MITRE

Sponsor: USEUCOM Contract No.: W56KGU-17-C-0010 Project No.: 0719S120

Three Discussions of Russian Concepts: 1.Russian Information Weapons; 2.Baltic Defenses (Estonia, Latvia, Lithuania) against Russian Propaganda; and 3.Russia's Development of Non-Lethal Weapons

Author: Timothy Thomas

March 2020

Approved for Public Release: Distribution Unlimited. Case Numbers 20-0235; 20-0050; 20-0051; 19-3194; and 20-0145.

McClean, VA

FOREWORD

Russia has long been captivated by the power of information as a weapon, most notably in a historical sense using propaganda to influence and persuade audiences. With the onset of the information age, the concept's development and application increased dramatically. The power of information-technologies when applied to weaponry increased the latter's capabilities due to increased reconnaissance and precision applications. The power of social media was used to influence populations both at home and abroad. Both developments fit perfectly into Russia's information warfare concept, whose two aspects are information-technical and information-psychological capabilities. Information's universality, covertness, variety of software and hardware forms and implementation, efficiency of use when choosing a time and place of employment, and, finally, cost effectiveness make it a formidable commodity when assessed as weaponry.

Russian efforts to define and use IWes are well documented. In the 1990s there were efforts to define information weapons (IWes) at the United Nations, efforts that failed. At the turn of the century an initial Information Security Doctrine was published in Russia, a doctrine later updated in 2016. Over a decade ago, Russia began hosting twice-yearly conferences on information topics, where each year the first conference was conducted in Garmisch, Germany and the second in Russia or another nation. Russian specialists began teaming up with Chinese specialists as well.

These and other issues will populate the contours that follow. Chapter One discusses the various types of IWes that Russia addresses. Through the years, they have defined an IWe in many ways, and a quick look at these definitions over the past 20 years is located at the Appendix to Chapter One. Russia considers precision guided weaponry, electronic warfare, reconnaissance assets, computers, and satellites, among other assets, as information-technical weaponry. Propaganda, nongovernmental organizations, nonlethal capabilities, reflexive control methods, neuro-linguistic programming, so-called color revolutions, and social media, among other assets, are considered as information-psychological means. Russian theorists continually stress the importance of attaining information superiority with such weaponry in order to control the initial period of war; and they recognize that the race to process information faster than your opponent is a race that must be won, since it is crucial to success. The discussion is a little longer than this author's article on the same topic that appeared in the summer edition of *Cyber Defense Review*.

Chapters Two, Three, and Four discuss Russia's IWes used against the three Baltic nations of Estonia, Latvia, and Lithuania in that order. These nations are on the frontline fight against Russian IWes, the latter composed primarily of information-psychological means. These nations, all NATO members, have developed measured yet insightful contingency plans that address Russian efforts. Estonia's leadership has noted that the key to changing the attitude of ethnic groups in Estonia is to bring them into Estonia's information space instead of just Russian information space. Latvia has proposed laws, developed an ideological foundation to overcome susceptibilities, and developed messages

and images to stabilize Latvian values. The nation's leadership is encouraging its citizens to educate themselves on Russian media techniques and methods of argumentation. Lithuanian officials have developed several templates that describe Russian propaganda targets, dissemination techniques, and information themes, and the nation has developed a new National Cyber Security Strategy.

Finally, in Chapter Five, Russia's focus on developing nonlethal weaponry (NLWs) is outlined, which some theorists describe as IWes. The Russian discussion of NLWs is divided into their use internally and externally. The former describes how Russia's National Guard will use NLWs for crowd control and other uses, while externally they will be used against terrorists first and then against an opponent along with traditional forms of warfare. For example, laser blinding devices might be fitted to drones along with a remote nonlethal electric shock device, according to one report.

It is thus important for Western audiences to understand the expanding nature of Russia's comprehension of IWes. Their forms and methods of application vary in some detail from the way that the West understands the concept.

Timothy Thomas
EUCOM Information Operations Domain Specialist
MITRE Corporation, 2020

TABLE OF CONTENTS

TABLE OF CONTENTS....5
Executive Summary for Information Weapons:....7
Executive Summary for Estonia:....7
Executive Summary Latvia:....8
Executive Summary Lithuania:....8
Executive Summary Nonlethals:....9
CHAPTER ONE: INFORMATION WEAPONS....10
Introduction....10
The Big Picture: IWes as Non-Nuclear Strategic Weapons....11
The First Important IWe Discussions....13
Moving On: Interesting 2001-2019 Discussions....15
Countering Russian IWes....27
From Information Weaponry to Kokoshin's Technosphere....28
Conclusions....29
Appendix: IWe Definitions....31
CHAPTER TWO: ESTONIA....33
Introduction....33
A Few Keys to Estonian Reporting on Russian Propaganda....34
A Look at Other Important Developments through the Years....36
Conclusions....43
CHAPTER THREE: LATVIA....45
Introduction....45
Countering Russian Propaganda: Some Latvian ideas (2013-2016)....45
Latvian and Russian Information Positions from 2017-2019....47
Conclusions....54
CHAPTER FOUR: LITHUANIA....55
Introduction....55
Information....55
Cyber 60
Conclusions....63
CHAPTER FIVE: NONLETHAL WEAPONS....64

Introduction.....64
A Change in Definition? 65
The Production Plan for NLWs.....67
Using NLWs Internally and Externally 69
Physical, Chemical, Biological, Radiation, and Information NLWs.....71
Conclusions.....73

EXECUTIVE SUMMARIES

Executive Summary for Information Weapons:

Information weapons (IWes) have a comprehensive meaning in Russia that encompasses both strategic and operational applications. IWes are considered as non-nuclear strategic weapons that have the capability, with their cyber and precision-weaponry components (among others), to conduct 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 IWes; 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 IWe developments and organizations. Such elements include nonlethal weapons (NLWs), which Russia is also pursuing, nongovernmental organizations (NGOs), 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 IWe. 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 relation 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.

Executive Summary for Estonia:

Russian influence operations aim to shape Estonia as an undemocratic community and a problematic partner for Estonia's allies. Russia's media offensive is focused both on

splitting Estonian society and using media tools to conduct foreign policy. Fake accounts from Russia are designed to interfere with internal Estonian discussions and polarize people's views, distort topics, and escalate public debates. Russia offers covert financial assistance, if necessary, to the Estonian government's opponents; discredits officials by stealing and leaking internal information; and intentionally spreads false information in social media, a specific way to target youth. Estonia's leadership has responded to these challenges, noting that the key to changing the attitude of ethnic groups in Estonia is to bring them into Estonia's information space instead of just Russian information space. This has resulted in the creation of Estonian TV channels that feature presentations in the Russian language. In addition, an increased military presence of NATO nations in Estonia strengthens the nations resolve and deterrent posture. Estonia's Defense Minister Hannes Hanso stated that a psychological gap between Russia and Estonia is growing and that "if we look at internal Russian politics we see that the legitimacy of the regime is built on confrontation with the West."[1] In his opinion, this anti-Estonian focus diverts the Kremlin population's attention away from its own domestic problems.

Executive Summary Latvia:

A Latvian writer for the news and information service *Delfi* noted that Russian propaganda is like carbon monoxide gas, since it flows into a room unnoticed, cannot be smelled, and puts people's logic to sleep. It disinforms, demoralizes, and destabilizes audiences. Latvian journalists and state officials believe that efforts to confront Kremlin propaganda cannot be accomplished alone with only simple bans or protests. Latvia needs to reinforce its own value system to strengthen its culture and self-confidence. These attempts to limit Russian disinformation have met with some success. Latvia has proposed laws, developed an ideological foundation to overcome susceptibilities, and developed messages and images to stabilize Latvian values. Latvia is encouraging its citizens to educate themselves on Russian media techniques and methods of argumentation. Educational opportunities are further supported by studies being conducted at Latvian think tanks, which are available for downloading and reading. Latvia's successes and disappointments are discussed in their information struggle to educate Latvian society in critical thought and thereby immunize them from Russian propaganda.

Executive Summary Lithuania:

Lithuanian officials have developed several templates that describe Russian propaganda targets, dissemination techniques, and information themes, among other issues. The nation has developed a new National Cyber Security Strategy and is regarded as the fourth best country in the world regarding cybersecurity issues. Russian propaganda works to create wedges by creating problems, violating international law, and creating geopolitical tensions. Lithuania's continued information and cyber diligence directed at Russia's propaganda assault helps everyone better picture what these wedges are and their shape as well as where the Kremlin is directing its efforts. To counter these wedges, Lithuanian officials developed what they call the five layers of Russia's propaganda image and they have outlined Russia's propaganda dissemination network. Russian propaganda's further goals are regime change and attempts to falsify history. A Lithuanian Army

[1] Gerard O'Dwyer, interview with Hannes Hanso, *Defense News*, 1 February 2016, p. 19.

representative noted that there is a Russian information campaign designed to focus on regime change.

Executive Summary Nonlethals:

Russian military analysts believe that nonlethal weapons (NLWs) offer commanders new options and ways to handle crises, providing flexible responses to situations and reducing the chances of serious injury among noncombatants. Physical NLWs are used to incapacitate opponents, control crowd behavior, or induce psychological effects, while others (chemical, biological, and radiological NLWs) are used to block access to areas or disrupt electrical components of transport, among other uses. New forms of NLWs are constantly under development in Russia, and the planning process seeks to identify NLW trends 20-25 years out. Russian discussions of NLWs divide their use into internal and external areas of application. The former indicates that the Russian National Guard will be involved in the use of NLWs for crowd control and other uses, while externally they will be used against terrorists first and then against an opponent in conjunction with traditional forms of warfare. For example, laser blinding devices, which can cause temporary loss of vision without harmful consequences, can be fitted to drones along with a remote electric shock device, according to one report. Perhaps NLWs are an aspect of President Vladimir Putin's asymmetric approach to conflict.

CHAPTER ONE: INFORMATION WEAPONS

Introduction

For many years now, Russia has defined and even expanded on its concept of "information weapons (IWes)."[2] 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 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.[3]

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 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 world-wide. 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 thus avoid "the truth." Their use appears to be a modern version of Soviet active measures, which were operations developed years ago

[2] 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. A shorter version of this chapter was previously published as an article in the Summer edition of *The Cyber Defense Review* (CDR).

[3] 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.

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 U.S 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."[4]

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; and with a discussion of both other ways to consider an IWe (as the overt rejection of the truth and as its use as an information deterrent) and with a Western analyst's thoughts on how to counter media-related IWes. A list of Russian definitions of IWes from different time periods is located at the Appendix.

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."[5] 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."[6] Numerous weapons depend on information technologies. Acoustic, electromagnetic effect, radiation, beam, and heat weaponry[7] are under development as is the "unity of intelligence collection and destruction," namely the development of reconnaissance-strike and reconnaissance-fire complexes.[8] Slipchenko views the development of space groupings as a key directional 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."[9]

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

Slipchenko's thoughts coincide with a Russian concept known as the strategic operation to destroy critically important facilities (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."[10] 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."[11]

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.[12]

As noted, these assets rely on information technologies.

A *Military Thought* article in 2014 mentioned SODCIT. It stated that determining combat missions, methods, and variations of long-range precision-guided munitions (PGMs) can be presented according to a priority-ranked subprocess that included SODCIT.[13] 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 their 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.[14]

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.

---

[10] Marina Yeliseyeva, "Lessons for All Time," *Krasnaya Zvezda (Red Star) Online*, 27 October 2010.
[11] Ibid.
[12] 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.
[13] 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.
[14] Ibid.

How did Russia ultimately arrive at this conclusion that IWes provide 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.[15]

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.[16]

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.[17]

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*,[18] which describes various forms of IWes. One

---

[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.

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 destroys 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 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 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, or affect reliable power sources.

The third form, the means for affecting programming resource control modules, was designed to disable or alert the operating algorithms of control systems through 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, is designed to stop or disorganize the functioning of subsystems exchanging 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 authors analysis of the fifth and sixth forms, which, because they are less prominently covered in the Western press, merit further discussion. The fifth form, propaganda and disinformation, can change the information component of 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 (25^{th} 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.[19]

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. 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 like 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: 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

[19] Ibid.

led Russian authorities to envision how 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 concern for Russia's 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 options. For example, cyber or information-strike weapons (described below) were soon developed and considered as Russian offensive IWes, while over-the-horizon radar stations were developed and considered as Russian defensive IWes.[21]

The following explanation 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's 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.[22] 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.).[23] Several other IWes 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

[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. The author would like to thank Dr. Harold Orenstein for the translation of this article.
[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.

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.[24]

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.[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 about information resources and warfare echo much of Slipchenko's theory and understanding of information's impact on Russian warfare techniques (no stereotyping, blurring of war and peace, etc.). Russia now has cyber forces without an indication that they have become an independent branch of service.

Also, in **2002**, two authors described IWes as nonlethal weapons (NLWs), noting the development of the mass media 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,[26] 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

[24] Ibid.
[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.

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, 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.[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, Russia's Defense Minister from 2001 until February 2007, noted the important potential of IWes to influence the conduct of future war. 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.[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, Ryabchuk 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 the continued

---

[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.
[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.

development of forms in which troops and methods for conducting 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]

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.[34]

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. ISO's help gain the initiative and superiority in the information sphere, including command and control of troops and the reflexive control of opponents. ISO's 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.[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 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.[36] 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

[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.
[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.

advance. Disorganizing the enemy's command and control system is critical to planning and coordinating friendly fire destruction elements.[37]

The authors then note that there are 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. Radio disinformation, active and passive jamming, false radar targets, and fake communication centers facilitate misleading an opponent. The ISO is basically an offensive action, but it can acquire a defensive character if needed.[38]

An influential **2012** article titled "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.[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, 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" 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] Methods for the 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. The military and political leaderships as well as world public opinion (when conducted with special information-

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

psychological operations) are specific targets of destruction.[41] 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. 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 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 in the authors' opinion.[43]

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."[44] The authors conclude as follows:

> 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 defined the initial period of war (IPW) in *Military Thought* as the time when forces are deployed before the start of a 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:[46]

---

[41] Ibid., pp. 36-37.
[42] Ibid., p. 37.
[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.

> 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 are malware and other types of 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. 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 achieved in its initial period."[48] Inserting key IWes into the systems of an adversary in peacetime creates favorable conditions for either winning victory before conflict starts or for the massive disorganization of an opponent, rendering his systems less dependable and more vulnerable to destruction with other types of weaponry.

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[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,[50] 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 operation will induce 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 a conflict appears inevitable, it is visualized information technologies will heavily influence and possibly dominate its opening, as there will emerge a targeted information operation, an electronic warfare operation, and high-precision weaponry loaded with information technology.[52]

---

[47] Ibid., p. 19.
[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.

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."[53] 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,[54] 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."[55] 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." For most Westerners, this appears to be exactly what Russia did in Ukraine, never mentioning Putin's influence on Ukrainian President Yanukovych and striking out on an information campaign that, according to even some Russian analysts, surpassed anything seen during the time of the Soviet Union. Information is also mentioned as one way to enhance 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 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, 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.[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" and how their utility could be quickly furthered through the adaptive use of information resources as a weapon:

---

[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.
[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.

> 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.[57]

"Information resources" the West uses against Russia, according to Russian sources reported in the *New York Times*, are nongovernmental organizations (NGOs) and operations aimed at the young. For example, President 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."[58]

In **2017** Chekinov and Bogdanov shifted focus from new generation wars to the importance of "new type" warfare, stating that globalization threatens war a "new type" of war, which could "become the pivot of historical life in the 21st century."[59] New type warfare is characterized using "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 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

---

[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. The author would like to thank Dr. Harold Orenstein for the translation of this article.

[58] Thom Shanker and Mark Landler, "Putin Says U.S. Is Undermining Global Stability," *The New York Times*, 11 February 2007 at https://www.nytimes.com/2007/02/11/world/europe/11munich.html, downloaded 9/1/2020.

[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.

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[63] 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."[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 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.[65]

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.[66]

Another **2019** article, this time 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 the detriment of its own

[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. The author would like to thank Dr. Harold Orenstein for the translation of this article.
[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.

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 such examples it is clear that openly using the "big lie" and presenting its (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.

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 to avoid responsibility. Yaffa 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 Russia 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 that makes 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 added 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 Yurchak as noting that "Since nothing about the representation of the world was verifiably true or false, the whole of reality became ungrounded."[74]

---

[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.

This idea that objective reality does not 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 in Russia 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 that is 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 except in other totalitarian-type regimes.

One final use of IWes should be noted, one that was not covered in any of the presentations above but was noted by Slipchenko is the use of information deterrence. He noted that "strategic non-nuclear forces will find wide use in new-generation wars and subsequently also will take on a deterrence function." Russia surreptitiously uses 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) 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 application of digital means to provide legal justification for its case, deterring other nations from entering the region. This type of deterrent force supports the Russian "containment" role of deterrence more than its usual "intimidation" role.

Countering Russian IWes

Only one aspect of countering Russian IWes, that being Russian attempts to create social division in societies, 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 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 adeptly identifies specific audiences inside electorates that appear amenable to their messages and through intricate strategic planning offers 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 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

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

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

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 is both a former Secretary of the Russian National Security Council and a Deputy Defense Minister of Russia's military. He 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 dimension, 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[77] 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."[78] 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,

[76] Ibid.

[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. The author would like to thank Dr. Harold Orenstein for the translation of this article.

[78] Ibid., p. 27.

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.[79]

Kokoshin also views quantum technologies and quantum cryptography as critically important. Because China may have the edge with quantum telecommunication network superiority, he also believes that China can perhaps 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 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 in Russia. Information resources are sued 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. They include forms and methods to introduce into an adversary's systems false scientific theories, paradigms, 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.

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

- 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, NGOs, high-precision weapons, electronic warfare assets, electromagnetic pulse weapons, software viruses,

[79] Ibid., p. 28.
[80] Ibid., p. 29.

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 adversaries cyber operations

- IWe targets: warfighting (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 (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; 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.

Appendix: IWe Definitions

There are several 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 few 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 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 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

---

[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.

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

---

[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. The author would like to thank Dr. Harold Orenstein for the translation of this article.

[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. The author would like to thank Dr. Harold Orenstein for the translation of this article.

[90] Ibid., pp. 57-58.

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

CHAPTER TWO: ESTONIA

Introduction

Estonia, since declaring its freedom from Russia on 6 September 1991, has endured several soft power attacks from Moscow. Most have been in the form of propaganda attacks, but a few have been more belligerent and even destructive. For example, in response to Estonian desires to move the so-called "Bronze Soldier" (for most Estonian's, a symbol of the Soviet occupation of the country) from its location in central Tallinn to the city's outskirts,[92] on 27 April 2007 Russia, which never directly admitted complicity, initiated a massive information technology attack against Estonia. Numerous institutions were targeted (banks, media, police, government institutions) and some Russian news stories denying their involvement continued into November 2017. The information weapons used were botnets that led to denial of services through a barrage of requests on the targeted sites. NATO later established its Cooperative Cyber Defense Center of Excellence in Estonia's capital, Tallinn.

In addition, other areas of perpetual tension continue to exist between Estonia and Russia. This pertains in particular to the large Russian population that elected to stay in Estonia after the latter's declaration of independence from the Soviet Union (a 2016 census indicated that the vast majority of the Estonian population was either ethnic Estonian [900,000 plus] or Russian [330,000 plus]).[93] As a result, the loyalty of some Russian residents to Estonia is sometimes questioned. One town, Narva, is of real concern to Estonian authorities. Narva is a key industrial and natural resource area which precariously juts out into Russia, sharing a border on three sides and thus could easily be cut off and isolated. In Narva, 96 percent of the population are native Russian speakers and 88 percent ethnic Russians. One report noted that 47 percent of the city's inhabitants are Estonian citizens and 36 percent are Russian Federation citizens.[94] Such an ethnic mix makes Narva not only attractive as a future asset to Russia, but also provides some justification for aggressive actions if they would so chose to assert them. Russia's annexation of Crimea further exacerbated this concern when Russia acted with impunity. For one month in 2018, Kersti Kaljulaid, Estonia's President, even moved her office from Tallinn to Narva as a sign of support to the city.[95]

But it is the drip of propaganda from Russian sources that concerns Estonian officials daily. The Estonian Information Board wrote in 2017 that Russian influence operations aim to shape Estonia as an undemocratic community and a problematic partner for their allies.[96] Along with attempting to legitimize the occupation of Crimea in the press and on TV, Russia appears to be using media as a foreign policy tool. It is also trying to

[92] Benoit Vitkine, "Estonia, Moscow's First Cyber Victim," second installment of five in the series "The Kremlin's Information Wars," *LeMonde.fr*, 14 March 2017.
[93] See https://www.worldatlas.com/articles/largest-ethnic-groups-in-estonia.html
[94] https://en.wikipedia.org/wiki/Narva
[95] Josh Rubin, "NATO Fears That This Town Will Be the Epicenter of Conflict with Russia," 24 January 2019, downloaded at https://www.theatlantic.com/international/archive/2019/01/narva-scenario-nato-conflict-russia-estonia/581089/
[96] No author provided, "EIB: Russia Trying to Introduce Tensions into Relations between Communities in the Baltics," *Tallinn BNS* (in English), 8 February 2017.

influence young people, who have little context of what a Soviet-era lifestyle was like. The Russian interpretation of news and the commentary of its guests intermix truth with lies. To help confront this media offensive, Estonia is providing its own Russian-speaking TV channels and other forms of media to counter Russian aggression.

A Few Keys to Estonian Reporting on Russian Propaganda

In the 2018 annual review conducted by Estonia's Internal Security Service, it was stated that the Kremlin attempts to manipulate the young, to create public tension over memorials, and to legitimize the annexation of Crimea. In this sense the government-controlled Russian media is used as a foreign policy tool. Russia appears to seek out anxieties and tensions that could be "escalated into something worse through provocation."[97] Young people lack the context of the operations that Russia conducted against the nation in the past. Russia's goal is to attract the young to Russia's sphere of influence through the cultivation of the myth of Russia's Red Army as liberators (instead of aggressors) and as partners in the fight against terrorism.[98] The report of the Internal Security Service mentioned numerous organizations and personnel that, Kremlin backed, seek to characterize Estonia as a Nazi nation or develop other anti-Estonian activities.[99]

One Estonian article discussed the Russian concept of what it means to be a "Russophobe." The Russian portal *Sputnik* defined a Russophobe as follows: If one speaks out against peoples lawfully expressed will, one is against Russians, and that is what is called Russophobia. The article listed some criteria under which *Sputnik* considers an Estonian to be a so-called Russophobe:

- Calling for Estonia's Russian-speaking population to be denied an education in their native language
- Habitually referring to Russians as "tibla" (offensive term for Russians or Soviets)
- Aiding the Ukrainian nationalist party Right Sector
- Blaming Russia for all mortal sins and personal problems
- Criticizing Russian authorities and calling for their overthrow
- Making offensive comments about the lawfully elected Russian head of state, Vladimir Putin
- Protesting against the Russian regime, which is supported by the majority of Russians
- And expressing doubt regarding whether the Russian population really supports its current legal president and his policies.[100]

[97] No author provided, "Estonia's ISS: Biggest Threat Arises from Russia's Foreign Policy Goals," *Tallinn BNS* (in English), 12 April 2018.
[98] Ibid.
[99] No author provided, "Russia-Related Networks in Estonia Part Four," *Tallinn Propastop*, 5 July 2018.
[100] Oleg Samorodni, "Russian Media Journal List of Russophobes Could be Warning: Estonian Businessmen Will Be Next on List," *Tallinn Eesti Paevaleht Online*, 19 June 2018.

It was also noted that this is a warning signal for people who have not been so addressed up to now but might be Russophobes. Politicians, journalists, and businessmen are all among those who need to accept a "word to the wise."[101]

Estonian Foreign Minister Sven Mikser stated in 2018 that Russia's media is directly or indirectly under Kremlin control and imparts its national message as part of its fight for information space with the Western world. As a result, Estonia has allocated resources that can serve as an alternative for the Russian-speaking population in Estonia.[102] That is, Estonia is providing its own Russian-speaking channels for this element of its population. Efforts in this area extend back to 2015, when Germany and Estonia decided to cooperate in the media sphere to counterbalance Russian propaganda. Specific steps then included supporting *Estonian Public Broadcasting* and online services in Russian, sharing TV and web programs produced in Russian by *Deutsche Welle*, and supporting training for journalists and journalism students via the German Academic Exchange Service. The idea was to offer Russian-speaking residents of Estonia a form of neutral information instead of just responding to Russian propaganda.[103]

Another 2018 report noted that Russian covert propaganda is hidden in between entertainment shows on the *Perviy Baltisky Kanal* (*First Baltic Channel* or *PBK*), *RTR Planeta* (*Planet*), and *NTV Mir* (*World*) that are all controlled by the Kremlin. The interpretation of news and the commentary of guests proceed from the viewpoint of Russia's official position, where truth and lies are intermixed. On the one hand, access to these shows helps spread Russian fake news among the population. Russian networks are even available in basic network packages, while European channels (such as Finnish channels) are only available in custom packages. Spreading misinformation or slander must be condemned and measures taken. Messages that incite hatred or undermine Estonia's constitutional order must be stopped. In the past Lithuania, Latvia, and Ukraine have already fined or banned some channels for a period due to the airing of programs with misinformation. On the other hand, since Estonia values democratic freedom of speech and the press if they comply with Estonia laws, it has continued to offer Russian networks based on these important national values. [104]

Europe's recent Action Plan, designed to improve cooperation between member states and institutions and to encourage civil society to counter disinformation, was unveiled in early December 2018. Estonia's representative to the European Union's Political and Security Committee stated that the Action Plan was important as "it demonstrates that democratic societies share a common desire to take concrete steps against the spread of disinformation."[105] The plan proposed to more than double the

[101] Ibid.
[102] No author provided, "Estonian Foreign Minister says Cooperating Only with Kremlin-Minded Media Would Mean Surrender," *Tallinn BNS* (in English), 4 January 2018.
[103] S. Tambur, "Germany to Help Estonia Counterbalance Russian Disinformation," *Tallinn ERR News* (in English), 20 April 2015.
[104] No author or title provided, *Tallinn Postimees.ee* (in English), 18 October 2018.
[105] No author or title provided, *Tallinn ERR News* (in English), 6 December 2018.

Strategic Communication (StratCom) task force budget, established to address Russia's disinformation campaigns, from 1.9 million to 5 million Euros.[106]

A Look at Other Important Developments through the Years

When viewed through the years, it becomes apparent that there has been a consistent pattern of Russian attempts to manipulate public opinion and persuade the Russian-speaking population of Estonia to follow the Russian information space. Luckily for Estonia, polls indicate that Moscow's propaganda effort has not achieved the results the Kremlin-backed offensive had sought. It is hard to know precisely "why" Russian attempts to manipulate public opinion have been thwarted but perhaps it has been because Estonia is more effective at communicating its values than Russia is at communicating its propaganda; or perhaps because Russian Estonians simply prefer their lifestyle in the Baltics under a democracy over what they lifestyle would be in Russia under a kleptocracy.

2014

There were several important developments in 2014 to protect Estonia from Russian influence operations, from training that was designed to counter disinformation to the deterrent effect of NATO deployments. One of the biggest developments was a decision announced by two generals, Estonian Defense Forces Command Major General Riho Terras and NATO's Supreme Allied Commander Transformation, General Jean Paul Palomeros, to create a NATO military cyber training center in Tallinn.[107] Later in the year a retired Estonian General noted that the presence of NATO troops on Estonian soil sends a political message to Russia; further, Estonia's Baltic Sea defense must be strengthened along with its air defense missile systems.[108] Additionally, a report out of Tbilisi Georgia noted that Estonia plans to build a fence along its Eastern border with Russia, and to construct around-the-clock technical surveillance for border security. The fence will be 70 miles long and was set to start in 2018.[109]

Not all the news was good. On 5 September 2014 Eston Kohver, an Estonian police officer, was abducted by the Russian Security Services. Estonia states he was abducted on Estonian territory while Russia states he was on Russian territory with weapons, money, and special equipment. In August 2015 he was sentenced to 15 years imprisonment, which Estonian Foreign Minister Marina Kaljurand called a provocation. Others can be expected, she noted, as Russia's actions are simply unpredictable.[110] Then, at the end of September 2015, Kohver was suddenly released.[111]

2015

In 2015 it was noted that over the past 23 years (1991-2014), the Kremlin's propaganda has not destabilized the Baltic countries.[112] Russia has continued its attempts

[106] Ibid.
[107] Bruce Jones, "NATO Approves Estonian Cyber Training Centre," *Jane's Defense Weekly*, 25 June 2014, p. 15.
[108] Ants Laaneots, "What Must We Ask from NATO?" Tallinn *Postimees*, 2 December 2014.
[109] No author or title provided, Tbilisi *Georgia Today Online* (in English), 3 September 2015.
[110] No author or title provided, *Interfax* (in English), 3 September 2015.
[111] No author or title provided, Tallinn *ERR News* (in English), 1 October 2015.
[112] Toomas Alatalu, "The Times Participating in Hybrid War," Tallinn *Eesti Paevaleht Online*, 3 April 2015.

to split NATO and EU partners with a policy of divide and rule, but it has not worked. A poll in 2015 showed that 68 percent of Estonians support the presence of NATO troops and 25 percent are against it. It was noted that the key to changing the attitude of other ethnic groups in Estonia is to bring them into Estonia's information space instead of their current viewing preferences in just Russian information space.[113] Another survey noted that while two-thirds of ethnic Estonians see Russia as the main global threat, only six percent of Russian-speakers living in Estonia feel that way.[114]

Japan's Vice-Minister of Defense visited Estonia in 2015 and stated that his nation was very interested in cooperating with Estonia in the field of cyber-security. While there, he visited the Information Systems Authority and the NATO Cooperative Cyber Defense Center of Excellence (CCD COE) in Tallinn.[115]

In October 2015, the US human rights organization Freedom House released its Internet Freedom Index. As before, Estonia was in second place behind Iceland (the US was sixth). Estonia not only has increased its Internet access over time but has also protected the population's right to privacy. In 2013 close to 97 percent of banking transactions were done with e-banking services, according to Freedom House reports.[116]

A final 2015 report noted that Moscow's "relentless information campaign" and movement of militias and Special Forces troops near border regions raise questions about military readiness and the intelligence capabilities of Estonian forces. Lieutenant General Riho Terras, the country's senior military officer in 2015, noted that "We need to make sure that we believe in Article Five [the principle of collective defense in NATO's founding treaty], but even more importantly, we need to make sure that Mr. Putin believes in Article Five. And I think we should put a lot of emphasis on that."[117] Terras added that maintaining defense spending is crucial, and he warned against moves to scrap Britain's aging nuclear arsenal. The article states that the UK is NATO's only European nuclear power, since France has a special opt-out that allows its nuclear forces to operate independently of the alliance.[118]

2016

In 2016 it was noted that the EU Department of External Relations launched an EU website (in Russian) to produce more information for examination in Russian information space. Further, the department launched a weekly "review of disinformation" has been initiated that aims at unveiling Russian fake news. It was also noted that NATO's leadership was thing about "creating a new communications directorate to counteract the Russian 'information weapon.'"[119]

---

[113] No author provided, "Two-thirds of Estonian Residents Support the Presence of NATO Troops. There is a Marked Difference in Attitudes of Estonians and Other Ethnic Groups," Tallinn *ERR News*, 30 April 2015.
[114] No author provided, "Estonians See Russia's Activity as the Main Global Threat," Tallinn *Baltic News Service*, (in English), 7 May 2015.
[115] No author or title provided, Tallinn *ERR News* (in English), 7 May 2015.
[116] No author or title provided, Tallinn *ERR News* (in English), 28 October 2015.
[117] No author or title provided, London *FT.com* (in English), 13 May 2015.
[118] Ibid.
[119] No author or title provided, Tallinn *Postimees Website*, 10 February 2016.

The Estonian Information Board (EIB, the nation's foreign security and intelligence agency) states that Russian military planning in the Baltic region contains a temporal advantage if it ever decides to conduct a limited military operation. The main goal of such operations would be to impose "control over some towns or areas close to the border."[120] Narva appears a likely first target for such an operation due not only to its geographical location but also due to the predominance of the huge number of Russians that populate the city. The Russian operation may include the threat of tactical nuclear weapons as a deterrent,[121] one source stated.

A potential Russian goal appears to be to restore its sphere of influence through expanding its media capabilities in the region. For example, Russia launched its *Sputnik* news portals in Estonia in both Estonian and Russian languages in February 2016.[122] *Sputnik* is led by Dmitry Kiselyov, a person who is on the EU sanctions list for being a "central figure of the government propaganda supporting the deployment of Russian forces in Ukraine."[123] The article noted that another media outlet, *Rossiya Segodnya (Russia Today)*, is the main propaganda tool of Moscow that is aimed toward the West.[124]

Estonia's Defense Minister Hannes Hanso stated in February 2016 that a psychological gap between Russia and Estonia is growing and that "if we look at internal Russian politics we see that the legitimacy of the regime is built on confrontation with the West."[125] This is the new normal. It diverts the Russian population's attention away from its own domestic problems. Also, of special interest was that Hanso believes Belarus is not a friend of Russia, as it and others have been "bullied into this position or they are given no other option."[126]

2017

In 2017 an Estonian historical expert on the Soviet era, David Vseviov, stated that there was talk about fear of Russia being "part of the Estonian's DNA ever since 1939," and it was revived with the 2014 annexation of Crimea and the war in Donbass. That year President Vladimir Putin stated that there was little way to criticize the Molotov-Ribbentrop agreement (where a secret protocol between Stalin and Hitler allowed for Moscow to invade Estonia along with other nations),[127] indicating his support for such a tactic.

In a February 2017 interview with Mikk Marran, Director General of EIB, it was noted that Russia's advantage occurs since the "entire influencing process is centrally managed…they observe the guidelines issued from the Kremlin." Russia's influence

[120] No author provided, "Biggest Military Conflict Danger in Baltics Arises from Russia's Misconceptions," Tallinn *Baltic News Service* (in English), 9 March 2016.
[121] Ibid.
[122] No author or title provided, Tallinn *ERR Website*, 13 March 2016.
[123] No author or title provided, Tallinn *ERR News* (in English), 25 February 2016.
[124] Ibid.
[125] Gerard O'Dwyer, interview with Hannes Hanso, *Defense News*, 1 February 2016, p. 19.
[126] Ibid.
[127] Benoit Vitkine, "Estonia Trains to Confront the Russian Threat," *LeMonde.fr,* 10 January 2017.

toolbox allows them to create confusion and then exploit it. Moscow also continuously maps the strength of Estonia's information systems. Marran added the following about contemporary intelligence gathering:

> 21st century intelligence is a combination of the classics and technology. Human intelligence will certainly remain an important part of intelligence because, as always, the information gathered from a person by a person is the most important. …However, the role of technology and software is growing, which means that intelligence is becoming increasingly more expensive. All the systems which are built up, need to be kept operational. They need maintenance and they need to be upgraded every three to five years. These are huge expenses. But if we do not spend that money, we will soon lag behind.[128]

There were also several warnings in 2017 about Russian provocations aimed at unsuspecting NATO soldiers. British troops, sent to participate in war games in Estonia, were warned that Russia sets honey traps, stages pub brawls, and uses other subversive efforts to blackmail soldiers on social media accounts. Russian efforts create a false impression of Western aggression using such stories.[129] Danish soldiers scheduled to arrive in Estonia later in 2017 were also warned to expect Russian provocations aimed at compromising them.[130]

In April 2017 Estonia's parliamentary committee published a new version of Estonia's security policy principles, which included cyber space as a new security environmental dimension. According to the bill:

> Estonia's main security risks are the deepening of global security problems, the declining impact of the Euro-Atlantic region, and of a value space that is based on democracy, the market economy, and a law-governed state, as well as the weakening of integration based on the European Union principles and Russia's provocatively aggressive behavior, including by using force near its borders as well as elsewhere in the world.[131]

It is envisioned that a new element, the so-called hybrid method, is being used against Estonia where both military and nonmilitary issues function in symbiosis.[132]

Later in the year Estonia's Internal Security Service's Annual Review was published, which focuses on counter-intelligence activities and how to defend against various destabilizing forces. Its focus was the Russian Special Services, a reference to

---

[128] Kart Anvelt interviews Mikk Marran, "Information Board Head: Our Aim Would Naturally Be Direct Connection into Putin's Head," Tallinn *Eesti Paevaleht*, 9 February 2017.
[129] No author provided, "Estonia's Intelligence Chief Warns of Provocations Targeting NATO Soldiers," *Tallinn BNS* (in English), 21 February 2017.
[130] No author or title provided, *Postimees website*, 21 April 2017.
[131] No author provided, "Estonia's Security Policy Principles to Include Cyber Space," Tallinn *Baltic News Service* (in English), 17 April 2017.
[132] Ibid.

intelligence organizations. The latter's influence and subversive operations were highlighted, especially the people and organizations working for them. A main objective of Russia's activities appears to be to destabilize the political systems of Estonia and others in the West. Russia recently organized and incited incidents in Serbia and Montenegro and generated scandals and controversies in the West to demonstrate that Western politicians are no less corrupt than those politicians the Western press accuses in Russia.[133] Finally, in November 2017 there was an important report published by the Estonian National Defense College's (ENDC) Center for Applied Studies. Titled "Russian Information Warfare against the Ukrainian State and Defense Forces: April-December 2014," the report is available in English at the website of ENDC.[134] It contains some examples of Russian efforts to control information space in Ukraine.

2018

In January 2018, the Estonian Police and Border Guard Board showcased its nine ELIX-XL drones which will survey the eastern border and monitor rescue operations and border incidents. They have a flight time of one hour and a range of five kilometers.[135] As Colonel Eero Rebo, Commander of the 2nd Infantry Brigade, noted:

> It is strategically important that the border is clearly marked and well-noticeable on the terrain, so that we know what is always going on. A good border is vital to a small country with such a neighbor [as Russia]. No less important is the daily prevention of criminal activity; the more so since we have heard from the media and read in the annual report of the Internal Security Service about the connections between smugglers and our eastern neighbors' special services.[136]

Estonian President Kersti Kaljulaid stated at the Munich Security Conference in February that NATO's Enhanced Forward Presence (EFP) in the Baltics and Poland has been successful in countering Russia's policy, but deterrence still requires a realistic reinforcement strategy. Only in this way can it convince an adversary that its defense is credible.[137] A sizeable deterrent near its border area is one way to strengthen its strategy.

Border security is important to Estonia for both geopolitical and security reasons, but it is only one of several factors supporting national security. For example, one report stated that decoupling Estonia from Russia's power grid and integrating Estonia with the Continental European power system prevents Russia from blackmailing Tallinn into

---

[133] Editorial, "Security Police and the Russian Threat," Tallinn *Postimees.ee*, 12 April 2017.
[134] No author provided, "Estonia Publishes Report on Information War against Ukraine," Tallinn *St. Ohtuleht Online*, 15 November 2017. See http://www.ksk.edu.ee/teadus-ja-arendustegevus/publikatsioonid/endc-occasional-papers-7/
[135] No author provided, "Estonia's Police Authority to Showcase Drones Purchased for Guarding the Eastern Border," Tallinn *Baltic News Service* (in English), 12 January 2018.
[136] Eero Rebo, "Ukraine and Georgia Are Warning of What Will Happen if Border is Not Completed," Tallinn *Eesti Paevaleht Online*, 12 February 2018.
[137] No author provided, "Estonian President: NATO's Russia-Policy Has Been Successful," Tallinn *Baltic News Service* (in English), 16 February 2018.

acquiescing to the Kremlin's demands.[138] This issue and other national security concerns must remain at the top of the Estonian leadership's considerations when addressing Russian geopolitical motivations.

Cyber security is one of those vitally important issues for Estonia. In May 2018, exercise "Locked Shields 2018" was kicked off at NATO's CCD COE in Tallinn. It embraced a technical and strategic game whose aim was to "rehearse protecting vital services and military systems in the event of a large-scale cyber-attack." [139] Teams had to report incidents, make strategic decisions, and solve challenges involving external communications and issues in the legal and media fields. Teams will be "protecting the computer systems and information systems of an imaginary country that has come under attack."[140]

In a June 2018 interview with *Defense News*, Jonatan Vseviov, Permanent Secretary of the Estonian Ministry of Defense, stated that Estonia is setting up a cyber command within the armed forces. Regarding policy, he noted it is important to maintain a strong degree of constructive ambiguity. Estonia cannot let adversaries know what events would trigger Article 5 because, if it did, then opponents would conduct attacks that would fall below that threshold. The cyber domain requires a whole-of-society approach to security.[141] It has been noted that cyber defense, military mobility, and a preparedness to respond to hybrid threats are for Estonia the most significant areas of EU-NATO cooperation.[142]

In late summer 2018, Estonia appointed Tiirmaa-Klaar as its first ambassador at large for cybersecurity. She noted that Estonia is well prepared to fend off cyber-attacks, with the State Information System's Authority (RIA) and private sector specialists working in cooperation with one another. But technical capacity alone is not enough, as strategic thinking is required as well to compose the bigger picture that is confronting Estonia. For example, if attacked, a response must be proportional and in accordance with international law. Sanctions in other domains may hurt the attacking nation more than a cyber counterattack. That is, strategic thinking is needed to determine the exact deterrent response against the assailant (such as finding ways to make them lose face, etc.). In December, RIA was in Ukraine to teach that nation's central electoral committee how to adopt basic cyber security measures.[143]

Regarding propaganda, the Tallinn website *Propastop* covered anti-Estonian manipulation, lies, and propaganda. Members of the Estonian Defense League, a voluntary military organization, run the site. They cover Russian-related networks that actively participate in media and communication propaganda efforts in Estonia. *Propastop* has

[138] No author provided, "Desynchronization of Baltic Grid Crucial Due to Geopolitical Aspects—Study," Tallinn *Baltic News Service* (in English), 13 April 2018.
[139] No author or title provided, *Caversham BBC Monitoring* (in English), 1 May 2018.
[140] Ibid.
[141] Aaron Mehta, interview with Jonatan Vseviov, "6 Questions with Estonia's No. 2 Defense Official," *Defense News*, 16 July 2018, pp. 18-19.
[142] No author or title provided, Tallinn *Baltic News Service* (in English), 11 October 2018.
[143] No author or title provided, Tallinn *Postimees.ee* (in English), 10 December 2018.

singled out Vladimir Putin's *Russkiy Mir* (*Russian World*) organization that allegedly supports Russian language instruction but is more commonly viewed as a front for influence operations. Apparent non-governmental organizations doing the same are the Pushkin Institute, the Baltic Youth Alliance, and the *Reval Media Agency*.[144] It was noted that a growing Russian community, demonstrating pro-Kremlin and pro-Russia and anti-Western sentiment, is observable in Baltic social media.[145]

One area that Russia has exploited in Estonia is the latter's value of a democracy's policies of freedom of speech and the press. If a nation complies with Estonia's laws, then they should be allowed on TV channels according to a center-right Pro Patria Party member. Contrasting this view was that of IKRE Parliamentary Group Chairman Mart Helme who believes that propaganda channels should be restricted.[146] It was noted that Russian TV channels are often included in basic packages offered by Estonian TV. This means that Estonia pays licensing fees to these Russian channels, which include *Pervyi Baltiiski Kanal*, *NTV-Mir*, *RTR-Planeta*, and *Ren TV*. Thus, while Estonia is trying to stop Russian propaganda, at the same time its people are paying Russia for its state news and comments. The latter are directed at destroying cooperation within Europe. Meanwhile European channels are "optional channels" which can be ordered but only for an additional fee.[147]

2019

Two reports in 2019 from the *Baltic News Service* indicated NATO's continued interest in uncovering Russian propaganda aimed against Estonia and other Baltic members. First, Estonia's Minister of Foreign Affairs Sven Mikser noted that the private sector, media, and state institutions are working together to fight disinformation. New developments, such as the European Union's action plan to fight disinformation, are important ways to confront Russian propaganda. Facebook reportedly closed 13 pages related specifically to Estonia (with 19,000 followers) since the pages were linked to employees of the Russian channel *Sputnik*.[148] Other fake accounts appeared designed to interfere with internal Estonian internal discussions, polarize people, distort topics, and escalate public debates.[149] Second, in July 2016, NATO established an EFP in Estonia, Latvia, Lithuania, and Poland. This resulted in a battalion-sized battle group deployed in each country to serve as a deterrent to Russia. In January 2019, the International Center for Defense and Security (ICDS) reported that Russia is the main risk to the EFP of NATO battle groups in the Baltics. Disinformation and incident exploitation involving EFP personnel are its main threats.[150]

---

[144] No author provided, "Russia-Related Networks in Estonia Part Five," Tallinn *Propastop*, 23 July 2018.
[145] No author or title provided, "Tallinn *Postimees.ee* (in English), 31 December 2018.
[146] No author or title provided, *BBC Monitoring* (in English), 23 October 2018.
[147] Urmas Paet, "Propaganda Channels in Estonia: Russian Influencers Only Chuckle, Have Fun with Europeans' Naivety," Tallinn *Eesti Paevaleht Online*, 25 October 2018.
[148] No author provided, "EU and Foreign Ministers Discuss Plan for Fighting Disinformation," Tallinn *Baltic News Service* (in English), 21 January 2019.
[149] Holger Roonemaa and Anna Pold, "Sputnik Secret Propaganda Network Involved 13 Estonian Pages," Tallinn *Postimees*, 18 January 2019.
[150] No author provided, "NATO eFP in Baltics, Poland Sends Strategic Message—Report," Tallinn *Baltic News Service* (in English), 28 January 2019.

In its March 2019 annual report, the Estonian Foreign Intelligence Service (FIS) warned that the Russian threat is not only asymmetrical but also covert and based on political subversion. There is also a potential Russian military threat to Belarus if a so-called color revolution developed there, which would initiate swift retaliatory action from Moscow. President Putin appears dissatisfied with Belarus President Lukashenko.[151]

The FIS also noted that Russian cyber spies have had some success in accessing information from Estonian government agencies, as they continuously map various Estonian information systems. Such information is often then used against Estonia in phishing campaigns.[152] Another FIS report noted that Russia is likely to intervene in European Parliamentary elections to gain some seats for pro-Russian or Eurosceptical political forces. In this way EU unity could be diluted. It was further noted that Russia supports its allies through Russian-controlled media; organizes high-level meetings and visits that attract media attention; offers covert financial assistance if necessary; discredits opponents (by stealing and leaking internal information); and intentionally spreads false information in social media.[153]

Conclusions

It is apparent that Russia continues to attempt to disrupt Estonian society with media and cyber offensives. Some media offensives are designed to split Estonian society while others serve as Russian foreign policy tools. Estonia's leadership has responded to these challenges, noting that the key to changing the attitude of ethnic groups in Estonia is to bring them into Estonia's information space instead of just Russian information space. Estonian TV channels in Russian as well as an increased military presence of NATO nations in Estonia and a higher degree of cooperation with the European Union have been major ways that Estonia has countered Russian efforts.

Despite all the dangers associated with cyber issues, Estonia continues to press forward with a digital policy that covers the country's enterprises from banks to industry. Recently Estonia developed an e-residency program that allows foreigners to obtain a digital ID and to start an Estonian company online without ever visiting the nation.[154] So far there has been no word of this effort being abused. Estonia's President, Kersti Kaljulaid, is a huge supporter of such programs. She realizes that other nations cannot emulate Estonia immediately so her advice to other nations wishing to start a similar system are somewhat limited. They should start with smaller services, she notes, say with school applications, to build trust in becoming a digital nation online before trying something more daunting like e-voting. The nation aims to have 10 million e-residents by 2025, with a focus on those living in Britain affected by Brexit. Officials estimate that Estonia lifts its GDP by 2 percent

[151] No author or title provided, Tallinn *ERR News Online* (in English), 12 March 2019.
[152] No author provided, "Foreign Intelligence Service: Russian Cyber Intelligence is Constantly Looking for Information in Estonia," Tallinn *Maaleht,* 20 March 2019.
[153] No author or title provided, Tallinn *Baltic News Service*, 12 March 2019.
[154] No author or title provided, *Delfi website*, 18 April 2017.

annually and saves paperwork due to the conduct of so many online contacts with the state.[155]

Estonia is also doing what it can at improving its national security through a comprehensive border security initiative, constantly improving its cyber security, and relying less on Russian products and services, especially energy issues. The nation is further focused on ensuring that the minds of its citizenry do not fall victim to Russian propaganda and influence methods. As the title to this work noted, Estonia is always confronting Russia's media and its attempts to manipulate public opinion. With historical animosity present on both sides, there are clearly problems that will not go away soon. Manipulation techniques will continue as far as one can see, or at least during the reign of President Putin.

[155] No author provided, "Charlemagne: The Church of Data," *The Economist*, 8 July 2017, p. 48.

CHAPTER THREE: LATVIA

Introduction

For many years, Latvia has been fighting against Russian soft power advances. Otto Ozols, writing for *Delfi,* noted that Russian information and propaganda utilizes three D's in its manipulation effort—disinformation, demoralization, and destabilization. It is lies and half-truths (disinformation) that demoralize and destabilize audiences through the erosion of trust. The same author noted that propaganda is like carbon monoxide gas, since it flows into a room unnoticed, cannot be smelled, and puts people's logic to sleep.[156]

Russia's propaganda is aimed at manipulating information on Latvia's TV, websites, and printed forms of communication. In response, Latvia has developed specific counters. A primary one has been a focus on educating its population about Russian methods that attack Latvian susceptibilities and weaknesses. It is important to teach Latvians how to be skeptical of media and news releases and how to recognize the covert (trolls, etc.) and sometimes the overt methods, such as fake news, that Russia uses. These Latvian counters, however, battle alternate Kremlin-sponsored sites available to Russian members of Latvian society, to include satellite TV and the Internet, and EU penalties that would be assessed if Latvia outright bans Russian TV. In addition to TV, other Russian influence tools include pseudo-academic and expert organizations, tools of economic influence, and spying and cyberspace activities.

This article initially will provide a short background summary of Latvian efforts to stop Russian propaganda from 2013-2016. It will then look at Russian efforts and Latvian counters in more detail from 2017-2019.

Countering Russian Propaganda: Some Latvian ideas (2013-2016)

One article in the Latvian journal *Delfi* noted that soft power cannot be combatted with simple bans, protests, normative acts, or government decisions. Latvia needs its own soft power to not only counter Russian advances but also to strengthen its culture and self-confidence. It is primarily Latvian values that facilitate social integration[157] and act as a soft power buffer against Russian aggression. These values should work in conjunction with a skeptical approach to Russian media advances and focus on educating the public about Russian techniques.

Russia has often proposed that the history of Latvia is different than that taught in Latvian schools. Latvia has warned its citizens of these Russian efforts to change history. Latvia's parliament has approved amendments that propose criminal liability and even imprisonment for glorifying, denying, white-washing, or doubting the Soviet occupation of the country.[158] It is important to study the Russian clichés and narratives that help establish how Russian propaganda efforts are disseminated in Latvia's information world, and to unmask the lies and falsehoods

[156] Otto Ozols, "3D Kremlin Carbon Monoxide Flowing Freely into Latvia," *Delfi*, 1 June 2016.
[157] Janis Kazocins, "Russian Soft Power: Normal Phenomenon or Challenge for Latvia?" *Latvijas Avize,* 2 September 2013, p. 3.
[158] *RAPSI*, a Russian website (in English), 16 May 2014.

emanating from the Kremlin.[159] One Latvian article noted that because of Russia's information war against Latvia, scholarly conferences and discussions are needed and the creation of information defense plans should become a priority. Such measures help to ensure that society is protected against both the degradation and destruction of peoples' consciences.[160]

A member of Latvia's parliament offered other ideas. First was a recommendation to ban certain TV channels and strengthen Latvian media outlets. Second was a need to improve state and local government services in line with what any normal society would do. Third was an attempt to develop cooperation with the only liberal Russian media outlet, *Dozhd*, which would offer Latvian citizens a more realistic view of Russian policy and thinking from an actual domestic source in Russia not in bed with Russia's propaganda offensive. Finally, there was a recommendation to establish a news studio in Latgale (a province in the Eastern part of Latvia, with little access to local news) so that local stories and government activities will be better equipped to counter Russian propaganda in such regions. Quality education is required but the availability of universal information to all of Latvia is equally as important.[161]

Russia has let Latvia know that national security is not just the business of the defense sector, as Kremlin behavior aims to influence the mindsets of Latvia's people and sow seeds of doubt against the nation's government. The *Baltic News Service* estimated that 70-80 percent of the information that Russia produces about Latvia is negative, such as Russian claims that there is a rebirth of fascism in Latvia, that the oppression of Russian-speakers there continues, and that only Russia, not NATO, can save Latvia.[162] Latvia needs countermeasures to these asymmetrical threats, and the Defense Minister has called for measures that include nonmilitary ones. After Russia's incursion into Ukraine, Latvia desired greater energy independence, greater coordination of its national efforts with those of other Baltic nations (such as border guard cooperation), and a greater need for the creation of a common information space with Estonia and Lithuania that reflects common values and ties.[163]

One 2016 report stated that it is not important to provide a separate TV channel that only operates in the Russian language, as that makes it appear there are two ethnic groups in Latvia. Rather, Latvia's media environment in just the Latvian language should be strengthened.[164] Latvian authorities also took a strong stand against the pro-Kremlin news site *Sputnik* in March 2015, shutting it down and calling it a propaganda tool and not a credible media source. Russia, of course, labeled this as blatant censorship,[165] ignoring the accusations against it.

---

[159] Sarmite Elerte, "Kremlin's Trolls," *Ir.Iv*, 18 July 2014.
[160] Viktors Avotins, "Misinformed Ones Will Lose," *Neatkariga*, 27 November 2014, p. 7.
[161] Juris Vilums, "Informational (in)Security in Latgale," *Delfi*, 17 December 2014.
[162] No author provided, "80 Percent of the Information about Latvia Broadcast on Russian TV is Hostile," *Tallinn BNS* (in English), 28 February 2015.
[163] No author provided, "Ukraine's Situation Holds Valuable Lessons for the Baltics," *Tallinn BNS* (in English), 6 February 2015.
[164] Edvins Snore, "Russian World Paid for With Latvian Money," *lrir.lv*, 20 March 2015.
[165] "Latvia Blocks Russian Sputnik Site as Kremlin 'Propaganda Tool'," *stopfake.org*, 30 March 2016.

Latvian and Russian Information Positions from 2017-2019

Countering Russian disinformation and propaganda in Latvia is difficult for two reasons. First, the size of the Russian diaspora from Soviet times still residing in Latvia is huge and desires Russian news sources. Second, much of the news on Russian channels is slanted against Latvian politics. This makes it difficult to keep both Russian and Latvian members of the population happy. In May 2018, for example, five Russian Television and Radio (*RTR)* stations were under investigation for content involving "vividly negative propaganda."

Latvia, like some of its other colleagues, does not think it wise to close a TV channel completely but instead develop amendments that would reduce the operations of offending Russian channels. Initially fines should be levied against channels that do not abide by the rules of neutrality in presenting facts.[166] A Latvian National Security Commission member stated that basic cable television packages eventually should exclude those propaganda channels supported by the Kremlin who continue to violate Latvian laws. Commission members were also informed of a 2018 Saeima [Latvian Parliament] Analytical Services study, whose goal was to describe "Russia's influence in Latvia's information world and ways of limiting this influence."[167] Politicians were advised to make sure that they do not become a problem through offering Russia a rationale or reason to claim that Latvia is a failed state.[168]

2017

It was noted in May 2017 that educating Latvia's population remains at the top of a list of potential counters to Russian propaganda. President Raimonds Vejonis, whose term ran from 8 July 2015 to 8 July 2019, advocated for teaching critical thought to the public to prepare them for a confrontation with fake news. Janis Sarts, the Director of NATO's Strategic Communication Center of Excellence in Riga, noted that independent thought is the best weapon against fake news. Russian expert Mark Galeotti stated that the three main directions of fake news are to divide, distract, and demoralize society. To him, as to President Vejonis, educating society and helping them think more critically is a vitally important asset to teach.[169] Inese Vaidere, a member of the European Parliament from Latvia, suggested a pilot project to the European Commission (content unknown) for countering Russian propaganda, and requested three million Euros for European Commission countries (especially the Baltic nations) to use in their efforts to counter Russian fake news and its disinformation campaigns designed to undermine Western democracy.[170]

Latvia's Foreign Minister in 2017, Edgars Rinkevics, noted that Russia may probe NATO's resilience to full-spectrum hybrid warfare. He added that this type of warfare includes propaganda and cyber-attacks. Power grids, banks, and security systems all could be left without power if Russia decides to conduct such activities. He noted that Russia's Zapad-2017 exercise, which was performed in its Western Military District that borders on the Baltics, were offensive and not

[166] Ausma Orupe, "Want to Reduce Russian Propaganda with the Force of Law," *Neatkariga,* 15 May 2018, pp. 2-3.
[167] Baiba Lulle, "Answers Exist—What about Political Will?" *Neatkariga*, 15 May 2018, p. 2.
[168] Ibid.
[169] No author or title provided, *Riga BNN* (in English), 7 December 2017.
[170] No author or title provided, *BBC Monitoring* (in English), 9 May 2017.

defensive, as Russia advertised them.[171] The implication was that Russia used the exercise as a planning venue for future operations if needed.

2018

There are numerous tools in Russia's manipulation bag of tricks. For example, some Russian propaganda pieces start with a "discovery" of some kind. Russian information agents pass off this information as important for the world's consideration. These "discoveries" often do more to hide or obfuscate the truth than to expose it. The technique offers misleading narratives to throw Western analysts off course with alternative versions of the truth made to seem as plausible as possible.

Russia believes it is engaged in an information war with the West for credibility.[172] To participate in an information war against Russia, Latvia needs to stimulate critical assessments of media content in society and not simply react to Russian propaganda with propaganda of its own. Latvian Foreign Ministry's Parliamentary Secretary Zanda Kalnina-Lukasevica reinforced this point in response to a question about the impact of Russian propaganda on Latvia.[173]

In a Latvian report titled "Russia's Influence in Latvia's Information World," it was noted that the differences between propaganda, fake news, and disinformation on the one hand and legitimate freedom of speech on the other are harder and harder to differentiate. Two issues must be addressed before fake news can be considered criminal: the law must define what kind of information is good and what kind is bad; and it must define which institutions have the right to differentiate between the two types of information. Most likely that job will be entrusted to the National Electronic Mass Media Council (NEPLP). In addition to laws, Latvia must strengthen its public education, media skills, and investigative journalism.[174] Internally strategic patience is important as it takes time to explain the goals behind Russia's messages. One expert at the Eastern European Policy Research Center, Andis Kudors, stated that people in Latvia live in different information bubbles. Latvians are very self-critical, such that when the Kremlin calls Latvia a failed state, some in that information bubble of self-criticism think that the state really is weak. Thus, the ideological foundations of the population must be strengthened. The goal is to provide "an elementary approach to media intelligence and an understanding about the political process so that the Kremlin's propagandists cannot manipulate" either.[175]

In a 2017 report from Latvia's Constitution Protection Bureau (CPB), it was noted that Russian propaganda uses cyber-attacks to spread fake news and that its secret services are developing extensive communication control systems to monitor and control data flows. Other Russian influence tools include pseudo-academic and expert organizations, tools of economic

[171] Roland Oliphant, "People Are Going to Die. West Warned over Covert Russian Cyber Attacks," *The Telegraph Online* (in English), 4 September 2017.
[172] Atis Klimovics, "Russian Propaganda Must Not Be Spread in Latvia," *Riga Latvijas Avize*, 13 February 2018, p. 3.
[173] No author provided, "Only by Cooperating Closely with the United States, NATO, and the European Union Is It Possible to Tackle New Security Risks," *Riga BNS* (in English), 19 February 2018.
[174] Girts Zvirbulis, "Seeking Weapons against Fake News," *Riga Latvijas Avize*, 29 March 2018, p. 4.
[175] No author or title provided, *Riga Neatkariga*, 12 November 2018, pp. 6-7.

influence, and spying and cyberspace activities.[176] In its 2018 report, the CPB noted that Russian methods of influence start with propaganda and end with military and cyber threats. Nonmilitary instruments of influence are usually the most discreet but have long-term effects, and their methods of disseminating provocative and discrediting information is becoming more specific. Specifically the report noted that "Russia has tried to influence internal processes in the EU and NATO member states in its own favor by using political and diplomatic resources, economic relations (especially in the energy sector), a demonstration of military potential, the development of cyberattack capabilities, as well as the targeted distribution of disinformation and propaganda."[177] In regard to military uses of propaganda (not noted in the CPB report), a source stated that Russian propaganda is aimed at NATO and its soldiers in Latvia. News reports are meant to sow distrust in Latvia and show that it is a failed state.[178]

Latvian TV channels are perhaps the biggest point of concern to most government officials, since so much of the Russian diaspora in Latvia accesses this forum that in turn is used to foment disinformation. Violations have been exposed by Latvian monitors of several Russian-language TV channels. However, Latvia's National Security Committee will have to produce some new proposals for restricting these propaganda outlets,[179] as Russia continues to find ways to work around proposals currently in effect. In early May 2018 criticism mounted against Latvia's National Council for Electronic Media, which, in the opinion of some members of Parliament, is toothless and has done little to suspend the broadcasting of Russian TV that is imbedded with inappropriate content. One member noted that "Russian propaganda channels are not journalism in the traditional sense of the word, but rather a weapon in hybrid war."

A Latvian commentary noted that 90 percent of the channels available to Latvians would be in the languages of the European Union and of the 47 channels available, four would then be in the Russian language. Of those four, it is doubtful that the Russian *Dozhd* (*Rain*) channel, which is not subordinate to the Kremlin, would be part of the offering. Latvian TV budgets are less than those of Russian TV. For example, it was noted that Russian TV channels are sometimes registered in EU member states, which "means that Latvia cannot unilaterally ban their rebroadcasting." While Latvia's citizenry recognizes and neutralizes the danger of Russian trolls, the latter should not be allowed to conduct messaging in an unlimited fashion. Germany, for example, in 2017 adopted a law in which networks with two million registered users must remove hate speech, fake news, and other unlawful material or risk a 50 million Euro fine. Latvia must prevent its soil (ethnic issues, economic situation, reasons to be called a failed state) from being a place where Russia's propaganda seeds can be dropped and grow. Media skills and media content oversight are needed to help self-regulate the media.[180] Further, it was noted that Russian propaganda channels should not be available on basic cable networks.[181]

---

[176] No author provided, "Activities of Russian Intelligence and Security Agencies Pose Major Threat to Latvia's Interests," *Riga BNS* (in English), 10 April 2018.
[177] Jolanta Plauka, "Changing Russia Becoming More Aggressive," *Riga Diena*, 12 April 2018, p. 5.
[178] No author or title provided, *Riga Latvijas Avize*, 30 May 2018, p. 3.
[179] No author provided, "Unity Urges Latvian Media Watchdog to Counter Kremlin Propaganda More Actively," *Riga BNS* (in English), 25 April 2018.
[180] Baiba Lulle, "Answers Exist—What about Political Will?" *Riga Neatkariga*, 15 May 2018, p. 2.
[181] No author provided, "Electronic Mass Media Council, Culture Ministry Not Doing Enough to Improve Protection of Latvia's Information Space," *Riga BNS* (in English), 2 May 2018.

To confront Russia's information war in specific parts of Latvia, new ideas are under discussion, according to media expert Rita Rudusa. Techniques include messages and visual images, where the most important thing is creating the emotional idea of a sense of belonging. The NEPLP wants to improve transmission in Latvia's border zone, where many inhabitants currently live in Russia's media world. Latvian Radio 4 needs to be used more as well in frontier regions. Latvian public TV needs to be strengthened and media outlets need to reflect events in a precise way. The Russian *Perviy Baltisky Kanal* (*First Baltic Channel* or *PBK)* channel, in contrast, makes people feel that Europe is amoral, and NATO does not protect anyone. Russia is focused on the young, because those over 50, the Kremlin believes, have fossilized media usage habits.[182]

There are other ways to influence Latvia than just via propaganda. Threats are another tool in play for the Kremlin. Latvia's ambassador to Russia, Maris Riekstins, noted that if Russian Iskander missiles, which can carry nuclear warheads, are permanently deployed in Kaliningrad, then NATO states will need to reassess ways to respond. Latvia is already in range of other Russian missiles. Still, the ambassador added, it would be madness for a non-NATO country like Russia to challenge NATO's safety and territorial integrity.[183] The Bucharest Nine (Poland, Romania, Hungary, Czech Republic, Slovakia, Bulgaria, Lithuania, Latvia, and Estonia) met in June 2018 to state that NATO's presence has complemented the alliance's deterrence policy.[184]

Riekstins also noted that a portion of Russia's society understands that it is important to separate what to believe and what not to believe in the Kremlin's propaganda. There is a parallel world of information there, where even in Russia some of the public understands that Russia is trying to manipulate the West while others believe the West is out to harm Russia.[185] In Latvia's society, there is the realization that Russia does a good job of manipulating and brainwashing with propaganda and influence in the Baltic states. That being the case, Latvians who are Russian and residing in Latvia are worth a pot of gold[186] due to their ability to serve as surrogates and influence the population toward Russia in other ways.

2018—a Russian Perspective about Latvia

In February 2018 Russia's *Sputnik Latvia*, a website of the Latvian branch of the Russian Government news agency, discussed a study recently concluded by Latvian scientists. The study, by Latvia's Center for East European Policy Studies, analyzed how Latvian and Russian media assess the same or similar events. The analysis was contained in the book *Reflection of International Developments in the Latvian Internet Media.* Eight events were covered that had caused a "great response" in Latvia's media: Crimea; MH 17; Western sanctions; Syria; the refugee crisis in Europe; Brexit; the NATO summit in Warsaw; and the doping scandal involving Russian athletes. In the discussion period, Brexit was mentioned but the focus was on the doping issues. These were the only two items of the eight discussed in this Russian report.

---

[182] No author or title provided, *Riga Ir.,* 24 May 2018, pp. 12-13.
[183] No author or title provided, "*Riga BNN* (in English), 6 February 2018.
[184] No author provided, "Latvian President Urges NATO Members to Keep Strengthening Resilience to Hybrid Threats," *Riga BNS* (in English), 8 June 2018.
[185] No author or title provided, *Riga LETA (*in English), 18 December 2018.
[186] Maris Krautmanis, "Russia against Usakovs," *Neatkariga*, 26 January 2018, p. 7.

The comments that follow are Russia's discussion of the report, and the author, Andrey Solopenko, makes references to the study and the opinions of the researchers who were involved in putting it together.[187] It offers a good example of how Russian specialists stress some issues and ignore others.

Solopenko noted that the study considered the content in six Latvian online media, the most popular being the *Delfi* portal, in its Latvian and Russian versions. The content of *TVnet* was also viewed in both the Latvian and Russian versions. Two other portals, Latvia's *LA.lv* and Russia's *Vesti.lv* were viewed separately, the first in Latvian and the second in Russian.[188] According to Latvian researcher Didzis Berzins, it was stated in the study that the Latvian language versions contained more facts or ascertaining information, whereas Russian texts offered an estimation or expression of an attitude. Latvian language sites offered exact quotations whereas Russian ones paraphrased them, which is due to literary tradition according to Berzins. With Brexit the Latvian media cited the words of British officials and with the doping scandal, Latvian sources cited the international anti-doping organization. In Russian publications, people connected with Russia, such as the Minister of Sports, were quoted regarding the doping issue. Russian sources in the latter case did not use the term "disqualification," the study noted, and hardly discussed the athletes who were accused but rather stated that the findings offered a prejudiced attitude toward the athletes. The *LA.lv* (Latvian portal) accused Russian authorities of wrongdoing and stated that the athletes should be punished. *Vesti.lv* (Russian portal) noted that the incident was an international conspiracy against Russia.[189]

Solopenko notes that the study's conclusions are that the use of Russian information used on Latvian news portals "multiplies the risks of the polarization of Latvian society."[190] Solopenko finishes his article noting that audiences view the sources that they trust, and the Russian-speaking population remembers "very well how this state's representatives have deprived them of their citizenship"[191] and have closed their schools and called them occupiers. These people have not forgotten that Russia expresses its support in defending their rights. For a cohesive society, Solopenko concludes, Latvia needs to cease such discriminatory policies.[192]

This article has been highlighted since it represents a very good example of a Russian propaganda argument, one that is meant to put Western logic to sleep. The outcome of the doping scandal is that the findings offered a prejudiced attitude toward the athletes. The logic of the Russian argument is thus focused on prejudice against Russia, not their implication in wrongdoing. More major cases, such as poisoning a former officer or invading and taking a slice of another country, are ignored as well. Likewise, the conclusive arguments that Solopenko makes are designed to highlight the problems of Russian-speaking Latvians, with no mention of the work

[187] Andrey Solopenko, "How Russian Media Hinder Democracy and How They Split Latvian Society," *Sputnik Latviya*, 7 February 2018.
[188] Ibid.
[189] Ibid.
[190] Ibid.
[191] Ibid.
[192] Ibid.

that has gone on to integrate these people into Latvian society and absolve them of these problems. Issues are cherry-picked to suit the *Sputnik* style and method/logic of argumentation.

Russian language media note that there have been several ways that Latvia has used to stop or limit Russian news outlets in the country. First, even if a decision was made to ban "Kremlin" channels on Latvian TV, consumers can still receive them via satellite TV or on the Internet. This means all attempts to combat Russian propaganda are doomed to failure.[193] Several Russian language TV programs have been registered in the UK and Sweden. If Latvia prohibits these channels from being viewed in Latvia, then the nation, according to EU regulations, will fine Latvia for each case in the amount of 464 thousand dollars. So, to keep this from happening, politicians decided to work through amendments to the Latvian Law on Electronic Media. The draft idea indicates that there would be no room for Russian channels at all in this law. But such measures can hardly be termed effective, the Russian source explained, since extended packages could be purchased and the alternate venues mentioned above (satellite TV, etc.) and smart TV are also available.[194] A second method of stopping Russian media was to separate Latvia's media from the Russian media (and the press of other countries) from one another in kiosks and on store shelves too, so that it was more obvious where Russian sources were located; and there may be attempts to impose increased import duties on Russian newspapers and magazines.[195]

Here are other Russian charges against Latvia's use of media:

- As a counter to Latvian methods to limit Russian media, Russia has stressed that the Baltic states used threats of a Russian bear and little green men to "deceive NATO" to get security guarantees and to get more funding.
- Latvian Foreign Minister Edgars Rinkevics stated that Russia's hybrid war has allowed it to interfere in Ukraine, Moldova, and Georgia. As a counter, Russia's *Sputnik Radio* commentator Armen Gasparyan noted that the Baltics have used threats of Russian occupation to squeeze money out of NATO. Where has the money gone? It was noted that it went for corruption, nothing else, according to Gasparyan.[196]
- Russian authorities note that Latvia needs to cease its discriminatory policies if it wants to achieve cohesion.[197]

The last two charges here, made in August 2018, are almost identical to the ones Solopenko made in February, a good example of Russia's use of themes they think have traction.

Russian media source *Vesti Segodnya* discussed how Latvia's CPB has accused Russia at every opportunity of conducting illegal activities. The CPB, the Russian source noted, should have

[193] Eduard Eldarov, "Murniece: More Frequent Bans Are Needed. Recipe for 'Freedom of Speech' from Saeima Speaker," *Riga Vesti Segodnya,* 10 May 2018.
[194] Abik Elkin, "Russia Is Being Removed from Broadcasting," *Riga Vesti Segodnya*, 15 May 2018.
[195] Abik Elkin, "According to the Laws of Wartime," *Riga Vesti Segodnya*, 26 May 2018.
[196] Armen Gasparyan, "Where Latvia Has Squandered the Money That the United States Allocated for its Defense," *Sputnik Latviya,* 21 August 2018.
[197] Solopenko, 2018.

issued a 2018 report on the work they had done. The report was used instead to describe how to counteract Russian activities. The report stated that information operations are the main way Russia confronts Latvia to create distrust and challenge Latvia's geopolitical course. The Russian source added that, in addition to Russia's media, Latvians like to cite "pseudo-academic and expert organizations" that they say try to negatively influence the Baltic state by creating distrust in the population. Finally, the Russian journal stated that Latvia believes organizations also work at discrediting Latvia at the international level. This includes exacerbating ethnic, linguistic contradictions, and differences in history's interpretation, and challenging Latvia's geopolitical course toward NATO and the EU. Organizations named by Latvia were the Historical Memory Foundation, the Russian Association of Baltic Studies, and the Kaliningradsky Blogpost.[198]

2019

Latvian discussions about Russian propaganda continued into 2019. One article noted that Russia has two kinds of destructive influence on Latvia's population. First, Russia's institutions that organize propaganda and information streams aim to deform democracy. Second, they are designed to reduce feelings of security in Latvia. On 31 January 2019, Latvia's NEPLP shut down *Rossiya RTR* for three months due to hate speech. It should have shut the channel down for a longer period, some believe, and if such hate speech continues, the channels license could be taken away.[199]

In another report, Latvia's main news outlet *LETA* cited a RAND study on Russian aggression in the Baltics and discussed several suggestions made in the study. The study advised Latvian security planners to prepare a wide range of technologies to enhance total defense capabilities, to coordinate strategic communication efforts among the Baltic countries to thwart Russian information warfare activities (and to create intelligence fusion centers to integrate civil, police, and military analysis capabilities), and to establish decentralized stockpiles and caches of relevant nonmilitary supplies to sustain resistance capabilities in case of war.[200]

Finally, an article published in *Delfi Online* discussed a Russian article that focused on Kremlin themes designed to divide Latvian society. The Latvian commentary noted that Vairis Godmanis and Viktors Domburs, who write often on Latvia but in English, usually discuss poverty in Latvia, crises in the nation's political life, and threats to the nation caused by NATO's presence. Some wonder if Godmanis and Domburs are really people. Maybe they are trolls. Articles sometimes appear on the little-known portal *Balticword* (already caught spreading fake information about the Baltic States), and from this portal they are sometimes republished in opinion-related news websites or other webpages and forums. One such webpage is *News Front*, which has been identified as an active Kremlin propaganda web portal headed by Konstantins Kniniks, a participant in Russian political TV shows.[201]

[198] Eduard Eldarov, "Moscow's Hand is Shaking Latvia," *Riga Vesti Segodnya*, 12 April 2018.
[199] No author or title provided, *Riga Delfi Online*, 1 April 2019.
[200] No author or title provided, *Riga LETA* (in English), 16 April 2019.
[201] No author or title provided, *Riga Delfi Online*, 16 June 2019.

Conclusions

Latvia is faced with an aggressive information war from Russia. Riga has a number of Russian-speaking citizens (at the beginning of 2018 it was noted that one-fourth of the population was Russian),[202] who are mostly those individuals or families left over from the time Latvia was part of the Soviet Union and decided to remain in Latvia. They tend to feel a need for more information from the Kremlin, as it more closely resembles their remembrance of how news sounded instead of what Latvia is providing. Russia is more than happy to accommodate that desire and, where possible, to overfill the plan with some information aimed at dividing Latvian society.

Latvian attempts to limit Russian disinformation have met with some success. They have proposed laws, developed an ideological foundation to overcome susceptibilities, and are developing the messages and images to stabilize Latvian values. Latvia is encouraging its citizens to educate themselves on Russian media techniques and methods of argumentation. Educational opportunities are further supported by studies being conducted at Latvian think tanks, which are available for downloading and reading, and by the work of the CPB to follow Russian efforts and help ensure Latvian digital and psychological security. Starting in September 2019 all secondary schools will transition to the Latvian language of instruction as well, a decision that was naturally protested by many Russians, protests covered by Latvia's Russian-language media.[203]

Russia, however, continues to contest any legislation and to protest democratic issues as moves to censor Russian material or to declare Latvian proposals as showing a lack of respect for the Russian diaspora. Russian messages are often provocative or demeaning, and the Kremlin continues to state that any move contrary to its intentions is due to an international conspiracy against Russian interests. That is, Russia believes only its understanding of objective reality is the correct one. Further, Latvia's desire to limit Russia's use of propaganda is often hindered by other issues, not the least of which are the alternate Kremlin-sponsored sites available to Russian members of society (Internet, etc.) and the penalties that would be assessed by the EU if Latvia bans Russian TV. Thus, Latvia must continue to battle Russian propaganda while continuing to search for resources and outlets to improve their propaganda-battle worthiness.

[202] See *Wikipedia*, https://en.wikipedia.org/wiki/Russians_in_Latvia
[203] No author or title provided, *BBC Monitoring* (in English), 8 May 2018.

CHAPTER FOUR: LITHUANIA

Introduction

For several years now Lithuania's government has complained about numerous information and cyber-attacks aimed at not only the government but also its population. In most of the cases under investigation, Russian propaganda vessels (*Russia Today* or *RT*, *Sputnik*, etc.), trolls, or secret operatives have been singled out as being responsible for the incursions or attempts at manipulation.

As a result of Lithuania's constant attention to this topic, the nation has developed several templates that are of interest to the U.S. and other nations. These templates describe Russian propaganda targets, dissemination techniques, and information themes, among other issues. The nation has developed a new National Cyber Security Strategy as well and is regarded as the fifth best country in the world regarding cybersecurity issues according to the national cyber security index.[204]

This report will examine the information and cyber-attacks that Lithuania has experienced and what lessons its analysts have learned and applied. The first part of the analysis focuses mainly on the propaganda of influence, while the second part focuses more on cyber issues (at times, in both periods, information and cyber issues are mixed). The period under examination is 2017-2019 and where specific templates are addressed, they are boldened.

Information

2017

V. N. Remarchuk, writing in the *Journal of the Academy of Military Science* in 2017, noted that "if society and the people are affected, then all the state power institutions, even with every technological perfection, will be doomed." [205] Soft power's importance thus lies in its ability to influence the behavior of the masses.[206]

It thus comes as no surprise that the main information activity of Russia is to try to influence Lithuanian society's will to resist. This is done, for example, by continuously pointing out fake NATO shortcomings and representations, such as that it will not come to rescue or defend Lithuania if Russia attacks it. The **ten targets of the propaganda** designed to reduce society's will were stated to be:

1. Lithuanian history
2. Foreign policy
3. Domestic policy
4. Lithuanian military
5. Defense capabilities
6. Ethnic communities (abused Russians and Poles)
7. NATO and the EU

[204] See, for example, https://ncsi.ega.ee/ncsi-index.
[205] V. N. Remarchuk, "The Destruction of the Modern State System by Means of 'Social Technologies,'" *Journal of the Academy of Military Science*, No. 2 2017, p. 48. The author would like to thank Dr. Harold Orenstein for the translation of this article.
[206] Ibid., p. 47.

8. Ties between Lithuania and Poland
9. Culture
10. The energy sector [207]

The Center for East European Studies further developed the goal of Kremlin propaganda, stated to be the creation of an image of a temporary Baltic state that will eventually side with Russia. This will help Russia create neutral space between Europe and itself. The **five layers of Russia's propaganda image** are: creating an image of a failing state; creating the myth that the nation is a neo-fascist state; creating mistrust in Western allies and stressing the need to agree with Russia; stimulating the fragmentation of Lithuanian society; and setting society against European ideas. The idea is to fuel nostalgia for the Soviet regime and to demonstrate that Lithuania had fueled tension in the region with artificial threats about Russia.[208]

The same source noted that **Russia's propaganda dissemination network** includes the Internet and public space; political and public organizations, informal movements, and defenders of minority rights; and history, historical heritage groups, and occurrences directed toward higher education and culture. Facebook pages, media outlets in either the Lithuanian or Russian languages, human rights defenses, public political organizations and information movements, historical heritage groups, and intellectual forums or other forms of activities are also part of the dissemination process. Television controlled by the Kremlin is the main dissemination channel along with *RT* and *Sputnik*.[209]

Propaganda has a further goal of regime change and the ability to falsify history. A Lithuanian Army representative noted that there is a **Russian information campaign** designed to do just that. The main narrative supporting regime change is that NATO is weak and detrimental to Lithuania. Russian citizens back home, on the other hand, are told NATO is strong and growing rapidly and is almost equal to the threat of fascism. Thus, Russia's propaganda is designed to fit the targeted population. Propagandists also note that everything is getting worse in Lithuania and that families are departing the country. The main narratives used to falsify, or influence history are attempts to discredit Lithuanian partisans from World War II who fought against Russia by trying to convince people that they were shooting and killing their own people.

The Russian *RT* budget appears well-funded to conduct reconnaissance. According to one report, in 2016 its budget was 600 million Euros, while the entire Lithuanian defense budget was 650 million Euros. There appears to be an information reconnaissance campaign underway against Lithuanian networks, which is designed to test how long it takes to access and hack into channels and post false news. Such posting of fake news must be countered immediately, as one cannot afford to be reactive[210] when Russia is so proactive. Another 2017 article also noted that Russia likes to darken the image of people who are dead and cannot defend themselves. This is particularly true regarding anniversaries designed to honor people who stood up to the Soviet Union, such as

[207] Ruta Latvenaite, "Information War with Russia Not to End for the Next Ten Years," *Lietuvos Zinios*, 24 April 2017.
[208] Center for Eastern European Studies Monograph, "Russian Propaganda: Analysis, Assessment, Recommendations," *EESC,* 18 July 2017, pp. 57-64.
[209] Ibid., pp. 72-76.
[210] Jurate Zuolyte, "Lithuanian Army Representative: In Information War, a Battle Over Hearts, Minds is Waged," *Delfi,* 17 October 2017.

World War II partisans (who are a continuous Russian target). Discrediting individuals is even more effective when done by people who would speak on behalf of Russians.[211]

Another source, in line with attempts to change the regime, noted that Russia tries to lower trust in the nation's institutions and in NATO and to create antagonism against liberal values. To counter such propaganda, Lithuania's Education and Science Ministry is trying to educate children about the threat of propaganda and the Culture Ministry has ordered a study of residents' ability to critically assess the media.[212]

2018

Lithuanian Foreign Minister Linas Linkevicius noted in 2018 that Russia often uses European platforms for its operations against Europe. *Russia Today* is registered in London, *RTR Planeta* in Stockholm, and *Yandex* in Amsterdam. Programmers, however, are in Moscow. Linkevicius states that, at times, some Lithuanian politicians are thinking that all is good with Russia. These people are naïve, he noted, and the hope is that they are not subject to the Stockholm syndrome, where a lack of experience or something else is causing them to make an incorrect analysis. Naturally not everything Russian should be rejected as there are very different people in different places there. But official propagandists will continue to try to divide Lithuania's population.[213]

In June 2018, a conference titled "Fake News Impact on Media Institutions: Poland's Experience and other Countries' Practices" was held in Kraków, Poland. Lithuanian LRT Director General Monika Garbaciauskaite-Budriene attended the session and made several important statements. She noted that the most important items on which to focus are 1) media literacy 2) the ability to distinguish reliable sources from unreliable ones, and 3) a need for better ethics, not legal regulation or better algorithms. She went on to discuss how truth is both a basic European tradition and value and they must be honored. Subjective opinions can skew the truth. Information can only be true or false, not subjective. Journalists too often feel pressure regarding promptness and let this feeling rule instead of taking the time to check information thoroughly. The authenticity of images must be also be checked and verified. Finally, she stated that journalists must continue to be trained in their profession as new digital devices appear often these days.[214]

Her commentary is important because Lithuania confronts fake report after fake report. For example, a fake hacker report from St. Petersburg, Russia claimed that Lithuanian Defense Minister Raimundas Karobils had harassed a journalist and admitted to being gay. The fake story stated that eight current or former diplomats also had spoken up about harassment. Lithuanian intelligence agencies had warned a year ago that Russia would be trying to discredit not only such

[211] Pumprickaite interview with Aukse Usiene, "Army Analyst: Ruta Vanagaite is Standing on the Frontlines of Information War," *LRT.lt,* 29 October 2017.
[212] Monika Kasnikovskyte, "Representatives of Academia Revealed Who Is Hurt Most by Russian Propaganda in Lithuania," *Balsas.lt,* 22 November 2017.
[213] Rita Miliute interview with Linas Linkevicius, "It is Dangerous When tolerance Turns into Naivety," *LRT.lt,* 1 August 2018.
[214] Eliminate Jursenaite interview with Moniak Garbaciauskaite-Budriene, "Journalists Must Seek Truth. This is the Best Antidote Against Fake News," *LRT.lt,* 23 June 2018.

official personas but also NATO forces through information and cyber-attacks. The aim is to spread provocative information.[215]

Based on a different type of reporting, on 14 February 2018 the Lithuanian Radio and Television commission took the Russian-language channel *RTR Planeta* off the air for a year for inciting war and hatred in their programming. However, in a dissenting opinion, a European Broadcasting Union representative stated that responding to Russian information with creative alternatives such as providing more profound information of higher quality would be more efficient than taking TV channels off the air.[216]

Thus, fake reporting, references to war and hatred, and means to create tension and confusion in society are all being used by Russia's propaganda outlets. Darius Jauniskis, Head of the State Security Department (VSD) of Lithuania, noted that Russia prepares information operations in peacetime to get the future battlefield prepared for action. Russia demonizes Lithuania as part of NATO and belittles it as a state. Such information actions are conducted constantly.[217] Propagandistic portals such as *Sputnik* and *Baltnews* employ the use of topics such as the presence and deployment of weapons as part of their information warfare strategy, which is reminiscent of the use of Soviet-era reflexive control measures (getting someone to do something for themselves that they are actually doing for you), according to a lecturer at Vilnius University.[218] Another report stated that *Baltnews* was engaged in "destructive activities in all three Baltic States; also, [it] cooperates with other companies, organizations, and persons…"[219]

Russia continues to ignore reality and historical truth. In 2018 the Baltic nations requested compensation for the Soviet occupation of their country during the last century. The Russian response was to state that Russia may decide to take Vilnius and Klaipeda back as part of its compensation. To Lithuanian analysts, this is another historical manipulation that Russia uses as it continues, in its own way, to ignore its occupation of the Baltic countries. When a demand is made for compensation for its occupation, Russia demands territory as its compensation.[220]

Based on this background, Lithuania's national security strategy has listed several **information themes** that Russia invokes. They are: attempts to skew historical memory; the spread of unfounded and misleading information about the democratic regime and the country's defense; attempts to pit ethnic and cultural groups one against another; attempts to weaken the national identity; information intended to discredit the country's membership in NATO; and information that weakens the citizens' resolve to defend Lithuania. It is necessary for Lithuanians to improve one's "information radar" as to what is real and fake; improve one's understanding of what is a fact, what is an interpretation, and what is simply a lie; and improve the ability to select information sources and their reliability. Critical thinking must be improved, investment in

[215] No author provided, "Fake News on Lithuanian Defense Minister Planted on News Portal," *BNS* (in English) 19 January 2018.
[216] No author provided, "European Broadcasting Union Representative Doubts Efficiency of Lithuania's Sanctions on Russian TV Channels," *BNS* (in English) 14 February 2018.
[217] Audrius Matonis interview with Darius Jauniskis, "VSK Head: Russia Tends to Cross Lines," *LRT.lt*, 3 April 2018.
[218] No author or title provided, *BBC Monitoring* (in English), 13 February 2018.
[219] No author provided, "Conservative MP Addresses Authorities Over Kremlin Propaganda Channels Operating in Lithuania," *ELTA* (in English), 31 August 2018.
[220] Zygintas Abromaitis, "Russian Propaganda Returns to Territorial Disputes with Lithuania," *LRT.lt*, 13 September 2018.

education must grow, and a reliance on more than one source is needed. News spread by social networks needs to be viewed in a critical way. Discord may be sewn in electoral processes, in relation to increased defense spending and the nation's socio-economic situation. A citizen's socio-economic situation can make them more vulnerable to propaganda. [221]

Finally, Lithuania has learned military lessons from the ongoing war in Ukraine. In an interview with a Ukrainian hybrid warfare expert, it was noted that Russia had used propaganda to attack army commanders by calling them unpatriotic, corrupt, and talentless. Soldiers received such messages directly to their cell phones in the field and were encouraged to rebel. The August 2014 battle of Ilovaysk was critical, as Russia's initial assault had caused some panic in Ukrainian society, with mothers, wives, and sisters calling soldiers and persuading them to save themselves and come home (the force had been surrounded by Russian forces and Ukrainian President Petro Poroshenko had called President Putin and requested a cease fire in order to get his forces home). It was not until army commanders could explain why things were done in certain ways that feelings began to change.[222]

2019

For some time, Lithuanian intelligence agencies have been stating that Russia's aggressive policy was the main threat to the nation's national security. The presence of Allied troops in the region in 2018 helped reduce the likelihood of Russia's use of military force against the region. To increase its ability to manipulate Lithuanian society, Russia increased its investment in what might be termed Lithuanian language propaganda, further indicating that it is reviewing strategies and the quality of its work to achieve its goals.[223]

In January 2019 Facebook announced that it had removed hundreds of pages and accounts in Lithuania that were linked to the Russian *Sputnik* channel or its employees. While the pages presented themselves as independent, they were spreading posts about anti-NATO sentiment. Some were in Lithuanian and some targeted divisive political issues.[224]

In a similar manner, Russian TV continued their propaganda assault of hatred with more fake news about Lithuanian partisans who were awarded the Freedom Prize in January 2019. *Channel 24 Russia* deemed the partisans to be criminals and offered fake statistics to create tension and distrust in Lithuania as part of Russia's information war,[225] which attempts to use propaganda to divide Lithuanians, undermine mutual trust, and influence democratic and decision-making processes. Lithuania's Deputy Minister of Foreign Affairs noted that disinformation presents a serious challenge for Western unity and security.[226] Character assassination, threatening letters to the Lithuanian embassy in Moscow, and defamation, fake news, intimidation, and various forms of pressure are the usual instruments that the Russian government uses to achieve its goals.[227] Any

[221] No author provided, "Are We Resilient Enough Against Information Threats," *15min.lt*, 31 October 2018.
[222] Aidanas Praleika, interview with Lyubov Tsybulskaya, "Ukrainian Expert: Moscow's Propaganda Hits Where It is Most Painful," *Lietuvos Zinios*, 20 November 2018.
[223] Milena Andrukaityte, "NSGK Chairman: Russia is Increasing Investments in Propaganda in the Lithuanian Language," *15min.lt*, 30 January 2019.
[224] No author provided, "Facebook Removes Hundreds of Accounts Linked to Sputnik Employees," *Baltic News Service* (in English), 17 January 2019.
[225] No author or title provided, *ELTA* (in English), 15 January 2019.
[226] No author or title provided, *ELTA* (in English), 11 April 2019.
[227] No author or title provided, *Lietuvos Zinios*, 15 April 2019.

issue that calls out Russian wrongdoing is severely chastised. For example, on 13 January Lithuania ruled against Russia and indicted its military for injuring and killing Lithuanians involved in that nation's 1991 demonstration for independence. Naturally, the Kremlin strongly condemned the ruling without providing any proof that Russia's military had not conducted such actions.[228]

It was also noted that in addition to the traditional tools of fake news, cyber-attacks, hacking, and disinformation campaigns, Russia also uses shadow money, corrupt influence, and other past tools to create useful political movements or to propose candidates that support Kremlin policies. Russia's long-term, traditional way of influence is a complex mixture of issues across the entire spectrum of activities, making it hard to recognize in its entirety.[229]

In summation, the three-year period under examination has found that some Russian information incursions have met with success while most have been singled out as outright slander or disinformation. Perhaps more importantly Lithuania has uncovered the most important Russian propaganda themes and dissemination techniques, as outlined above, for which they must be prepared to defend themselves.

Cyber

2017-2019

In late 2017 the Lithuanian Defense Ministry stated that Kaspersky Lab software products posed a potential threat to Lithuania's national security, especially since several critical infrastructures (not named) were using it. Government agencies were told to stop using the product while businesses will have to assess the risk of using Kaspersky products on an individual basis.[230] Another report stated that five percent of public bodies and agencies were using the software, according to the National Cyber Security Center (NCSC). Kaspersky Lab, the report noted, stated that it does not have inappropriate ties with any government.[231] The Lithuanian government noted that it had collected information carefully and did not jump to conclusions. Rather, specific evidence was collected about the software. Defense Deputy Edvinas Kerza noted that "at least two criminal groups linked with Russia's special services" were distributing malware.[232]

In addition to Kaspersky products, the NCSC recommended against using the Yandex Taxi ride-sharing app. The app is registered in Amsterdam, but its information technology specialists are in Moscow. The device collects and stores personal data and requests permission to activate a device's camera or microphone or manage its wireless network access.[233]

---

[228] No author or title provided, *ELTA* (in English), 23 April 2019

[229] Viktorija Rimaite, "Lithuania Will Not Manage to Escape Kremlin Tentacles: Old Weapons Pose Danger as Well," *Irytas.lt*, 9 May 2019.

[230] No author provided, "Russian Kaspersky Lab Software Poses Threat to Lithuania's Security—Government," *BNS* (in English), 21 December 2017.

[231] No author provided, "Lithuanian Critical System Managers Scrap Kaspersky Lab Software," *BNS* (in English), 27 January 2018.

[232] No author provided, "Lithuania's Government Ready for Litigation with Kaspersky Lab—Deputy Defense Minister," *BNS* (in English), 1 March 2018.

[233] No author provided, "Lithuania's Cyber Security Center Recommends Against Using Yandex.Taxi App," *BNS* (in English), 30 July 2018.

Simultaneously, hacking incidents are increasing against Lithuania. Some have been coordinated with information attacks. Subjects of the attacks have included figures such as Lithuania's National Defense Minister Raimundas Karoblis and Lithuanian troops participating in NATO exercises; and some have included energy or other specific agencies. Russia has been identified as a major culprit behind the attacks, and in many cases criminal groups or trolls were singled out as responsible for the incursions. Lithuania's Deputy Defense Minister Edvinas Kerza noted in one interview that 27 percent of incidents were directed at the energy sector, 22 percent toward the public sector, and 21 percent toward the foreign affairs and security policy sectors. The result is a hybrid threat.[234]

Lithuania has a host of "virtual elves" that try to act as a counterbalance against the efforts of pro-Kremlin trolls to control virtual information space. The elves' aim is to unmask Russian disinformation and fight those who spread it. In response, a Russian search system listed Lithuanian activists who are contesting Russian propaganda. The Russian goal was to organize attacks against the elves and create obstacles that prevent virtual space from supporting Lithuania.[235]

In response to Russia's expanded use of cyber activities, on 13 August 2018 Lithuania approved a new **national cyber security strategy**, which has replaced the existing Electronic Information Safety Development Program for 2011-2019. This was due to new cyber security challenges, especially cyber-attacks against public and energy sectors, airports, media outlets, and infrastructure for national security. Five goals were identified: bolstering cyber resistance and defense capabilities; fighting online crime; promoting innovations and a cyber security culture; promoting private-public cooperation; and strengthening international cooperation.[236]

The threat of cyber-attacks from Russia involves specific criminal groups funded by Russian authorities. They can create viruses undetectable by commercial measures with a goal of taking control of computer networks and systems.[237] Cyber-attacks appear most often on Lithuanian national holidays, when Russia is being accused of some wrongdoing, or when Russian citizens are banned from entering Lithuania. Russia then observes how Lithuania responds to such provocations and it tests Lithuania's level of cybersecurity at the same time. Media outlets are used to spread disinformation (lies about the situation) and panic (lies about shutting down infrastructure) through intrusions.[238]

Defense Minister Karoblis, in another interview, discussed the danger of two Russian programs designated as 1C and ABBYY. A cyber-attack in Ukraine used 1C, an accounting program that was then banned in Ukraine immediately but not in Lithuania. However, the system is being used in Vilnius in a proportional manner until a new program can be constructed. Interim

[234] Audrius Matonis interview with Edvinas Kerza and Rytis Rainis, "Criminal Groups Have Been Identified That Are Financed by Russian Authorities," *LRT.lt,* 13 August 2018.
[235] Rasa Pakalkiene, "Lithuanian Elves Have Gotten on the Kremlin's Last Nerve: Their Lists Have Been Published," *Lietuvos Zinios,* 8 January 2018.
[236] No author provided," Lithuanian Government Approves New Cyber Security Strategy," *BNS* (in English), 13 August 2018.
[237] No author provided, "Russia Poses Biggest Cyber Threat for Lithuania, Vice Minister Says (Media)," *BNS* (in English), 14 August 2018,
[238] Egle Kristopaityte, "Expert about Attack Against Karoblis: There Will Be More Such Campaigns Before Presidential Election," *15min.lt,* 19 January 2018.

measures are in place until fully secured software is installed. This helps Lithuania continue to pay, for example, the police in the meantime.[239]

The public is not the only target of Russian cyber-attacks. NATO troops in Estonia, Latvia, Lithuania, and Poland have been told that cyber-attacks are being aimed at their cellphones. As a result, soldiers are surrendering their cellphone service cards and communicating only via safe channels.[240] One 2017 report referenced a Wall Street Journal article that "cited troops, officials, and government representatives of NATO member-states" as stating that Russia had planned to hack mobile phones in order to obtain information about capacities and the ability to intimidate troops. The campaign was targeting 4,000 NATO troops in Poland and the Baltics.[241] Fake news stories have apparently been trying to use soldiers to cause problems in Lithuanian-Polish relations. In one such fake report, a Lithuanian soldier had reportedly said some Polish soldiers look like pigs due to their poor physical preparedness. Of interest is that the author of the fake story is apparently also a made-up character. The domain name that was spreading these stories was registered in Poland, but it is not known who controls it.[242] In a 2019 story about military exercises, it was reported that news portals were hacked. As a result, fake news was inserted into the portal, to include reporting about water shortages near Kaunas and the testing of weapons of mass destruction. Kremlin trolls were cited as the source of the news, aimed to cause panic among the population.[243]

The outlook for the future is not completely negative, in fact the Russian activity is driving positive change. Deputy Defense Minister Kerza said there is more than one plan under consideration for what the state would do if a mass cyber-attack occurred. Lithuania has invested in underground infrastructure and the network connections are known and who would ensure the systems function. Opponents will not know who our technicians are or where our cables are located. They are not announced. Lithuania is preparing not only for cyber defense but also for cyber-attacks. As Kerza warned "We do not aim to claim that we would be trying only to defend ourselves,"[244] a clear statement of the preparation of offensive operations if required.

Further, the July 2019 issue of Defense News had an article on Lithuania's cybersecurity posture, which is already, according to the 2018 Global Cybersecurity Index, the fourth best prepared country in cyberspace, behind only the UK, U.S., and France. The article noted that the Ministry of National Defense now has sole responsibility for setting cyber policy; that a Cyber Security Center was established in Kaunas in 2018; and that Lithuania participated at the

[239] Indre Makaraityte interview with Raimundas Karoblis and Marius Laurinavicius, "We Have Not Realized Yet That We Are at War with Russia," *LRT.lt,* 26 September 2018.
[240] Julija Petrosiute and Vykintas Pugaciauskas, "NATO Troops in Baltic States Will Have to Get Used to Life Without Unsafe Internet, Mobile Applications," *LRT.lt,* 6 January 2018.
[241] Vaidotas Beniusis, "NATO Troops Warned About Phone Hacking Threat Upon Arrival in Lithuania," *BNS* (in English), 6 October 2017.
[242] Andrius Vaitkevicius, "Liars from Poland Who Slandered Lithuanian Soldier Hiding under Picture of Doctor from Druskininkai," *Irytas.lt,* 12 November 2018.
[243] No author provided, "Kremlin Trolls Try to Spread Panic," *Kauno Diena Online,* 21 June 2019.
[244] Vaidas Saldziunas, "What Would Be Happening in Lithuania, If Internet Was Disconnected during a Cyber Attack: There are a Few Plans," *Delfi,* 25 November 2018.

international level by leading the European Union's permanent structured cooperation (PESCO) project on rapid response teams for cyber issues.[245]

Finally, political commentator Marius Laurinavicius noted that Lithuania's problem is that it does not realize yet that it is at war with Russia. The current government "is not creating an anti-hybrid strategy" and it does not prioritize issues as it should. For example, the chairman of the ruling party, LVZS leader Ramunas Karbauskis, has a business with a person funding a Russian troll factory and no one seems to worry about this.[246] Another report stated that Lithuania's NCSC warned in June 2019 about a risk posed by some Wi-Fi equipment as it uses Russian technology.[247]

Conclusions

One insightful commentary noted that Russian foreign policy creates political wedges by creating problems, violating international law, and creating geopolitical tensions.[248] Russian propaganda creates similar information wedges. Lithuania's continued information and cyber diligence directed at Russia's propaganda assault helps everyone better picture what these wedges are and their shape as well as where the Kremlin is directing its efforts.

The discussion above listed Russian propaganda targets, dissemination techniques, and information threats/themes that compose Russia's information campaign to influence Lithuania's population. Lithuania has a historical grudge with Russia,[249] which makes its focus very precise and documented. Many of these lessons can be applied to other nations that wish to counter Russian efforts to manipulate them, since other European nations also have their own grudges.

Russia, meanwhile, continues to ignore the importance of values and a quest for truth. Instead, it works to develop its own objective view of reality, one that is not shared by the European community at large. The Kremlin, from its responses to date, indicates that it is destined to ignore the realities (and there are many) that do not reflect well for actions it has committed. It is prone in many cases (MH-17, Skripal poisonings, Olympic doping, etc.) to invent its own version of reality.

[245] Jen Judson, "A Necessary Rise," *Defense News*, 8 July 2019, p. 9.
[246] Makaraityte interview with Raimundas Karoblis and Marius Laurinavicius.
[247] No author provided, "Lithuania's Cyber Security Center Warns About WiFi Equipment Risk," *BNS* (in English), 11 June 2018.
[248] Unidentified correspondent interview with Egidijus Motieka, "Kremlin Created System of Geopolitical Wedges in Europe; May Manipulate New Lithuanian President," *LRT.lt,* 30 March 2019.
[249] See, for example, Joana Lapeniene, "Year is About to End, Information Warfare Continues," *LRT.lt,* 31 December 2017.

CHAPTER FIVE: NONLETHAL WEAPONS

Introduction

For several years now Russian military authors have discussed the definition and potential use of nonlethal weapons (NLW). NLWs are thought to be a crowd control mechanism or a more humane way to conduct armed conflict. Regarding the latter, they are a way to capture or immobilize people hiding in buildings or behind barricades instead of killing them. Most definitions of the term center on these uses. What is difficult to ascertain is how advanced Russian efforts are in the production of NLWs since most of these experiments are conducted in secret laboratories. Since Russia believes that the US is developing NLW incapacitants (and they discuss US regulations and purported capabilities in some detail in their writings), they are likely to use such accusations to verify their own developments. One NLW analysis demonstrated why Russian authority fears so-called color revolutions:

> Analysis of today's conflict situations shows that political events in such countries as Iraq, Libya, Syria, and Ukraine develop according to similar scenarios. In some cases, it is worth noting the use of incapacitants to stir up panic, various kinds of provocation, and the inadequate behavior by some groups of the public aimed at discrediting the authorities or individual political leaders.[250]

Discrediting authorities and political leaders are what concerns suspicious Kremlin leaders the most.

Russian military authors clearly indicate that NLWs are under development. One source noted that research is directed at developing "basic theoretical principles of NLWs, in particular, the legitimacy of their employment" and "identifying the extent and timing of their employment in combat," among other issues.[251] The planning process for new weaponry indicates that, once the NLW program is endorsed by the various ministries concerned with their development, the National Military Industrial Commission and Security Council then submit the program to the leadership, both political and military, for approval. Russian NLW development trends are to be projected out 20-25 years, with predictions of critical military technologies that effect NLW development projected 15 to 20 years out. NLWs are used in exercises. One article noted that laser blinding devices, which cause temporary loss of vision without harmful consequences, can be fitted to drones and delivered up to three kilometers. Loudspeakers, sirens, video cameras, and other devices can be fitted to the drone.[252] The capabilities of the Filin blinding weapon, purportedly capable of temporarily blinding an opponent up to two kilometers away, are being increased along with its emitter power and angle of exposure.[253]

---

[250] L. N. Ilyin and V. V. Rylin, "Several Aspects of the Use of Nonlethal Toxic Agents," *Voennaya Mysl' (Military Thought),* No. 12 2018, p. 90.
[251] D. V. Zaitsev, D. Yu. Soskov, and A. V. Foteyev, "Weapons of Nonlethal Action on the Basis of Radiation: Physical Particularities and Prospects for their Use," *Voennaya Mysl' (Military Thought),* No. 4 2013, p. 31.
[252] No author or title provided, *Interfax (*in English), 15 May 2019.
[253] No author provided, "Russian Blinding Weapon Becomes More Powerful," *News.ru,* 17 March 2019.

This article covers specific incapacitants and their most likely utility. First, the changes in the definition of NLWs in Russia are explored. Second, the method by which NLWs are planned and produced is discussed. Third, explanations of when and how NLWs are used for internal and external situations are examined along with tactical innovations. Finally, Russia's cupboard of physical, chemical, biological, and radiological NLWs are examined. While not a game changer, NLWs are set to become an interesting addition to Russian capabilities on both the modern battlefield and, more likely, in domestic crowd control operations.

A Change in Definition?

Often described as a way to "humanize" armed violence, Russia's NLW concept has morphed in meaning over the years from a focus on personnel and equipment to a more focused approach on personnel. The ability of NLWs to disable equipment, however, is still mentioned, so the change appears to be only one of emphasis.

The term in 2011 was defined as the ability to incapacitate enemy manpower as well as disable enemy weapons, equipment, or infrastructure for a limited time. Weapons were defined by purpose and effect, with the latter including electronic shock, acoustic, kinetic, and biotechnological effects, or a combination of them. Viewed as a supplement to conventional weapons, they could be used in counterterrorist, peacekeeping, and special forces operations to halt hostile moves, limit conflict escalation, or use force where conventional weapons are unacceptable.[254]

In 2014 incapacitants were described as disabling personnel temporarily to reduce lethality and irreversible harm to humans, but other uses were also described. When applied only to humans, the goal was to achieve results only by more humane methods. NLWs were to be used in both low-intensity (contain movement, limit conflict escalation) and high-intensity (frustrate repairs, interfere with manpower mobilization) conflicts.[255] More importantly, they were to immobilize personnel for specific time periods in accordance with the developing situation and penetrate any type of cover.[256] Psychotropic agents include anesthetics, narcotic analgesics, and antidepressants, among others. Other chemical NLWs were to cause malfunctions in weapons and equipment. Thus, there was an equipment aspect to the 2014 NLW concept as well. They included antifriction compounds, chemical substances that accelerate the corrosion of alloys, and substances that degrade the quality of petroleum, oils, and lubricants as well as impair optical instruments.[257] It was stated that deregulators and substances that cause irreversible injury are banned by the Chemical Weapons Convention of 1993, and that Russia would never use such substances under any circumstances.[258]

[254] A. A. Nogovitsyn, A. V. Grudzinsky, and A. I. Sporykhin, "Nonlethal Weapons and the Outlook for their Use by the Forces of the Collective Security Treaty Organization," *Voennaya Mysl' (Military Thought)*, No. 3 2011, pp. 52-53.
[255] L. N. Ilyin and V. V. Rylin, "Incapacitants as a Weapon of Nonlethal Action," *Voennaya Mysl' (Military Thought)*, No. 9 2014, pp. 41-42.
[256] Ibid., pp. 37-38.
[257] Ibid., p. 37.
[258] Ibid., pp. 39, 42.

In 2015 a Russian article opened with a definition of NLWs that again included both personnel and weapons and equipment, noting that a NLW is

> A weapon designed to temporarily disable or immobilize personnel, weapons, military, and specialized machines and equipment, and infrastructure facilities and to reduce fatalities to a minimum without causing irreversible injuries to the health of human targets, or significant physical destruction of material assets and pollution of the environment.[259]

In the same article, however, the authors later noted that the definition is too broad and inaccurate from the point of view of logic. It is hardly inhumane to use NLWs against equipment! Thus, the authors wrote that a better definition would be "weapons designed to incapacitate adversary personnel temporarily and minimize irreversible injuries to their health or incur fatalities."[260] This discussion led to the eventual exclusion of equipment from most definitions of the term NLW. This change had appeared under consideration earlier, in 2013, when it was noted that NLWs incapacitate manpower for a specific time period without causing lasting harm to personnel.[261] It was stated that equipment should not be considered part of the target set.[262]

The 2015 article added that NLW's included acoustic, optical (laser and incoherent optical), and extremely high frequency (EHF) radiation weaponry. Incoherent optical radiation can only be used in dark hours and fair weather, and so it was determined to be less useful. So was laser radiation, since it cannot be used on a large scale due to constraints from Protocol IV of the 1995 Vienna Convention. This left only acoustic and EHF radiation for potential NLW use. They were described as all-weather with no limitations due to international law and able to fit on many vehicles due to small-sized radiation emitters. The radiation generator has an immobilization range of up to 60 meters for acoustic use and up to 250 meters for the EHF unit.[263]

In 2018 it was stated that a NLW is meant to impact only living beings, thus supporting the finding from three years earlier. The NLW term was defined as "weapons intended for the temporary disablement of adversary manpower with a minimum of lasting health disorders and fatalities."[264] The authors also defined two other terms. First, a nonlethal injury was defined as a NLW that impacts man where "the result of the factual use of NLWs by the adversary implies loss of combativity or incapacitation of the impact target for the duration of time **equal to or exceeding** the time needed to carry out the combat (special) task…."[265] Second, the term "nonlethal suppression" was defined as "the result of the factual use of NLWs by the adversary implying loss

[259] 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.
[260] Ibid., 52.
[261] D. V. Zaitsev, D. Yu. Soskov, and A. V. Foteyev, "Weapons of Nonlethal Action…", p. 32.
[262] Ibid., p. 31.
[263] D. V. Zaitsev, V. I. Orlyansky, and D. Yu. Soskov, "Nonlethal Weapons Can Be Used…", p. 55.
[264] D. Yu. Soskov, D. V. Zaitsev, and S. V. Kholod, "Developing a Conceptual Apparatus for Issues of Nonlethal Weapon Actions," *Voennaya Mysl' (Military Thought)*, No. 8 2018, p. 75.
[265] Ibid., p. 76.

of combativity (incapacitation) of the target for the time **less than that needed** to carry out the combat (special) task for which the said NLW was used."[266]

The Production Plan for NLWs

In 2002, new theories were advanced for waging armed conflict and for performing specific missions. Specific weapons, such as acoustic and optical ones, were deemed humane NLWs. The following order was recommended to determine the selection of NLW priorities at that time:

- The role of these weapons in support of national security
- The types of conflicts and situations in which it was proposed to use NLWs
- The cost of the development, production, and use of each type of NLW
- The volume of resources needed to create them
- The theoretical and experimental ground for equipping troops within allowable timetables and cost
- The infrastructure for their use
- And the ability to organize training in the NLW field.[267]

Two combination types of NLWs were deemed possible, information weaponry combinations and physical/chemical weaponry ones. Today, radiation and biological issues have been added to the NLW mix as the concept evolves over time.

In 2012, a *Military Thought* article noted that NLWs should be designed to comply with the following military criteria:

- Simple design that has an acceptable weight and size
- Compliance with combat kit
- Preference to NLW carriers already in existence
- Performance characteristics matching the required task without the use of conventional weapons
- Adversary effects varying in intensity depending on the situation
- And compatibility characteristics with conventional weapon requirements.[268]

The basic criteria involved in a military-economic assessment of NLWs included the following factors:

- Safety in use, to include the ratio of the area on which an adversary is exposed to friendly firepower versus the area exposed to friendly NLWs

[266] Ibid., p. 77.
[267] Vitaliy Tsygichko and Vladimir Dyachenko, "Non-Lethal Weapons," *Yadernyy Kontrol (Nuclear Control)*, 18 September 2002, pp. 58-67.
[268] A. Yu. Pronin, A. V. Leonov, and L. M. Kaplyarchuk, "Basic Criteria for a Military-Economic Assessment of Nonlethal Weapons," *Voennaya Mysl' (Military Thought*), No. 10 2012, pp. 43-50.

- Costs of the funds allocated over the lifetime of a NLW
- Combat efficiency of employing a NLW to fulfill its missions in a specified time
- Compatibility of a NLW with conventional weapons, that is their integration
- Proportion of the NLWs percentage of a unit's total weapons complement to fulfill tasks
- And the assurance that the use of NLWs do not go against existing law.[269]

Problems facing the planning and development of NLWs evolved in 2018. They included a lack of precise definitions of terms and their classification, since NLWs were defined differently for the Interior Ministry, the Armed Forces, and the Federal Security Service. This was a serious problem, since all of these agencies use NLWs for policing and counterterrorist operations, which all of these agencies handle. These are important points for the agencies to solve together. Another problem was determining whether NLWs are direct action (incapacitation) or special-purpose NLW agents. The latter NLW agents do not incapacitate an adversary physically but provide an opportunity, for example, for restricting an opponent's freedom of movement.[270]

It was noted that a NLW development program should include the following steps:

1. An analysis is made of indigenous and foreign trends, with a forecast offered of where NLWs seem headed.
2. A forecast is developed of potential constraints from existing international law, and humanitarian, ecological, socio-moral, and other issues that might restrict NLW use.
3. A discussion is conducted of scenarios and NLW employment opportunities.
4. The results of steps 2 and 3 help validate priority areas of NLW development for the military and law enforcement ministries.
5. Research is required into aspects of the employment, maintenance, manufacturing, and other constraints on NLW development.
6. Five-year, ten-year, and 15-year guidelines are drawn up, especially those to be followed by all agencies.
7. A Targeted NLW Development Program is prepared, and its feasibility assessed in relation to existing financial, manufacturing, technological, workforce, and other constraints. Where unsatisfactory results are discovered, the process returns to Step 3.[271]

Once step seven's "Targeted NLW Development Program" is endorsed by the various ministries concerned, then the National Military Industrial Commission and Security Council

[269] Ibid.
[270] V. V. Selivanov, D. P. Levin, and Yu. D. Ilyin, "Methodologies for Nonlethal Weapon Development," *Voennaya Mysl' (Military Thought)*, No. 2 2015, pp. 14-15.
[271] Ibid., pp. 21-23.

submit it to the leadership, both political and military, for approval.[272] NLW development trends need to be projected out 20-25 years, while critical military technologies with an effect on NLW development are projected out only 15 to 20 years.[273] Such a planning and development list suggests, due to its logic, that other Russian weapons planning and development scenarios might follow a similar seven step process.

Three types of NLW developments were discussed based on how they affected their targets. First were NLWs with a physical effect, from electromagnetic radiation, acoustics, mechanical constraints, kinetic energy, and electric discharge. Second were chemical NLWs, which have irritant (mucous membranes), odorant (psychophysical effects), and toxins, hallucinogens, simulants, and chemical neuroinhibitory agents. Third were biological NLWs, such as those causing irritation of the sense organs.[274] In addition to these three, targeted radiological NLWs were also mentioned.

Using NLWs Internally and Externally

There are several internal and external circumstances under which NLWs could be used. Internal armed conflicts (IAC) are those (1) between various illegal armed formations or (2) between illegal formations and state law enforcement agencies. Settling these types of conflicts early can prevent a transition to war. IACs are classified according to the causes of their emergence, the degree of state power structure involvement (as one of the opposing sides), the size of the state territory involved (local, regional, etc.), and the organization type (planned or spontaneous) and intensity. Subversive and terrorist activities are inherent in internal struggles, and a state's failure to solve such activities early can result in an atmosphere of fear that permeates society and creates a lack of confidence in state authorities. NLWs help reduce the combat efficiency of opponents in IACs and limit the number of fatalities.[275]

NLWs employed in police operations generally fall in line with the use of acoustic and electromagnetic radiation weapons and are one option available to reduce fatalities. It is important to develop various NLW systems, including those using electric current and radiation, to help power entities solve such special problems. When protecting major facilities, electroshock mines can be laid, since they help block unauthorized access to important areas.[276] It was noted that:

> At the same time, the distinctive features shared by all IACs suggest that NLWs must be used more extensively for their neutralization effect. Elimination of illegal armed forces with minimal civilian casualties, along with keeping life support, social, and transportation infrastructure facilities in a normal operational mode, will not only help restore the constitutional order in the conflict area, but will also ensure sustainable development of the country at large.[277]

---

[272] Ibid., p. 24.
[273] Ibid., p. 21.
[274] Ibid., pp. 15-18.
[275] D. Yu. Soskov, S. F. Sergeyev, and D. V. Zaitsev, "Using Nonlethal Weapons in Internal Armed Conflicts," *Voennaya Mysl' (Military Thought)*, No. 4 2018, pp. 56-58.
[276] Ibid., pp. 58-59.
[277] Ibid., p. 61.

One Russian military opinion was that NLWs are an effective information warfare asset. 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."[278] 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. This shows that in Russia, moods can be both "provoked" and then "defused" (with NLW) by the same government officials!

In regard to the external use of NLWs, they are being tested during exercises, with priority given to the Collective Security Treaty Organization (CSTO) due to the challenges these forces are facing in regard to terrorism, drugs, weapons, and ammunition trafficking along their borders.[279] In the three examples below, a special operations brigade of Kyrgyzstan's Armed Forces conducted the first bullet. Russian troop tactical exercises conducted the examples in bullets two and three:

- To seize a population center captured by militants, smoke screens were deployed from 70 meters to obscure the vision of a sniper hiding in a building. This would be followed, when buildings were stormed, by thermobaric hand and under-barrel grenades. Sound-and-light cluster hand grenades were also used on fighters in rooms. The Osa complex, with target acquisition and terrain illumination capabilities (signal and flare cartridges), was potentially utilized in this exercise.
- To fight off adversary ambushes, incapacitating agents were used, such as thermobaric hand grenades, which are 2.5 times more effective than conventional ammunition since they can hit adversaries concealed behind cover and in shelters.
- To clear corridors for military convoys on roads blocked by the population, a combination of sound-and-light, smoke, and irritant-charged hand grenades were used that explode without scattering splinters and produce only a psychological effect on crowds.[280]

When constructing a plan for the use of NLWs, it must be stated precisely how conventional and NLWs are to be employed together. This is particularly important in regard to time limits, since the employment of NLWs implies that effects only last for a certain period of time. Using NLWs against staffs and control centers will produce the greatest disorganization in an opponent's control cycle.[281] NLWs can achieve surprise since they can inhibit countermeasures and destabilize an opponent psychologically. Actions must be taken with resolve once enemy

[278] 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.
[279] A. A. Nogovitsyn, A. V. Grudzinsky, and A. I. Sporykhin, "Nonlethal Weapons and the Outlook for their Use by…," p. 55.
[280] Ibid., pp. 56-58.
[281] V. M. Moiseyev and V. I. Orlyansky, "Nonlethal Weapons: Tactical Principles," *Voennaya Mysl' (Military Thought),* No. 6 2011, p. 33.

troops are incapacitated and are unable to put up a real fight. In the offense they are most effective on an adversary's troops hiding in buildings, while when confronting a defending adversary NLWs reduce freedom of maneuver and help disorganize his control, reconnaissance, and information gathering.[282]

It was noted that the Russian Academy of Missile and Artillery Sciences was working on the organization and methodological support for developing NLWs, while the Scientific Research Institute of Applied Chemistry was working on developing, manufacturing, and delivering NLW ammunition and related devices.[283] Thus, NLW development is supported by both military and civilian industry.

Physical, Chemical, Biological, Radiation, and Information NLWs

In 2005 an article in Russia's *Military-Industrial Courier* listed mechanical devices, guns, direct effect sources, circular effects, light and smoke, physical and chemical compositions, and chemical and biological substances as types of NLWs:

- Mechanical devices (basket throwers, water cannons, and catapults to disperse materials)
- Guns (electromagnetic, subsonic, radio wave, super-high frequency)
- Direct effect sources (generators, phased or pulsed emissions)
- Circular effects (vortex generators, vibroacoustic devices)
- Next-generation light and smoke elements (smoke and pyrotechnic means, etc.)
- Physical and chemical compositions, compounds, and suspensions (foams, gels, powder, etc.)
- And chemical and biological substances (odorants, irritants, marker agents, viruses, etc.). [284]

These types of NLWs can be dispersed by various delivery means.

After 2005 a more succinct list of NLWs was developed, with physical, chemical, biological, radiation, and information weapons receiving the most attention. Of interest is that both personnel and equipment are mentioned as targets in the discussion below, with some articles written as late as 2018, indicating that the definitions discussed above may still not be fixed in stone.

Physical-based NLWs include lasers that can incapacitate manpower and optoelectronic surveillance devices; microwave weapons that disable weapons and equipment by knocking out electronic components; high-frequency weapons that raise body temperatures; and acoustic

[282] Ibid., pp. 31-32.
[283] A. A. Nogovitsyn, A. V. Grudzinsky, and A. I. Sporykhin, "Nonlethal Weapons and the Outlook for their Use by…," p. 59.
[284] Vladimir Lyashchenko, "Features of Trade in Arms Based on New Physical Principles," *Voyenno-Promyshlenny Kuryer (Military-Industrial Courier),* 8 June 2005.

weapons that cause dizziness, psychoneurotic breakdowns, and loss of hearing and sight. The range of these weapons is thought to be a few hundred meters to two or three kilometers.[285]

Chemical NLWs are those that can cause drowsiness and behavioral dysfunctions; that use adhesive (blocking) properties or alter the quality of fuels and lubricants; that increase the brittleness of metals; and that stall engines or block up ventilation systems. Many are offered in any caliber for NLW ammunition.[286] One article noted that NLW systems of greater efficiency are under development, especially for the use of a variety of chemical irritants. This includes a special NLW ammunition is available for machine guns that produce a large irritant cloud. It was also noted that:

> Another weapon is an irritant aerosol sprayer that can be used as a nonlethal landmine. Still another is a portable autonomous aerosol sprayer programmable to be activated in water in special operations. Small-size ammunition, for example, close combat irritant-containing grenades fired from under the barrels of grenade guns and hand grenades, may have a key role in neutralizing point targets, such as snipers hiding in dispersed locations on terrain or in buildings.[287]

Another chemical-related NLW discussion covered its advantages. They include the following: incapacitating targets for specific time periods; the ability to selectively affect targets and penetrate various types of shelter; the use of "damage control" operations that suit the situation; and the ability to integrate with and complement standard armaments. Chemical NLWs lower the chances of casualties among civilians and friendly units and can include operations such as peacekeeping, the de-escalation of armed conflicts, hostage rescues, and humanitarian support operations, where traditional warfare capabilities are less useful.[288] It was stated that:

> The idea of non-lethality may also aid the efforts targeting areas of drug production, storage, and transportation, as well as forces preparing inter-or intra-national armed actions… At present, commitments to respect state sovereignty restrict conditions in which pre-emptive strikes against these targets are possible. The use of NLWs makes such strikes 'politically acceptable.'[289]

Biological NLWs carry microorganisms that can harm humans, animals, and plants or disable weapons and other such items. Bacteria can decompose lubricants and block fuel flow passages, or it can cause swelling in artillery and firearm barrels.[290]

Radiation weaponry was the focus of another set of authors.[291] Electromagnetic radiation is broken into frequency ranges, to include optical and radio. Optical NLWs include laser radiation

[285] V. M. Moiseyev and V. I. Orlyansky, "Nonlethal Weapons: Tactical Principles," p. 27.
[286] Ibid.
[287] L. N. Ilyin and V. V. Rylin, "Incapacitants as a Weapon of Nonlethal Action," p. 41.
[288] V. B. Antipov and S. V. Novichkov, "On the Question of the Development and Use of Nonlethal Chemical Weapons," *Voennaya Mysl' (Military Thought)*, No. 9 2009, p. 54.
[289] Ibid., pp. 60-61.
[290] V. M. Moiseyev and V. I. Orlyansky, "Nonlethal Weapons: Tactical Principles," pp. 27-28.
[291] D. V. Zaitsev, D. Yu. Soskov, and A. V. Foteyev, "Weapons of Nonlethal Action…", p. 33.

blinding devices and are used against snipers, observers, and fighting vehicle drivers. Its long range, straight propagation, and little divergence are important principals for deployment. Radio frequency NLWs use extremely high frequencies (EHF). The latter can have NLW effects at a range of 15-700 meters. Most missions only require 250 meters. Acoustic radiation offers good utility in water and in the dispersal of large crowds of rioters at a range of around 60 meters. They do, however, have a wide divergence angle and thus low selectivity. On the positive side, they can be used in any weather or season.[292] While the article favored radiation weaponry and stated that it holds the greatest promise, it also noted that no single incapacitating agent is suitable for all operations. The specific effects of all NLWs indicates that they can only be used "in tactical situations for which they have been found to be fit."[293] A way must be found to develop "nonlethal weapons using several incapacitating agents in combination, the effect of which is yet to be studied."[294]

One article described information weapons as NLWs. The development of the mass media creates the prerequisites for the use of an inflation NLW in the opinion of some writers. Of interest is that psychological NLWs were also considered but have not yet been scientifically confirmed. These type of NLWs included telepathy, telekinesis, clairvoyance, and other psychological means.[295]

There continued to be NLW links to equipment. In 2018 NLWs were listed as a type of weapon based on new physical principles (NPP). For example, NLWs included glues, fuel-diluent chemical formulations, and enmeshing networks.[296] Another article stated that NLWs included traumatic weapons, foam and water cannons, emitters within a spectrum of several hertz to ultrahigh frequencies, and chemical and biological reagents based on adhesion or the ability to change physical and chemical characteristics of substances (elasticity, viscosity, electronical properties, mechanical density or sliding properties).[297] Their use is still thought to be focused on restricting freedom of movement, but they also have the ability to incapacitate humans.

Conclusions

NLWs are often described as a way to keep crisis escalation in check and to give leaders more time to resolve a conflict before it passes a point of no return. Russian military analysts appear in agreement, as they believe NLWs offer commanders new options and ways to handle crises. Flexible responses to situations offer more efficient methods for controlling them and reducing the chances of serious injury among noncombatants. Recent exercises and discussions in military journals indicate that NLWs are increasing in importance and use. Further, NLWs offer several distinct advantages, to include high efficiency of use, the ability to neutralize an

[292] Ibid., pp. 34-35.
[293] Ibid., p. 37.
[294] Ibid.
[295] Vitaliy Tsygichko and Vladimir Dyachenko, "Non-Lethal Weapons," pp. 58-67.
[296] A. V. Nazarenko and V. P. Gerasimov, "Maintaining and Recovering the Combativity of Units against Weapons Based on New Physical Principles," *Voennaya Mysl' (Military Thought)*, No. 8 2018, p. 22.
[297] N. V. Ageyev, "Matrix Method of Weapons Classification with Multidimensional Bases of Decomposition," *Voennaya Mysl' (Military Thought)*, No. 9 2018, pp. 56-57.

adversary's fighting capabilities, parameter control and selective effect capability, choice of time to take effect, and compatibility and potential integration with existing types of weapons.

However, it is just as clear that a final definition of what constitutes NLWs is still in flux. The definitions and explanations of NLWs do not coincide with their proposed use against people and equipment. While there seems to be a push to make NLWs a humane choice of engagement, articles continue to appear that describe chemical and biological NLWs that damage equipment.

Further, Russian NLWs are not described in the Western press at nearly the same rate as other developments, such as hybrid or asymmetric warfare. They deserve more attention. Perhaps NLWs are part of President Vladimir Putin's asymmetric approach to conflict. With a focus on NLW development trends projected out 20-25 years and critical military technologies predicted at least 15 to 20 years out, the concept appears to continue to play an active role in Russia's weapon technology planning process. Further, it is the types of NLWs that should concern the West, since they are not just physical and information but chemical, biological, and radiological. All can affect a situation and cause unforeseen consequences, to include serious psychological effects.

Finally, Russia's division of NLW use into internal and external areas is of interest. The former implies that Russia's National Guard will undoubtedly utilize NLWs when confronting demonstrators or other protestors, or when confronting terrorists inside the country. Externally to Russia it is most certain that they will be used against terrorists first and then perhaps later against a traditional opponent. Most likely they will be used in conjunction with traditional means of warfare in the latter case.

An article in *Armeyskiy Sbornik (Army Journal*) in January 2019 noted that warfare will be waged with the objective of disorganizing enemy efforts in the political and military spheres, with the goal being to coerce a side to accept proposed terms. This will require NLW effects, the author noted. More importantly, the journal is planning on publishing a series of articles on NLWs.[298] This makes it clear that the concept is drawing additional attention in the Russian military at the moment, indicating that it has become another military priority in Russia to monitor in the near future.

[298] N. Poroskov, "In Search of a 'Humane' Weapon," *Armeyskiy Sbornik Online (Army Journal Online)*, January 2019, pp. 74-81.