Universum Historiae et Archeologiae
The Universe of History and Archeology
Універсум історії та археології
Универсум истории и археологии
ISSN 2664–9950 (Print)
ISSN 2707–6385 (Online)
2021. Vol. 4(29). Issue 1, pp. 100–109
DOI 10.15421/26210414
http://www.uha.dp.ua

LCC DK 510: DK 670

Information operations as the main component of Russian aggression against Georgia in August 2008

A. I. Sorokivska-Obikhod
PhD Student scientific and organizational department
ORCID: 0000-0002-4413-9480
ariadnasor@ukr.net

Hetman Petro Sahaidachnyi National Army Academy
32, Heroes of Maidan street, Lviv, Ukraine, 79026

Abstract. *The aim of the article* is to reveal the essence of the mechanisms and information tools used by the Russian Federation during the Russian-Georgian war in August 2008; to analyze the main components of information operations and to reveal each component of information support of Russia's invasion of Georgia in 2008. It should be noted that the Russian Federation actively fought for control over the information space in order to obtain geopolitical dividends, and the main goal of Russia's information operations was to form an opinion among the international community about the aggressor state Georgia, which began hostilities against another ethnic minority on its own territory. *Research methods*: structural and functional analysis, search, formal-logical, system-structural, analytical. *Main results*: practical examples of information operations conducted by the Russian Federation during the Russian-Georgian military conflict in August 2008 are analyzed; the information operation's main components: computer network operations, electronic warfare, military deception, operational security, psychological operations that accompanied the kinetic operations of the conflict's parties are identified and studied. The study reveals the fact of Russia's thorough information preparation for the war, implementation of multifaceted anti-Georgian information «throw-ins» and struggle for the world's information space control. *Concise conclusions*: the Russian-Georgian war of August 2008 showed the growing influence of information war and revealed a number of Russia's Armed Forces shortcomings in this area at the same time. The conflict accelerated the Russia's military reform implementation, which has taken into account the latest information technology advances. The Russian side pushed Georgian President Mikhail Saakashvili to the war, which Russia used to strengthen its international influence. The Russian Federation succeeded in suppressing the Georgian leadership's communication with its own citizens and outside the world, and a brief Internet confrontation between Russian and Georgian hackers sparked widespread debate about the power of the Internet to influence the public opinion during the conflict. *Practical meaning*: the article materials can form a theoretical basis for the formation and implementation of various methods of counteracting the information and psychological influence of the Russian Federation in the post-Soviet space. *Originality*: a comprehensive study of the sources devoted to the theme of the Russian-Georgian war in August 2008 is carried out and introduced into scientific circulation. The information war is a part of Russia's hybrid war. This was confirmed by the statement of General Valery Gerasimov that «the political goals of the 21st century can be achieved by non-military and informational means» and «the operation to force Georgia to peace» has revealed the lack of common approaches for the use of Armed Forces outside the Russian Federation». *Scientific novelty*: for the first time an extended analysis of historical sources that described the information operations conducted by the opposing sides during the Russian-Georgian conflict in 2008 is carried out. In Ukrainian historiography, this problem has not been studied yet. Russian publications were not used because of their bias. *Type of article*: descriptive-analytical.

Keywords: Information warfare; Geopolitics; Hybrid war; Russian aggression; Post-Soviet space.

Received 04.11.2019
Reviewed 19.05.2021
Accepted 14.06.2021

Universum Historiae et Archeologiae
The Universe of History and Archeology
Універсум історії та археології
Универсум истории и археологии
ISSN 2664–9950 (Print)
ISSN 2707–6385 (Online)
2021. Vol. 4(29). Issue 1, pp. 100–109
DOI 10.15421/26210414
http://www.uha.dp.ua

УДК 355.48 (470+479.22) «2008»

Інформаційні операції як головна складова російської агресії проти Грузії у серпні 2008 року

А. І. Сороківська-Обіход
ORCID: 0000-0002-4413-9480
ariadnasor@ukr.net
Національна академія сухопутних військ імені гетьмана Петра Сагайдачного
вул. Героїв Майдану, 32, м. Львів, Україна, 79026

Анотація. *Мета статті*: розкрити суть механізмів та інформаційних інструментів, які використовувала РФ під час російсько-грузинської війни у серпні 2008 р., провести аналіз основних складових інформаційних операцій та розкрити кожну складову інформаційного супроводу російського вторгнення до Грузії у 2008 р. Варто зазначити, що РФ активно вела боротьбу за контроль над інформаційним простором з метою отримання геополітичних дивідендів, а головною метою інформаційних операцій РФ стало формування у міжнародної спільноти думки про державу-агресора Грузію, яка розпочала на власній території бойові дії проти іншої етнічної меншини. *Методи дослідження*: структурно-функціональний аналіз, пошуковий, формально-логічний, системно-структурний, аналітичний. *Основні результати*: проведено аналіз практичних прикладів інформаційних операцій, які проводила Російська Федерація під час російсько-грузинського військового конфлікту у серпні 2008 р., визначено та досліджено основні компоненти інформаційних операцій: операції у комп’ютерних мережах, електронну боротьбу, воєнний обман, операційну безпеку, психологічні операції, що супроводжували кінетичні операції сторін конфлікту. У дослідженні розкрито факт ретельної інформаційної підготовки РФ до війни, проведення багатопланових антигрузинських інформаційних «вкидів» та боротьбу за контроль світового інформаційного простору. *Стислі висновки*: російсько-грузинська війна серпня 2008 р. показала зростаючий вплив інформаційної війни та водночас виявила ряд недоліків Збройних Сил РФ у цій сфері. Конфлікт прискорив проведення російської військової реформи, що врахувала новітні досягнення в галузі інформаційних технологій. Російська сторона підштовхнула президента Грузії М. Саакашвілі до війни, яку вона використала для посилення свого міжнародного впливу. РФ вдалося подавити комунікацію керівництва Грузії із зовнішнім світом та власними громадянами, а коротке протистояння в Інтернеті між російськими та грузинськими хакерами викликало широку дискусію про силу Інтернету впливати на громадську думку під час конфлікту. *Практичне значення:* матеріали статті можуть скласти теоретичне підґрунтя для формування та реалізації різних методів протидії інформаційно–психологічному впливу РФ на пострадянському просторі. *Оригінальність*: проведено комплексне дослідження джерел, присвячених тематиці російсько-грузинської війни у серпні 2008 р., та введено до наукового обігу. Інформаційна війна є частиною гібридної війни РФ. Підтвердженням цього стала заява генерала Валерія Герасимова про те, що «політичних цілей XXI століття можна досягти невійськовими та інформаційними засобами, «Операція примушування Грузії до миру» виявила відсутність єдиних підходів до застосування формувань Збройних Сил за межами Російської Федерації». *Наукова новизна*: вперше здійснено розширений аналіз історичних джерел, які описували проведення інформаційних операцій протиборчими сторонами під час російсько-грузинського конфлікту 2008 р. В українській історіографії вказану проблему ще не досліджено. Російські публікації не використовувалися через їхню заангажованість. *Тип статті*: описово-аналітична.

Ключові слова: інформаційна боротьба; геополітика; гібридна війна; російська агресія; пострадянський простір.

Надійшла до редколегії 04.11.2020
Прорецензована 19.05.2021
Рекомендована до друку 14.06.2021

Universum Historiae et Archeologiae
The Universe of History and Archeology
Універсум історії та археології
Универсум истории и археологии
ISSN 2664–9950 (Print)
ISSN 2707–6385 (Online)
2021. Vol. 4(29). Issue 1, pp. 100–109
DOI 10.15421/26210414
http://www.uha.dp.ua

УДК 355.48 (470+479.22) «2008»

Информационные операции как главная составляющая российской агрессии против Грузии в августе 2008 года

А. И. Сорокивская-Обиход
ORCID: 0000-0002-4413-9480
ariadnasor@ukr.net

Национальная академия сухопутных войск имени гетмана Петра Сагайдачного
ул. Героев Майдана, 32, г. Львов, Украина, 79026

Аннотация. *Цель статьи*: раскрыть суть механизмов и информационных инструментов, которые использовала РФ во время российско-грузинской войны в августе 2008 г., провести анализ основных составляющих информационных операций и раскрыть каждую составляющую информационного сопровождения российского вторжения в Грузию в 2008 г. Стоит отметить, что РФ активно вела борьбу за контроль над информационным пространством с целью получения геополитических дивидендов, а главной целью информационных операций РФ стало формирование у международного сообщества мнения о государстве-агрессоре Грузии, которая начала на собственной территории боевые действия против другого этнического меньшинства. *Методы исследования*: структурно-функциональный анализ, поисковый, формально-логический, системно-структурный, аналитический. *Основные результаты*: проведен анализ практических примеров информационных операций, которые проводила Российская Федерация во время российско-грузинского военного конфликта в августе 2008 г., определены и исследованы основные компоненты информационных операций: операции в компьютерных сетях, электронная борьба, военный обман, операционная безопасность, психологические операции, сопровождающие кинетические операции сторон конфликта. Исследование раскрывает факт тщательной информационной подготовки РФ к войне, проведение многоплановых антигрузинских информационных «вбросов» и борьбу за контроль мирового информационного пространства. *Краткие выводы*: российско-грузинская война августа 2008 г. показала растущее влияние информационной войны и одновременно выявила ряд недостатков Вооруженных Сил РФ в этой сфере. Конфликт ускорил проведение российской военной реформы с учётом новейших достижений в области информационных технологий. Российская сторона подтолкнула президента Грузии М. Саакашвили к войне, которую она использовала для усиления своего международного влияния. РФ удалось подавить коммуникацию руководства Грузии с внешним миром и собственными гражданами, а короткое противостояние в Интернете между российскими и грузинскими хакерами вызвало широкую дискуссию о силе Интернета влиять на общественное мнение во время конфликта. *Практическое значение*: материалы статьи могут составить теоретическую основу для формирования и реализации различных методов противодействия информационно-психологическому воздействию РФ на постсоветском пространстве. *Оригинальность*: проведено комплексное исследование источников, посвященных тематике российско-грузинской войны в августе 2008 г. и введено в научный оборот. Информационная война является частью гибридной войны РФ. Подтверждением этого стало заявление генерала Валерия Герасимова о том, что «политических целей XXI века можно достичь невоенными и информационными средствами», а «операция по принуждению Грузии к миру» обнаружила отсутствие единых подходов к применению формирований Вооруженных Сил за пределами Российской Федерации». *Научная новизна*: впервые осуществлен расширенный анализ исторических источников, описывающих проведение информационных операций противоборствующими сторонами во время российско-грузинского конфликта 2008 г. В украинской историографии указанная проблема еще не исследована. Российские публикации не использовались из-за их заангажированности. *Тип статьи*: описательно-аналитическая.

Ключевые слова: информационная борьба; геополитика; гибридная война; российская агрессия; постсоветское пространство.

Поступила в редколлегию 04.11.2020
Прорецензирована 19.05.2021
Рекомендована в печать 14.06.2021

DOI 10.15421/26210414

Formulation of the Problem. The main goal of the Russian Federation is military and political dominance in the post-Soviet space, which is achieved through the «strong state concept» use. This policy is implemented through the creation of «buffer zones» and «instability zones»; redistribution of the spheres of influence; splitting of the existing unions; preventing the creation of new unions; acquisition of new markets. Georgia is one of the «strong state concept» realization objects. The Russia's regular military units invaded Georgia in August 2008. Under the international law, these actions fall under the military aggression. The Russian military actions were performed under the slogan «operation to force Georgia to peace» and were carefully planned and prepared by the top military and political leadership.

Historiography. The amount of scientific works related to the subject of our research is so significant that it is impossible to cover it in full in one article, so we will mention the most significant ones. In Ukrainian historiography, this problem has not yet been studied. Russian publications are not used because of their bias. Polemic with Russian researchers may be the subject of a separate study. Immediately after the end of the conflict began the scientific processing of the results and consequences of the hostilities in Georgia in 2008. Of particular interest among Western researchers was the conflict sides' information operations conducting that accompanied the hostilities. The following works are devoted to the Russian-Georgian August 2008 war: «The Russian Military and the Georgia War: Lessons and Implications» (Cohen, A. & Hamilton, R., 2011), «The 2008 Russian Cyber Campaign Against Georgia» (Shakarian, P., 2011), «The Bear Went Through the Mountain: Russia Appraises its Five-Day War in South Ossetia» (Thomas, T., 2009), «Russia's Conventional Armed Forces and the Georgian War» (McDermott, R., 2009), «Russia's Rapid Reaction: But Short War Shows Lack of Modern Systems» (Nicolle, A. 2009), «Russian's War in Georgia: Causes and Implications for Georgia and the World» (Cornell, S., Nilsson, N., Popjanevski, J., 2008), «The New Cold War: Putin's Russia and the Threat to the West» (Lucas, E., 2009), «Russian Propaganda War: Media as a Long- and Short-range Weapon» (Rogoza, J., 2008), «Cyberwar Case Study: Georgia 2008» (Hollis, D., 2011).

The Aim of the Study is to reveal the mechanisms and information tools essence used by the Russian Federation during the Russian-Georgian war in August 2008, to analyze the information operations main components and to reveal each component of military operations information support.

The Main Material and Results. The information war is a part of Russia's hybrid war. This was confirmed by the statement of General Valery Gerasimov that «the political goals of the 21st century can be achieved by non-military and informational means and «the operation to force Georgia to peace» has revealed the lack of common approaches for the use of Armed Forces outside the Russian Federation» (Gerasimov, V., 2013). Tensions between Russia and Georgia began long before the start of the 2008 Russian-Georgian war. A stimulating factor was the election of pro-Western President M. Saakashvili in 2004, under whose leadership Georgia applied to join NATO. Although South Ossetia is part of the internationally recognized territory of Georgia, it is ruled by Russian-backed separatists whose main goal is to split Georgia and assert Russian control over the strategically important South Caucasus (Cohen, A. & Hamilton, R., 2011, c. 4).

Even before the official start of hostilities a struggle began between the parties to control the information space. Thanks to the use of more powerful resources, the Russian Federation managed to gain a partial advantage and form in the international community the opinion about the aggressor state Georgia, which began fighting against another ethnic minority on its own territory. Although the international community condemned Russia for its aggression against Georgia, thanks to successful Russian information operations, part of the responsibility for the start of hostilities was placed on the then Georgian government. Russia's military aggression against the independent state of Georgia was conducted under the slogan «operation to force Georgia to peace» and was presented in the information space as a «fair» response to the Georgian shelling of the South Ossetian capital Tskhinvali and the facts of the deaths of Russian peacekeepers. In turn, Georgia insisted that the Georgian actions were provoked by the movement of a significant number of Russia's regular military units through the Roki tunnel in South Ossetia. During the war, both sides used tactics that contained the main components of information operations: computer network operations, electronic warfare, military deception, operational security, psychological operations (Nicolle, A., 2008, pp. 23–27).

Computer network operations. It is generally accepted that information is power and more and more information necessary for decision-making is digitized and transmitted through computer networks and other electronic devices. Computer network operations are purposeful actions that are aimed at the using and optimizing these networks in order to improve human efforts in war conditions, achieve information superiority and deny the enemy this ability. They include a broad concept of military calculations for receiving strategic benefits from computer networks use. According to the American «Joint Publication 3–13 Information Operations» computer network operations include computer network attack (actions aimed at destroying, denying or violating enemy information), computer network defense (actions to protect, monitor, analyze, detect and respond to network attacks, intrusions, failures or other unauthorized actions that may jeopardize or damage information systems and security networks) and computer network exploitation (intrusion into the enemy's network in order to extract confidential information) (Joint Publication 3–13, 2012).

The Russian-Georgian war of 2008 was a particularly interesting example of computer network operations. Some of the events that took place provide a unique insight into Russia's strategic and tactical operations, highlighted security vulnerabilities and initiatives for computer networks protection. From the very beginning, the Russia's leadership denied the computer network operations participation that took place before and during the wartime. However, the head of the National Security Council Georgian Eka Tkeshelashvili in 2009 stated that there is a lot of evidence of Russia's organization and direct involvement in computer attacks (Shachtman, N., 2009).

Even before the start of hostilities on July 20, a cyber attack had been carried out – the website of Georgian President M. Saakashvili was blocked for 24 hours (Independent International Fact-Finding Mission on the Conflict in Georgia Report, 2009, Vol. II, p. 218). The planning of these attacks was carefully prepared in advance. The US Cyber-Consequences Unit report stated that when cyber attacks began, they did not involve any stage of reconnaissance or mapping, but went directly to using the tools that were best suited to disrupt websites. This indicated that the necessary reconnaissance and attack scenarios had already been done in advance (Bumgarner, J. & Borg, S., 2009, p. 3). Despite the published report, the Russian leadership further denied any involvement in the cyber attacks conducting due to difficulties in identifying the exact sources of network attacks.

On August 7, at the same time as Russian Armed Forces units crossing the border, a cyber attack was carried out against Georgia, which had a Russian trace. Several Georgian servers and Internet traffic were seized and relocated under external control. Russian cyberspace actions continued during the following war days and became the first large-scale coordinated cyber attack to take place in parallel with and complementary to a conventional military offensive (Hollis, D., 2011). The targets of the cyber attack were the websites of the government, financial, business institutions and the Georgian media. The main purpose of the cyber attack was to support the Russian invasion of Georgia. As a result, communication between the government and the public deteriorated; many payments and financial transactions were suspended; there was confusion about the situation development; the Georgian government's efforts to disseminate information about the invasion were thwarted; the government was deprived of many information sources; it became more difficult to inform the outside world about what was happening, reducing the chances to receive the outside help, the Georgian government's ability to resist the Russian invasion was thwarted (Shakarian, P., 2011, p. 63).

The measures of the «first phase» of the DDOS attack (distributed denial of service) were carried out by botnets and were aimed at Georgia's news and government websites. This coordination strategy allowed Russia to effectively block lines of communication between the Georgian government and the population, and deprived Georgia's ability to communicate within the country and with the outside world during hostilities (Shakarian, P., 2011, p. 64). These cyber attacks continued throughout the Russian offensive. After the introduction of Russian troops into Georgia, the «second phase» began, with attacks on a number of government, educational, financial and media sites (including the BBC and CNN). In turn, international banks, wanting to reduce losses, stopped banking operations in Georgia during the conflict. Georgia's banking system did not work for ten days. This cut off mobile services in the country, further isolating Georgia from the rest of the world. By attacking Georgia's business sites, Russian hackers aimed to inflict similar economic damages (Shakarian, P., 2011, p. 66). The Russian side also created a website «StopGeorgia.ru», which contained instructions for ordinary users on how to quickly and easily conduct cyber attacks against the Georgian side. This allowed to attract more Russian users to cyber attacks.

In response, the Georgian side moved websites to the «blogosphere» under the shield google.com, and also used the Poland President website, which allowed to manage the work of websites and helped to communicate with the outside world. The cyber attacks were carried out with an interval of 30 minutes, they began at about 17:15 on August 8 and ended at about 12:45 on August 11 when Russia announced a ceasefire (Cohen, A. & Hamilton, R., 2011, p. 45).

A Project Gray Goose Phase II report was published in March 2009, revealing more links between the Russian government and the cyber attack on Georgia. The report describes the involvement of the Russian youth political group «Nashi» in the Georgian cyber attacks. The so called Democratic Anti-Fascist Movement «Nashi» is a youth organization funded by the Russian government. The report details the opening of the «StopGeorgia.ru» online forum on August 9, 2008, which was a virtual list of cyber-targets in Georgia and malware software. After conducting a study of IP addresses in the report, it was concluded that the website «StopGeorgia.ru» was probably created by agents of GRU of the General Staff of the Armed Forces of the Russian Federation. Thus, Russian military intelligence compiled a list of targets for groups of hackers who carried out cyber attacks after the start of the military invasion (Grey Goose Phase II, 2009).

Electronic warfare. According to «Joint Publication 3–13 Information Operations» electronic warfare is the electromagnetic spectrum and directed energy use to control the electromagnetic environment, attack the enemy and prevent enemy attacks. The main goal is to deprive the enemy of the advantage and provide friendly unimpeded access to the electromagnetic spectrum. Electronic warfare can be carried out from the ground, water, air and space using manned and unmanned systems, aimed at people, communications, radar, military and civilian objects. The electronic warfare includes electronic attack (actions called «jamming» of communication systems and radar systems), electronic protection (actions aimed at protecting friendly forces from electronic attacks by the enemy) and electronic warfare support (actions to detect, intercept, identify, locating and localizing sources of electromagnetic radiation) (Joint Publication 3–13, 2012).

It is worth noting the inconsistency of standards, imperfection and inefficiency of Russia's electronic warfare during hostilities. The weakness of Russian units was electronic protection, which created the safe use of the electronic spectrum by friendly forces. The command and control of the Russian forces were disorganized due to poor communication. Radio communication did not work, leaving divided Russian units in electronic isolation on the battlefield (Thomas, T. 2009).

The prevailing capabilities of Georgian communications and electronic warfare units muffled the Russian communications. Russian units were unable to effectively counter the Georgian side's electronic attacks and used less secure means of communication (mobile phones). As an example, the Russian commander of the 58th Army general Anatoly Khrulev used a satellite phone borrowed from a journalist to communicate with units and was later injured as Georgian guidance systems found signals from Russian radios and mobile phones and destroyed them (Nicolle, A., 2008; McDermott, R., 2009). Mobile phones used by Russian commanders instead of obsolete Soviet radio stations often transmitted their signals through Georgian-controlled local South Ossetian networks (Cohen, A. & Hamilton, R., 2011).

Another Russian Armed Forces weakness was electronic warfare support: due to the lack of space and electronic intelligence data, they didn't know the Georgian units exact location and used outdated topographic maps. Russian operations were complicated by the lack of satellite targeting for artillery support, as in August 2008 the grouping of satellites of the Russian global navigation system GLONASS had not yet been completed and deployed units were not provided with receivers. Russian servicemen used compasses and maps. Due to the lack of satellite targeting for artillery support, it was not possible to use high-precision weapons and accurately control artillery fire (McDermott, R., 2009).

In addition, outdated equipment of the friend-or-foe recognition system was used, which led to numerous losses due to firing at friendly units (McDermott, R., 2009). Russian electronic attacks of silencing the enemy's air defense system were also unsuccessful: Georgian air defense systems destroyed four Russian aircraft (a Tu-22M3 strategic bomber and three Su-25 attack aircraft). Due to the lack of intelligence data on the presence of Soviet-made SAMs ZRK «Osa» 9K33 (Soviet classification GRAU) and ZRK «Buk» 9K37 (Soviet classification GRAU) in Georgia, the Russians failed to neutralize these weapons in time. Russian ground forces were badly hit by Georgian SAMs. Also, the Russian side did not have aircraft capable of night operations, and Georgian aircraft operated around the clock. Due to the lack of means to silence the enemy's air defense system, Russian units failed to achieve air dominance and provide adequate support to the ground forces, which demonstrated the significant shortcomings of all components of electronic warfare. Dominance in the air was achieved only after the capture of Georgian air defense facilities by Russian ground forces at the end of the conflict (Nicolle, A., 2008).

Military deception. The «Joint Publication 3–13 Information Operations» states that military deception is the activity of deliberately misleading decision-makers, creating favorable conditions for friendly forces and harming the enemy in order to gain an advantage in hostilities. These actions are closely related to operational security, which allows to hide from the enemy important information about opportunities, limitations, intentions and activities or provide a plausible alternative explanation of details that the enemy may observe, while deception reveals false information to introduce the enemy delusion. Military deception is achieved by creating or intensifying an artificial fog of war (uncertainty about own capabilities and intentions and the enemy's intentions during hostilities) through visual deception and psychological operations (Joint Publication 3–13, 2012).

Russia actively uses the practice of denial and military deception (disguise), which is an integral part of military planning and operations in peacetime and during hostilities. Disguise is defined as a form of support for hostilities and daily activities of troops (forces). It is a set of interrelated organizational, operational, tactical and engineering measures used to hide units and structures from the enemy in order to mislead him about the presence, location, composition, status, actions and intentions of friendly forces (McDermott, R., 2009).

In the spring of 2008, Russia significantly increased the number of peacekeeping forces in Abkhazia, increasing tensions in the region (Blandy, C., 2009). Even before the start of the 2008 war, Russian forces attacked Georgian villages, destroying drones and radars to provoke Georgia into conflict. The Russia's military units build-up was carried out before the start of the conflict. Russia conducted large-scale military exercises «Kavkaz-2008» near the Georgia's borders and after they ended, Russian units did not return to their permanent deployment places, but remained in the training areas. The concentration of Russian units near the border with Georgia was aimed at involving the Georgian leadership into the armed conflict (Cornell, S., Nilsson, N., Popjanevski, J., 2008).

The Russian media played a key role in deceptive propaganda spreading. Thus, «Channel One» showed an interview with an allegedly Abkhazian pilot who destroyed a Georgian UAV on April 20, 2008, which supposedly could indicate preparations for a possible Georgian invasion of Abkhazia. The Russian side used this fact to justify the number of Russian peacekeepers increase, as well as additional units, equipment and weapons. Mass propaganda continued in the following months, when the media reported about the gathering of Georgian forces near the Abkhazian border. In July 2008, «Channel One» reported that Georgia was planning an invasion of South Ossetia, trying to convince the public that the aggressive Saakashvili should be stopped (Lucas, E., 2009).

The illegal distribution of Russian passports among Georgian citizens in the conflict regions (Abkhazia and South Ossetia) also played an important role. Thanks to «passportisation» campaign the Russian leadership was able to justify participation in hostilities on the territory of Georgia as «protection of Russia's citizens» from Georgian aggression. In fact, the Russian-Georgian conflict of 2008 was an organized military deception campaign aimed at increasing Russia's geopolitical influence in the South Caucasus. There were not only regional events that indicated that the Russian Federation was carefully planning a «five-day war». The Defense Academy of the United Kingdom report states that several reliable Abkhazian sources informed about the Russian offensive preparations in August 2008 on Georgian units in the Kodori Gorge (controlled by Tbilisi) and provided more accurate information on who, where and when will attack Georgian units (Blandy, C., 2009).

Operational security is an ongoing process that is used to control information and encompasses physical, informational, computer and communication security to identify and protect critical information. Operational security consists in protecting individual data pieces that can be summarized and grouped to obtain a broader situation picture. This process result is the countermeasures development (technical and non-technical) such as software use to encrypt e-mail, precautions against eavesdropping, careful study of photos background elements and posts on social networks. This process identifies specific information that needs to be protected and consists of identification of critical information (information that the adversary can use to its advantage), analysis of threats (identifying potential adversary capabilities), analysis of vulnerabilities (studying each aspect of the planned operation to identify indicators that can disclose important information), assessment of risk (determination of the threat level), application of countermeasures (reduction of risks that will pose the greatest operations threat) (Joint Publication 3–13, 2012).

The operational security was observed among the Russian units. On March 11, 2007, a Georgian-controlled Kodori district was attacked by a helicopter. The Russians denied any involvement stating that the attack was a Georgian provocation. The United Nations Observer Mission in Georgia investigation acknowledged Russia's responsibility for the incident. On August 6, 2007, a Russian pilot violated Georgian airspace and attempted to destroy a radar installation. Russia denied any involvement and convinced the international community that Georgia was again trying to provoke Russia. Subsequently, the United Nations Observer Mission in Georgia established Russia's involvement in this event. On September 20, 2007, Russian forces attacked a Georgian construction crew near the Kodori Gorge. Georgian units responded. Although an analysis by the Open Sources Center found that the attack was carried out by Russian and Abkhazian troops, Russian and Abkhazian officials denied the incident. The Abkhazian side refused the request to investigate this incident by United Nations Observer Mission in Georgia with the aim to hide the presence of Russian troops from the international community (Open Source Center, 2009).

Psychological operations are planned operations of information transfer to influence the target audience, the main purpose is to change enemy's behavior and create a favorable environment for the organizer of the operation. Types of psychological operations are propaganda and disinformation disseminated through visual, audio, audiovisual, print and electronic media at the strategic, operational and tactical levels (Joint Publication 3–13, 2012).

During the Russian-Georgian war in August 2008, Russia conducted psychological operations on several target audiences: Georgian President Mikhail Saakashvili, the Georgian people, the Georgian armed forces, the United States, NATO and the international community. The Russian side created strong enemy images. For this purpose, the concepts of «we» («our state / homeland / nation») and «they» (enemy, foe) were used. The pro-government Russian media consistently adhered to the Kremlin's official line, using the term «we» to consolidate the Russian community and create the solidarity between the author and the reader (for example, «we lost about 80 people killed», «our people are being killed in Ossetia»). The main target was pro-Western President Mikhail Saakashvili, who sought Georgia's membership in NATO, which was strongly opposed by Russia. The General Staff of the Armed Forces of the Russian Federation developed a detailed plan to encourage Saakashvili to engage in ill-considered military action and thus demonstrate his instability as a NATO partner, while creating a pretext for Russia's invasion of Georgia. For this purpose, the theory of reflexive control (control of the decision-making process by the opponent) was used at the strategic level. Control over the opponent's decision-making, which is the formation of a certain behavioral strategy towards him with the help of reflexive interaction, is achieved not directly, not by force, but by giving the opponent the basis according to which he can logically make his own decision, but such that will be favorable for the other side (Blandy, C., 2009).

On August 13, 2008, the official newspaper of the Ministry of Defense of the Russian Federation «Krasnaya Zvezda» published a detailed psychoanalysis of Mikhail Saakashvili, which stated that «he has a paranoid disorder of a hysteria personality type with a narcissistic complex, he considers the world around him as a hostile environment» (Ruchkin, V., 2008). Other observers also noted his vulnerability. Later, United States Secretary of State K. Rice said: «he is proud, he can be impulsive, we are all worried that he might allow Moscow to provoke him to use force» (Kucera, J., 2011). The Russian side successfully exploited this weakness by encouraging South Ossetian separatists to shell Georgian villages in order to provoke Saakashvili to a military response. The rapid response of Russian units indicated a high level of readiness and careful advance operation planning.

Throughout and after the end of the conflict, Russia claimed a criminal case against Saakashvili for genocide against Ossetians and war crimes in South Ossetia, comparing him to Slobodan Milosevic / Radovan Karadzic (Cohen, A. & Hamilton, R., 2011). These statements demoralized the Georgian leader and encouraged his pro-Russian political enemies to take action. The focus on Saakashvili was aimed to discredit him at the international and domestic levels. By dividing the president of Georgia and the Georgian people, Russia sought to change the political regime without the use of physical force. At the beginning of the conflict, the Russian state media completely denied the Georgian state as an aggressor, but later the reports distinguished between the «criminal» Mikheil Saakashvili and the Georgian people, to whom Russian President Dmitry Medvedev expressed «fraternal» support (Rogoza, J., 2008).

Russia sought the legitimacy of its invasion of Georgia by influencing the international community, calling its operation a peacekeeping operation and countering «ethnic cleansing» and «Ossetian genocide», while keeping Ossetian attacks on Georgians secret. NATO and the United States have failed to counter Russian influence effectively. The United States failed to defend Georgia and NATO retreated, signaling that it was better not to interfere in the affairs of a state under Russian influence.

The Georgian Armed Forces were an important target audience. The usual tactical level measures of psychological operations, such as leaflet distribution or broadcasting directed at ground forces were not noticed. They would have limited benefit during such a short campaign. It can be argued that the psychological impact of the Russian offensive speed was a decisive war factor. The Russians refused to engage in combat in the first clashes and advanced southward into Georgia, causing panic among Georgian servicemen (Cohen, A. & Hamilton, R., 2011). After about 72 hours of fighting, during which Georgian troops demonstrated a decent level of combat readiness, August 11 saw a sudden and total demoralization. Georgian units lacked combat experience and were shocked by Russia's response (Nicoll, A., 2008).

Results. The Russians managed to effectively conduct psychological operations on target audiences. They pushed Saakashvili to the war they wanted, which they used to increase their international influence at the expense of the United States, NATO and Georgia. Russian forces used impressive speed to cause the psychological collapse of the Georgian resistance and suppressed Georgia's communication with the outside world, actively opposing Georgian propaganda.

Discussion. The materials of the article can form a theoretical basis for the formation and implementation of various methods of counteracting the information and psychological influence of the Russian Federation in the post-Soviet space.

Conclusions. The Russian-Georgian war of August 2008 showed the growing impact of the information war and at the same time revealed a number of shortcomings of the Russian Armed Forces in this area. The conflict also accelerated Russia's military reform, which will include the latest advances in information technology. The Russian side pushed Mikhail Saakashvili to war, which Russia used to strengthen the international influence. Russia has managed to suppress Georgian leadership's communication with own citizens and the outside world, and a brief confrontation on the Internet between Russian and Georgian hackers sparked widespread debate about the power of the Internet to influence public opinion during the conflict.

The Russian Federation builds relations with the neighbors, as with the former colonies, without considering them as fully sovereign states. To achieve the goals, Russia uses separatism and irredentist claims in neighboring states to blackmail and, if necessary, to dismember them. Russia uses the concept of a strong state as an instrument of foreign policy towards Moldova, Georgia and Ukraine. The main tool in spreading Russian influence in the post-Soviet space is propaganda. The main goals of Russian propaganda are declared in the documents of the country's foreign policy and national security: Vladimir Putin's political manifesto «Russia and the changing world» and program article of the Chief of the General Staff of the Russian Federation Valery Gerasimov «The value of science in prediction», which highlights the main provisions of the new military doctrine of the Russian Federation.

Vladimir Putin sees this concept as «a mechanism for achieving foreign policy goals without the use of force, interference or aggression» and emphasizes the strategic importance of «reintegration» of Russian compatriots living abroad. He examines various global challenges and notes that «the modern world order and stability cannot be imagined without strong Russia» and outlines the fundamental components of instability – non-governmental organizations, which are the main sources of separatism and extremism that only destabilize countries (Putin, V., 2012).

According to the «Gerasimov's Doctrine», the main goals of Russian propaganda are: defense (avoidance of «color revolutions» and ideological treatment of the local population), offensive (influence on Western societies through misinformation and rumors (fabrications) spreading to protect «Russian national interests»), severance of relations between the EU and its strategic partners, paralysis of the decision-making process in the EU and NATO structures, creation of various myths (the United States is going to start a war and the countries of Central and Eastern Europe will be used as shields), the spread of various false doctrines («post-Soviet space is a legitimate zone of Russian influence»), discrediting the countries of the Eastern Partnership with the use of the Orthodox Church, public organizations and foundations, representation of Ukraine as an aggressor and a country with a fascist regime and promoting the image of indomitable Russia (Gerasimov, V., 2013).

References

Blandy, C., 2009. Provocation, Deception, Entrapment: The Russo-Georgian Five Day War. Advanced Research and Assessment Group, *Defense Academy of the United Kingdom,* March 2009, England: Shrivenham, Available at: https://www.files.ethz.ch/isn/97421/09_january_georgia_russia.pdf [Accessed: 10.09. 2020] (in English).

Bumgarner, J., Borg, S., 2009. Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008. *US-CCU Special Report*. Available at: http://www.projectcyw-d.org/resources/items/show/138 [Accessed: 20.09. 2020] (in English).

Cohen, A. and Hamilton, R., 2011. The Russian Military and the Georgia War: Lessons and Implications. *Strategic Studies Institute*, June 2011, 112 p. (in English).

Cornell, S., Nilsson, N., Popjanevski, J., 2008. Russian's War in Georgia: Causes and Implications for Georgia and the World. *Central Asia Caucasus Institute Silk Road Studies Program Policy Paper,* August 2008. Available at: https://www.silkroadstudies.org/resources/pdf/SilkRoadPapers/2008_08_PP_CornellPopjanevskiNillson_Russia-Georgia.pdf [Accessed: 19.09. 2020] (in English).

Georgia says it Killed Four in Kodori Clash, Suspects Russia. 2009. *Open Source Center*. Available at: https//www.opensource.gov/portal/server.pt/gateway/PTARGS_0_0_200_240_1019_43/html [Accessed: 26.09. 2020] (in English).

Gerasimov, V., 2013. Tsennost nauki v predvidenii, *Voenno-promyshlennyy kurer,* issue 8 (476). Available at: https://www.vpk-news.ru/articles/14632 [Accessed: 26.09. 2020] (in Russian).

Hollis, D., 2011. Cyberwar Case Study: Georgia 2008. *Small Wars Journal*. Available at: http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008 [Accessed: 24.09. 2020] (in English).

Independent International Fact-Finding Mission on the Conflict in Georgia Report. September 2009, Volume II, p. 218. Available at: https://www.mpil.de/files/pdf4/IIFFMCG_Volume_II1.pdf [Accessed 15 September 2020] (in English).

Joint Publication 3–13. Information Operations. Joint Chiefs of Staff, 27 November 2012. Incorporating Change 1 (20 November 2014). Available at: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf [Accessed: 25.09. 2020] (in English).

Kucera, J., 2011. Condoleezza Rice Warned Georgian Leader on War With Russia. *The Atlantic,* 16 November 2011. Available at: http://www.theatlantic.com/international/archive/2011/11/condoleezza-rice-warned-georgian-leader-on-war-with-russia/248560/# [Accessed: 17.09. 2020] (in English).

Lucas, E., 2009. *The New Cold War: Putin's Russia and the Threat to the West.* New York: Palgrave Macmillan, pp.141–147 (in English).

McDermott, R., 2009. Russia's Conventional Armed Forces and the Georgian War. *Parameters*. Available at: https://www.offiziere.ch/wp-content/uploads-001/2019/01/McDERMOTT-Russia%E 2 %80 %99s-Conventional-Armed-Forces-and-the-Georgia.pdf [Accessed: 14.09. 2020] (in English).

Nicolle, A., 2008. Russia's Rapid Reaction: But Short War Shows Lack of Modern Systems. *IISS Strategic Comments,* vol. 14, issue 7, September 2008, pp. 23–27 (in English).

Project Grey Goose Phase II. 2009. The Evolving State of Cyber Warfare. *GreyLogic,* 20 March 2009. Available at: http://www.fistfulofgold.com/Documents/ProjectGreyGoose.pdf [Accessed: 15.09. 2020] (in English).

Putin, V., 2012. Rossiya i Menyayushchiysya Mir. *Rossiyskaya Gazeta*. Available at: www.rg.ru/2012/02/27/putin-politika.html [Accessed: 26.09. 2020] (in Russian).

Rogoza, J., 2008. Russian Propaganda War: Media as a Long- and Short-range Weapon. *Center for Eastern Studies,* Warsaw, Poland, November 2008, issue 9, pp. 1–5 (in English).

Ruchkin, V., 2008. Virus vozhdizma. *Krasnaya Zvezda.* 13 August 2008. Available at: http://old.redstar.ru/2008/08/13_08/4_06.html [Accessed: 18.09. 2020] (in Russian).

Shachtman, N., 2009. Top Georgian Official: Moscow Cyber Attacked Us – We Just Can't Prove It. *Wired*. Available at: http://www.wired.com/dangerroom/2009/03/georgia-blames/ [Accessed: 29.09. 2020] (in English).

Shakarian, P., 2011. The 2008 Russian Cyber Campaign Against Georgia. *Military Review*. Available at: https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20111231_art013.pdf [Accessed: 15.09. 2020] (in English).

Thomas, T., 2009. The Bear Went Through the Mountain: Russia Appraises its Five-Day War in South Ossetia. *The Journal of Slavic Military Studies*. Available at: http://dx.doi.org/10.1080/13518040802695241 [Accessed: 08.09. 2020] (in English).