about information warfare and track record of waging it;
- a legal framework that allows for information warfare to be waged during times of peace and war;
- organized structures for waging information war;
- and the need to use world-renowned academics, such as Nobel laureates.[110]

Information-psychological aspects of warfare will no longer be viewed as "add-ons" but rather as key components of waging war, the authors note. It is a preferred method of attack and it will be used in training for and waging information warfare, and in scenarios. Forms and methods of its application will rely on 21st century breakthrough technologies. Training key groups of personnel for waging information warfare will be the basis for long-term success. Increasing the number of hours dedicated to mathematics and physics in high schools will provide Russia with future power in the information sphere.[111]

In the third article from 2017 in *AMS*, the authors listed the principal reasons and condition for the escalation of the information struggle to the level of information warfare. Sixteen reasons were listed, but only a few were related to information issues. They included the following information-escalation-related reasons: there has been an increase in resources devoted to influencing human consciousness and subconsciousness, with the end goal being behavior control; the hegemony of the West in nanotechnology, biotechnology, information and telecommunications technology, energy, and science as a whole on the basis of a new technical structure—information—has caused other nations to respond in kind; and the fact that information warfare can make any state vulnerable to a revolutionary situation via an integrated use of the effects of various information resources and technologies.[112] The authors, in their conclusion, noted that three categories (technical resources for intelligence; resources and technologies that produce

[110] Ibid., pp. 13-14.
[111] Ibid., p. 16.
[112] V. K. Novikov, S. V. Golubchikov, and V. V. Zakharov, "The Principal Reasons and Conditions for the Initiation and Conduct of Information Warfare," *Vestnik Akademii Voennykh Nauk (Journal of the Academy of Military Science)*, No. 4 2017, pp. 30-31. The author would like to thank Dr. Harold Orenstein for his translation of this article.

information-technical and information-psychological effects; and methods and forms for their employment) now make it possible to wage war in a nonviolent fashion.[113]

In September 2018, the journal *Armeyskiy Sbornik (Army Journal)* published an article on the topic of information-psychological warfare, which the authors labelled as a type of "undeclared war." The discussion noted that such wars have no concept of front and rear, since a country's entire population and its state apparatus are targets. The authors prioritized six strategic priorities that an opponent can use to achieve its objectives, namely, worldview, chronology, fact-based, economic, weapons of genocide, and weapons of annihilation, in that order.[114] Information-psychological effects are part of waging fourth-generation wars (4GW), whose objective is to crack open an opponent's culture code and subordinate an opponent to one's will. This strategy was used in Iraq, Afghanistan, Libya, Syria, and Ukraine by the US. Thus, again, this article, like the others, addresses what the authors view as the West's or US's strategy.[115]

Eight principles of this strategy were listed: asymmetric conflict; mobility; web site interactions; "war without rules"; chaos; special effects; autonomous or semi-autonomous combat teams; and the individualization of responsibility or "victory without management." The authors then stated that the US's Military Information Support Operations (MISO) is a 4GW strategy. The latter, they add, proposes a wide set of technologies that form MISO tactics and aim to exhaust the military and financial resources of an enemy country. These tactics include the illegal application of standards of domestic and international law; economic and political sanctions, such as organizing color revolutions, demonstrations, rallies, and so on; tactics of terror, such as the organization of rebel movements; tactics of destroying family values; and high-speed operations, such as high-tech psychological warfare consisting of the manipulation of the mass media.[116] The authors concluded the following:

> Information-psychological warfare affects the unconscious, irrational states of people, their emotions, feelings, instincts, prejudices, preconceptions, and the mythological constructs of the population of a potential enemy…This is achieved through the mass introduction to people's awareness of a multitude of false stereotypes of perception and thought, and of perverted notions about views dominating their environment as well as about events occurring in the world.[117]

For those Western analysts following Russian propaganda and media/social network manipulation, it appears these authors are discussing Russian tactics and not those of MISO.

The next issue of *Armeyskiy Sbornik* continued the discussion. The initial pages of the article continued to lambast Western propaganda, noting that the West's ideological warfare is guided by the thoughts of Goebbels; that statesmen tell bald-faced lies and express hatred toward Russia; and that you can declare anyone to be a hero, even a fuehrer called Adolph. US pilots were

[113] Ibid., p. 32.
[114] I. Sitnova and A. Polyakov, "Fourth-Generation War: Priorities, Principles of Strategy, and Tactics," *Armeyskiy Sbornik (Army Journal)*, No. 9 2018, pp. 5-8.
[115] Ibid.
[116] Ibid.
[117] Ibid.

accused of bombing schools, infirmaries, and hospitals.[118] Perhaps such vitriol is designed to support the moral-psychological hardening of soldiers toward those in the West, especially considering the restoration of deputy commanders of political affairs in the Armed Forces, as described below.

The article stated that western civilization has developed a fourth-generation weapon to be used against its enemies. The West affects people via the use of social psychology, information, and disinformation, which are multiplied by the capabilities of the Internet. The young are a target of such activities. What is required to confront the threat is a strong ideology, one that helps people understand the essence of events occurring in the world.[119]

At the end of the article, the author noted that America or the Europeans will try to prepare the consciousness of the Russian population to accept alien values and ideology. Success here will mean a faster path to a "bloodless" seizure of the state. The West, to accomplish this, must prepare the Russian population to be anti-Russian in the following way:

> First, undermine trust in state authority, plant doubt as to its legitimacy, then subject national, spiritual, moral, cultural, and social traditions to criticism, and then the mechanism of overthrowing old idols and deifying new ones is turned on. In that way the coming generation turns in time into the principal destructive force within its own country.[120]

To counteract such efforts the restoration of a strong ideology is required. The underestimation of ideology's role in bringing up Russian citizens causes concern. Ideology allows people "to gain an understanding of the essence of a particular event."[121] Without ideology, agitation, and propaganda, it is impossible to think that a future statesmen or political figure can move Russia forward. Ideology, it is noted, "represents a part of the social consciousness in which views, ideas, theories, and teachings of one class or another about society and social relations are systematized and theoretically substantiated."[122] It seems as though this is not being recalled often enough in Russia today, the author concludes.[123] To a Western mind, the author's statements are reminiscent of what was preached by Soviet commissars.

Reinstating Political-Military Officers in the Force

On 30 July 2018 President Putin appointed the former head of the Western Military District (and former head of the Chief of the Operations Directorate of the General Staff), Colonel General Andrey Kartapolov, as Russian Deputy Defense Minister and Chief of the Main Military-Political Directorate (GVPU) of the Armed Forces.[124] The directorate, a new one, indicates that Russia's military is falling back on an old system of political officers to handle the impact of nonmilitary

---

[118] V. Kutishchev, "In Order for the Enemy Weapon to Misfire…: We Continue the Conversation about Fourth-Generation War," *Armeyskiy Sbornik (Army Journal)*, No. 10 2018, pp. 10-16.
[119] Ibid.
[120] Ibid.
[121] Ibid.
[122] Ibid.
[123] Ibid.
[124] *Interfax* (in English), 30 July 2018. No author or title provided.

trends (social media, etc.) on a soldier's morale. The development of a strong patriotic education in soldiers is required in the opinion of the Ministry of Defense. Kartapolov will be working to improve the moral and the psychological stability of servicemen through the directorate.

In 1991 Russia's military political headquarters was named the Main Military Political Directorate of the USSR Armed Forces, tasked to work on the morale and psychological state of servicemen. In 1992 the directorate was renamed as the Main Administration/Directorate for Personnel Work. However, over two decades later it has been deemed inappropriate to handle the many issues that now complicate the life of young servicemen, such as their access to information on the Internet.

In February 2018 the idea of creating a Main Administration for Political Work was proposed. The rationale for the new proposal was that Armed Forces personnel need an explanation regarding the levers of cyber-systems and information-propaganda being used against them to undermine their moral character[125] and discredit the image of Russia, part of what some see as a global information and psychological confrontation. The administration would be an expanded version of the Main Directorate for Personnel Work (*главного управления по работе с личным составом* [ГУРЛС or GURLS]). GURLS organized education activities, emotional and psychological support, and discipline work. It facilitated state-patriotic education of personnel, implemented measures for the social protection of servicemen, organized cultural and leisure-related work, and coordinated interaction among various agencies and religious associations.[126] Subordinate to the organization is the Russian Federation Armed Forces Center for Military Patriotic work, the Russian Federation Armed Forces center for Psychological Work, and the 49th Equipment and Facilities Center.[127]

An August report stated that the new Main Military-Political Directorate will affect the Defense Ministry's mass media system. The question asked was whether the military newspapers of the military districts and fleets should be transferred to the new organization. This would ensure complicity of tasks and goals across the military. Only the main military newspaper, *Krasnaya Zvezda (Red Star)* would remain independent of military-political entities.[128]

In early September 2018 Kartapolov noted that the protection of soldier's patriotism is needed because there is an undisguised information war being conducted against Russia, composed of propaganda, deception, and the suppression of Russia's point of view, which can change society's conscience and have serious consequences.[129] He did not, however, offer any examples.

---

[125] No author listed, "An Expert Has Defined the Mission of the Armed Forces' Military-Political Directorate," *RIA Novosti*, 30 July 2018.
[126] No author listed, "Source: The Defense Ministry is Planning to Revive the Main Political Directorate," *RIA Novosti*, 5 February 2018.
[127] No author listed, "Main Military Political Directorate Set Up at Ministry of Defense. Colonel General Andrey Kartapolov Appointed as Chief of Directorate," *TASS*, 30 July 2018.
[128] Aleksey Ramm, Aleksandr Kruglov, Bogdan Stepovoy, and Roman Kretsul, "Directorate of Patriotism: Main Military-Political Directorate is Being Established in the Defense Ministry and in Other Security Departments," *Izvestiya Online*, 1 August 2018.
[129] Sergey Valchenko, "Political Workers Will Teach Soldiers to Love the Homeland and Will Defend It from Information Subversion. The Main Political Directorate Chief: 'No Commissars or Lenin Rooms Whatsoever,'" *MK Online* 5 September 2018.

He added that the military-political agencies will work with the population as well as the military, in particular with the youth and younger generation. One of the reasons for reinstituting the Main Military-Political Directorate, he observed, were the shortcomings observed during the conflict in Syria. He stated that "We saw that in the phase of the accomplishment of combat mission, those methods, techniques, and forms, which were set forth in the system, did not fully operate and were not as effective."[130] He identified a shortcoming in what he termed the "socio-state training programs."[131]

Kartapolov noted that the administration is similar to its Soviet predecessor but minus the communist party component. The Soviet system developed methods, modes, and forms of conveying important information to soldiers. The content will be different from Soviet times, but the forms and methods will remain the same. This is needed to confront the information war around Russia and the alteration of society's political consciousness, according to Kartapolov. It offers information protection for personnel and molds servicemen with a firm conviction of the necessity to serve the Fatherland.[132]

The ideological base will be the history of Russia, the cultural tradition of its people, and the conviction that Russia must live and develop. A main cathedral for the Armed Forces is being built that will be a training center for military clergy. Belief in God and belief in the cause of service to the motherland are very close, and chaplains can mold a soldier's belief in God and political officers will mold belief in the country and the rightness of his cause. The latter must also work with social networks, as the tablet must become the political worker's weapon. Subordinate to the administration are two suborganizations, the Culture Department and the Directorate for Work with Citizens' Appeals.[133]

There are three stages to forming the military-political agencies. Phase one is the formation of the Main Military-Political Directorate, which was to be completed as of 1 October 2018, including the recertification of current employees. The second stage was to be completed by 1 December 2018, when a system of military-political agencies is formed. The third stage will be completed sometime in September 2019, when a system of cadre training is complete. Cadre will be focused on a particular branch of service or combat arm. Work with individuals will replace working with groups. In the end, priests and political-workers will be at the front, in the trenches. Psychologists are planned to be military and not civilian personnel, and it is even possible to have political officer positions at the platoon level. It is envisioned that the position of deputy commander for military-political work must become a desirable step to molding future major military commanders.[134] The role of the clergy will be expanded as well, with Kartapolov noting that the church will be called upon to serve as a center of spiritual education and as a center of historical enlightenment.[135]

---

[130] Ibid.
[131] Ibid.
[132] Viktor Demin interview with Andrey Kartapolov, "Kartapolov— 'We Will Borrow the Best from the Soviet System, But We Will Change the Content," *Zvezda (Star) TV Online*, 10 September 2018.
[133] Demin, Ibid.
[134] Ibid.
[135] Mariya Tomilenko, "To Strengthen the Army's Spirit," *Krasnaya Zvezda (Red Star) Online*, 7 September 2018.

In November 2018, it was reported that company deputy commanders for political affairs were posted in motorized rifle companies, and they will report directly to company commanders. They will have numerous duties:

- Instill in subordinates a deep understanding of the state's policy in guaranteeing defense;
- Developing in servicemen patriotism and loyalty to military duty and the military oath;
- Be responsible for professional training and ideological convictions
- Understand their direct subordinate's allegiance to religious confessions, individual psychological, emotional, political, and military-professional qualities and special traits;
- Ensure that no drugs are used, or excessive liquor consumed;
- Maintain contact with relatives and friends of soldiers and sergeants performing draft service;
- Organize leisure activities and amateur performance groups;
- Prepare weekly reports about distinguished servicemen for the formation's newspaper, radio newsreel, and wall news display;
- Instill in soldiers' confidence in their weapons and readiness to perform combat tasks in any conditions;
- Identify soldiers with a bad attitude and set them on the true path.[136]

New equipment will be supporting the military-political directorate. Recently Russia announced the fielding of a multimedia all-terrain vehicle that has educational and psychological warfare potential. Each military district is to receive two mobile multifunction information systems (PMIK). It is a van that carries multimedia equipment for "educational" work and leisure activity organization. The vehicle can also produce combat news bulletin leaflets, newspapers, rule booklets, and so on in electronic form. Digital products can be disseminated via a Wi-Fi network.[137]

It was noted above that the second stage in forming military-political agencies would be completed by 1 December 2018. Kartapolov stated on 19 December that structures subordinate to the Military-Political Directorate are the Defense Ministry Department of Culture and its organizations and institutions (the Central Museum of the Armed Forces, the Central Academic Theater of the Russian Army, the Central House of the Russian Army, and all creative teams) as well as the Defense Ministry Directorate for Work with Citizens' Appeals. In the same interview Kartapolov discussed the development of the Main Temple of the Armed Forces. It would honor

[136] Aleksey Ramm, Aleksey Kozachenko, and Bogdan Stepovoy, "The Main Military-Political Directorate Will be Responsible for the Climate: Company Deputy Commanders for Political Affairs are Back in the Army: the First Political Officer Posts Have Been Created in the Armed Forces," *Izvestiya Online*, 8 November 2018.
[137] Aleksandr Kruglov and Aleksey Ramm, "Military Educators Have Received Multimedia All-Terrain Vehicles. Advanced Technologies are Being Used for Informing Soldiers and Organizing their Leisure Activities in Field Conditions," *Izvestiya Online*, 11 March 2018.

the victory in the Great Patriotic War. A unique complex in the temple's precincts will be called the "Road of Memory" with photos of Muslims, Christians, Jews, Buddhists, and others.[138]

As noted earlier, regarding the restricted use of social networks, the Defense Ministry has recommended that servicemen not only stop using social networks such as Odnoklassniki, VKontakte, Facebook, and others but also to switch off geolocation services on mobile phones and abstain from Internet posts. Officials warn that foreign intelligence services monitor user data, which could lead to operational failure. Soldiers were asked not to post inappropriate interethnic or interfaith messages, and relatives of soldiers were asked not to circulate information about the service activities of their soldiers.[139] Instead of smartphones, officers and servicemen have been advised to use push-button phones that do not have photo or geolocation capabilities but can send SMS messages.[140]

A final point of note is that the November 2018 issue of *Armeyskiy Sbornik (Army Journal)* contained a long article on the military-political teaching plan for the year. It covered specific topics for officers, soldiers who entered the Armed Forces via contracts, and soldiers who were drafted.[141]

OLDER CONCEPTS STILL IN VOGUE

The information age, as demonstrated above, is full of new means for confronting or deterring an opposing force. However, there remains in the Russian road map a strong desire to implement several thoughts that first germinated in the 1990s but were never approved by an international organization. There were several presentations that Russia made at the United Nations in regard to rules and regulations that it felt nations should be required to follow in the information age as well as definitions of specific terminology. At the time it appeared to U.S. representatives that such terminology requirements would be designed to limit what the U.S. could do and so no agreement was ever reached.

Russia's military has continued to discuss topics similar to those they first advanced in the UN in their official documents. Two important documents are discussed here. The first is a 2011 document on information space. The second is an update of information-related concepts in the 2014 Military Doctrine of Russia, the latest it has written at the current time. It offered their view of information space in a 2011 document and several thoughts were updated in the 2014 military doctrine. Supporting these views was General Major Igor Dylevskiy's presentation at the 6th International Security Conference in Moscow in 2018. His presentation, also summarized below, demonstrates the continuity in Russian information goals over the past 25 years.

---

[138] Aleksandr Pinchuk, "Political Officers Called on to Stand Alongside Soldiers," *Krasnaya Zvezda (Red Star) Online*, 19 December 2018.
[139] Aleksandr Kruglov and Bogdan Stepovoy, "Soldiers and Officers Have Been Taught How to Communicate Safely on the Internet," *Izvestiya Online*, 13 February 2018.
[140] *Interfax* (in English), 16 February 2018. No author or title provided.
[141] No author provided, "Instructional Plan for the Military-Political Preparation of the Armed Forces of the Russian Federation in 2019," *Armeyskiy Sbornik (Army Journal)*, No. 11 2018, pp. 91-101, as downloaded from https://dlib.eastview.com on 16 January 2018.

Conceptual Views of the Activities of the Armed Forces of the Russian Federation in Information Space (CV) 2011

This is the first official document from the Russian Ministry of Defense that discusses the emergence of a global information space, defined as "The sphere of activity related to the generation, development, conversion, transmission, use, and storage of information, which influences *inter alia* the individual and public consciousness, the information infrastructure, and the information itself."[142]

The *CV* defines the terminology, principles, rules, and confidence-building measures of information space from the military's point of view, adding that in the Russian Armed Forces an "integral system has now evolved which is designed to ensure effective deterrence, prevention, and resolution of military conflicts in information space."[143] Unfortunately Russia often violates many of the principles and rules it lists.

Principles: The principle of legality notes that the RF is guided by the norms of international law which calls for abiding by respect for national sovereignty (in Crimea and Donbass Russia did not abide by this point), non-interference in the internal affairs of other states (hacking in most European countries nullifies this point), and non-use of force or the threat of force. International humanitarian law limits the indiscriminate use of information weapons (the latter are defined in the CV as "information technologies, systems, and methods used to wage information warfare") and the prohibition of treacherous methods of waging information warfare.[144] Other principles are as follows:

- A "priority" principle is to collect relevant and reliable information regarding threats as well as the protection of information resources.[145]
- The "integration" principle attempts to utilize all resources, to include staff activities and troop operations involving intelligence gathering, operational deception, electronic warfare, communications, secure and automated command and control, staff information work, and the protection of information systems against all types of effects.[146]
- The "interaction" principle coordinates the work of federal executive bodies.
- A "cooperation" principle aims to create a regime of international law that governs, among other things, military activities of states in the global information space.[147]
- Finally, the "innovation" principle simply seeks out highly skilled personnel to resolve information security problems.[148]

[142] "Conceptual Views on the Activities of the Armed Forces of the Russian Federation in Information Space," *Ministry of Defense of the Russian Federation*, 2011, p. 5.
[143] Ibid., p. 4.
[144] Ibid., pp. 6-7
[145] Ibid., p. 7.
[146] Ibid., p. 8.
[147] Ibid., pp. 8-9.
[148] Ibid., pp. 9-10.

Rules: The first rule is associated with "deterrence and conflict prevention." This rule should include a system:

- To deter conflicts in information space;
- Keep resources in a state of readiness to confront information space threats;
- Organize cooperation among partner states;
- Conclude a UN treaty on international information security;
- Take measures to detect early conflicts in information space;
- Control factors over the escalation of a conflict;
- Counter conflict developments;
- Prevent conflict from spreading;
- Neutralize factors leading to conflict;
- And explain causes and origins of conflict to the international community.[149]

The second rule is about conflict resolution. Conflicts are to be decided through negotiations and reconciliation, are to be prevented whenever possible, and are to exercise individual or collective self-defense rights in a crisis phase in information space. Retaliatory actions are to be determined taking into account other states security, forces are to be deployed on other state's territories in accordance with international law, and Russian and foreign media are to be kept informed of the evolving situation.[150]

Confidence-building measures: These measures include exchanging concepts for ensuring security in information space, exchanging information about crisis events and threats in information space, and consulting on issues of concern to the parties.[151]

***Military Doctrine* 2014**

This document noted several ways that information had become important. Two external information trends were noted, one a shift of military dangers and military threats into information space; and the other the use of information and communication technologies for military-political objectives, such as carrying out actions that contradict international law and aim at the sovereignty, political independence, and territorial integrity of states.[152] Internal information dangers included attempts at disorganizing not only the functions of state authorities but also the information infrastructure of the Russian Federation; and activities that have an information effect on the population, above all on the young, for the purpose of undermining the historical, spiritual, and patriotic traditions of Russia.[153]

[149] Ibid., pp. 10-12.
[150] Ibid., pp. 12-13.
[151] Ibid., p. 14.
[152] "Military Doctrine of the Russian Federation," *President of Russia website*, 26 December 2014, sections 11 and 12l.
[153] Ibid., sections 13a, 13c.

The doctrine noted that features of modern conflicts were the integrated use of force and information and other nonmilitary measures; the use of information management systems; and the ability to impose a simultaneous effect on the enemy to the full depth of his territory in global information space.[154] In order to deter conflict, state of the art information technologies are required to lower the risk of information and communications technologies being used for military-political objectives in contradiction to international law and the sovereignty of nations.[155] With regard to military organizations, information interaction among federal executive authorities and others is required; and information security systems must be upgraded.[156] Finally, with regard to armaments, information confrontation forces and assets must be developed; information exchange systems must be upgraded so that Armed Forces information space is unified with Russian Federation information space; and information-control systems must be created and integrated with fire control systems and automated command and control entities of strategic, operational-strategic, operations, operational-tactical, and tactical scales.[157]

The doctrine deemed it necessary to develop a dialogue with other nations on their approaches to opposing military dangers and threats. In this way large-scale use of information and communications technologies for military-political purposes could be spotted before they rise to a point where conflict is inevitable.[158]

General Major Dylevskiy's Presentation at the 6th Moscow International Security Conference

General Major Dylevskiy is well-known for his multiple articles in *Military Thought* on Russian and US information operations. He is someone who understands Russia's position and focus well. His 2018 presentation at the International Security Conference was in many respects a reiteration of points that Russia has been making about information technologies either since the early 1990s at the United Nations (UN) or after "color revolutions" that transpired around the world after 2000. The presentation contained three basic points of discussion. The first was his concern over regimes being overthrown with modern technologies. He noted that disinformation, extremist statements, racist flash mobs, and cross-border computer attacks on critically important facilities can cause social explosions. Technologies can have the ability to produce information-psychological influence and result in color revolutions. Of great interest was his comment that informational-psychological influences resulting in color revolutions are "far more destructive for a country's economy, social sphere, and other spheres of vital activities than those that result from the destruction of individual critically important facilities."[159] It is surprising that his comments would underscore the importance of information-psychological actions. It can take months or years to change someone's information-psychological character, whereas destroying a critical facility

[154] Ibid., sections 15a-c.
[155] Ibid., sections 21a, 21s.
[156] Ibid., sections 35b, 35j.
[157] Ibid., sections 46c, 46d, and 46g.
[158] Ibid., section 55f.
[159] Unattributed transcript, "Theses from a Speech by Major General Igor Dylevskiy, Deputy Chief of the Russian Federation Armed Forces General Staff Main Operations Directorate, at the 6th Moscow Conference on International Security," *www.mil.ru*, 5 April 2018.

can be accomplished in a matter of minutes or hours once a decision is made. Russia's focus on information-psychological activities appears to border on paranoia at times, as the discussion of Russia's perception of the West's information-psychological advances against Russia was described earlier.

Dylevskiy's second point of discussion was his focus on special information technologies, resources, and methods that are termed information weapons. Discussions of information weapons and attempts to control them have been examined in Russia for many years. The Shanghai Cooperation Organization offered the definition of information weapons above. Such weapons can: establish oversight over an opponent; interfere in the operation of an opponent's automated systems and certain types of arms; influence armed forces' command and personnel; and influence the population.

The third point of discussion was Dylevskiy's request for additional laws to reduce the likelihood of information weapons being used in an attack. In particular he asked if Article 51 of the UN charter allowed for the right of self-defense or collective defense in case of an information attack. However, there is no definition, he noted, of an international law term "armed attack involving the use of information weapons." Further, if an attacker is a person not acting under orders from a state structure but as a terrorist, extremist, or mercenary, then they cannot be regarded as a source of an armed attack as the UN now defines it. Thus, at the moment, there is no clarity as to whether there is a basis for carrying out retaliatory attacks using information weapons against an undefined or unclear source of an information attack.

Dylevskiy expanded his presentation with a discussion of the information sphere, which has no defined borders as the physical environment does. Russia's *Information Security Doctrine* notes that the information sphere comprises the

> Sum total of information, hardware and software facilities, information systems, Internet websites, communication networks, information technologies entities whose activities are connected with forming and processing information, with developing and using those technologies, and with guaranteeing information security, as well as the aggregate of mechanisms for regulating the corresponding social relations.[160]

However, both traditional weapons and information technologies can impact information-sphere assets. Such impacts should be considered an act of aggression and qualified as an infringement of another state's sovereignty, he notes. Again, however, this depends on an identification of the source of the attack. Finally, he discussed a state's responsibility for the use of information weapons. Here he again cites a lack of law, since combatants are no longer just the armed forces of two states but could be defined in numerous categories (private armies, terrorists, insurgents,

[160] Ibid.

etc.) of combatants. A definition of a combatant operating in information space needs to be made in accordance with an international law methodology.[161]

This is not the first time that Dylevskiy had discussed these issues. In 2015, for example, he and four other information experts described what they felt was needed to assure information security. They covered many of the same issues that Dylevskiy would discuss in his 2018 address. Initially the authors blamed NATO and the US for information being used by terrorists to train and recruit people, for the use of information as a weapon against Iranian nuclear facilities, and for the use of information as a subversion technique that generated "color revolutions" that overthrew leaders.[162] The authors promoted the concept of an "information weapon nonproliferation regime" as a result. They also noted that there are numerous technical and legal issues to solve.[163]

Information weapon varieties that the authors listed to be curtailed in 2015 were:

> Electromagnetic weapons (radio jammers, electromagnetic pulse weapons, and directed energy weapons); software weapons (computer viruses, computer works, Trojan programs, hidden management utilities, and so on); and hardware weapons (bookmarks to permit unauthorized access to computer information, download and transmit it to an addressee, and mount attacks against computer networks to modify or destroy information stored and circulating in them).[164]

An international information weapons nonproliferation regime was defined as follows:

> A system of patterns, principles, norms, rules, and procedures for preventing the proliferation of information weapons codified in international agreements and national laws, and also international and national agencies involving all members of the world community and nongovernmental organizations. They have total prohibition of information weapons as their end goal.[165]

The rest of the article focused on the need for dialogue, confidence building measures, exchanging national concepts of security assurances in the information environment, prompt exchange of information about critical events, and consultations on information environment activities. The principle of equal and inseparable security of all member of the world community should also be upheld.[166]

Conclusions

There are many items associated with the information age that one cannot see. While electrons running through wires are the most invisible in terms of both intent and location, other

[161] Ibid.
[162] I.N. Dylevsky, V. P. Elyas, S. A. Komov, A. N. Petrunin, and V. O. Zapivakhin, "Military-Political Aspects of the State Policy of the Russian Federation in the Area of International Information Security," *Voennaya Mysl'* (*Military Thought)*, No. 1 2015, pp. 11-12.
[163] Ibid., pp. 12-13.
[164] Ibid., p. 15.
[165] Ibid.
[166] Ibid., p. 16.

information resources or components, perhaps hidden by location or in the development stage, only become apparent after their expression and discovery in new armaments. While General Staff thinking is available in some instances, for the most part it remains hidden as well.

Western analysts will need to follow closely Russian future war forecasts, developments in military art, and the formation of information-related forms and methods of warfare. Thought is always the first to enter battle and Russia's military encourages creativity and innovation in military art.

Another important area of concern is Russian thoughts on the IPW and an evolving interest in planetary warfare. First, Russian hackers appear to be involved in trying to place malware in the circuits of a broad swath of nations in Europe and North America. There is hardly a nation in either that has not been touched. Success in planting malware helps assure information superiority in times of conflict and allows Russia to maintain an advantage in the IPW. It offers opportunities for the initiation and application of a concept such as SODCIT in times of conflict. The information age has offered Russia's excellent and talented group of algorithm writers a leg up in surveilling and reconnoitering other nations systems, especially when backed by an authoritarian regime. Second, in regard to planetary warfare, while the concept is seldom mentioned (Chekinov and Slipchenko may be the only ones to mention the idea specifically to date) Russian declarations of information, space, and oceanic theaters of military operations signify a planetary interest in planning, as does Russian interest in the global information space. Satellites and cables enable nations to reach out and touch another nation on the other side of the globe with precision and force as never before.

Some of the items listed in this overview were suggested in Russia's 2016 *Information Security Doctrine*, a political directive. Five initiatives in the document offered ways to ensure information security in the defense arena. These initiatives were: strategic deterrence and preventing military conflicts originating from the use of information technologies; improving the system of information security, to include information warfare forces and assets; forecasting, detecting, and evaluating information threats; protecting RF interests in information space; and neutralizing information and psychological attacks.[167] All of these items have been developed further, as the discussion above indicates.

Thus, Russia's current approach to contesting or controlling the multi-dimensional information environment is expansive. It is a mixture of old and new strategies. Overall, it is fair to say that Russia's military is keeping in step with new advances in scientific achievements and how they can be used in weapon applications. Some uses are deceptive while others are opaque. There is much to be on guard against, both seen and unseen.

Information strategies now in use include updated reflexive control mechanisms, new disorganization planning, indirect and asymmetric uses of nonmilitary activities, and new and creative uses of military art. Russian theorists have developed different varieties of information deterrence (media, legal, satellite inspections, etc.) to keep adversaries at bay. Such work indicates

[167] "Information Security Doctrine of the Russian Federation," *President of Russia Website*, Edict No. 646. Dated 5 December 2016.

that the Defense Ministry intends to employ all types of information resources to help deter any opponent from infringing on what Russia determines to be its territorial sovereignty, whether it be former USSR territory or new resources in the Arctic. Russia supports such efforts with information troops.

Russian information operations have long been broken into information-technical and information-psychological subsections, and this tendency continues. The former can have an offensive or defensive technical character and is associated not only with information systems but also with the components that enable precision-guided and other types of weaponry. The information-psychological aspect is more specifically designed to warn and protect military personnel and the population from information-psychological offensives that potential adversaries might conduct. The Defense Ministry is clearly worried that its soldiers could be influenced by adversaries, almost to the degree of paranoia. Otherwise, why would they have decided to reinstitute its tradition of a military-political officer directorate, which is charged with protecting the moral and patriotic fervor of servicemen.

It should be noted that the military's 2011 *Conceptual Views* and 2014 *Military Doctrine* (the latest doctrine) offered some of the more traditional guideposts and terminology. These views were supported by the 2018 presentation of information warfare expert General Major Dylevskiy, making it clear that Russia has not given up on pursuing old goals while developing new ones.

Russian theorist Sergey Chekinov noted the following in 2010:

> The dialectical development of modern armed struggle processes is a reason to argue that the information component of armed struggle will be given a greater weight in 21st century wars. Its significance will rise because the troops will be supplied with weapon systems based on wide-scale employment of information technologies, quick-acting reconnaissance and communication systems, automated troops and weapon control systems, electronic warfare systems, and so on.[168]

Chekinov's thoughts, and those of others, correctly forecasted some of the changes that information technologies would bring. This paper attempted to bring the impact of those and other information components to the forefront. It appears that Russia is using technologies and working in peacetime to "prepare to deter" by implementing its IPW and disorganization theories and working to achieve new forms and methods of employing information-aided military art to gain the initiative in potential conflicts. It continues to research the use of nonmilitary information power as well. What is important is understanding how Russia's military thinks about future conflict and how it will apply its theories. All in all, there is much to contemplate and work to be done by the West if it is to comprehend just what Russia is up to.

[168] Chekinov, "Predicting Trends…"