REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
01/01/2020	Technical Report	

4. TITLE AND SUBTITLE
Information Weapons: Russia's Non-Nuclear Strategic Weapons of Choice

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

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Thomas, Timothy L.

5d. PROJECT NUMBER
072S120-J3

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-20-0235

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
United States European Command

10. SPONSOR/MONITOR'S ACRONYM(S)
USEUCOM

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
Information weapons (IWe) have a comprehensive meaning in Russia that encompasses both strategic and operational applications. IWes are considered as a non-nuclear strategic weapon that has the capability, with its cyber and precision-weaponry components (among others), to conduct the economic, social, or physical disorganization or destruction of an opponent's infrastructure or normal operating procedures and induce deterrence without the use of nuclear weapons or groundbased forces. Different in scope and application from the Western understanding, Russia's IWe concept is thus worthy of closer examination.

15. SUBJECT TERMS
Information Warfare social disruption; infrastructure; cyber manipulation; information weapons; economic disruption;

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE		27	Susan Carpenito
					19b. TELEPHONE NUMBER *(Include area code)* 781-271-7646

MITRE

Sponsor: USEUCOM ECJ39
Det. No.: P663
Contract No.: W56KGU-18-D-0004-S120
Project No.: 072S120-J3

The views expressed in this document are those of the author and do not reflect the official policy or position of MITRE, the Department of Defense, or the US government.

Approved for Public Release, Distribution Unlimited. Public Release Case Number 20-0235

©2020 The MITRE Corporation.
All rights reserved.

McLean, VA

Information Weapons: Russia's Non-Nuclear Strategic Weapons of Choice

Author: Timothy Thomas

January 2020

Executive Summary:

Information weapons (IWe) have a comprehensive meaning in Russia that encompasses both strategic and operational applications. IWes are considered as a non-nuclear strategic weapon that has the capability, with its cyber and precision-weaponry components (among others), to conduct the economic, social, or physical disorganization or destruction of an opponent's infrastructure or normal operating procedures and induce deterrence without the use of nuclear weapons or ground-based forces. Operationally, IWes can affect tactical decision-making and cause chaos in planning. Three goals that are pursued include the development and use of IWe; the ability to limit other nations access to IWes (from the 1990s to as late as 2015 Russia was pressing for the adoption of universal laws or resolutions to prohibit the development of IWes) and to defend against their use by other nations; and the use of IWes to influence and manipulate others. Russians note that IWes universality, covertness, the variety of the forms of software and hardware implementation, radicalism of effects, adequate choice of time and place of employment, and, finally, cost effectiveness make them formidable assets. The Kremlin remains obsessed with confronting what it considers to be Western IWes developments and organizations. Such elements include nonlethal weapons (NLW), which Russia is also pursuing, nongovernmental organizations (NGO), so-called color revolutions, and other factors not normally associated with IWes in the West. These concerns are further advanced due to the Kremlin's paranoia and suspicion of the intentions of others to use IWes. Russia's military is as concerned with the development of IWes as is the Kremlin, pointing out that two issues will determine the outcome of future conflicts: gaining information superiority in the initial period of war and processing information faster than your opponent, making IWes crucial to success. General Staff Chief Valery Gerasimov has noted that information resources have essentially become one of the most effective types of weapons, which continue, from the military's viewpoint, to be broken into information-technologies (those embedded in weaponry) and information-psychological developments (those that assist in the development of influence operations). Military sources have discussed the former in regard to the development of information-strike, precision-guided, electronic, and theater IWes. With regard to the latter, the military has investigated how to manipulate objective reality through the use of the media and more exotic weapons (psychotronic, whose use is suspect) that exert an effect on a person's mind and subconscious; cyber manipulation via trolls and bots; neuro-linguistic programming; and disinformation, fake news, and propaganda, all designed to manipulate public opinion. They can cause an opponent to make "unconscious decisions" that are advantageous to the other side, an idea that mirrors Russia's reflexive control concept. One astute Russian military theorist also noted that information has had such an enormous impact on military leaders that it has changed "Napoleon's Square" (based on will and brains) to a cube (will, brains, informatics) for decision-making and planning (which is important for systems versus systems warfare thinking). Different in scope and application from the Western understanding, Russia's IWe concept is thus worthy of closer examination.

Introduction

For many years now, Russia has defined and even expanded on its concept of "information weapons (IWe)."[1] At one point there was an attempt to get the concept introduced into United Nations resolutions, which was a way at the time to guarantee Russian information and national security. This occurred in the 1990s, when Russia was at its weakest and unable to compete with other nations in information warfare capabilities. Russia's information warfare weakness was so pronounced that at one point it caused a prominent Russian scientist to state the following at an international conference in Moscow in 1995:

> In studying the potential catastrophic consequences from an enemy's use of strategic information warfare systems on, for example, the economy or government control…we must unequivocally declare that in the case of their use against Russia, we reserve the right to conduct a first strike (nuclear) against the information warfare system and forces which are directing that weapon, and then also against the aggressor-government.[2]

This unambiguous warning was intended to send a message to other nations, and it served its purpose well. Don't mess with Russia if you want to keep Russia from messing with you.

Since the revival of Russia's military prowess, a variety of its authors have continued to focus on information-related topics, to include the following: information warfare, information struggle, information resources, information confrontation, information sphere, information field, information effects, information superiority, information security, and, in line with the focus of this article, IWes. At times IWes address the information-related technologies used in precision-guided and reconnaissance type weaponry, and at other times IWes are presented more simply as a weapon that helps in the manipulation of social media and propaganda. Seldom does the West consider information to be a "weapon" as Russia does, nor does the West break the term into information-technical and information-psychological aspects.

The information-technical aspect of IWes includes information technologies that are used extensively by Russia and many other nations in global positioning, reconnaissance, electronic warfare, and other types of equipment worldwide. The information-psychological aspect refers not only to Russia's use of information as an online weapon in the social and political arenas, which has become unsettling to Western audiences, but also to Russia's use of disinformation, fake news, nongovernmental organizations, and a tendency to define objective reality as the Kremlin sees fit and avoid "the truth." Their use appears to be a modern version of Soviet active measures, which were operations developed years ago in Section A of the First Chief Directorate of the KGB. Their aim was to shape operations abroad and influence events in another country and were often referred to as political warfare. Related terms were "assistance programs" or "assistance operations," tactics designed to change the policy or position of a foreign government in a way that would "assist" the Soviet position. A Russian foreign intelligence officer who defected to the U.S in 2000

[1] The IWe acronym is used to distinguish the term from information war and irregular war, which are both shortened to IW and cause enough confusion without adding another IW acronym.

[2] V. I. Tsymbal, "The Concept of Information Warfare," presentation at a September 1995 conference in Moscow, Russia, p. 7, attended by the author of this article.

noted that there is no difference between "active measures" and "assistance operations," and that when the KGB went away after the demise of the Soviet Union, the active measures office was renamed to assistance operations. Active measures reportedly were based on 95 percent objective information "to which something was added to turn the data into targeted information or disinformation."[3]

Thus, a Russian information weapon must be considered for its utility in weaponry, in political and psychological warfare, and in the use of the media; and as a non-nuclear strategic weapon of choice. This article will examine several Russian views of IWes that cover these aspects, beginning with the bigger picture of an IWe as a strategic weapon. That discussion is followed with an overview of the Russian military literature that addressed IWes over the past two decades. The discussion includes theater information weapons, information-strike weapons, cyber weapons, and social-media weapons, among others. The analysis then shifts to a very brief discussion of two items: first, other ways to consider an IWe (as the overt rejection of the truth and as its use as an information deterrent) and second, an example is offered of a Western analyst's thoughts on how to counter media-related IWes. The analysis concludes with a very brief look from one Russian specialist about the next generation of weapons, quantum computing and artificial intelligence concerns. A list of Russian definitions of IWes from different time periods is located at the Appendix.

First the Big Picture: IWes as a Non-Nuclear Strategic Weapon

IWes appear to be considered as a non-nuclear strategic weapon in Russia since their reach is wide, even to continents far away (a planetary weapon) and, according to Russian new-generation warfare expert Vladimir Slipchenko, is based on a shift from a "quantitative-force sphere to a quantitative-intelligent sphere."[4] He added that countries are creating "strategic non-nuclear forces, which will find wide use in new-generation wars and subsequently also will take on a deterrence function."[5] There are numerous weapons that depend on information technologies. Acoustic, electromagnetic effect, radiation, beam, and heat weaponry[6] are under development as is the "unity of intelligence collection and destruction," namely the development of reconnaissance-strike and reconnaissance-fire complexes.[7] The development of space groupings, in Slipchenko's opinion, will be a key direction as forces transition from a ground-based force to one based on aerospace and information. Intelligence collection from space will provide information that "will become the basis for planning massive high-precision strikes in the course of a strategic air-space-sea strike operation."[8]

Slipchenko's thoughts appear to coincide with a Russian concept known as the strategic operation to destroy critically important facilities (SODCIT). Numerous outlets have discussed the term. In 2010, a *Red Star* article noted that changes in the nature of wars would be reflected in the

[3] Andrei Soldatov and Irina Borogan, *The New Nobility*, Public Affairs New York, 2010, pp. 108-109.
[4] V. I. Slipchenko, *Beskontaktnye Voyny (Noncontact Wars*), Publishing House Gran-Press, 2001, p. 55.
[5] Ibid., p. 82. Slipchenko wrote on new-generation warfare more than a decade before Bogdanov and Chekinov did so in 2013, to great fanfare.
[6] Ibid., pp. 85-88.
[7] Ibid., pp. 90-91.
[8] Ibid., p. 161.

various forms in which the Armed Forces are used. The author noted that "SODCIT has been developed."[9] Retired Colonel General Viktor Barynkin added "it has become expedient to combine strategic defensive and offensive operations and strategic operations in the ocean theater of hostilities into a single strategic operation."[10] In the conduct of such operations, IWes will play a crucial role due to their expansive reach.

In 2013 the journal *Air-Space Defense* stated that:

> 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.[11]

As noted, these assets rely on information technologies.

A 2014 article in *Military Thought* that mentioned the SODCIT concept stated that determining combat missions, methods, and variations of long-range precision-guided munitions (PGM), which are supported by an information infrastructure, can be presented according to a priority-ranked subprocess that included the development of the concept of SODCIT.[12] 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 SODCIT.[13]

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, and others.[14]

Thus, the term SODCIT implies the extended use of IWes as a non-nuclear strategic weapon or asset. Such 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. For Western analysts, the concept should raise our concerns over Russia's potential planning intentions.

---

[10] Ibid.
[11] 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.
[12] 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.
[13] Ibid.
[14] Viktor Bondarev interview by V. Kutishchev, "Russian Aerospace Forces," *Armeyskiy Sbornik (Army Journal)*, No. 3 2017, pp. 33-34.

How did Russia arrive at this conclusion of IWes becoming a non-nuclear strategic operation? The following discussion over the past two decades offers how the concept of an IWe gradually evolved and incorporated new developments in information technologies, which led to new ways to consider information-technical and information-psychological applications of the concept.

The First Important IWe Discussions

Detailed descriptions of IWes and their uses began to develop slowly in the 1990s. One of the first (and still outstanding) Russian articles to define and discuss an IWe was authored in 1996 by Major S. V. Markov and published in the journal *Bezapasnost (Security).* Leading specialists till refer to his many thoughts and definitions. Markov defined an IWe as

> A specially selected piece of information capable of causing changes in the information processes of information systems (physical, biological, social, etc.) according to the intent of the entity using the weapon.[15]

This understanding of an IWe and its impact on the information-technical and information-psychological activity of Russia produces a much different national will and language of dialogue than to which the West is accustomed. Markov is convinced that it is imperative to develop international and state control over the creation and use of IWes.[16]

The IWe can be used in the following ways according to Markov:

- To destroy, distort, or steal data files;
- To mine or obtain the desired information from these files after penetrating defense systems/firewalls;
- To limit or prevent access to them by authorized users;
- To introduce disorganization or disorder into the operation of technical equipment;
- And to completely disable telecommunications networks and computer systems and all the advanced technology that supports the life of society and the operation of the state.[17]

In 2000, five authors at the Institute of Systems Analysis superseded Markov's IWe article in importance. They wrote the first authoritative detailed introduction to and explanation of IWes. In a pamphlet titled *The Information Weapon—A New Challenge to International Security*,[18] they described various forms of IWes, and one of the authors, Andrey Krutskikh, eventually became President Putin's point man on cyber issues.

---

[15] S. V. Markov, "Several Approaches to the Determination of the Essence of the Information Weapon," *Bezopasnost (Security),* No. 1-2, 1996, p. 53.
[16] Ibid.
[17] Ibid., p. 56.
[18] V. N. Tsygichko, D. S. Votrin, A. V. Krutskikh, G. L. Smolyan, and D. S. Chereshkin, *The Information Weapon—A New Challenge to International Security*, Institute of Systems Analysis, Moscow, 2000, pp. 20-21. This IWe discussion is taken from Timothy Thomas, *Cyber Silhouettes*, Foreign Military Studies Office, Fort Leavenworth, KS, 2005, pp. 168-171.

The authors wrote that IWes could be classified based on a number of attributes. These included single and multi-mission/universal purposes; short- and long-range operations; individual, group, and mass destruction capabilities; various types of carriers; and destruction effect. They further classified IWes as belonging to one of six forms:

1. Means for the precision location of equipment that emits rays in the electromagnetic spectrum and for the destruction of that equipment by conventional fire;
2. Means for affecting components of electronic equipment;
3. Means for affecting the programming resource control modules;
4. Means for affecting the information transfer process;
5. Means for propaganda and disinformation;
6. And means for using psychotronic weapons.

The pamphlet then discussed the significance and potential types of each of these weapons.

The first form, the means for precision location, included the effective detection of individual elements of C2 information systems, to include their identification, guidance, and physical destruction (by firing for effect). The second form, the means for affecting electronic equipment components, included the temporary or irreversible disabling of individual elements of electronic systems. Weapon types included at the time were means of forcible electronic suppression (such as generators of super-high frequencies) and means to disable equipment (such as the head resonance of hard disks), burn out monitors, erase RAM, and affect reliable power sources.

The third form, the means for affecting programming resource control modules, disabled or alerted the operating algorithm of control systems of software by using special programming means. These weapon types included the means for defeating information security systems; penetrating the enemy's information systems; disabling all of, or a specific portion of, an information system's software, possibly at a very specific point in time or when a specific event occurred in the system; making a covert, partial change in an operational algorithm of a piece of software; collecting data that is circulating in the enemy's information system; delivering and inserting certain algorithms into a specific place in an information system; and affecting the security systems of facilities (with viruses, worms, etc.).

The fourth form, means for affecting the information transfer process, can stop or disorganize the functioning of subsystems for the exchange of information by affecting the signal-dissemination environment and operating algorithms. Types of weapons belonging to this class included electronic equipment, especially ground and air stations (helicopters, unmanned airborne vehicles, etc.) that interfere with radio communications; disposable, air-droppable interference transmitters; means that affect the protocols of data transmission by communication systems and the data transmission itself; means that affect algorithms used for addressing and routing; means for intercepting and disrupting information as it passes through the technical channels of its transmission; and means for causing system overload by making false requests of a communications system.

The fifth form, means for propaganda and disinformation, can change the information component of C2 systems; create a virtual picture of the situation that differs from reality; change the system of human values; and damage the moral-psychological life of the enemy population. Types of this weapon included means for causing disinformation in secure systems and means for modifying navigation systems, information and meteorological-monitoring systems, precision-time systems, and so on.

Finally, for the sixth form, psychotronic weapons, the authors described weapons that affect a person's psychology and subconscious in order to reduce one's will, suppress and or temporarily disable a person, or zombify the person. These weapon types included:

- Psycho-pharmacological substances;
- Psycho-dyspeptics;
- Tranquilizers, anti-depressants, hallucinogens, and narcotics;
- Specially structured medicines;
- Special-beam generators that affect the human psyche;
- Special video graphic and television information (25th frame effect, elevating blood pressure, inducing epileptic seizures, etc.);
- Means for creating virtual reality that suppresses the will and induces fear (projecting an image of "God" onto clouds, etc.);
- And technologies of zombification and psycholinguistic programming.[19]

Information technologies can also be utilized as IWes, the pamphlet notes. Those information technologies that are integral components of high-precision ammunition are used to guide missiles via position finding and reconnaissance as well as by visual, electronic, and other factors. These functional subsystems can also be treated as IWes in that they gather, process, and disseminate information. The pamphlet defined information war as "actions taken for securing information superiority by damaging information, information-based processes, and information systems of the enemy along with protecting one's own information, information-based processes, and information systems." This definition is similar to the US definition at the time and contradicts several other purely Russian definitions. It is unknown exactly why the authors chose this definition.

Moving On: The 2001-2019 Discussions

As a result of Russia's description of the West's focus on noncontact warfare and advanced cyber weapons in the 1990s, Russian theorists came to believe that adversaries wanted to develop a "clean" war run by special agents and programmers against Russia while it was still vulnerable. In response, Russian authorities began to envision how IWes could help offset the Kremlin's national security weaknesses. Russian theorists saw the many benefits of IWes and praised them for their universality, covertness, and variety of implementation forms (software and hardware), their radical effects and ability to select a precise time and place of employment, and, finally, their cost effectiveness. Admiration for these attributes, however, also caused concern for the nation's

[19] Ibid.

national security,[20] since other nations were farther along in IWe developments. Russia began to manufacture both offensive and defensive IWes and, due to their number of outstanding mathematicians, began to catch up quickly with other nations in the software realm of options. For example, cyber or information-strike weapons (described below) were soon developed and considered as Russian offensive information weapons, while over-the-horizon radar stations were developed and considered as Russian defensive information weapons.[21]

The following discussion covers Russia's focus on IWes over the past two decades. The discussion demonstrates the growing importance of the concept and how it has been integrated into Russia's understanding of information warfare, with its information-technical and information-psychological components; and how it has underscored the growing importance of nonmilitary means to influence and win confrontations.

In **2001**, the PIR Center in Moscow published a document that included a significant chapter on IWes. It noted, like the military, that information superiority now determines the outcome of battles. Those who process battlefield information the slowest become more vulnerable. Disabling command and control systems of an opponent is a keyway to obtain information superiority. IWes can be high-precision weapons, electronic warfare assets, electromagnetic pulse weapons, or software viruses, among others. The document noted that the effectiveness of a weapon in accomplishing information warfare missions can be a criterion for assessing an IWe.[22]

The authors then discussed types of IWes and their characteristics and effects. With regard to the means of IWes, six were mentioned, but they were the same six noted by the authors of the 2000 IWe pamphlet above. That came as no surprise, since one of the authors of the 2000 pamphlet also coauthored the PIR Center report (V. N. Tsygichko). IWe effects were divided into three areas, information technologies (as components of munitions and reconnaissance, propaganda, and software systems), energy (as components of EW, microwave, and cruise or unmanned aerial vehicles), or chemical (gases, aerosols, pharmacologic agents, etc.).[23] IWes offer several other advantages. There is generally freedom of access to many information systems, especially in social media; traditional borders are blurred, making it difficult to know if we are witnessing a crime or an act of war; there is a difficulty in controlling perceptions due to the wide range of "facts" available; and there is the potential for the covert preparation of the battlefield years in advance through the placement of specific software.[24]

In **2002**, in an important article in *Armeyskiy Sbornik* (*Army Journal*), noted Russian military author Vladimir Slipchenko, who used the term new-generation warfare as early as 2000,

---

[20] N. P. Shekhovtsov and Iu. E. Kuleshov, "Information Weapons: Theory and Practice of Their Employment in Information Warfare," *Vestnik Akademii Voennykh Nauk (Journal of the Academy of Military Science)*, 2012, No. 1, p. 39.
[21] A. A. Tsepelev, "Over-the-Horizon Radar Stations as Russian Defensive Information Weapons," *Voyennaya Mysl' (Military Thought*), No. 12 2018, p. 53.
[22] Aleksandr V. Fedorov and Vitaliy N. Tsygichko, "Information Weapons as a New Means of Warfare*,"* Chapter Three, of *Information Challenges to National and International Security*, PIR Center, Moscow 2001, pp. 69-109.
[23] Ibid.
[24] Ibid.

noted that information's role will only grow in the coming century. IWes will be system destroying, he noted, in that they will disable entire combat, economic, and social systems, making them an effective non-nuclear strategic weapon. Offensive means include destroying or disrupting an adversary's information infrastructure, his process of operational command and control, and attacks on computer networks. Defensive measures include operational and strategic camouflage, physical defense of information infrastructure facilities, disinformation, electronic warfare, and other means. Slipchenko added that electronic suppression will remain the most important component of a nation's information resources and predicted that they will eventually become an independent type of countermeasure. Finally, he added that cybernetic warfare could also become an element of independent development.[25]

Of special interest is that the majority of what Slipchenko wrote about in 2001/2002 has come to pass in contemporary times. Electronic warfare is now thought to be an independent branch of service, and the basic content of General Staff Chief Valery Gerasimov's yearly addresses to the Academy of Military Science in regard to information resources and warfare echo much of the theory and understanding of information's impact on war that Slipchenko first advanced (no stereotyping, blurring of war and peace, etc.). Russia now has cyber forces but there has been no indication that they have become an independent branch of service.

Also in **2002**, two authors described IWes as nonlethal weapons (NLW). The development of the mass media, they noted, creates the prerequisites for the use of an information NLW. Of interest is that psychological NLWs were also considered as IWes but have not yet been scientifically confirmed. These type of NLWs included telepathy, telekinesis, clairvoyance, and other psychological means.[26] These measures have been under study in Russia for decades but have produced no discernable results.

In **2003** an article in the journal *Military Thought* noted that with the end of the Cold War, there was a desire to eliminate many weapons of mass destruction. This caused the military to focus more attention on precision guided and other IWes, to include those of a nonlethal form. The Persian Gulf War, the article noted, integrated precision guided weapons with global navigation, intelligence, communications, command and control, and electronic warfare systems and created theater information weapons (TIWe). Specialists began to consider information-strike operations, which would allow a force to reach military objectives without land forces. TIWes, the authors noted, are the information-technical component of IWes. The information-psychological component, on the other hand, is designed to break the enemy's will to resist, where the main targets are troop morale, public opinion, and the decision-making systems of the opposing side.[27] One goal is to develop the means and methods for a targeted information-psychological impact, one that might cause an opponent to make "unconscious decisions" that are advantageous to the other side. This could include the use of psychotropic substances or the use of manipulative

[25] Vladimir Slipchenko, "A New Form of Struggle: In the Coming Century, The Role of Information in Noncontact Wars Will Only Grow," *Armeyskiy Sbornik* (*Army Journal*), No. 12 2002, pp. 30-32.
[26] Vitaliy Tsygichko and Vladimir Dyachenko, "Non-Lethal Weapons," *Yadernyy Kontrol (Nuclear Control)*, 18 September 2002, pp. 58-67.
[27] S. P. Nepobedimiy and V. F. Prokofyev, "The Intellectualization of Weapons and Weapons against Human Intelligence," *Voennaya Mysl' (Military Thought*), No. 7 2003, p. 26.

information amid distracting messages. New technologies increase the opportunities to develop and use such effects, such as neuro-linguistic programming.[28]

In a **2003** book titled *The Information Weapon*, the author examined IWes more narrowly, focusing on hackers, the cyber weaponry of various nations, and the revelation (to that book's author) that the Cold War had not ended.[29] In **2007**, Sergey Ivanov, the Russian Defense Minister from 2001 until February 2007, noted the importance of IWes for their ways to influence the conduct of future war. He was particularly impressed with IWes application to any theater of war and in their ability to conduct operations without becoming involved in a military conflict:

> The development of information technology has resulted in information itself turning into a certain kind of weapon. It is a weapon that allows us to carry out would-be military actions in practically any theater of war and most importantly, without using military power.[30]

In **2008**, Major General V. D. Ryabchuk wrote on the intellectual-information confrontation between and among states, adding that confrontations are a mix of information, the intellect, and forecasting. The strong influence of informatics and computer science on operations has necessitated that the information-confrontation factor be added to Russia's calculation of the correlation of forces. Further, the influence of informatics has changed operations, in Ryabchuk's opinion, to include a so-called "Napoleons Square," composed of a base of "will" and a height of "brains." Informatics has expanded the square to a cube due to its ability to add depth to an assessment. This enhances a commander's intelligence gathering beyond his inherent capabilities.[31] While not directly naming informatics as an IWe, he strongly implies that this is how they should be understood.

In **2009**, again while addressing IWes only tangentially, another *Military Thought* article stated that breakthroughs in information technologies had "provided a basis for developing a totally new generation of tools of warfare" and "stimulated continued development of forms in which troops and methods to conduct military operations are used."[32] A 21st century warfare trend was stated as follows:

> Growing weight will be given in wars anticipated in the 21st century to information as a component of armed struggle because troops are equipped with weapon systems using information technologies, electronic warfare, and other systems. Accordingly, trying to achieve superiority in the use of information over the adversary will become a principal condition for successful military operations.[33]

---

[28] Ibid., p. 27.
[29] V. I. Khozikov, *The Information Weapon*, Publishing House Neva, 2003.
[30] Oscar Jonsson, *The Russian Understanding of War*, Georgetown University Press, 2019, p. 94, as quoted in Steve Blank, "Russian Information Warfare as Domestic Counterinsurgency," *American Foreign Policy Interests*, p. 34.
[31] V. D. Ryabchuk, "The Problem of Military Science and Military Forecasting in Conditions of an Intellectual-Information Confrontation," *Voyennaya Mysl' (Military Thought*), No. 5 2008, pp. 68-69.
[32] V. N. Gorbunov and S. A. Bogdanov, "On the Character of Armed Conflict in the 21st Century," *Voyennaya Mysl' (Military Thought*), No. 3 2009, p. 2.
[33] Ibid., p. 6.

In **2011**, two Russian military specialists wrote on information-strike operations in the journal *Armeyskii Sbornik (Army Journal)*. The classic triad of fire, strike, and maneuver, in their opinion, no longer expressed the essence of a battle or operation. Radio-electronic, electronic-fire, and information-strike operations were the new forms of armed struggle. The latter is of particular importance and was defined as follows:

> The information-strike operation (ISO) is the totality of mutually associated information strike engagements (*srazhenie*), information-strike battles (*boi*), and information strikes (*udar*), coordinated with respect to goal, missions, place, time, and method of conduct, carried out with the aim of disorganizing an adversary's troop and weapons command and control system and destroying his information resources.[34]

IWes conduct information strikes against an adversary's information resources. The types of strikes include information-psychological (disinform or mislead an adversary), information-psychotropic (use of specialized means against a person's psyche), radio-electronic, and program-computer. ISO's help gain the initiative and superiority in the information sphere, to include over the command and control of troops and the reflexive control of an adversary. ISO characteristics include having no spatial limitations, a variety of forms and methods of use, no limitations from weather or season, and the ability for their secret use in peacetime. Targets include command posts and communication nodes.[35]

ISOs can be conducted in three stages. First, information support systems of command and control for intelligence, air defense, and rocket defense are disorganized. Second, under cover of jamming, strikes are made by destruction means—operational-tactical and tactical rockets. Third, the information support of tactical and army aviation and field artillery is disorganized.[36]

To prepare an ISO, an adversary's command and control system must be studied and exposed. The timeliness and completeness of identifying objectives for fire and radio-electronic destruction must be determined in advance along with the quality of one's own measures for defending against such weaponry. To disorganize a functioning adversary, precision weapons must be fully utilized. Disorganizing an opponent's command and control system lies at the center of planning and coordinating friendly fire destruction elements.[37]

The authors then note that there are various types of information-psychological weapons that can improve the forms and methods of conducting an ISO. Energy-information-psychological weapons are under study for ways they can modulate super high frequency ultrasonic infrared waves that affect the human nervous system. Psychotropic-information weapons use narcotics and chemicals to produce information-control effects on biological processes and the nervous system. Technical means (generators, etc.) of virtual information-psychological and other types of

[34] I. N. Chibisov and V. A. Vodkin, "The Information-Strike Operation," *Armeyskii Sbornik (Army Journal*), March 2011, p. 46.
[35] Ibid., pp. 46-47.
[36] Ibid., p. 47.
[37] Ibid., p. 48.

weaponry offer different potential capabilities to affect the human psyche [author: no actual results were offered, just these theories]. Information-psychological weapons are to be integrated with fire, radio-electronic, and energy effects to broaden the operational-strategic methods for achieving ISO goals. Radio disinformation, active and passive jamming, false radar targets, and fake communication posts and centers will facilitate misleading an opponent. The ISO is basically an offensive action, but it can acquire a defensive character if needed.[38]

An important **2012** article titled "Information Weapons: Theory and Practice of their Employment in Information Warfare," stated that the infosphere's inexhaustible supply and replenishment capability of information resources, its reliability and ability to duplicate these resources, the compactness of information carriers, and information's bloodless reactions or responses to actions in the infosphere have led to the intensification of information warfare. IWes can be used in secret, can cross borders and impact sovereignty, and can be used in military and civilian structures. More importantly, the authors stated that IWes cause the greatest losses when used against command and control systems and the human mind.[39]

The authors classified IWes according to effects, which they termed as physical, informational, software, or radio electronic. Physical effects included specialized storage batteries for high-voltage impulses, means to generate electromagnetic impulses, graphite bombs, and microbes that interfere with electronic circuits and insulation materials. Information effects included mass information resources, global networks, and voice "disinformation" stations. Software attack weapons included computer viruses, logic bombs, and means to suppress information exchanges. No radio-electronic effects were offered. However, the term "dynamic IWes" was defined as a "unified system of comprehensive, combined, beam, targeted, and strike employment of all forces and means of technical, communications, and information-psychological effects against the subconscious of the objective of the attack."[40] The methods for the implementation of dynamic IWes are mathematical, algorithmical, or software-hardware, and are most effective when employed as a set in offensive, defensive, or support forms. The military and political leaderships as well as world public opinion (when conducted with special information-psychological operations) are specific targets of destruction.[41]

The authors noted that information-psychological effects are

> A purposeful psychological attack against concrete areas of the human mind, the minds of a group of people, or the public consciousness as a whole. Effects can be implemented with respect to the means of information stimuli by using the entire spectrum of methods and forms of technical, visual, aural, medical, physical, painful, and virtual suppression of the will.[42]

Information confrontation was stated to be a special set of countermeasures designed to forestall an enemy's destructive designs against the mind of a person making C2 decisions. The

[38] Ibid., pp. 48-49.
[39] Shekhovtsov and Kuleshov, p. 35.
[40] Ibid., p. 36.
[41] Ibid., pp. 36-37.
[42] Ibid., p. 37.

goal of information confrontation is to protect one's own information resource security via the use of several means: the physical protection of objects, covert surface surveillance, technical equipment, effective camouflage, disinformation, and counterpropaganda combined with radio-electronic warfare. Other protective means are required to ensure there is no power disruption. It is usually electromagnetic impulses or electromagnetic bombs that are the most threatening to computer networks.[43]

Electromagnetic weapons (EMW) are well-known for their ability to disrupt or interfere with information system operations. They can disrupt a country's economy, production, and defense capabilities. Disrupting systems that are exchanging information for command decisions can have serious consequences. C4ISR are the main targets of EMW effects. It was noted that "the principle of EMW action is based on short-term electromagnetic radiation of great power, capable of incapacitating radio-electronic devices that comprise the basis of any information system."[44]

In conclusion, the authors noted the following:

> Universality, covertness, variety of the forms of software and hardware implementation, radicalism of effects, adequate choice of time and place of employment, and, finally, cost effectiveness make IWes extremely dangerous. They are easily camouflaged as protection resources of, for example, intellectual property. They make it possible to even conduct offensive operations anonymously, without a declaration of war.[45]

Near the end of **2012**, S. G. Chekinov and S. A. Bogdanov discussed the initial period of war (IPW) on the pages of *Military Thought*. The IPW was defined as the time when forces are deployed before the start of a conflict in order to create favorable conditions for committing their main forces. Under new military, political, and economic conditions, the IPW has acquired a special significance for winning a conflict.[46] The authors noted the following:

> The IPW may become the hardest phase in which the warring sides will be striving to make the most of the power of its groups of forces built up in advance and deployed in secret to achieve the main goals of the war. This period will be the most critical phase of the war and have a great effect on its outcome.[47]

Of interest is that malware and other types of information technologies secretly placed in the infrastructure or computers of potential opponents would help achieve the main goals of a war, such as the complete disorganization of an opponent's command and control system. IPW success allows for one side to control the operations of its forces and assert supremacy over an opponent. The authors noted that "major military, political, and strategic objectives of the war must be

[43] Ibid.
[44] Ibid., p. 38.
[45] Ibid., p. 39.
[46] S. G. Chekinov and S. A. Bogdanov, "The Initial Period of War and its Influence on a Country's Preparation for Future War," *Voyennaya Mysl' (Military Thought*), No. 11 2012, pp. 15-16.
[47] Ibid., p. 19.

achieved in its initial period."[48] Obviously the best way to do that is to develop and insert key IWes into the systems of an adversary in peacetime, creating favorable conditions for either winning victory before conflict starts or the massive disorganization of an opponent such that his systems are less dependable and more vulnerable to destruction with aerospace or other types of weaponry.

In early November **2013** the State Duma Security and Anticorruption Committee recommended the adoption of an amendment to a Federal Security Service (FSB) law that will allow it to conduct police investigations to counter threats to Russia's information security. Earlier such actions were applicable only to state, military, economic, or environmental security threats. The report stated that harmful software, for example, can be used as an information weapon[49] that could threaten security. That same year, Russia's Security Council noted that information and communication technologies are a looming threat as IWes, since they can threaten strategic stability, violate the territorial integrity of other nations, and act in both the military and political spheres of interest.

In **2013** Chekinov and Bogdanov discussed new generation warfare, highlighting on numerous occasions the importance of information technologies. Along with other authors they believe that information technologies have significantly changed the nature, methods, and techniques used by state and government agencies and military organizations and operations. In the latter case the remote engagement of troops is now possible.[50] They noted that "decisive battles in new generation wars will rage in the information environment," where computer operators will manipulate computers at a distance from the conflict. Using information pressure, an information operation will be conducted that induces world public opinion to accept the need to restore democracy and fight tyranny.[51] Once information superiority is achieved in peacetime, conflict may even be avoided. If conflict appears inevitable, it is visualized that information technologies will dominate the opening period of a conflict, as there will emerge a targeted information operation, an electronic warfare operation, and high-precision weaponry loaded with information technology.[52]

In **2015**, during a presentation in Garmisch, Germany, noted Russian information warfare experts I. N. Dylevsky and S. A. Komov offered a paper on "Rules of Conduct in Information Space—An Alternative to an Information Arms Race." In the paper, it was noted that "Another aspect of confrontation in the information sphere is a rapid advancement and proliferation of information weapons."[53] Their use can lead to industrial disasters or, worse yet, critical infrastructure (finance, energy, transport, etc.) destruction. It is time, the authors write, to adopt

[48] Ibid., p. 25.
[49] Unattributed report, "A State Duma Committee Has Approved Amendments Relating to Information Security," *RIA Novosti Online (RIA News Online)*, 8 November 2013.
[50] S. G. Chekinov and S. A. Bogdanov, "On the Nature and Content of a New Generation War," *Voyennaya Mysl' (Military Thought*), No. 10, 2013, pp. 13-14.
[51] Ibid., p. 20.
[52] Ibid., p. 23.
[53] Ninth International Forum "Partnership of State Authorities, Civil, Society, and the Business Community in Ensuring International Information Security," 20-23 April 2015, Garmisch Germany, p. 36.

universal laws to prohibit their development.[54] Unfortunately, the authors did not expand on how this could be done or how nations could control the risk of their development elsewhere.

Later that year, again in *Military Thought*, it was noted that nonlethal weapons (NLWs) are an effective information warfare asset, implying their application as an IWe. In handling internal issues, NLWs can "defuse the bellicose moods stoked by propaganda and isolate the most outrageous advocates of the indiscriminate use of military force."[55] Ironically, the "mood" of recent anti-Kremlin demonstrations in Moscow was provoked due to Kremlin decisions to keep certain people off of election ballots there, thus moods can be both "provoked" and then "defused" (with NLW) by the same government officials.

Also in **2015**, Russia's *National Security Strategy* was published, and it used the term information 36 times. The term cyber does not appear. The main use of information, it seems, is as an instrument "set in motion in the struggle for influence in the international arena" (along with political and financial-economic instruments). The Strategy also noted that the confrontation in the global information arena is "caused by some countries' aspiration to utilize informational and communication technologies to achieve their geopolitical objectives, including by manipulating public awareness and falsifying history." For most Westerners, this appears to be exactly what Russia did in Ukraine, never mentioning Putin's influence on Yanukovych and striking out on an information campaign that, according to even Russian analysts, surpassed anything seen during the time of the Soviet Union. Information is also mentioned as a measure to be implemented in order to help ensure strategic deterrence. The "inadvertent" mention of the Status-6 top secret torpedo on Russian TV is an example of an influence operation designed to utilize information deterrence as a way to counter the US's use of its Prompt Global Strike system. Information associated with extremism or terrorism is taken to be a significant threat to public security; and in order to counter such threats, an information infrastructure must be developed that ensures the publics access to information on issues relating to the sociopolitical, economic, and spiritual life of Russia's citizens.[56]

In **2016**, during his annual speech at the Academy of Military Science, General Staff Chief Valery Gerasimov discussed the impact of so-called color revolutions. He noted how their utility could be quickly furthered through the adaptive use of information resources as a weapon:

> Essentially, any "color" revolution is a state revolution organized from without. Their basis is information technologies, which envision the manipulation of the protest potential of the population in combination with other nonmilitary means. Here, mass targeted effects on the consciousness of the citizens of a state—the objects of aggression by means of the global 'Internet' network—acquire important significance. Information resources have essentially become one of the most

[54] Ibid.
[55] D. V. Zaitsev, V. I. Orlyansky, and D. Yu. Soskov, "Nonlethal Weapons Can Be Used to Prevent Armed Conflicts," *Voennaya Mysl' (Military Thought)*, No. 10 2015, p. 51.
[56] Edict of the Russian Federation President, "On the Russian Federation's National Security Strategy," *President of Russia Website*, 31 December 2015. See sections 13, 21, 36, 43, and 53 of the document.

> effective types of weapons. Their extensive use makes it possible to 'shake up' the situation in the country from within in a matter of days.[57]

The "information resources" of the West that are used against Russia, according to their sources, are nongovernmental organizations and operations aimed at the young. For example, in President Vladimir Putin's 2007 speech in Munich, he said his concerns about the work of NGOs grew from the fact that they "are used as channels for funding, and those funds are provided by governments of other countries." That flow of foreign money to assist opposition political organizations in Russia, he said, is "hidden from our society. "What is democratic about this?" he asked. "This is not about democracy. This is about one country influencing another."[58]

In **2017** Chekinov and Bogdanov had changed their focus from new generation wars to discussing the importance of new type warfare. They stated that the process of globalization is threatening war of a "new type," which could "become the pivot of historical life in the 21st century."[59] New type warfare is characterized by the use of "political pressure, information sabotage, cashing in on humanitarian issues, secret service activity, and unfair and cunning diplomacy."[60] Earlier in the article the authors addressed the growing impact of information warfare. Information, computers, and telecommunication technologies suppress adversaries by disorganizing command and control and introducing chaos into their work. This work misinforms army personnel and the population and psychologically crushes them.[61] The realm of the virtual, both informational and cognitive, is exploited.[62] Again, while not specifically mentioning IWes, the implication is clear, that they are a major component of new type warfare.

In **2019,** the journal *Vestnik Akademii Voennykh Nauk (Journal of the Academy of Military Science)* published an article on the impact of information processes on Russia's national security. It stated that the establishment of an information society, the globalization of information processes, and the democratization of society (to include the increase in the socio-political life of the population) had produced an information struggle in societies. Internally the struggle was for the ability to control large numbers of people and not just power and money. Externally the information struggle is conducted in times of both peace and war between states, whether they be allies or enemies. Twenty-first century struggles now include a state's information capabilities, which work to achieve a strategic advantage[63] and information superiority.

---

[57] V. V. Gerasimov, "The Organization of the Defense of the Russian Federation under Conditions of the Enemy's Employment of 'Traditional' and 'Hybrid' Methods of Conducting War," *Vestnik Akademii Voennykh Nauk (Journal of the Academy of Military Science)*, No. 2 2016, p. 20.
[58] Thom Shanker and Mark Landler, "Putin Says U.S. Is Undermining Global Stability," *The New York Times*, 11 February 2007, downloaded 9/1/2020 at https://www.nytimes.com/2007/02/11/world/europe/11munich.html
[59] S. G. Chekinov and S. A. Bogdanov, "The Evolution of the Essence and Content of the Notion of 'War' in the 21st Century," *Voyennaya Mysl' (Military Thought*), No. 1 2017, p. 43.
[60] Ibid., p. 40.
[61] Ibid., p. 37.
[62] Ibid., p. 32.
[63] V. F. Lata, V. A. Annenkov, and V. F. Moiseev, "Information Confrontation: A System of Terms and Definitions," *Vestnik Akademii Voennykh Nauk (Journal of the Academy of Military Science)*, No. 2 2019, pp. 128-129.

Information, the authors noted, moves through space and time via processes of "searching, collecting, storing, processing, presenting, accumulating, disseminating, and decision-making."[64] Depending on how information is used and where it is located (in military weapons technology, in a human's mind, in command and control processes, etc.) it can produce different effects (precise targeting, manipulation of data, etc.). The authors defined IWes as follows:

> Information weapons are the totality of technical, software, and other special resources, constructively intended for the formation of information effects for the purpose of disrupting information processes by means of effects against the elements of an information resource (information target) by a special pattern of organized flows of emissions of energy of different physical natures or a specific pattern of selected and structured information.[65]

The authors believe that the concept of "means of information effects" more broadly describes the essence of IWes. Technical effects, linguistic and software products, and other means can produce effects against an opposing side's information resources. Effects used to gain information superiority against an opponent include radio-electronic warfare resources, software that disables automated C2 systems, psychotropic generators, special pharmacological means, and the mass media. Information superiority was defined as superiority in timeliness, reliability, and completeness attained by C2 organs for use in the processing and timeliness of decision-making and control in the execution of plans.[66]

Another **2019** article, this time published by a US author, discussed Russia's use of the "big lie," that is Russia's tendency to define objective reality as the Kremlin sees fit and thereby avoid responsibility for the "truth." This is a different type of IWe. The article described Russia's recent admonition to Iran to never admit guilt in the downing of the Ukrainian airliner that it had recently caused. A deputy head of Russia's State Duma's Defense Committee noted that it was far more important to blame the US.[67] This has been a typical Russian response, to avoid responsibility at all costs, even to its own credibility. Russia is quick to openly deny complicity in any accusation leveled against it by other nations. To date, their responsibility for the shootdown of MH-17 airliner over Ukraine and their involvement (based on credible evidence) in the poisonings of former Russian intelligence operators Aleksandr Litvinenko and Sergey Skripal (both on England's territory) are such examples. So is their failure to accept responsibility for the doping of their athletes in the Sochi Winter Olympics, a charge first levied by a Russian! From such examples it is clear that openly using the "big lie" and presenting their (in some cases, numerous) alternative explanations of objective reality provides Russia with the mistaken assumption that it can deflect attention from concrete facts and avoid responsibility for their wrongdoings or mistakes.

---

[64] Ibid., p. 130.
[65] Ibid., p. 136.
[66] Ibid., pp. 136-137.
[67] See Julia Davis, 11 January 2020 at https://www.thedailybeast.com/russia-to-iran-dont-admit-guilt-blame-the-us-instead.

Joshua Yaffa, in a late 2019 article in *The New Yorker*, provided another good example of how Russia uses lying to manipulate objective reality and the truth in order to avoid responsibility. The author spent many years in Russia, interviewed hundreds of people, and recently wrote a book titled *Between Two Fires* that discusses how Russians have adapted to the authoritarian views of President Vladimir Putin. The books interview with Konstantin Ernst, the head of Russia's *Channel One* TV, a pro-Kremlin outlet, was one of the most interesting for its observation of how Russian uses objective reality to its benefit.[68] Ernst noted that "Today the main task of television is to mobilize the country. Our task No. 2 is to inform the country about what is going on."[69] Ernst considers himself a statist, described as the belief in the inherent virtue of the state.[70] You are expected to "intuit" the rules of the state rather than have them spelled out, a system making everyone err on the side of caution.[71] False stories are an integral part of the Putin system's postmodern approach to propaganda as a result.

> Today, state outlets tell viewers what they are already inclined to believe, rather than try to convince them of what they can plainly see is untrue. At the same time, they release a cacophony of theories with the aim of nudging viewers toward believing nothing at all, or of making them so overwhelmed that they simply throw up their hands. Tring to ascertain the truth becomes a matter of guessing who benefits from a given narrative.[72]

Ernst noted that "its's become increasingly clear to me that justice, democracy, the complete truth—they don't exist anywhere in the world. People who make television are citizens of a specific country, from a certain nationality, with particular cultural codes."[73] Alexei Yurchak, a Russian-American anthropologist, in a book titled *Everything Was Forever, Until It Was No More*, agrees with Ernst's sentiment. Jaffa quoted him as noting that "Since nothing about the representation of the world was verifiably true or false, the whole of reality became ungrounded."[74]

This idea that objective reality doesn't exist is seldom understood in the West, but it is well understood in Russia as the state's IWe, which can be applied at any time the state so desires. Thus, the only way to get ahead is to "intuit" what is expected of you while simultaneously trying to extract some benefit for yourself out of the situation, all the while avoiding the state's IWe designed to bring charges against you. Since the government engages in half-truths about reality, the people do too. This internal IWe does not work or have the same authority beyond Russia's borders.

One final use of IWes should be noted, one that was not covered in any of the presentations above but was noted by Slipchenko ("strategic non-nuclear forces will find wide use in new-generation wars and subsequently also will take on a deterrence function"), is the use of information deterrence. There is a Russian surreptitious use of IWes in legal cases that may not be obvious. For example, there is the case of Russian efforts to use the UN to support its legal claims to the Arctic, where Russia has spent much time and money to digitally (that is, information-wise)

---

[68] Josha Yaffa, "Channeling Putin," *The New Yorker*, 16 December 2019, pp. 22-27.
[69] Ibid., p. 25.
[70] Ibid.
[71] Ibid., p. 26.
[72] Ibid., p. 27.
[73] Ibid.
[74] Ibid., p. 23.

map the Arctic Sea. If Russian representatives can prove their case with images or numbers, it may be able to reserve for itself exclusive access to the region's oil and gas riches and would, in effect, have "informationally deterred" other nations from the region with its digital use of legal means. This type of deterrent force supports the Russian "containment" concept more than the usual "intimidation" role of deterrence.

Countering Russian IWes

Only one aspect of countering Russian IWes, that being social division, is covered here and only briefly. Counters to Russian attempts to use social media to divide audiences were explained most succinctly through the testimony of Clint Watts before the Senate's Intelligence Committee. Watts, a former FBI Special Agent on a Joint Terrorism Task Force and National Security Branch consultant, noted that the West is facing a different threat, that being Russian active measures online. These measures are supported through Russia's ability to implore the "plausible deniability" of their participation and thus influence in these measures. Watts noted that through the use of such measures, *Russia Today* (*RT)* and *Sputnik*, two media outlets, have tarnished reputations of political figures and undermined democratic institutions; weakened confidence in financial markets; undermined citizen trust in government; and incited fears of global conflicts (nuclear, climate, etc.). Russia does so through its adept identification of specific audiences inside electorates that appear amenable to their messages and through intricate strategic planning ahead of time of methods that might work. Social media's generation of automated responses are used to drown out opposing viewpoints.[75]

To counter these efforts, Watts offered several recommendations. First, the U.S. State Department would develop a website that responds to false claims about U.S. policy outside U.S. borders; and a Homeland Security website would to do the same for domestic operations. Second, hackers would continue to be brought to justice. Third, the Treasury and Commerce Departments would develop an education campaign for U.S. businesses to thwart damaging false claims. Fourth, Homeland Security would work to improve public-private partnerships to expand the sharing of cyber trends. Fifth, U.S. intelligence agencies would work to counter Russian active measures. Sixth, newspapers, cable -news channels, and social-media companies would vow not to report on stolen information that amplifies Russian influence campaigns. Seventh, social media companies should tag fake news stories for readers, which would help counter "information bubbles" where voters see stories and opinions that suit their preferences/biases. Finally, social media companies could band together to create an Information Consumer Report that would evaluate all media organizations across a range of variables to produce news ratings representative of the outlet's accuracy. Consumers would then know the danger/risk of going to the sites with lower ratings.[76]

From Information Weaponry to Kokoshin's Technosphere

Attention is now shifting from IWes to artificial intelligence (AI) and quantum computing issues. Both topics are beyond the scope of this article, but a mention of their importance is nonetheless called for, especially how they might be integrated with IWes.

[75] See http://www.thedaily beast.com/articles/2017/01/22/can-the-michelin-model-fix-fake-news.html
[76] Ibid.

Andrey Kokoshin is a former Secretary of the Russian National Security Council and Deputy Defense Minister. He also is a renowned researcher on military and scientific issues. He wrote in a 2019 issue of the *Journal of the Academy of Military Science* that the military technosphere is a complex combination of technologies from several generations which must be studied and used to forecast and implement change. These technologies will impact plans affecting both operational and strategic issues. Various components of the technosphere, to include the combat and non-combat employment of forces and means, need to be assessed[77] for the way technical issues can strengthen or weaken their use. Presently crucial technosphere developments include AI and quantum computing capabilities along with the use of information influence.

Kokoshin stated that information effects against an opponent, along with political and psychological ones, can act as deterrents in confrontations. Each effect relies on "a persuasive, carefully thought-out demonstration of our military technical and operational-strategic capabilities."[78] Information confrontations can include fakes and deliberate disinformation, and this can contribute to an escalation of the situation and affect decision-makers. While not citing the term IWes directly, Kokoshin then stated that AI systems, robotics, and military confrontations in space are all based on information technologies, implying that they are IWes.

For Kokoshin, AI's development strategy is of particular complexity. It requires taking into consideration uncertainty and risks, since some AI applications may have unexpected consequences. This is especially the case when decision-making and command and control issues are under consideration. Further, leaders need information about the political-military, operational-strategic, and tactical situations during information confrontations and struggles for cyberspace superiority. The latter two issues must be included in war games to create a precedent for decision-making support systems.[79]

Kokoshin added that quantum technologies and quantum cryptography are also areas of the utmost importance. Quantum telecommunication network superiority may lie with China, in his opinion, which may allow China to deliver "a blow against the contemporary information-centric methods of waging war" that the US Armed Forces have developed.[80]

Conclusions

Russia is far removed from the days when it was weak and threatened the US with a nuclear attack in the event an information attack was conducted against the Kremlin. Russia now possesses its own arsenal of IWes, one that has different forms than the West. Information technologies lie at the center of IWes and, while they can be found in the arsenals of most nations, they are used in different information-technical and information-psychological ways in Russia. They include forms and methods to introduce into an adversary's systems false scientific theories, paradigms,

[77] A. A. Kokoshin, "Prospects for the Development of the Military Technosphere and the Future of Warfare and Noncombat Employment of Military Force," *Vestnik Akademii Voennykh Nauk (Journal of the Academy of Military Science)*, No. 2 2019, p. 26.
[78] Ibid., p. 27.
[79] Ibid., p. 28.
[80] Ibid., p. 29.

concepts, and strategies, designed to influence another nation's state administration, population, and military force.

For Russia, a nation with a history of using propaganda, active measures, and manipulation techniques (such as reflexive control, getting someone to do something for themselves they are actually doing for you), the information age has served as a blessing. It now possesses the capabilities, forms, and methods that allow Russian operators to disorganize or deter potential opponents simply with the application of various information techniques.

The discussion above has produced the following characteristics, types, advantages, targets, and problems toward which Russian theorists direct the attention of their IWes:

> IWe characteristics: universality, covertness, variety of the forms of software and hardware implementation, radicalism of effects, adequate choice of time and place of employment, and, finally, cost effectiveness;
>
> IWe types: NLWs, color-revolutions, nongovernmental organizations, high-precision weapons, electronic warfare assets, electromagnetic pulse weapons, and software viruses; energy-information-psychological weapons, psychotropic-information weapons, technical means (generators, etc.) of virtual information-psychological weaponry, and information-psychological weapons integrated with fire, radio-electronic, and energy effects;
>
> IWe advantages: can be used in secret, can cross borders with impunity, and can be used against military and civilian structures; offer freedom of access to adversary information systems, such as social media; and allow for the covert preparation of battlefields years in advance with placement of specific software in an adversary's cyber operations;
>
> IWe targets: combat, economic, and social systems, along with computers; programmable apparatuses, command and control means, communication and decision-making channels, and the human intellect and mass consciousness;
>
> IWe problems (from the Russian perspective): IWes threaten strategic stability and the violation of territorial integrity; it is hard to get UN agreement to limit IWe development; it is important to guard against the Western use of color revolutions and nongovernmental organizations to falsify history and manipulate public opinion against Russia; be vigilant for information sabotage;
>
> IWe effects: physical, informational, software, or radio electronic; special pharmacological means and the mass media; information technologies that intensify the accuracy of munitions and reconnaissance assets and offer the pervasive application of propaganda and software; energy (as components of EW,

microwave, and cruise or unmanned aerial vehicles); and chemical (gases, aerosols, pharmacologic agents, etc.).

Russia considers IWes as a non-nuclear strategic weapon capable of inflicting numerous types of destruction or influence against potential opponents, from disorganizing command and control and disabling critical infrastructure to manipulating and persuading public opinion and causing chaos in state administrations and electoral processes. Information resources are used to manipulate objective reality in favor of the Russian perception of events, all the while disregarding logic and the accumulation of available evidence and proof offered by other nations or organizations that totally offset the Russian version of events.

Thus, the Russian understanding of an IWe is much broader than how the term might be understood in the West. There is much for analysts to consider as they ponder Russian access to and use of the IWe. It can come in many forms, and Russia will continue to search for new and innovative applications of their use.

Recommendations:

Since SODCIT capabilities appear to be considered as a non-nuclear strategic IWe, the global implications of this concept need to be studied and assessed for their potential use against the West. The two concepts are closely aligned yet are seldom discussed in parallel. Cyber and satellite operations, which seemingly are without borders, are most likely two aspects of Russia's SODCIT concept that depend heavily on information. Both allow 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.

Western analysts need to closely study Russian IWe concepts for their range and adaptation/use in current events; and analysts need to develop countermeasures against Russian developments designed to thwart democratic processes in other countries. The range and application of IWes can be very different from what a Western perspective might be, and only with a close eye on Russian developments can an overall Russian IWe adaptation plan (technical or psychological) to current events be uncovered and dissected. With regard to sensitivity issues, Russia's use of IWes is different when considered from the perspective of an authoritarian government beset by paranoia and suspicion. There is no objective reality in such a system, especially when it is possible to blame problems on an opponent's use of information resources. What might be considered in the West as alternative opinions are only considered as anti-state opinions in Russia. You are either with us or against us, in the view of a statist like Channel One producer Konstantin Ernst. Russia's focus on technical (cyber, electronic, etc.) and psychological (unrest in a population, demands for open elections, nonstate controlled media positions, etc.) capabilities must be studied.

When assessing Russian activities, Western analysts must be sure to consider both the information-technical or information-psychological ways that Russian might use the forms and methods of information resources and IWes. This breakdown has been consistent for the past twenty years, yet this template is rarely used by Western audiences dissecting Russian behavior. The information-technical component is recognized more easily in the West, since Western scientists are quick to note the use of information technologies in weaponry. The information-psychological aspect is not as well known, researched, or understood. With a Western template it is difficult to consider the use of NGOs, for example, as an IWe. For Russia, an NGO is merely a Western method of influencing the youth or a way to give money to organizations willing to revolt against the Russian system. The same applies to psychotronic weapons, which the authors described as weapons that affect a person's psychology and subconscious in order to reduce one's will, suppress and or temporarily disable a person, or zombify the person, have been under study for over a decade. Such Russian research should remain an area of focus for the West in case breakthroughs are achieved in Russian research methodologies.

Appendix: IWe Definitions

There are a number of ways that IWes have been defined over the past twenty years. This section will summarize several of them. The concept has been a consistent theme and interest of Russian analysts for a number of years.

1996

An information weapons is a specially selected piece of information capable of causing changes in the information processes of information systems (physical, biological, social, etc.) according to the intent of the entity using the weapon.[81]

2000

An IWe is a means to disrupt (copy, deny, or destroy) information resources at stages of their creation, development, dissemination, and (or) retention. The objectives of this action include programs and information support; programmable apparatus, telecommunication means and other means of information and command and control; communications channels that support the circulation of information sources and integrated command and control systems; and the human intellect and mass consciousness.[82]

2002

An IWe is a tool aimed at activating (or blocking) processes of interest to the subject using the weapon in an information system. It is not necessary "to input energy" into an IWe in order to destroy an adversary. It is assumed from the outset that the adversary has all the necessary means for self-destruction. Any technical, biological, or social tool (system) for the purposive generation, processing, transfer, presentation (display), or blocking of data and/or processes operating with data can act as an IWe. The use of an IWe involves: 1. Analyzing the methods and mechanisms to activate programs of self-destruction, self-suppression, self-restriction, and so on that are built into a specific system of an adversary; 2. Developing a specific IWe; 3. Using an IWe against a specific object within the framework of the planned information operation.[83] IWes are directly related to algorithms, which is why any system capable of processing an algorithm based on input data may be said to be an informant system—an object of information warfare.[84]

2010

IWes are special devices and means designed to eliminate (destroy) or modify information by way of influencing an information resource, an information environment, information carriers, or

---

[81] S. V. Markov, "Several Approaches to the Determination of the Essence of the Information Weapon," *Bezopasnost (Security),* No. 1-2, 1996, p. 53.
[82] V. A. Zolotarev, V. A. Yaremenko, A. N. Pochtarev, and A. V. Usikov, *Russia (USSR) in Local Wars and Regional Conflicts in the Second Half of the 20th Century*, Kuchkovo Polye Publishing Moscow, 2000, pp. 458-463 (section on information warfare).
[83] S. P. Rastorguyev, *Introduction to the Formal Theory of Information Warfare*, Vuzovskaya Kniga Moscow, 2002, pp. 7-8.
[84] Ibid., pp. 15-16.

information processes, as well as subjects that use information in their activities…the author sees IWes as, first of all, material items (that is, material devices and means) that influence objects and subjects of the material world, and, only indirectly, information (or traces of the interactions among the material world objects existing as data)…An IWe purposefully actualizes in the opposing side's information sphere such processes as the weapon user desires. As a rule, these processes are aimed at causing self-elimination or malfunctions of the enemy's social or respective technological information system.[85]

2011

IWes—information technologies, systems, and methods used to wage information warfare.[86]

2012

IWes are means of destroying, distorting, or misappropriating masses of information, extracting from them what is necessary after overcoming protection systems, restricting or preventing legitimate users from accessing them, disorganizing the operation of technical resources, and incapacitating telecommunication networks, computer systems, and all high-tech support for the everyday life of society and the functioning of the state.[87]

Dynamic IWes are a unified system of comprehensive, combined, beam, targeted, and strike employment of all forces and means of technical, communications, and information-psychological effects against the subconscious of the objective of the attack.[88]

2014

IWes are 1. The forces and means of generating information directed at doing harm to an enemy, and 2. Its delivery to the target of destruction.[89] Cognitive weapons are a new generation of IWes. The latter is defined as "the introduction into an enemy country's intellectual environment of false scientific theories, paradigms, concepts, and strategies that influence its state administration in the direction of weakening significant national defense potentials."[90]

2019

Information weapons are the totality of technical, software, and other special resources, constructively intended for the formation of information effects for the purpose of disrupting information processes by means of effects against the elements of an information resource (information target) by a special pattern of organized flows of

[85] V. S. Pirumov, Project Leader, *Actual Problems for the Security of Modern Society: Strategy of Survival*, Moscow 2010, p. 42.
[86] "Conceptual Views on the Activities of the Armed Forces of the Russian Federation in Information Space," *Ministry of Defense of the Russian Federation*, p. 5.
[87] N. P. Shekhovtsov and Iu. E. Kuleshov, "Information Weapons: Theory and Practice of their Employment in Information Warfare," *Vestnik Akademii Voennykh Nauk (Journal of the Academy of Military Science)*, No. 1 2012, p. 35.
[88] Ibid., p. 36.
[89] S. S. Sulakshin, "Cognitive Weapons—A New Generation of Information Weapon," *Vestnik Akademii Voennykh Nauk (Journal of the Academy of Military Science)*, No. 1 2014, p. 57.
[90] Ibid., pp. 57-58.

emissions of energy of different physical natures or a specific pattern of selected and structured information.[91]

[91] Lata, Annenkov, and Moiseev, p. 136.