Information Weapons: Russia's Nonnuclear Strategic Weapons of Choice

Timothy L. Thomas

INTRODUCTION

For many years now, Russia has defined and even expanded its concept of "information weapons (IWes)."[1] At one point, Russia attempted to get the concept introduced into United Nations resolutions, which at the time helped 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. At this time, Russia's information warfare weakness was so pronounced that a prominent Russian scientist stated the following at an international conference in Moscow in 1995:

> In studying the potentially 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 stark 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

Approved for Public Release. 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 U.S. Government.

Timothy L. Thomas is an analyst for the MITRE Corporation. He worked for 27 years at the Foreign Military Studies Office (FMSO) at Fort Leavenworth, Kansas. He retired from the U.S. Army as a Lieutenant Colonel in the summer of 1993. Mr. Thomas received a B.S. from West Point and an M.A. from the University of Southern California. He was a U.S. Army Foreign Area Officer who specialized in Soviet/Russian studies. His military assignments included serving as the Director of Soviet Studies at the United States Army Russian Institute (USARI) in Garmisch, Germany; as an inspector of Soviet tactical operations under CSCE; and as a Brigade S 2 and company commander in the 82nd Airborne Division. Mr. Thomas has done extensive research and publishing on military affairs about both Russia and China. He served as the assistant editor of the journal *European Security* and as an adjunct professor at the U.S. Army's Eurasian Institute, and was an adjunct lecturer at the USAF Special Operations School.

times IWes are presented more simply as weapons that help in the manipulation of social media and propaganda. The West seldom considers 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 technologies 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, non-governmental organizations, and a tendency to define objective reality as the Kremlin sees fit, and thus 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. They aimed 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 US in 2000 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, Russian IWes must be considered for its utility in military, political, and psychological warfare, plus also its utility in manipulating news and social media.

As a result, Iwes have become non-nuclear strategic weapons of choice. This article will examine several Russian views of IWes that cover these aspects, beginning with the bigger picture of IWes as strategic weapons. That discussion is followed by an overview of the Russian military literature that has 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 concludes with a very brief commentary by one Russian specialist about the next generation of weapons, such as quantum computing and artificial intelligence concerns.

THE BIG PICTURE: IWES AS NON-NUCLEAR STRATEGIC WEAPONS

IWes are considered non-nuclear strategic weapons in Russia due to their wide reach, even to continents far away (thus, a planetary weapon). According to Russian new-generation warfare expert Vladimir Slipchenko, IWes have also enabled a shift from a "quantitative-force sphere to a quantitative-intelligent sphere."[4] He adds 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] Numerous weapons 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] Slipchenko views the development of space groupings as a key shift 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 coincide with a Russian concept known as the Strategic Operations to Destroy Critically Important Targets (SODCIT) as discussed by numerous outlets. In 2010, a *Red Star* article flagged changes in the nature of wars that would manifest in the various forms in which the Armed Forces are used: "SODCIT has been developed."[9] Retired Colonel General Viktor Barynkin added that "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 conducting such operations, the expansive reach of IWes will play a crucial role. For example, as the Russian journal *Air-Space Defense* stated in 2013:

> 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.

Thus, the term SODCIT implies the extended use of IWes as non-nuclear strategic weapons or assets. Such use in conjunction with aerospace forces or precision-guided munitions is significant since both possess long-reach capabilities into the depth of an adversary's territory anywhere on the globe. Russian planetary warfare theorists must find such concepts intoxicating. For Western analysts, SODCIT should raise concerns as to what Russia is planning.

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

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 considered outstanding) Russian articles to define and discuss an IWe is the article by Major S.V. Markov, which was authored and published in 1996 in the journal *Bezapasnost (Security)*. Leading specialists still 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.[12]

This understanding of IWes and its impact on the information-technical and information-psychological activity of Russia produces a much different national will and language of dialogue than that to which the West is accustomed. Markov is convinced that international and state control over the creation and use of IWes is essential.[13]

According to Markov, IWes can be used in the following ways:

- 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
- 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[14]

In 2000, the work of 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,[15] which describes various forms of IWes. One author, Andrey Krutskikh, became President Putin's point man on cyber issues and where he continues to serve today.

These authors classified IWes based on several attributes to include single and multi-mission/universal purposes; short- and long-range operations; individual, group, and mass disruption or destruction capabilities; various types of carriers; and destructive effect. They further classified IWes as belonging to one of six forms:

1. Means to precisely locate equipment that emits rays in the electromagnetic spectrum and destroy that equipment by conventional fire
2. Means to affect components of electronic equipment
3. Means to affect the programming resource control modules
4. Means to affect the information transfer process
5. Means to disseminate propaganda and disinformation
6. Means to use psychotronic weapons

The pamphlet then discussed the significance and potential types of each of these weapons. The authors analysis of the fifth and sixth forms, which, because they are less prominently covered in the Western press, merit discussion. The fifth form, propaganda and disinformation, can change the information component of command and control (C2) systems by creating a virtual picture that alters reality, changes the system of human values, and manipulates the moral-psychological life of the enemy population. This type of weapon can create disinformation in secure systems and alter navigation systems, information and meteorological-monitoring systems, precision-time systems, and so on.

The sixth form, psychotronic weapons, describes weapons that leverage psychology and the subconscious to attack a person's will, and otherwise suppress and/or temporarily disable or zombify that person. These weapon types include:

- 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 (e.g., projecting an image of "God" onto clouds, etc.)
- Technologies of zombification and psycholinguistic programming[16]

The authors note that information technologies can serve as IWes, which are integral components of high-precision ammunition that can be used to guide missiles via position finding and reconnaissance, as well as by visual, electronic, and other means.

MOVING ON: INTERESTING 2001–2019 DISCUSSIONS

Russia's perception of the West's focus on noncontact warfare and advanced cyber weapons in the 1990s led Russian theorists to conclude that adversaries wanted to develop a "clean" war run by special agents and programmers against a still vulnerable Russia. This led Russian authorities to envision IWes as helping to 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. But recognizing these attributes also raised concerns for Russia's national security,[17] since other nations were farther along in IWe developments.

The following discusses specific elements of Russia's focus on IWes over the past two decades and demonstrates the growing importance of the concept and how it has been integrated, through Russian eyes, into information warfare and its information-technical and information-psychological components; and how IWes have underscored the growing importance of nonmilitary means to influence and win confrontations.

In **2001**, the PIR Center in Moscow published a paper that included a key chapter on IWes, noting that, like the military, information superiority now determines battle outcomes. Invariably, the first to process battlefield information is less vulnerable. Disabling an opponent's command and control systems is key to information superiority. IWes can be high-precision weapons, electronic warfare assets, electromagnetic pulse weapons, or software viruses, among others. The paper noted that an IWe's effectiveness in achieving information warfare missions is often pivotal.[18] The authors then discussed the same six IWe types and their characteristics and effects as were discussed by the 2000 IWe pamphlet authors–no surprise, because one of the 2000 pamphlet authors 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.).[19] Several other IWe advantages included general freedom of access to many information systems, especially in social media; the blurring of traditional legal and ethical borders (are we witnessing a crime or an act of war?); the difficulty in controlling perceptions due to the wide range of "facts" available; and the potential for the covert preparation of a battlefield years in advance through the placement of specific software.[20]

In **2002**, in an important article in *Armeyskiy Sbornik* (Army Journal) by Vladimir Slipchenko, who used the term "new-generation warfare" as early as 2000, noted that information's role will only grow in the coming century. IWes will be system-destroying, he noted, as they will disable entire combat, economic, and social systems, rendering 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 would remain the most important component of a nation's information resources, predicting they eventually would become an independent countermeasure. He also flagged cybernetic warfare as a promising potential element of independent development.[21]

Also, in **2002**, two authors described IWes as nonlethal weapons (NLWs), noting the development of the mass media as an information NLW prerequisite. Of interest is that psychological NLWs also were considered as IWes but had not yet been scientifically confirmed. These NLW types included telepathy, telekinesis, clairvoyance, and other psychological means,[22] all measures under study in Russia for decades but have yet to produce known discernable results.

In **2003**, an article in the journal *Military Thought* noted that the Cold War's end brought with it a desire to eliminate many weapons of mass destruction. This caused the military to focus more attention on precision-guided and other IWes, both lethal and nonlethal. 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 (TIWes). Specialists began to consider information-strike operations, whereby a force could achieve military objectives without land forces. These authors viewed TIWes as 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,[23] to include using psychotropic substances or manipulative information amid distracting messages. New technologies increase the opportunities to develop and use such effects as neuro-linguistic programming.[24]

In **2007**, Sergey Ivanov, Russia's Defense Minister from 2001 until 2007, noted the important potential of IWes to influence the conduct of future wars. He was particularly impressed with the widespread applicability of IWes in conducting 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.[25]

In **2011**, two Russian military specialists wrote on information-strike operations in the journal *Armeyskii Sbornik (Army Journal)*. They viewed the classic triad of fire, strike, and maneuver as no longer capturing 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 particularly important as defined below:

> 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.[26]

IWes conduct information strikes against an adversary's information resources. The types of strikes include information-psychological (which disinform or mislead an adversary), information-psychotropic (to disrupt a person's psyche), radio-electronic, and program-computer. ISOs help gain information initiative and superiority, including command and control of troops and the adversary's reflexive control. ISOs have no spatial limitations, a variety of forms and methods of use, no weather or seasonal constraints, can often be used covertly, and can target command posts and communication nodes.[27]

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 the cover of jamming, destructive strikes are made—operational-tactical and tactical rockets. Third, information support of tactical and army aviation and field artillery is disorganized.[28] To prepare an ISO, an adversary's command and control system must be studied and exposed, and objectives for fire and radio-electronic destruction determined in advance. Disorganizing the enemy's command and control system is critical to planning and coordinating friendly fire destruction elements.[29]

The authors then note the various types of information-psychological weapons that will enhance an ISO, and energy-information-psychological weapons under study for ways to 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 (e.g., generators) of virtual information-psychological and other types of weaponry offer different potential capabilities to affect the human psyche (author's note: 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. The ISO is basically an offensive action, but it can acquire a defensive character if needed.[30]

An influential **2012** article entitled "Information Weapons: Theory and Practice of Their Employment in Information Warfare" views the infosphere as an inexhaustible information space, supply and replenishment source, and one that also features the compactness of information carriers, and bloodless responses—all infosphere features that have exponentially intensified information warfare. IWes can at least be partially kept secret, can cross borders and impact sovereignty, and can be used in both 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.[31]

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, the 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 the means to suppress information exchanges. No radio-electronic effects were offered. However, "dynamic IWes" were 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."[32] Methods for implementing dynamic IWes are mathematically, algorithmically, or software-hardware based, and are most effective when employed as a set in offensive, defensive, or support forms.[33] The authors noted that information-psychological effects result from:

> 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.[34]

Electromagnetic weapons (EMW) are well-known for disrupting or interfering with information system operations. They can disrupt a country's economy, production, and defense capabilities. Disrupting systems that exchange information for command decisions can have serious consequences. C4ISR is the main target 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."[35]

The authors conclude as follows:

> Universality, covertness, variety of the forms of software and hardware implementation, the 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.[36]

Near the end of **2012**, S.G. Chekinov and S.A. Bogdanov defined the initial period of war (IPW) in *Military Thought*, as the time when forces are deployed pre-conflict, to create favorable conditions for committing their main forces. Under the new military, political, and economic conditions, the authors attribute special significance to IPW for winning a conflict:[37]

> 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.[38]

Of interest are malware and other information technologies secretly placed in the infrastructure or computers of potential opponents in peacetime that would help accomplish some of the main means for winning a war, such as totally upending an opponent's command and control system. Such technologies are IWes. The authors noted that "major military, political, and strategic objectives of the war must be achieved in its initial period."[39]

In early November **2013**, the State Duma Security and Anticorruption Committee recommended amending a Federal Security Service (FSB) law to allow police investigations to counter threats to Russia's information security, such actions previously permitted only as to state, military, economic, or environmental security threats. The report indicated that harmful software, for example, can be used as an information weapon[40] 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,[41] noting that "decisive battles in new-generation wars will rage in the information environment," where computer operators will manipulate computers far away from the conflict. Information operations will induce world public opinion to accept the need to restore democracy and fight tyranny.[42] Once information superiority is achieved in peacetime; conflict may even be avoided. If a conflict appears inevitable, it is visualized information technologies will heavily influence and possibly dominate its opening phases, as there will emerge a targeted information operation, an electronic warfare operation, and high-precision weaponry loaded with information technology.[43]

In **2015**, at a presentation in Garmisch, Germany, noted Russian information warfare experts I.N. Dylevsky and S.A. Komov offered a paper titled "Rules of Conduct in Information Space—An Alternative to an Information Arms Race," noting that "[a]nother aspect of confrontation in the information sphere is a rapid advancement and proliferation of information weapons."[44] Their use can lead to industrial disasters or, worse yet, critical infrastructure (finance, energy, transport, etc.) destruction. The authors, while urging that it was time to adopt universal laws to prohibit their development,[45] did not expand on how this could be done, or how nations could control the risk of their development elsewhere.

Later that year, *Military Thought* described nonlethal weapons (NLWs) as effective information warfare assets, implying their potential 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."[46] Ironically, the "mood" of recent anti-Kremlin demonstrations in Moscow was provoked or exacerbated by the Kremlin's decision to keep certain people off election ballots. So, moods can either be "provoked" or "defused" (with NLW) by the same government officials.

Russia's *National Security Strategy*, published in 2015, referred 36 times to the term "information" without ever mentioning the term "cyber." The primary 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* reported that 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." Information is also mentioned as one way to enhance strategic deterrence. Information associated with extremism or terrorism is taken to be a significant threat to public security and, countering such threats requires an information infrastructure that ensures the public's access to information on issues relating to the sociopolitical, economic, and spiritual life of Russia's citizens.[47]

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" and 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 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.[48]

"Information resources" the West uses against Russia, according to a *New York Times* source, are nongovernmental organizations (NGOs) and operations aimed at the young. For example, President's Putin's 2007 speech in Munich expressed concerns about NGOs, alleging 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."[49]

In **2017**, Chekinov and Bogdanov shifted focus from new-generation wars to the importance of "new-type" warfare. stating that globalization threatens a "new type" of war, which could "become the pivot of historical life in the 21st century."[50] New-type warfare is characterized using "political pressure, information sabotage, cashing in on humanitarian issues, secret-service activity, and unfair and cunning diplomacy."[51] Earlier in the article, the authors addressed the growing impact of information warfare. Information operations use manipulated information, computers, and telecommunications technologies to 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.[52] The realm of the virtual, both informational and cognitive, is exploited.[53] Again, while not explicitly mentioning IWes, the article clearly views IWes as major components 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 information society, globalized information processes, and the democratization and heightened importance of socio-political factors in society had created an information struggle. Internally, the struggle is about controlling large numbers of people. Externally, the information struggle rages both in times of peace and war among states, regardless of whether the states are allies or enemies. Twenty-first century struggles include a state's information capabilities, which work to achieve the strategic advantages[54] that come from information superiority.

Information, the authors note, moves through space and time via processes of "searching, collecting, storing, processing, presenting, accumulating, disseminating, and decision-making."[55] Depending on how information is used and where it is located (in military weapons technology, in a human mind, in command and control processes, etc.), it produces 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.[56]

The authors believe 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.[57]

A final **2019** article 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 never to 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.[58] This has been a typical Russian response to avoid responsibility at all costs, even to the detriment of its own credibility. Russia is quick to openly deny complicity in any accusation leveled against it by other nations. To date, its responsibility for the shootdown of MH-17 airliner over Ukraine and its involvement (based on credible evidence) in the poisonings of former Russian intelligence operators Aleksandr Litvinenko and Sergey Skripal (both on UK territory) are such examples. So is its failure to accept responsibility for the doping of its athletes in the Sochi Winter Olympics, a charge first levied by a Russian!

FROM INFORMATION WEAPONRY TO KOKOSHIN'S TECHNOSPHERE

Now shifting attention from IWes to artificial intelligence (AI) and quantum computing issues, while these topics are beyond the scope of this article, their mention is important, given their significance in the continuing evolution of IWes.

Andrey Kokoshin, former Secretary of the Russian National Security Council and Deputy Defense Minister, 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, and in several dimensions, that must be studied and used to forecast and implement change. These technologies will affect both operational and strategic plans. Various components of the technosphere, to include the combat and non-combat employment of forces and means, need to be assessed[59] for how technical issues can strengthen or weaken their use. Crucial technosphere developments currently include AI and quantum computing capabilities, along with the use of information influence.

Kokoshin stated that the ability to impose information effects on an opponent, including political and psychological effects, can deter confrontations. Each effect relies on "a persuasive, carefully thought-out demonstration of our military-technical and operational-strategic capabilities."[60] Information confrontations can include fakes and deliberate disinformation, and these can contribute to an escalation of the situation and affect decision-makers. While never citing the term "IWes" directly, Kokoshin describes AI systems, robotics, and military confrontations in space all as information-based technologies, thus implying that they are IWes.

Kokoshin views AI's development strategy as complex, requiring consideration of uncertainty and risks: some (if not all) AI applications may have unexpected consequences, particularly when decision-making and command and control issues are at stake. Further, leaders need information as to political-military, operational-strategic, and tactical situations during information confrontations and struggles for cyberspace superiority. The last two issues must be included in war games to create a precedent for decision-making support systems.[61]

Kokoshin also views quantum technologies and quantum cryptography as critically important. Because China may have the edge with quantum telecommunications network superiority, he also believes that China can perhaps deliver "a blow against the contemporary information-centric methods of waging war" that the U.S. Armed Forces have developed.[62]

CONCLUSIONS

Russia is far removed from the days when it threatened the US with a nuclear attack if an information attack was conducted against the Kremlin. Russia now possesses its own arsenal of IWes, one with different forms than what the West is familiar with. Russia believes IWes are non-nuclear, strategic weapons capable of inflicting numerous types of destruction or influencing 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 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 by Russia. 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 that totally offset the Russian version of events.

Russian theorists focus their IWes in the following characteristics, types, advantages, targets, and challenges:

- IWe characteristics: universality, covertness, variety 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, NGOs, high-precision weapons, electronic warfare assets, electromagnetic pulse weapons, 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: warfighting, 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 (Note: this is a 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; we must 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.)

In Summary, 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, especially as Russia will continue to search for new and innovative applications of their use.

NOTES

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, 7, attended by the author of this article.
3. Andrei Soldatov and Irina Borogan, *The New Nobility,* Public Affairs New York, 2010, 108-109.
4. V.I. Slipchenko, *Beskontaktnye Voyny (Noncontact Wars)*, Publishing House Gran-Press, 2001, 55.
5. Ibid., 82. Slipchenko wrote on new-generation warfare more than a decade before Bogdanov and Chekinov did so in 2013, to great fanfare.
6. Ibid., 85-88.
7. Ibid., 90-91.
8. Ibid., 161.
9. Ibid.
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*, April 10, 2013.
12. S.V. Markov, "Several Approaches to the Determination of the Essence of the Information Weapon," *Bezopasnost (Security)*, No. 1-2, 1996, 53.
13. Ibid.
14. Ibid., 56.
15. 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, 20-21. This IWe discussion is taken from Timothy Thomas, *Cyber Silhouettes*, Foreign Military Studies Office, Fort Leavenworth, KS, 2005, 168-171.
16. Ibid.
17. N.P. Shekhovtsov and I.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, 39.
18. 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, 69-109.
19. Ibid.
20. Ibid.
21. 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, 30-32.
22. Vitaliy Tsygichko and Vladimir Dyachenko, "Non-Lethal Weapons," *Yadernyy Kontrol (Nuclear Control)*, 18 September 2002, 58-67.
23. S. P. Nepobedimiy and V. F. Prokofyev, "The Intellectualization of Weapons and Weapons against Human Intelligence," *Voennaya Mysl' (Military Thought)*, No. 7 2003, 26.
24. Ibid., 27.
25. Oscar Jonsson, *The Russian Understanding of War*, Georgetown University Press, 2019, 94, as quoted in Steve Blank, "Russian Information Warfare as Domestic Counterinsurgency," *American Foreign Policy Interests*, 34.
26. I.N. Chibisov and V.A. Vodkin, "The Information-Strike Operation," *Armeyskii Sbornik (Army Journal)*, March 2011, 46.
27. Ibid., 46-47.
28. Ibid., 47.
29. Ibid., 48.
30. Ibid., 48-49.
31. Shekhovtsov and Kuleshov, 35.
32. Ibid., 36.
33. Ibid., 36-37.
34. Ibid., 37.

NOTES

35. Ibid., 38.
36. Ibid., 39.
37. 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, 15-16.
38. Ibid., 19.
39. Ibid., 25.
40. Unattributed report, "A State Duma Committee Has Approved Amendments Relating to Information Security," *RIA Novosti Online (RIA News Online)*, November 8, 2013.
41. S. G. Chekinov and S. A. Bogdanov, "On the Nature and Content of a New Generation War," *Voyennaya Mysl' (Military Thought)*, No. 10, 2013, 13-14.
42. Ibid., 20.
43. Ibid., 23.
44. Ninth International Forum "Partnership of State Authorities, Civil, Society, and the Business Community in Ensuring International Information Security," April 20-23, 2015, Garmisch Germany, 36.
45. Ibid.
46. 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, 51.
47. Edict of the Russian Federation President, "On the Russian Federation's National Security Strategy," *President of Russia Website*, December 31, 2015. See sections 13, 21, 36, 43, and 53 of the document.
48. 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, 20.
49. 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.
50. 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, 43.
51. Ibid., 40.
52. Ibid., 37.
53. Ibid., 32.
54. 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, 128-129.
55. Ibid., 130.
56. Ibid., 136.
57. Ibid., 136-137.
58. See Julia Davis, "Russia to Iran: Don't Admit Guilt—Blame the U.S. Instead," https://www.thedailybeast.com/russia-to-iran-dont-admit-guilt-blame-the-us-instead, accessed January 11, 2020.
59. 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, 26.
60. Ibid., 27.
61. Ibid., 28.
62. Ibid., 29.