4/07/2021

U.S. DEMOCRACY AS THE TARGET OF RUSSIAN SECRET SERVICES

MICHAŁ WOJNOWSKI, PH.D.

WARSAW INSTITUTE

— SPECIAL REPORT —

SOURCE: FLICKR / ELVERT BARNES

Part II

Russian Interference in the U.S. Presidential Elections in 2016 and 2020 as an Attempt to Implement a Revolution-like Information Warfare Scheme

- **While adapting Western theories and terminology, Russians make assumptions aligned with their domestic needs. The whole procedure is designed to conceal methods and tools Soviet spy agencies had brushed up for decades.**
- **Russian analysts say that efforts to forecast election campaigns and the vote in the United States as well as predict its winner depends on the syndrome of political instability that encompasses competition inside the ruling party, social unrest, and the force of extra opposition groups.**
- **Russian interference in the U.S. election, thus in its social and political life, involved an array of active measures, with cyberspace operation on top of that. In both its theory and practice, Russian information warfare affected the U.S. election process through two intertwined operations of intelligence agencies and related entities, taking place at the strategic, operational, and tactical levels.**
- **Bringing into focus solely how these cyber attacks occurred leaves out other actions––traditional and far more perilous––such as foreign contributions to political parties or nourishing political influence.**

Information warfare as an active measure weapon of Russian special services

Despite the demise of the Soviet Union, the Russian policy towards the United States still resembles somewhat a cold war where its factors seem to prevail over provisions of the deal. Russian intelligence outfits took on a major role in framing the country's foreign and security policies past 1991, notably thanks to Yevgeny Primakov (1929–2015), the first director of the Foreign Intelligence Service (1991–1995), Russian foreign minister, and then its prime minister. He formulated a doctrine that was premised on Russia being able to prevent the world from becoming unipolar, which is another way of stating that the international power had to be diluted while the North Atlantic Alliance could not expand any further. Primakov envisaged Russia's overriding goal to enfeeble Washington by all means and tools it had––and still has[1]. Like in the Cold War era, these were Russian intelligence agencies that were entrusted with a mission to put through the foreign policy by using modified active measures. Efforts like those were described in the report *Soviet Active Measures in the Post-Cold War Era 1988-1991* prepared at the request of the United States House of Representatives by the United States Information Agency in June 1992[2]. The report found that despite the collapse of the Soviet Union, active measures that involved attempts to manipulate public opinion or curb U.S. government actions by instigating opposition to its policies and interests still posed a threat to U.S. security[3]. Not only did Russia refuse to cease these operations, but refined them as information warfare saw considerable progress once based upon cutting-edge information technologies incorporated into Russian active measures. In the 1980s, Marshal Nikolai Ogarkov sparked a scientific and technical revolution in the Soviet armed forces. Along with America's tremendous success in the First Gulf War (August 2, 1990 – March 3, 1991) upon the use of modern technologies, this prepared the ground for modifying, upgrading, and introducing brand-new solutions in the army and special services[4]. In addition to a revolution that embraced science, technology, and computer sciences, a factor that accelerated both theory and practice of information warfare in Russia was the revival of geopolitics, a scientific and ideology-related base. It is about Russia's clash with the Western civilization embodied by NATO and the United States[5]. Like it was with Soviet-time methods for propaganda, disinformation, and agitation, the theory of Russian information warfare now derives from cross--disciplinary scientific research that originated back in the early 1990s. It involved a raft of institutions, facilities, and organizations. Notably, research staff comes from the army and special services[6]. The definition of "information warfare" is ambiguous and generates a lot of discussion. A comprehensive explanation of this term was provided by Colonel General Anatoliy Nogovitsyn (1952–2019), a Russian military official, the deputy chief of General Staff of the Armed Forces of the Russian Federation and the head of the Military Scientific Committee of the Russian Armed Forces[7]. Colonel General Nogovitsyn delineated information warfare as inflicting damage on information systems, processes, and resources or critically important structures and furthermore massively brainwashing troops and the population with the objective of destabilizing society and a hostile state as a whole. The top mission of information warfare is to damage both the national identity and the way of life of citizens of a hostile state. Information warfare has its ideological undertone that says its purpose is to obfuscate both philosophical and methodological premises for national cognition, sow discord, deprive the nation of its self-confidence in the future, and plant a false, moral, and economic superstructure. Information warfare has some features that set it apart from other concepts of warfare and present new challenges to its sides. They notably involve low costs for developing and using information warfare tools, an increase in the role of percep-

SOURCE: FLICKR

tion management, and growth in economic and social dependence on computer systems, which turns state information infrastructure into a new strategic goal. Posing a threat to key components of the national information infrastructure may push for action-taking processes and disturb the whole state management system[8].

Information warfare is thus tantamount to active measures. While adapting Western theories and terminology, Russians make assumptions aligned with their domestic needs. The whole procedure is designed to conceal methods and tools Soviet spy agencies had brushed up for decades, as confirmed by the authors of the study drafted under the auspices of the Foreign Intelligence Service of the Russian Federation. They argue that a handful of official terms had been coined during the Cold War at various stages to compromise intelligence agencies hostile to the Soviet Union. These notions included "operations of influence" (акции влияния), "operational disinformation" (оперативная дезинформация), "active measures" (ктивные мероприятия), "operational games" (оперативные игры), "support measures" (мероприятия содействия), or "asymmetric measures" (асимметричные действия). Notwithstanding the difference between these terms, they prompted and still prompt a whole array of actions to mislead an actual or potential adversary and elicit a favorable reaction, albeit unattainable through a repertoire of explicit methods and means[9].

Russian geopolitical doctrines outline information warfare as a tool for accomplishing goals both at home and abroad. So its role in Russian foreign policy aligns with the concept of a "protracted conflict," a notion first used by Robert Strausz-Hupé, the renowned American diplomat and geopolitical theorist when describing the Soviet/Russian strategy for forging ties with other nations[10]. Russian elites see politics as a constant struggle for power and resources, with war and peace being just separate stages of the very same process. The idea behind a "protracted conflict" consists of destroying a hostile state or making it dependent through infiltrating its top institutions––a strategy intended to win political, social, economic, and cultural influence through all existing forms of violence. The Russian approach defines these measures as an inherent part of its political domains that relies upon the process of competition, confrontation, and struggle, to which sometimes adds up an armed intervention[11]. This perception of how to frame policies is typical for Russian President Vladimir Putin and his top aides, as confirmed by the paper titled *The Image of Victory*, co-authored by Anton Vaino, who has served as the Kremlin chief of staff since August 12, 2016[12]. The Kremlin official said the top tool for fulfilling political goals is manipulative methods, or those to wield power and a way of covered psychological influence on individuals, social groups, and nations[13]. It serves as an instrument for pursuing Russian geopolitical interests:

- Preserving its zone of influence in what Russia names "near abroad" states and get their go-ahead for Moscow to manage them in line with the Kremlin's interests.
- Keeping its influence stretch between Kaliningrad and Crimea, an area that Russian military analysts believe could serve its purpose for Western countries to isolate Russia and further destabilize it.
- Neutralizing Central and Eastern Europe, detracting the United States from being a regional power, and pushing its influence out of Europe.
- Seeking to undermine the integrity of NATO and compromise the cohesion of the European Union through some bilateral deals, also between Moscow and Berlin or Moscow and Paris[14].
- Deranging Western and allied plans to fight against the Russian threat.
- Boosting Russian economic potential, also by keeping its military might in time of peace.
- Securing conditions and opportunities for the Russian Federation to influence international relations.
- Getting access to cutting-edge scientific, technological, economic, cultural, and other resources, taking the lead in scientific research into combat measures in non-war-related domains.
- Fostering conditions to allow Russia to take the reins in international projects as well as cultural, scientific, and political events[15].

Democratic elections as the purpose of information warfare according to Russian security services officials

Russian officials see democratic elections in Western countries as a socio-political event that should be used to fulfill Russian geopolitical goals. Such is a conclusion from what Russian special service officers said, describing in detail the purposes, methods, and means for exerting influence during an election campaign. Their papers are essential to discover mechanisms as they reflect the real action. Modern ways for election meddling have been on the agenda of both debates and research of Russian scholars having their roots in special services since at least the 1990s. It was first described by Sergey Rastorguev, Colonel of the Federal Security Service of the Russian Federation, or the FSB[16]. He pinpointed election interference as an instrument for pushing through the state's geopolitical goals. Rastorguev claimed that in a world whose social groups and political circles see close economic and information-related intertwines, states both keep a close eye on the struggle for power in neighboring countries and are able to influence its course through agencies and any other tools they have. A (democratic) transition in the state governance system in many places across the globe, and notably transferring tools that paved the way for power, led to the emergence of a new form of state expansion. Under its methods, elections, defined as a tool for selecting representatives in modern representative democracies, turned into an information warfare scheme. According to Rastorguev, its core purpose is to take control of states and nations by injecting into a foreign country a group of trusted people and those who back ideology and interests through information-related mechanisms for influence known as democratic elections. Only a gullible person is able to believe that a new president is elected solely by citizens while their choice has nothing to do with geopolitical reshuffles, Rastorguev says[17]. The Russian scholar adds that the vote is a battlefield where the struggle continues to win media outlets, law enforcement agencies, secret services, and electoral commissions––all of which being powerful enough to affect the outcome. It is also a strain to win the support of people who serve as role models for others and thus can create a profound impact on the result. There is a repertoire of measures targeting these people: corruption, persuasion, blackmailing, or replacing them with others[18]. Rastorguev's words matter a lot as the scholar has a reputation as the "founder and chief ideologist of the modern Russian information warfare theory." He also laid down the general principle of information warfare, saying that "proven intertwines between non-existent facts turn into the rule to determine behavior patterns of existing actors." Rastorguev also did research on neuroinformatics, the field related to neuroscience data and information processing by artificial neural networks, and cybernetics. He was in favor of a thesis about similar processes of formation, evolution, and demise in complex biological and information systems, saying there was a link between a viral infection and information warfare operations[19]. Rastorguev's theories were echoed by Andrey V. Manoylo, a former FSB colonel[20]. With what Russia has done so far, elections are an inherent component of information warfare that also includes disinformation, propaganda, lobbying, manipulation, controlled crisis, and blackmailing. Manoylo argues that using election campaigns to achieve political or any other goals is now typical for the harsh reality. The official says the mass use of media outlets and other means for electoral interfering exerts a bigger impact on human consciousness and subconsciousness[21].

In their papers, Russian scholars provided an overview of both methods for manipulating society, but also candidates and political parties involved in election campaigns. Russian sources named them as **"dirty election technologies,"** used to meddle in election campaigns both at home and abroad. Col. Manoylo classified them as follows:

- "polishing the reputation of a candidate" (лакировка имиджа кандидата), or attributing features to the candidate that they do not actually have.
- "unachievable dreams" (несбыточные мечты), or giving unfulfillable election promises.
- "doubles" (дублеры), defined as registering doubles for a candidate, tasked with "distracting" voters' attention from any negative features of the frontrunner.
- "political decoys" (двойники), or people employed to register to the election as they have the same names as other candidates to deceive voters and increase the chance of winning of a dissimilar candidate.
- "compromising material" (компромат), the most frequently used methods for influencing the candidate and its voters.
- bribery (подкуп), or corrupting voters, electoral clerks, judges, journalists, and election staff members.
- "smear campaigning" (юридические ловушки), or intentional, premeditated effort to undermine an individual's legal conduct by instigating complaints pursuant to the election code from "institutions" or "third parties" to

SOURCE: FLICKR / GILBERT MERCIER

compromise the candidate and their staff members.

- "candidate against all" (кандидат против всех), a repertoire of actions to create negative publicity of elections or make citizens cast invalid ballots. The purpose is to undermine the legitimacy of elections.

- "ballot day" (день голосования), or a series of complex activities, coordinated in time and place, to breach the voting procedure, by impersonating a political force or a party[22].

Col. Sergey Mironenko is another official to observe the growing importance of election in information warfare[23]. He sees the election campaign as an "information conflict." While studying U.S. electoral campaigns, he outlined a list of factors that weighed much on the presidential race and its outcome. They look as follows: 1) did its frontrunner stand against a fierce rival in the primaries? 2) was there any social agitation when the party that nominated its candidate was still in power? 3) did the country suffer from any economic crisis and recession in the election year? 4) has the incumbent president made any major political shifts? 5) are there political groups other than the Republican and Democratic Party that marked their activity throughout the election year?[24] Reliable answers to Questions 1, 2, and 5 alongside comprehensive analyses are essential for Mironenko to forecast election campaigns and the vote in the United States and predict the winner depends on the syndrome of political instability that encompasses competition within the ruling party, social unrest, and the force of extra opposition groups. And for its part, offering an insight into Questions 3 and 4 helps make a forecast of whether major presidential decisions can mitigate any negative consequences of the economic crisis[25]. Analysis from Col. Mironenko shows that election campaigns could be an efficient factor to shake the country's domestic situation. In doing so, it is vital to spark and then nurture disputes in the ruling party, back opposition forces, notably its non-parliamentary groups, but also alternative social, grassroots, and extremist movements, or inflame conflicts and uproar. Yet not even the most elaborated strategy guarantees victory in an information warfare operation targeting elections. Col. Rastorguev claims that information warfare is mostly a creative process that involves the most experienced and talented staff[26] and intelligence composed of the following parts:

Fig. 1. Intelligence model and its task features

Analytical section	forecasting and predicting events and their course (situation models) and staging information and psychological operations targeting candidates and voters at the strategic, operational, and tactical levels
Intelligence section	collecting intelligence on any objects of information influence through operational and reconnaissance methods
Information processing section	staging information to then use it in PR-related projects and launch information and psychological operations (articles, books, brochures, leaflets, memes, information inserts, etc.)
Executive section	preparing the ground for the channels of communication to reach the audience and target groups. Its task is also to categorize voters by ethnicity, social class, and others and to collect intelligence on media outlets to either acquire it or use it to transmit any desired content
Statistical section	surveying audience and target groups to categorize voters by their behavior based on information collected from various sourcesg

Source: author's own study based on С.П. Расторгуев, Философия информационной войны, Москва 2003, p. 358.

In its report *NATO 2030. United for a New Era* (November 25, 2020), a paper drafted at the request of NATO Secretary General Jens Stoltenberg, scholars noted that "campaigns to undermine faith in democratic institutions in the Alliance," understood as election meddling, are a threat to NATO members and the whole bloc, imperiling its stability and cohesion[27]. It has been confirmed by the research of Dov H. Levin, a British political scientist, who found that 74 percent of Russian electoral interference between January 1, 1946, and December 31, 2000, took place in NATO countries, which was and still is the main adversary of the Soviet Union/ the Russian Federation[28]. It seems that Russia ramped up efforts to intervene in elections in the 21st century, a conclusion that came from an investigation by USA Today News journalists, published on September 7, 2017. They made public a study by the Alliance for Securing Democracy (ASD), a bipartisan national security advocacy group un primarily by former senior United States intelligence and State Department officials. It said Russia had allegedly meddled in elections in as many as 27 countries worldwide (sic!) since 2004. These included Belarus, Bulgaria, Canada, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Hungary, Italy, Latvia, Lithuania, Macedonia, Moldova, Montenegro, Norway, Poland (the report contained no mention on the nature of alleged interference), Portugal, Spain, Sweden, Turkey, United Kingdom, Ukraine, and the United States. U.S. pundits say the first known attempts to intervene in elections occurred in Estonia, Georgia, and Lithuania. Operations in these countries ended in success, which meant that Russia slowly stretched its influence also to Western nations[29]. Reports from the European Platform for Democratic Elections found that between 2018 and 2020 Russia made efforts to intervene in elections in post-Soviet regions and nations (Azerbaijan, Abkhazia, South Ossetia), the Kingdom of Cambodia, and five African states: the Republic of Madagascar, the Democratic Republic of Congo, the Republic of Zimbabwe, South Africa, and the Republic of Mozambique[30]. In a nutshell, Russian pursuits to compromise democratic institutions, foster a sense of chaos in the countries above, and make way for Moscow-friendly officials and parties that now reach worldwide.

Russian methods for interfering in U.S. presidential elections

On January 6, 2017, the U.S. Intelligence Community released a joint assessment titled *Assessing Russian Activities and Intentions in Recent U.S. Elections* that stated that Russian President Vladimir Putin had ordered an influence campaign in 2016 aimed at the U.S. presidential election. It also assessed that the General Staff Main Intelligence Directorate or the GRU, Russian institutions, and propaganda machine, had run the Putin-ordered campaign[31]. Russian meddling in the U.S. elections, thus in its social and political life, involved an array of active measures, with cyberspace operation on top of that. In both its theory and practice, Russian information warfare affected the U.S. election process through two intertwined operations of intelligence agencies and related entities, taking place at the strategic, operational, and tactical levels. Below is the list of activities.

Information operation (информационная операция - **ИО)**

It encompasses a raft of joint and coordinated activities that take into account the purpose, place, time, and operative methods as well as run smoothly to win and keep an information advantage over the other party. It is possible to secure this advantage by penetrating resources and systems (infrastructure, networks, communications technologies, and societies of countries involved in the conflict) of the adversary while protecting own information systems and resources[32]. An information operation may be designed to illegally access information resources of the adversary by using software and hardware solutions to infiltrate adequate systems, collect intelligence by hacking, intercepting, or decrypting information through specially-designed devices (electronic intelligence), damage or compromise these systems, and deprive the enemy of access to some components of information infrastructure[33]. Contemporary elections are yet no free from cyber threats, including cyber attacks and failure, that may occur as voting preparations entail a whole range of new technologies. General elections make a fundamental contribution to democratic governance thus any threats they are exposed to shall be classified as fundamental[34]. One example consisted of Russian attempts to infiltrate U.S. election infrastructure in the run-up to the 58th United States presidential vote that took place on November 8, 2016. The term “election infrastructure” means information and communications technology and systems used by or on behalf of the Federal Government or a state or local government in managing the election process, including voter registration databases, voting machines, voting tabulation equipment, and equipment for the secure transmission of election results[35]. The first part of the report drafted by the U.S. Senate Intelligence Committee on Russian interference in the U.S. elections in 2016 said the Russian military intelligence, in short GRU, made attempts to penetrate and access election infrastructure in all 50 states between 2014 and 2017. The authors of the paper determined that internet-connected election-related networks in 21 states were potentially targeted by Russian government cyber actors In June 2016, Illinois experienced the first known breach by Russian actors of state election infrastructure during the election. Illinois election clerks discovered anomalous network activity, specifically a large increase in outbound data, on an Illinois Board of Elections' voter registry website. An FBI investigation found that through an SQL injection attack, hackers accessed up to 200,000 exfiltrated records that included information on each voter's name, address, partial social security number, date of birth, and either a driver's license or other identification documents. The intruders could create, penetrate, update, modify, or delete records stored in databases. Nonetheless, the report mentioned no details on where the hackers got intelligence from and what they could possibly use it for. Russian hackers had both tools and capabilities to alter the electoral register yet the Committee found no evidence to suggest this really had happened. Russia may have been probing vulnerabilities in voting systems to exploit later, said the report. One possibility is that Russia's deliberate intention was to expose its activities to make U.S. society doubt whether the electoral process was legitimate or not[36]. Yet there are many ways for state and non-state actors to exert influence on elections by interfering in election infrastructure. It is possible to disrupt voting by preventing citizens from using electronic voting booths or destroying the electoral register. Polling booths could be infected with malware that counts the vote for one candidate as cast on the other. Another risk is that ballots in a polling booth are intercepted and modified, a move that reshuffles the result, also remotely, as was the case in Ukraine. A report from the Australian Strategic Policy Institute found that foreign election interference was identified in Colombia, Finland, Indonesia, North Macedonia, Ukraine, and the United States. The attackers identified in unclassified reports were Russia (in one instance, combined with Venezuela) and China. Russia was by far the dominant actor, according to the authors of the report[37]. Notwithstanding that, the report on foreign threats to the 2020 U.S. federal election by the U.S. National Intelligence Council on March 15, 2021, stated that there was no indication that Russia attempted to alter any technical aspect of the voting process or gain access to election infrastructure. The assessment further noted that this was possible as state and local officials helped thwart these pursuits and the Russian Federation shifted its strategy that encompassed a raft of activities to elevate the scope of information and psychological campaigns[38]. Like in the time of the Cold War, Russia staged an operation that involved compromising material (компромат), or damaging information to create negative publicity of a candidate or its political party to influence voters. One example is that the Russian military intelligence agency broke into the computer system of the National Democrat Committee and hacked 20,000 emails that Wikileaks then released. Some of the emails disparaged Clinton's rival, Senator Bernie Sanders. Disclosing emails sought to sow discord in the Democratic Party. Russia hacked into Republican state political campaigns and email accounts belonging to Trump's campaign staff. They yet did not make them public as FBI former director James Comey told the Senate Intelligence Committee that the Republican emails were better secured[39]. In 2019, Russian military hackers successfully infiltrated the Ukrainian gas company Burisma; they could be searching for potentially embarrassing material on the Bidens in the run-up to the 2020 elections. Interestingly, there is a resemblance between the Burisma hacking scandal and the Hillary Clinton email controversy in 2016. Conspirators who worked for the GRU then sent spear phishing emails to the work accounts of Clinton campaign employees to steal passwords and penetrate the computer system[40].

Information and psychological operation (информационно-психологическая операция – ИПО)

Dmitri Trenin, a former colonel of Russian military intelligence and the director of the Moscow Carnegie Center[41], spoke of U.S.-Russia ties before the 2020 election, saying that the Russian way towards the United States comes from its leaders that are aware of its country's weak spots once confronted with Washington.

Trenin said Russian activities are both deliberate and asymmetric so in the past five years Washington has made failed attempts to push Moscow onto a foreign policy path it would like to see it[42]. "Our political culture bears more Asian traits than European," Trenin says, "and there is nothing wrong with it. No one should feel ashamed of their parents: a Tatar father and a Byzantium mother[43]." Russian military officials say any country disposing of cutting-edge information technologies and a developed information structure is in a better position than its adversary. But when it is impossible to win this advantage, asymmetric measures should come forth, through any means to form social awareness to exert influence on what people and groups[44] do. Thus information and psychological operation serve a particular role in the Russian theory of information warfare and related activities. They are methods for forming and practicing combinations of measures to alter the view of the world as stored by many individuals, groups, or whole communities[45]. The view of the world (картина мира) offers visual, acoustic, and emotional reflection of the world where an individual has its proper place and holds links to reality. Once modified, these views form beliefs and values. The core components of this idea are a world perception, worldview, and attitude[46]. Colonel Manoilo says the top purpose of information and psychological operations is to "divide and polarize society, tear it into shreds, and make each truly hate the other." "Then someone must turn them against each other and instigate a struggle for self-destruction or blend their aggression into one to make hostile to the legitimate government,"[47] he added. Methods for staging and carrying out these operations date back to the 1960s KGB-elaborated idea of reflexive management that allows one side to use the resources of its adversary to the fullest. Reflexive management, or adjusting views of the world or the human, refers to insidious and illusion-related activities such as provocation, schemes, camouflage, or disinformation. In short, according to this concept, parties to any conflict while making decisions rely on both reality and pictures of the external world they have rooted in their minds. The term reflection (from Latin *reflexio*) means that the reasoning of the opponent has its reflection in the mind of a conflicting party. Reflexive management is thus referred to as the process of communicating the basis for decision-making from one party to the conflict to the other. The core is what is known as a package of information, defined as a string of prompts that affect both the perception and drive of the influenced object while preserving continuous messages, full compliance with the profiled model, individual cognitive patterns, and situation. What makes this method special is that it nurtures a false motivation that does not rely on human intuition, but a peculiar model remaining under a watchful eye of the subject. Whether reflexive management is successful or not hinges on the method of profiling used for that purpose. Psychological models based on traditional, behavioral, or even psychoanalytic concepts proved little efficient. The thing is that the subject model should reflect both its behavior patterns and their ability to understand themselves and others, also those seeking to take control of their actions, thus the model should be reflexive. Influencing an information system of the adversary through reflexive management methods helps elicit a set of desired reactions[48]. Both modern information technologies and social media boost the efficiency of reflexive management. There is a close intertwine between reflection and the virtual world. A social media user integrates with a world––virtual and subjective––that emerges through the flow of information reflecting specific and real events or such situations as elaborated by specially trained employees in accordance by Rastorguev's principle that "proven intertwines between non-existent facts turns into the rule to determine behavior patterns of existing actors." Thus, through such a tool as social media it is possible to induce some reactions from their users, also by staging rallies against the country's

SOURCE: FLICKR

military and political leaders. A notably helpful method is to use reflexive management schemes against individual users or small groups by hitting them with what is known as a targeted information impact, a technique that paves the way for generating hostile actions and then control them. So individuals being under psychological scrutiny have no clue that they are being exposed to manipulative procedures. Through reflexive management methods in social media, it is also possible to foster the activities of agents of influence. This happens through modifying beliefs and stereotypes that exert influence on behavior patterns to authenticate some activities of organizations, associations, groups, or influential persons. This paves the way for agents of influence who get access to social and organizational resources[49].

Interestingly, in January 2012, the Russian Foreign Intelligence Service opened three classified bids for research projects to perform intelligence-related tasks in Internet centers and regional social networking sites, covertly control Internet content, and form means for distributing information in social networks. The SVR said the bids won by ITERANET––a Russian service integrator in communications and computer technologies, whose former CEO is Igor Matskevich, former head of the Institute of Cryptography, Communication, and Informatics by the Academy of Federal Security Service of Russian Federation ––were for the project to "develop software to automatically disseminate information in large social networks and set up methods of organizing and managing virtual Internet communities of experts and creates tasks with workflow. The virtual army would be tasked with disseminating information in some social networks through existing user accounts to influence public opinion, collect statistics and analyze the efficiency of information sharing and measure how popular the information eventually becomes"[50].

Reflexive management was also employed in social media to stage an information and psychological operation to target U.S. voters in a campaign run by the Internet Research Agency (Агентство интернет-исследований). It is a St Petersburg-based agency whose leader is Yevgeny Prigozhin, a Russian oligarch dubbed "chef" to Vladimir Putin as he has in the past supplied food to Russia's senior officials and built an empire on catering and maintenance contracts for the army as well as Moscow schools and hospitals, which allegedly gave him money to run the Internet Research Agency[51]. Published on August 14, 2020, a long-running investigation by Bellingcat, The Insider, and Der Spiegel has uncovered that Yevgeny Prigozhin's operations were "tightly integrated with Russia's Defense Ministry and its intelligence, the GRU[52]." Another fact in favor of Prigozhin's strong position in the Russian power structures is that any institutions having links to them managed to gain dominance over the criminal market of Russia's internal political violence, earlier controlled, albeit unofficially, by the FSB and the Ministry of Internal Affairs, including the Centre for Combating Extremism, known also as Centre "E", and the Operational-Search Directorate[53]. Perhaps the Internet Research Agency serves a similar purpose as front groups did during the Cold War and offers its services or covers information and psychological operations that the Russian military intelligence agency performs to target NATO and EU nations.

Both Russian theoretical and practical studies on information warfare and empirical data in U.S. government reports and papers are enough to give an insight into the unfolding and effects of an information and psychological operation targeting U.S. voters. Efforts to stage and then perform the operation runs under the same logical schemes as the Internet Research Agency. It is as follows:

1. Political stratification of society is the extent to which such inequalities are encapsulated to split a coherent society into segments, factions, and groups. Russian information warfare theorists define a social segment as a unified group of citizens who act politically and socially upon their strictly defined political beliefs and views while seeking to enforce their rights and freedoms either jointly with other sides of the political process or independently of them. As the process of political stratification takes place in society, no means for penetrating collective consciousness apply yet. Stratification was intended to select target groups and either forge new or use already existing channels of communication to transmit the message[54]. Col. Vladimir Krysko says that this stage involves the study into the subject of psychological warfare (operation), or a lengthy and complex process of gathering and processing intelligence on the adversary: their mentality, habits, norms, and values[55]. An intelligence group made what it turned out to be a reconnaissance tour across the United States (June 4–26, 2014). Among them were two Russian Internet Research Agency operatives, Anna Bogacheva and Alexandra Krylova, who had the mission to gather intelligence for information warfare purposes. The women traveled to southern states to grasp U.S. political and social divisions. They stayed in Nevada, California, New Mexico, Colorado, Illinois, Michigan, Louisiana, Texas, and New York. The women claimed to be U.S. nationals to forge contacts with social and political activists. They managed to gather very valuable intelligence: to efficiently influence elections in another country, the Internet Research Agency had to center on what is known as "purple," or "battleground" states, where both Democratic and Republican candidates receive strong support without an overwhelming majority of support for either party. At that time these were Colorado, Virginia, and Florida[56]. Naturally, these efforts came as just one chunk of a large intelligence mission to identify features of U.S. social media. Russian operatives classified U.S. society by ideology, ethnicity, and race. They first divided it into the African American community and White Anglo-Saxon Protestant, or WASP, the latter of which was then split into liberals and conservatives. There were also separate target groups containing the Hispanic population, Muslim Americans, and the LGBT community. Thus Internet Research Agency employees, or "specialists," could create fake accounts or impersonate U.S. citizens and institutions, build whole necessary infrastructure (websites or social media groups) to launch information and psychological operations online. The Russian-based agency sought to attract a U.S.

audience by buying sponsored ads and propagating sensitive political and social content. Interestingly, Internet Research Agency operatives were told to instigate political tension by offering aid to extremist groups, disappointed with the U.S. political situation, and opposing social movements, which Colonel Mironenko named as the features of sowing political instability[57]. The aim was to stir up ethnic, religious, and ideological rows to destabilize the United States internally so as to put through a soft or color information warfare scenario[58]. The operation reached far, encompassing many types of social networking sites, including the following reports from Facebook. The U.S. Senate Intelligence Committee found that the Internet Research Agency bought 3,393 ads−−while a total of 3,519 were published−−seen by 11.4 million U.S. nationals. Internet Research Agency employees generated 470 Facebook pages whose content, or some 80,000 posts, reached 126 million people in the United States[59].

2. Political polarisation of social factions (groups) of key strategic importance for the operation. To transform segments, groups, and factions emerged as part of the stratification process into an obedient tool for accomplishing the goals of information and psychological operation, it is vital to form a system of political norms favorable to the belligerent party. It is known as a political imperative. Framing such a system occurs through exerting an influence on a social class or group by employing ideological patterns as developed by a center tasked with information and psychological operations. Here the purpose is not to smash these groups or cripple them−−as the very term "polarization" suggests−−but to put them together to act efficiently. The next stage is to morph them into destabilizing units, or "fomenting groups," that are easily provoked into subversive activities[60]. Russian perpetrators addressed targeted segments:

African Americans. Russian narrative had the task to undermine their trust in state institutions and democracy as a whole. It orbited around the anger of African Americans against structural and economic inequalities. The Russian agency brought to the focus issues such as police brutality, poverty, unemployment, and no access to schooling. The campaigns eventually carried the conviction that the best way to improve lives of the African Americans is to boycott the vote and focus on other issues.

Conservative and right-wing voters. Here the purpose was to encourage conservative U.S. voters to cast their ballot for Donald Trump and spark outrage by disseminating posts containing negative assessment from foreigners who position got better at the expense of U.S. citizens. The Russian-devised narrative sought to strike at national minorities, notably Muslim and African American population (also by labeling a person wearing burka with the slogan: "who is behind that mask? A man? A woman? A terrorist?" or by propagating the image of Muslims as terrorists and sexual deviants). Furthermore, propaganda messages targeted also groups in favor of carrying guns and nationalist milieux, notably Texas secessionists and southerners. They also disseminated reports on the alleged bad treatment of veterans and policemen by the Obama administration while reportedly refugees were treated better back then.

LGBT communities and liberal voters. The main goal of this narrative was to incite the dispute between LGBT communities and those having a negative attitude to them (religious groups, conservative and right-wing voters). As was the case of African Americans, efforts were made to undermine their trust in the political system, allegedly intolerant and oppressive. The Russian agency employed LGBT circles as a "fomenting group," looking to deepen chasms between liberal and conservative voters by claiming political rights for sexual minorities.

Hispanic voters. Russia used the same mechanism for African Americans and LGBT communities, trying to erode trust in the U.S.

political system while insisting on sensitive themes such as discrimination, deportation, or federal health care. Moreover, efforts were made to incite nationalist moods to easily antagonize Hispanic voters and other national and ethnic minorities.

Muslim population. The Internet Research Agency tended to promote a positive narrative on Islam and the Muslim population as a whole. On the one hand, it praised Muslims for their being attached to traditions and sympathy towards victims of terrorist attacks while on the other, it diffused stories on that Muslim population disbelieved in the U.S. government, notably its intentions and foreign policy. A possible interpretation of this narrative was to depict the Muslim community as volatile[61].

3. Initiate political activities of factions (community groups) in accordance with the role assigned to them in the operations plan. At this point operatives exert an informational influence on a target group through an external center tasked with information and psychological missions. This is to elicit a response from the segment, group, or faction to make them react in line with the political imperative. At this stage of the information and psychological operation activities are transferred from the virtual world to reality. What seems to corroborate the thesis on the stirring up of racial, ethnic, and religious conflict and destabilizing the U.S. internal situation is that the Internet Research Agency resorted to social media pages to convene a couple of political rallies throughout the country between June and November 2016. Russian-staged flash mob rallies attracted both supporters and opponents of Donald Trump and Hillary Clinton, an attempt to spark a confrontation between the two feuding political camps[62]. Here are a few examples. On May 21, 2016, a Russian--sponsored group "Heart of Texas" advertised a "Stop Islamification of Texas" rally outside a new library at the Islamic Da'wah Center, a move that sparked a harsh response from members of the Muslim population who arrived at the site to take part in a "Save Islamic Knowledge" rally for the same place and time, staged by a separate Russian group. A dozens or so people attended the meeting, carrying weapons, Souther Cross flags, and White Life banners. "Heart of Texas" administrators encouraged people to bring guns to the gathering[63]. On May 25, 2016, Westboro Baptist Church, a fundamentalist church infamous for its harsh anti-gay rhetoric, held a rally at the graduation ceremony at the Lawrence Free State High School, Kansas. A group named LGBT United made a counter manifestation through a Facebook ad. The Agency created the account just for that purpose, paying $50 for the ad that got roughly 4,800 hits. It targeted Kansas residents aged 14 to 65, mainly those advocating for LGBT rights and supported Bernie Sanders and Hillary Clinton[64]. Protestors marched in Dallas on July 10, 2016, as part of the Black Lives Matter movement. The response was a Blue Lives Matter countermovement, staged by the agency--controlled group Heart of Texas[65]. On November 12, 2016, some 5,000 to 10,000 protesters marched down New York streets in a rally "Trump is NOT my President." Behind the march was BlackMattersUS[66].

4. A controlled chain reaction is defined as an activity of a social group that an aggressor seeks to elicit, stimulated through a new batch of information-related stimuli to stir up tensions and fuel social conflicts.

5. Revising the initial plan for a information and psychological scheme served as feedback to the operation scenario that assesses whether the operation deems efficient––by comparing its actual outcomes with earlier expectations––and adding up some adjustments[67]. Although the Kremlin's attempts to interfere in the U.S. presidential elections, Russian officials did not order to complete the information and psychological operation. In 2018 materials gathered by David Holt, an FBI agent, that helped indict a Russian woman were made public. In 2017, thus shortly

SOURCE: FLICKR / ELVERT BARNES

after the U.S. election, the operation was going under way, according to the document. Instead, it was revised and feedback was given. It has been confirmed by some snippets from guidelines for Russian Internet trolls that involve both remarks and details recorded while the operation was at its stage one to amplify Russian efforts[68].

Similar operations were run by outfits having links to Russian intelligence outlets in the run-up to the U.S. presidential elections on November 3, 2020. Back then journalists wrote, citing American intelligence operatives, that Russia had not ceased these operations, but brushed them up significantly. On March 12, 2020, The New York Times printed a detailed article outlining the role of the Russian intelligence services and its media outlets in stoking racial tensions ahead of the November's presidential elections. The journalists noted that the Russian Foreign Intelligence Service amplified its mission compared to the 2016 U.S. election campaign. Back then its operatives inflamed racial tensions through a bunch of false Black Lives Matter accounts and efforts to deter black Americans from voting. In 2020, The Russian government has stepped up endeavors to ignite racial tensions in the United States, also trying to incite violence by white supremacist groups and to aggressively spread hate messages. Furthermore, federal investigators were examining how a neo-Nazi organization with ties to Russia was funded[69]. The operation involved also facilities linked to Yevgeny Prigozhin and what is known as the Lakhta Project. The Internet Research Agency outsourced its activities in July 2019 to Akra, Ghana, through the Eliminating Barriers for the Liberation of Africa (EBLA), to continue to stoke racial, political, and religious splits among Americans. The new outfit somewhat mirrored tasks of the Internet Research Agency; it set up a number of fake social media accounts that allegedly impersonated U.S. nationals and institutions to promote content inciting political tensions in the United States[70].

Similar missions date back to the Cold War when Communist intelligence outfits dispatched a slew of their operatives to African countries. The officers occupied an intermediary role in disseminating Moscow-made disinformation to hit the United States, West Germany, and the United Kingdom. Their African whereabouts were helpful to shadow their true intentions[71]. Social networking sites are now a substitute for agents of influence. A new feature that Russians used in the run-up to the 2020 presidential elections was attempts to take the reins in emerging conspiracy movements such as QAnon. In 2019, accounts that Twitter had deleted amid suspected their link to the Russian Internet Agency generated a glut of posts tagged #QAnon. Furthermore, Kremlin-linked white propaganda outfits such as RT or Sputnik kept adding new stories on QAnon, beginning with a fake report on arresting Hillary Clinton for an unknown reason and alleged Hollywood-based child sex trafficking ring or the Covid-19 pandemic. Cindy Otis, a former CIA analyst who is now the vice president for analysis for Alethea Group, said that RT, Sputnik, and other Kremlin-endorsed outlets produce more posts on the QAnon conspiracy theory to use it to back up its top narrative as the United States allegedly fell apart amid its abundant internal splits[72].

Conclusions

Recent findings show that Russian content is particularly effective at achieving its goal of generating strong reactions along partisan lines[73]. In addition to compromise trust in the American democratic system, Russian interference in the U.S. sought to destabilize the country by stoking racial, ethnic, religious, and national animosities to sow chaos and enfeeble the United States worldwide. Through this Russia could go ahead with its geopolitical pursuits: push the United States out of Europe, seek to undermine the integrity of NATO, and compromise the cohesion of the European Union to neutralize Central and Eastern European nations.

It is possible to detect Russian intervention––if not immediately, then often after an incident. Nonetheless, there are far more subtle ways to intervene in democracies. Bringing into focus solely how these cyber attacks occurred leaves out other actions––traditional and far more perilous––such as foreign contributions to political parties, nourishing political influence, or infiltrating top fields and democratic institutions, as outlined in the first part of this report.

As this report sees some volume-related limitations, it provided an insight into the most important instances of Russian information and psychological operations against U.S. democracy.

Przypisy końcowe

[1] A. Grajewski, Tarcza i miecz. Rosyjskie służby specjalne 1991 – 1998, Warsaw: 1998, p. 223, J. Darczewska, P. Żochowski, Active Measures. Russia's Key Export, Warsaw: 2017, pp. 32–37.

[2] F. Schoen, Ch.J. Lamb, Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference, Washington 2012, p. 96.

[3] Soviet Active Measures in the "Post-Cold War" Era 1988-1991. A Report Prepared at the Request of the United States House of Representatives Committee on Appropriations by the United States Information Agency June 1992, http://intellit.muskingum.edu/russia_folder/pcw_era/exec_sum.htm [Accessed on March 23, 2021].

[4] В.И. Ковалёв, Ю.А. Матвиенко, «Сетецентрическая» война как новая парадигма вооружённой борьбы, „Информационные войны" 2013, No. 2, p. 5; D.R. Herspring, Nikolay Ogarkov and the Scientific–Technical Revolution in Soviet Military Affairs, „Comparative Strategy" 1987, No. 6, pp. 29–59; A. Campen, First Information War: The Story of Communications, Computers and Intelligence Systems in the Persian Gulf War, Arlington 1992.

[5] J. Darczewska, Anatomia rosyjskiej wojny informacyjnej. Operacja krymska – studium przypadku, Warsaw: 2014, pp. 13–15; T.L. Thomas, Russia's Information Warfare Structure: Understanding the Roles of the Security Council, FAPSI, the State Technical Commission and the Military, „European Security" 1998, No. 7, pp. 156–172; S. Blank, Russian Information Warfare as Domestic Counterinsurgency, „American Foreign Policy Interests: The Journal of the National Committee on American Foreign Policy" 2013, No. 35, pp. 21–44; G.L. Tulchinsky, Information Wars as a Conflict of Interpretations: Activating the 'Third Party', „Russian Journal of Communication" 2013, No. 5, pp. 244–251.

[6] В.П. Шерстюк, О развитии в МГУ научных исследований и учебного процесса в области информационной безопасности, w: Научные и методологические проблемы информационной безопасности (сборник статей), В.П. Шерстюк (red.), Москва 2004, pp. 37–47, read more: Г.Г. Почепцов, Информационная война-2013 в представлениях российских экспертов [online], http://psyfactor.org/psyops/infowar24.htm [Accessed on: March 23, 2021], K. Kraj, Rosyjska wspólnota organów bezpieczeństwa, Kraków –Wrocław 2017, pp. 59–60.

[7] Ноговицын Анатолий Алексеевич, http://viperson.ru/people/nogovitsyn-anatoliy-alekseevich [Accessed on: March 23, 2021].

[8] А.А. Ноговицын, В центре внимания – информационная безопасность, „Красная звезда" 2009, No. 34, p. 1.

[9] История российской внешней разведки. Том 2. 1917-1933 годы, Е. Примаков (ed.), Москва 2014, p. 13. Cf. T.L. Thomas, The Russian Understanding of Information Operations and Information Warfare, In: Volume III of Information Age Anthology: The Information Age Military, D.S. Alberts, D.S. Papp (ed.), Washington 2001, p. 783, J. Darczewska, Diabeł tkwi w szczegółach. Wojna informacyjna w świetle doktryny wojennej Rosji, Warsaw: 2015, pp. 14–15.

[10] United States. Senate. Committee on Un-American Activities. House of Representatives. Eighty-Fifth Congress, Second Session, May 1958. Communist Strategy of Protracted Conflict. Consultation with Dr. Robert Strausz-Hupé, Mr. Alvin J. Cottrell, Mr. James E. Dougherty, Washington 1958, pp. 1-5.

[11] M. Wojnowski, Paradygmat wojny i pokoju. Rola i znaczenie materializmu dialektycznego w rosyjskiej nauce wojskowej w XXI w. „Przegląd Bezpieczeństwa Wewnętrznego" 2017, No. 17, pp. 41–43.

[12] Антон Эдуардович Вайно, http://kremlin.ru/catalog/persons/307/biography, [Accessed on: March 23, 2021], Кто такой Антон Вайно, новый глава Администрации президента России? https://www.currenttime.tv/a/vaino/27916751.html [Accessed on: March 23, 2021].

[13] А.Э. Вайно, А.А. Кобяков, В.Н, Сараев, Образ Победы, Москва 2012, pp. 36–38; Cf. А.Э. Вайно, АА Кобяков, ВН Сараев, Глобальная неопределенность, „Экономические науки" 2011, No. 8, pp. 33–40.

[14] R.S. Cohen, A. Radin, Russia's Hostile Measures in Europe. Understanding the Threat, Santa Monica 2019, p. 10.

[15] Е.А. Дербин, О совершенствовании стратегического руководства обороной России, „Вестник Академии военных наук" 2019, No. 2, pp. 48–49.

[16] Sergey Rastorguev (1958 - 2017) is a doctor of technical sciences, professor, colonel of the Federal Security Service, former deputy head of the Scientific and Research Institute of Information Technologies of the FSB (Scientific and Technical Service of the FSB), see Расторгуев Сергей Павлович, https://www.mosgu.ru/about/otkrytaya-kafedra/, [Accessed on: March 23, 2021], Структура ФСБ: Центральный аппарат, http://agentura.ru/dossier/russia/fsb/structure, [Accessed on: March 23, 2021].

[17] С.П. Расторгуев, Философия информационной войны, Москва 2003, p. 340.

[18] Ibidem, p. 358. In Russian information warfare theory, the information field is the interaction of actors such as legal or natural persons, including government agencies, media, etc., see: С.Н. Бухарин, В.И. Ковалев, С.Ю. Малков, О формализации понятия информационного поля, „Информационные войны" 2009, No. 4(12), p. 4.

[19] Read more about Rastorguyev's scientific and research activity: С. Гриняев, Памяти выдающегося российского ученого, Сергея Павловича Расторгуева, http://csef.ru/ru/oborona-i-bezopasnost/265/pamyati-vydayushhegosya-rossijskogo-uchenogo-sergeya-pavlovicha-rastorgueva-7778, [Accessed on March 23, 2021].

[20] Andrey Manoylo (October 14, 1975) is a former colonel of the FSB, professor of political science at the Moscow State University, and a former member (2011–2018) of the Scientific Committee of the Rus-

sian Security Council. Manoilo advises on information and psychological operation to BRICS and the Shanghai Cooperation Organization. In 1998 he began his service in the FSB, a year later he graduated from the FSB Executive Staff Preparation Course at the FSB Academy in Moscow, during which he trained in the specialty of operational activity. From 1999 to 2002 he was seconded to carry out service assignments (information-analytical work) in the Russian embassies in Denmark and Norway, and later in the Middle East and Latin America. Since 2012 he has been working at Moscow State University as a lecturer in political science. His area of scientific interest includes such areas as Russian foreign policy, international relations, information warfare, notably civilization and cultural factors, psychological operations, and "color revolutions." He now chairs the Association of Information Operations Specialists. He also created a website vbrosam.net to combat fake news, see: Андрей Викторович Манойло, https://evartist.narod.ru/text24/0022.htm, [Accessed on: March 23, 2021]., Андрей Викторович Манойло, https://myrotvorets.center/criminal/manojlo-andrej-viktorovich/, [Accessed on: March 23, 2021].

[21] А.В. Манойло, А.И., Петренко, Д.Б. Фролов, Государственная информационная политика в условиях информационно-психологической войны, Москва 2012, p. 326.

[22] А.В. Манойло, А.И., Петренко, Д.Б. Фролов, Государственная информационная политика…, pp. 327, 402. Cf. А.А. Максимов, Чистые и грязные технологии выборов в Россий, Москва 1999, pp. 176–179.

[23] Sergei Vladimirovich Mironenko – Reserve Colonel, intelligence officer, an electronics engineer and economist, holder of the doctor's degree in history, speaks English and Chinese. Member of the Association of the Study of the History of Homeland Secret Services in Moscow, a member of the editorial board of the newspaper Самарские Чекисты. After completing education at the KGB's Yuri Andropov Red Banner Institute (Academy of Foreign Intelligence), he stayed in southeastern Asia where he worked as an officer at the First Chief Directorate of the KGB responsible for foreign intelligence missions. In February 1982 he was expelled from Singapore for intelligence activities. Already as a Ph.D. holder, he served as a lecturer on intelligence and counterintelligence at the Yuri Andropov Red Banner Institute. He retired as an army colonel. He is a researcher and journalist interested in cognitive aspects of social awareness, election campaigns, and Soviet-Japanese intelligence competition in the 20th century, see: K. Kraj, Interview with Colonel Dr. Sergey Vladimirovich Mironenko, Retired Officer of Soviet and Russian Civilian Intelligence, "E–Terroryzm" 2017, No. 1 (56), pp. 6-7, Мироненко С.В. - 70! "Самарские чекисты" 2017, No. 9, p. 3.

[24] С.В. Мироненко, Понятие «Безопасность избирательной кампании», „Вестник Самарского государственного аэрокосмического университета" 2004, No. 2, p. 29.

[25] Ibidem, p. 29, А. Горбань, Нейроинформатика и ее приложения, „Открытые системы" 1998, No. 4–5, pp. 37–41.

[26] С.П. Расторгуев, Философия информационной войны…, pp. 358.

[27] NATO 2030. United for a New Era. Analysis and Recommendations of the Reflection Group Appointed by the NATO Secretary General, https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf., p. 26, [Accessed on: March 23, 2021]

[28] D.H. Levin, Levin, Meddling in the Ballot Box. The Causes and Effects of Partisan Electoral Interventions, Oxford 2020, p. 155.

[29] O. Dorel, Alleged Russian Political Meddling Documented in 27 Countries since 2004, https://eu.usatoday.com/story/news/world/2017/09/07/alleged-russian-political-meddling-documented-27-countries-since-2004/619056001/, [Accessed on: March 23, 2021].

[30] A. Shekhovstov, The Globalisation of Pro-Kremlin Networks of Politically Biased Election Observation: The Cases of Cambodia and Zimbabwe, https://www.epde.org/en/documents/category/biased-observation.html, [Accessed on: March 23, 2021], A. Shekhovtsov, Fake Election Observation as Russia's Tool of Election Interference: The Case of AFRIC, Berlin 2020, pp. 41–42.

[31] Intelligence Community Assessment. Assessing Russian Activities and Intentions in Recent US Elections, https://www.dni.gov/files/documents/ICA_2017_01.pdf [Accessed on: March 23, 2021].

[32] И. Головин, Информационная война, „Мир безопасности" 1998, No. 8–9, p. 79; С.И. Макаренко, И.И. Чукляев, Терминологический базис в области информационного противоборства, „Вопросы кибербезопасности" 2014, No. 1, pp. 15–18; С.П. Расторгуев, М.В. Литвиненко, Информационные операции в сети Интернет. Под общей редакцией доктора военных наук, профессора генерал–лейтенанта А.Б. Михайловского, Москва 2014, pp. 7–17, Военная мысль в терминах и определениях. Том 3. Информатизация Вооруженных Сил, (ed.) Н.Н. Тютюнников, Москва 2018, pp. 133–136.

[33] А. Солдатов, И. Бороган, Новое дворянство. Очерки истории ФСБ, Москва 2011, pp. 22, 165, Interagency OPSEC Support Staff, Intelligence Threat Handbook, Washington 2004, pp. 12–13.

[34] M.T. Kłoda, Stany Zjednoczone Ameryki: przegląd projektów prawa stanowego USA dotyczących badań nad wykorzystaniem technologii blockchain w elekcjach państwowych, „Przegląd Sejmowy" 2020, No. 4 (59), pp. 252–253.

[35] Statement by Secretary Jeb Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector, January 6, 2017, www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical, [Accessed on: March 23, 2021].

[36] Based on the Report of the Select Committee on Intelligence, United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election. Volume 1. Russian Efforts Against Election Infrastructure with Additional View, pp. 4, 8, 12, 15–20, 22–24, 35–39, 51, https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf [Accessed on: March 23, 2021]. The Senate Select Committee on Intelligence Responsibilities and Activities was created by the Senate in 1975 to oversee and make continuing studies of the intelligence activities and programs of the United States.

[37] F. Hanson, S. O'Connor, M. Walker, L. Courtois, Hacking Democracies. Cataloguing Cyber-Enabled Attacks on Elections, Canberra 2019, pp. 10–11.

[38] National Intelligence Council. Foreign Threats to the 2020 U.S. Federal Elections, March 10, 2021, p. [i], p. 1–2, https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf [Accessed on: March 23, 2021].

[39] B. Piasecki, Wpływ dezinformacji na procesy demokratyczne na przykładzie wyborów prezydenckich w USA w 2016 roku, In: Zjawisko dezinformacji w dobie rewolucji cyfrowej. Państwo. Społeczeństwo. Polityka. Biznes, (ed.) M. Wrzosek, Warsaw 2019, p. 54.

40 National Intelligence Council. Foreign Threats to the 2020 U.S. Federal Elections…, p. 3.

41 Д. Тренин, Российско-турецкого альянса не существует, https://russiancouncil.ru/, [Accessed on March 23, 2021].

42 Д. Тренин, Выборы в США и российско-американские отношения, https://globalaffairs.ru/articles/vybory-v-ssha-i-rossijsko-amerikanskie-otnosheniya/ [Accessed on: March 23, 2021].

43 Д. Тренин, Эпоха американской невинноsti. Итоги Лектория СВОП, https://globalaffairs.ru/articles/epoha-nevinnosti-lektorii-svop/ [Accessed on: March 23, 2021].

44 А.В. Раскин, Рефлексивное управление в социальных сетях, «Информационные войны» 2015, No. 3, pp. 14–15.

45 С.Н. Бухарин, Ю.А. Матвиенко, Информационно-психологическая война как одна из форм разрешения социально-политических противоречий в современном обществе «Информационные войны» 2008, No. 4, pp. 2-9. Cf. Г.Г. Почепцов, Информационно-психогическая война, Москва 2000, pp. 49–50.

46 Е.С. Яковлева, Фрагменты русской языковой картины мира: модели пространства, времени и восприятия, Москва 1994, K. Ajdukiewicz, Das Weltbild und die Begriffsapparatur, „Erkenntnis" 1934, No. 4, pp. 259–287.

47 А.В. Манойло, Структура современных операций информационной войны, "Вестник Российской нации" 2018, No. 4–5, p. 199.

48 D. Chotikul, The Soviet Theory of Reflexive Control in Historical and Psychocultural Perspective: A Preliminary Study, Monterey 1986, pp. 90–91, P. Sienkiewicz, Systemy kierowania, Warsaw: 1989, pp. 210–211, В.А. Лефевр, Рефлексивное управление, моделирование и мораль. Доклад на международном симпозиуме «Рефлексивные процессы и управление», Москва 2000, In: Рефлексия, В.Е Лепский (ed.) Москва 2003, pp. 454–455, А.В. Раскин, И.В. Тарасов, Рефлексивное управление как технология информационного воздействия, „Информационные войны" 2014, No. 2, pp. 15–17, К. Сивков, Четвертое измерение войны. Каким должен быть Генеральный штаб информационной безопасности, „Военно-промышленный курьер" 2018, No. 39 (752), p. 4, K. Basaj, Dezinformacja, czyli sztuka manipulacji, „Biuletyn Rządowego Centrum Bezpieczeństwa" 2018, No. 25, pp. 14–17.

49 А.В. Раскин, Рефлексивное управление в социальных сетях…, pp. 15–17.

50 И. Барабанов, И. Сафронов, Е. Черненко, Разведка ботом. СВР займется социальными сетями, „Коммерсантъ" 2012, No. 158/P, p. 1.

51 Д. Коротков, Сотни троллей за миллионы, https://www.fontanka.ru/2014/05/29/170/ [Accessed on: March 23, 2021], US Senate. Open Hearing on the Intelligence Community Assessment of Russian Activities and Intentions in Recent U.S. Elections. Hearing before the Select Committee on Intelligence of the United States Senate, One Hundred Fifteenth Congress, first session, Tuesday, January 10, 2017, Washington 2018, p. 20.

52 Read more: Bellingcat Investigation Team. Putin Chef's Kisses of Death: Russia's Shadow Army's State-Run Structure Exposed, https://www.bellingcat.com/news/uk-and-europe/2020/08/14/pmc-structure-exposed/ [Accessed on March 23, 2021].

53 Л. Яппарова, Рынок политического насилия. Близкие к Кремлю бизнесмены Пригожин и Малофеев с бригадами ветеранов Сирии и Донбасса потеснили отморозков под контролем ФСБ и МВД, https://meduza.io/feature/2019/11/21/my-sami-siloviki [Accessed on: March 23, 2021], «Грязные» политические технологии структур Евгения Пригожина и их влияние на выборный процесс в Российской Федерации, https://dossier.center/contra/ [Accessed on: March 23, 2021].

54 АВ Манойло, Технологии несилового разрешения современных конфликтов, Москва 2014, pp. 283–287.

55 В.Г. Крысько, Секреты психологической войны (цели, задачи, методы, формы, опыт), Минск 1999, pp. 182–183.

56 Report of the Select Committee on Intelligence, United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election. Volume 2 Russia's Use of Social Media with Additional Views (Redacted), pp. 29–30, https://www.intelligence.senate.gov/sites/defau.lt/files/documents/Report_Volume2.pdf, [Accessed on March 23, 2021], Internet Research Agency Indictment, pp. 12–13, https://www.justice.gov/file/1035477/, [Accessed on: March 23, 2021], S. L. McLean, Purple Battlegrounds: Presidental Campaign Strategies and Swing States Voters, w: Presidential Swing States: Why Only Ten Matter, (ed.) S. Hunter Hecht, D. Schultz, Lanham 2015, pp. 1–29.

57 Internet Research Agency Indictment, pp. 14, Report of the Select Committee on Intelligence, pp. 30–32, US Department of Justice. Special Counsel Robert S. Mueller, III, Report On The Investigation Into Russian Interference in The 2016 Presidential Election, vol. 1-2, Washington 2019, p. 22. Cf. В.Г. Крысько, Секреты психологической войны (цели, задачи, методы, формы, опыт), Минск 1999, pp. 182–183.

58 В.К. Новиков, С.В. Голубчиков, Современные сценарии ведения информационных войн и их итоги, „Вестник Академии военных наук" 2017, No. 2, p. 65.

59 Exposing Russia's Effort to Sow Discord Online: The Internet Research Agency and Advertisements, https://intelligence.house.gov/social-media-content/ [Accessed on: March 23, 2021].

60 А.В. Манойло, Технологии несилового разрешения современных конфликтов…, p. 288., R. Mucchielli, La subversion, Paris 1976, p. 111.

61 P.N. Howard, B. Ganesh, D. Loitsiou, The IRA and Political Polarization in the United States, Oxford 2018, pp. 17–19, 18–19. Cf. R. DiResta et al, The Tactics & Tropes of the Internet Research Agency, Washington 2018, pp. 33–39, 69–71.

62 A. Parlapiano, J.C. Lee, The Propaganda Tools Used by Russians to Influence the 2016 Election, https://www.nytimes.com/interactive/2018/02/16/us/politics/russia-propaganda-election-2016.html [Accessed on: 23 III 2021].

63 K.H. Jamieson, Cyberwar. How Russian Hackers and Trolls Helped Elect a President, Oxford 2018, pp. 12, 71, 84, 88, 91, 94, 127, 134–135.

64 J. Hlavacek, Facebook ad Promoting 2016 Lawrence Protest Among Those Paid for by Russian Trolls, https://www2.ljworld.com/news/2017/nov/01/facebook-ad-promoting-2016-lawrence-protest-among-/ [Accessed on: March 23, 2021].

65 Read more on the protest: J. Geraghty, What Russia Really Wants: A Divided, Paralyzed America, https://www.nationalreview.com/corner/what-russia-really-wants-divided-paralyzed-america/ [Accessed on: March 23, 2021.], M. Kosoff, How Russia Secretly Orchestrated Dozens of U.S. Protests, https://www.vanityfair.com/news/2017/10/how-russia-secretly-orchestrated-dozens-of-us-protests, [Accessed on: March 23, 2021.].

66 Read more on the protest: A. Berland, Thousands Attended Protest Organized by Russians on Facebook, https://thehill.com/policy/technology/358025-thousands-attended-protest-organized-by-russians-on-facebook [Accessed on: March 23, 2021.].

67 А.В. Манойло, Технологии несилового разрешения современных конфликтов…, pp. 283, 295–296, 299.

68 Criminal Complaint. United States District Court for the Eastern District of Virginia. USA vs Elena Alekseevna Khusaynova, https://www.justice.gov/opa/press-release/file/1102316/download/pdf, s. 14, 16, 19, [Accessed on: March 23, 2021].

69 J.E. Barnes, A. Goldman, Extremists in US get a Prod from Moscow. Russia Trying to Stoke Racial Tensions in US, „The New York Times. International Edition," March 12, 2020, p. 1, 5.

70 Sh. Vavra, Russian IRA troll farm outsourced new operation to Ghana, Nigeria, https://www.cyberscoop.com/rus-

sia-ira-troll-farm-disinformation-outsourced/ [Accessed on: March 23, 2021], United States of America v. Artem Mikhaylovich Lifshits Indicement, pp. 14–15, https://www.justice.gov/opa/press-release/file/1315491/download, [Accessed on: March 23, 2021.], The Graphika Team. IRA in Ghana: Double Deceit. https://public-assets.graphika.com/reports/graphika_report_ira_in_ghana_double_deceit.pdf [access: March 23, 2021],

[71] V. Volkoff, Dezinformacja. Oręż wojny, Warsaw 1991, p. 81.

[72] J. Menn, Russian-backed Organizations Amplifying QAnon Conspiracy Theories, Researchers Say, https://www.reuters.com/article/us-usa-election-qanon-russia-idUSKBN25K13T, [Accessed on: March 23, 2021.]

[73] T.C. Helmus, Russian Propaganda Hits Its Mark. Experimentally Testing the Impact of Russian Propaganda and Counter-Interventions, Santa Monica 2021.

Michał Wojnowski, Ph.D. – senior researcher at the Center for Studies and Education for Security, University of Wroclaw, Poland (https://www.cseb.uni.wroc.pl), member of the Polish Society for National Security (http://www.ptbn.online/).

Warsaw Institute
Wilcza St. 9, 00-538 Warsaw, Poland
+48 22 417 63 15
office@warsawinstitute.org

The opinions given and the positions held in materials in the Special Report solely reflect the views of authors.