# The Russian Influence Strategy in Its Contested Neighbourhood


**Marco Marsili**

## 1 Introduction

The Helsinki Final Act of 1975 (also known as the Helsinki Accords), that concluded the first Conference on Security and Cooperation in Europe—re-established in 1995 as the Organization for Security and Cooperation in Europe—reaffirmed the fundamental principle of renouncing the threat or use of force against the territorial integrity or political independence of any state (Marsili, 2020, 44). Through this agreement, the Soviet Union (USSR) gained the implicit recognition of the "sphere of influence" that was determined in Eastern Europe after the end of World War II. This political and geographical area encompasses Armenia, Azerbaijan, Georgia, Moldova, and Ukraine (European External Action Service [EEAS], 2016a). These countries, plus Belarus, participate in the European Neighbourhood Policy (EEAS, 2016b), and at the same time they are partners of the North Atlantic Treaty Organization (NATO, 2020a), and members of the Euro-Atlantic Partnership Council (EAPC).

The Helsinki Accords did not affect the U.S. recognition of the sovereignty of Estonia, Latvia, and Lithuania that were forcedly incorporated into the Soviet Union following the secret protocols to the Molotov-Ribbentrop Pact with Nazi Germany in August 1939. The annexation was never accepted by the United States—see the Welles Declaration of 23 July 1940—since the three states regained de facto independence in 1990–1. Before gaining de jure independence in the aftermath of World War I the Baltic nations were part of the Russian Empire, and now they are members of

M. Marsili (✉)
Centro de investigação do Instituto de Estudos Políticos, Universidade Católica Portuguesa, Lisbon, Portugal
e-mail: info@marcomarsili.it

Centro de Investigação e Desenvolvimento, Instituto Universitário Militar, Lisbon, Portugal

Centro de Estudos Internacionais, Instituto Universitário de Lisboa (ISCTE-IUL), Lisbon, Portugal



H. Mölder et al. (eds.), *The Russian Federation in Global Knowledge Warfare*, Contributions to International Relations,
https://doi.org/10.1007/978-3-030-73955-3_8

the European Union (EU) and NATO. Too late for Moscow to impede the NATO-EU enlargement towards North-East, but maybe not too late to avoid further "territorial losses" in the Caucasus and in Central and Eastern Europe (Kivirähk et al., 2009, 13; Iasiello, 2017, 55, 59).

After the attempts to assimilate by force the Baltic states, Russia is pursuing a policy of attack on the sovereignty and territorial integrity of Ukraine and Georgia, through the annexation of Crimea, the support for destabilizing proxies in Eastern Ukraine (Donbass) and the inclusion of Abkhazia and South Ossetia into its security field (Kivirähk et al., 2009; Darczewska, 2015, 36; Wetoszka, 2016, 63; Müür et al., 2016, 33; Mölder, 2016, 109; Kofman et al., 2017, 1; Pompeo, 2020).

Although NATO has claimed that never promised Russia it would not expand after the Cold War (NATO, 2018), Moscow feels encircled and threatened by the Allies (Darczewska, 2015, 10, 12, 17; Sliwa, 2017, 16; Tashev et al., 2019, 141) and strives to regain control over the sphere of interest defined by the Helsinki Accords that the Atlantic Alliance and the EU have gradually challenged (Kivirähk et al., 2009, 12, 36; Kanet, 2011; Kofman et al., 2017, 45–46; Sliwa, 2017, 21–22; Värk, 2017, 47–48; Beehner et al., 2018, 35). Among the scholars is a broad consensus that Moscow is trying to re-establish its zone of privileged influence in the Black Sea region, disturbing and incapacitating the nations' sovereign decisions—i.e., Ukraine and Georgia—and their processes of Euro-Atlantic integration (Kivirähk et al., 2009, 9–10; Darczewska, 2014, 18, 26, 33–36; Winnerstig, 2014, 11, 142; Mölder, 2016, 100; Sazonov et al., 2016, 8–9; Müür et al., 2016, 30–31; Renz & Smith, 2016, 16–18; Kofman et al., 2017, 1, 45–46; Anastasov, 2018; Creţu & Ardeleanu, 2019, 335–336; Popa, 2019, 347–348; Tashev et al., 2019, 130).

In the aftermath of the Soviet Union breakup, unconventional conflicts erupted in the newly formed independent republics: Armenia–Azerbaijan (Nagorno-Karabakh or Artsakh), Georgia (South Ossetia and Abkhazia), Moldova (Transnistria or Transdniestria) and Ukraine (Crimea and Donbass, i.e., Donetsk and Luhansk People's Republics). Somehow, these conflicts are the legacy of the Cold War (Marsili, 2020, 45).

The Russian Federation (RF) intervened in these conflicts to protect the Russian ethnics population of these breakaway territories, without prejudice to the obligations, set forth in the Helsinki Accords, to respect principle of the inviolability of frontiers and non-interference in the internal affairs of other nations. The war against Georgia took place in August 2008 to support the self-proclaimed republics of South Ossetia and Abkhazia. In the aftermath of the contested recognition of Abkhazia and South Ossetia as independent states by Moscow, the NATO severed a first time the cooperation with the RF; the collaboration was resumed later, but was suspended again in 2014, following the Russian annexation of Crimea (NATO, 2020b).

Although Moscow does not consider that such interventions constitute an unlawful invasion of a sovereign country—but rather views it as a domestic affair—the Russian government had to justify some way its interference and to present it to the public opinion as "fair and just" and not as acts of aggression (Kivirähk et al., 2009, 13, 16; Darczewska, 2015, 34; Snegovaya, 2015, 7; Pakhomenko & Tryma, 2016, 43, 52; Blank, 2017, 82; Boyte, 2017, 95; Iasiello, 2017, 52, 58; Sazonov, 2017, 75; Värk,

2017, 48). This conundrum was solved through the resort to hybrid warfare, of which information operations are an essential component.

## 2 Information Warfare: Definition and Scope

There is no common definition of the term "hybrid warfare" and therefore it is correspondingly ambiguous (Renz & Smith, 2016, 12; Wetoszka, 2016, 64; Cullen & Reichborn-Kjennerud, 2017, 3; Tashev et al., 2019, 132). While it is a blend of traditional and irregular tactics, hybrid warfare makes overt and covert use of a wide range of tools: military and civilian, conventional and unconventional, including information and influence operations (Hoffman, 2007, 7; Heickerö, 2010, 20; Brangetto & Veenendaal, 2016, 117–118; Wetoszka, 2016; Cullen & Reichborn-Kjennerud, 2017, 3; Theohary, 2018, 4). These "hot topics" became very popular in the geopolitical context that emerged after the end of the Cold War, when hybrid conflicts replaced the traditional ones (Marsili, 2019, 172).

In a semantic sleight of hand, hybrid warfare was originally confined to an activity committed by non-state actors (NSAs) at the express detriment of the nation-state (Hoffman, 2007). In other words, hybrid warfare was linked almost exclusively with NSAs. Afterwards the concept of hybrid warfare developed in a way that is now commonly accepted to describe the interplay between conventional and unconventional means used also by governments and regular armies[1] (Hoffman, 2007, 29, 58; Cullen & Reichborn-Kjennerud, 2017, 3; Marsili, 2019, 178).

The low barriers of entry the information environment have enabled both state and non-state actors, individuals and private groups, terrorists, and criminals, to access it and to turn it into a battlefield (Eriksson, 1999, 60, 61; Thomas, 1996a, 86, 90; Cilluffo & Gergely, 1997; Bishop & Goldman, 2003, 116; Hollis, 2007, 1049; Schreier, 2015, 23; Department of Defense, 2016, 2). As the resources required for IW are likely to be much lower than for conventional military capabilities, IW is considered a 'power equalizer' (Eriksson, 1999, 60). Accordingly, both nation states and NSAs resort to IW to achieve strategic objectives (Theohary, 2018, 9). Covert operations[2] and support to proxies, such as independentists and secessionists, are facilitated by the nature of hybrid and information warfare, although the inclusion of IW in the broader concept of hybrid warfare is disputed but is widely accepted by most of the scholars (Iasiello, 2017, 60–61).

As Vertuli & Loudon, (2018, xi) stresses, is worthy of attention that he U.S. Army doctrinal definition of IO has changed three times over the last decade: from a focus on five core capabilities to information engagement (2007), to inform and influence

[1] A *regular army* is the official army of a state or country (the official armed forces).

[2] A covert operation is a military operation intended to conceal the identity of (or allow plausible denial by) the sponsor and intended to create a political effect which can have implications in the military, intelligence or law enforcement arenas — affecting either the internal population of a country or individuals outside it.

activities (2011), to its current incarnation focusing on information-related capabilities (2016). This shows to what extent information warfare is a nebulous concept, but widely cited as a keystone in any present and future campaigns (Chekinov & Bogdanov, 2013).[3] In the near future militaries are unlikely to adopt purely non-physical strategies of conflict, while it is more likely that attacks will surely continue to combine physical and cyber capabilities (Bishop & Goldman, 2003, 118). Physical destruction will remain a compelling proximate goal and cyber-attacks are likely to be used in support of lethal operations on the battlefield and against the adversary's homeland (Bishop & Goldman, 2003, 118). This hypothesis is supported by the reasoning that Western societies would seem more inclined to accept non-lethal IO than the traditional use of military force (Bishop & Goldman, 2003, 120).

IW blurs the peace-war boundary (Bishop & Goldman, 2003, 121), transcends the traditional domains of warfare and finds itself at the intersection of the information, physical and cognitive/social domains. Boundaries between "conventional" and "unconventional" warfare are fading, and even the physical/kinetic and virtual dimensions of conflict are blurring.

The virtual realm encompasses electronic warfare (EW); electromagnetic spectrum operation (EMSO); cyberspace operations (CO); information warfare (IW); psychological (warfare) operations (PSYOP), now better known as military information support operations (MISO); information operations (InfoOps or IO), also known as influence operations; Strategic Communications (STRATCOM); Military Deception (MILDEC); computer network operations (CNO); operations security (OPSEC). Most of these concepts intertwine and overlap; moreover, they rely heavily on the U.S. and NATO military doctrine (Hollis, 2007; Porche et al., 2013; Brangetto & Veenendaal, 2016; Vertuli & Loudon, 2018; Tashev et al., 2019).[4]

Information warfare is sometimes referred to as persuasion or IO or even PSYOP. (Theohary, 2018, 1). Therefore, we uphold the holistic approach that integrates PSYOP, CO, and EW as constituents of IW as a whole, considering in turn the latter a component of hybrid warfare (Bakshi, 2018, 178–179; 184). We can agree with practitioners like Jones (1999, 12) when he says that IW, that is the sum of many things, including those mentioned above, has been largely superseded by the 'more technically acceptable term Information Operations'.

Information warfare is well defined, in its components, purpose and scope, in the Annual Report that the Secretary of Defence, Les Aspin, presented to the President and the Congress in 1994 (227–8). Thomas (1996a, 85, 88) considers IW a "psychological weapon" that serves "to manipulate perceptions, emotions, interests, and choices" and in doing so intimidates and pressures other governments. Other scholars (Theohary, 2018, 1–2; Bishop & Goldman, 2003, 115; Tashev et al., 2019, 133–134) define IW a strategy to use information to pursue a competitive advantage and to

[3] For a broad survey of information warfare literature, see, inter alia, Merrick et al. (2016).

[4] See, e.g., Department of Defense, *Joint Publication (JP) 1-02, Dictionary of Military and Associated Terms;* U.S. Joint Chiefs of Staff, *JP 3-0* on Joint Operations, *JP 3-12* on Cyberspace Operations, JP 3-13 on Information Operations, JP *3-13.1* on Electronic Warfare, JP *3-13.2* on Military Information Support Operations, JP *3-13.3* on Operations Security, JP *3-13.4* on Military Deception, JP 3-58 on MILDEC, *JP 3-61* on Public Affairs and *JP 5-0* on Joint Planning.

achieve foreign policy goals; a form of political warfare that targets governments, political leaderships, military, private sector, general population, news and media in order to influence public opinion or to compel decision-makers.

IW has become a key issue in conflict and competition, not only military (Bishop & Goldman, 2003, 115); it includes actions taken to achieve information superiority over adversaries (Cilluffo & Gergely, 1997, 84–85; Bishop & Goldman, 2003, 121, 133). The scope of IW goes beyond the military and touches on the political, diplomatic and economic spheres of information (Cordey, 2019, 9); the targets include enemy population beliefs, enemy leadership beliefs, and the economic and political information systems upon which society relies to function (Bishop & Goldman, 2003, 119).

Certainly, IW cannot be reduced only to attacks against computer networks—Schreier (2015, 19–30) spells out the difference between IW or IO and cyberwarfare. Dorothy E. Denning, a pioneer in computer security, in her 1999 classic book defines IW as "operations that target or exploit information media in order to win some objective over an adversary". However, this definition is so broad that it includes a set of techniques and technologies that ranges from of electronic warfare to propaganda.

A report prepared by Theohary (2020) for the U.S. Congress, in which she recaps an array military activities that fall under the broad definition of IO, underlines that currently there is no official definition of IW, thus preferring the wording "information operations" that links strategic objectives with a wide range of tactics, techniques and procedures (Theohary, 2018, 2).[5] A forenote to a 2003 issue of the *Military Intelligence Professional Bulletin*, published by the U.S. Department of the Army, focuses on the information environment (including IW and EW) and points up that the understanding of IO is "simultaneously frustrating and intriguing" and a "daunting task". Nevertheless, we will continue to use these terms, despite their shortcomings.

In the opinion of the current author the term "warfare" is not synonym of "armed conflict" defined by the Hague and Geneva Conventions and therefore it does not fit to operations in virtual domains (Marsili, 2019). Information and influence operations (IIO) are located in a "grey zone"[6] between peace and war which includes ambiguous contexts such as hybrid conflicts (Schreier, 2015, 19, 23; Gorkowski, 2018, 26; Cordey, 2019, 10, 19) and below the threshold of war (Theohary, 2018, 2; 2000). Bishop and Goldman (2003, 115, 123–125) find that, although IW employs a broad array of non-lethal tools, a cyberattack can have deadly consequences. Zhaohong (2016, 49) perceives information as an operational warfare to provide non-kinetic capabilities for achieving strategic outcomes. Renz and Smith (2016, 22) exclude that the use of information in itself represents an act of war. The question is whether an IW campaign could be considered an armed attack or use of force under international law that could trigger a military response or whether it falls below the threshold of damage and destruction resulting from a kinetic attack (Hollis, 2007; Theohary, 2018, 16).

[5] For a wide review of the literature on influence operations and techniques (propaganda, PSYOP, IW, etc.), see Cordey (2019).

[6] For a definition of grey zone warfare, see Theohary (2018, 4).

In a seminal paper Thomas (1996a, 86–7) defines information attack "an assault on the territory of a sovereign state" affecting, inter alia, international relations, political institutions and social structures. He (disproportionately) concludes that information technologies have the same potential of nuclear or conventional weapons during the Cold War (Thomas, 1996a, 90). Likewise, Bishop and Goldman (2003, 113, 132) equal information deterrence to nuclear deterrence. Hollis (2007) wonders whether IO constitutes a use of force or an armed attack, lacking the physical characteristics of traditional weaponry, or if should be considered a crime under domestic law. He gathers that the law of war includes no specific provisions, thus leaving much room for interpretation (Hollis, 2007, 1035).

Therefore, is strongly questioned how IIO capabilities should be considered. Eriksson (1999, 57) finds that the huge potential of IW places it among weapon of mass destruction. Some scholars (Thomas, 1996b, 26; Hildreth, 2001, 11; Khan, 2013, 146–7; Giles, 2016a, 34), which quote V.I. Tsymbal (1995), a prominent Russian analyst, remind us that some Russian officials perceived IW as a strategic threat to such an extent that they benchmarked its functional outcome against weapons of mass destruction. Other researchers (Heickerö, 2010, 15, 52; Tashev et al., 2019, 134) compare them even to nuclear weapons. Whatever it is, the Russian doctrine considers IW a conflict between two or more states in the information space (Theohary, 2018, 9) and accordingly the RF employs IIO as a weapon.

The Russians have taken the information threat so seriously that in 1998 they boosted an UN-sponsored treaty to ban IW[7]—what makes us smile, considering the current Russian military doctrine, and the large use that Moscow made, in recent years, of this resource. I rather prefer to label non-lethal actions, like IO are, as "military operations other than war" (MOOTW), according to the definition provided by the U.S. Department of the Army (1995). While a clear concept has not yet crystallized, IW can be considered "a form of comprehensive warfare, a strategy, not merely a set of techniques" (Johnson, 1997, 49–50)—a seminal report by Jensen (1997) provides an historical overview of IW and emphasizes strategic issues. Whatever it is, in present-day conflicts IO are considered an essential element of an overall winning military strategy (Schreier, 2015, 19; Zhaohong, 2016, 51).

As any other weapon, IO can be split in offensive and defensive activities: the former includes MILDEC (measures designed to mislead the enemy by manipulation, distortion and falsification of evidence) and PSYOP (measures to influence attitudes and behaviour of allies and enemies)—the latter comprise: counter-deception and counterpropaganda or counter-psychological operations (Hutchinson, 2006, 219). PSYOP also cover perception management (PM), public information (PI), and public diplomacy (PD). IO methods such as PSYOP present alternative ways to accomplish larger strategic goals without resorting to force at all by convincing the adversary (or those who support it) to change their policies or positions (Hollis, 2007, 1032).

The concept of "influence operations" is broader than that of "information operations" and incorporates EW, OPSEC, CO, PSYOPS, and MILDEC, thus including

[7] UN General Assembly, *Developments in the field of information and telecommunications in the context of international security*, A/RES/53/70, 4 December 1998.

also non-military and coercive activities such as propaganda (Cordey, 2019, 4, 10). Influence operations whose purpose is to persuade foreign audiences (Larson et al., 2009). Mixing information operations and warfare, the RAND Corporation turns out a concept of influence operations that incorporates "the dissemination of propaganda in pursuit of a competitive advantage over an opponent". The term "influence operations" in the context of IW is used to describe "efforts to influence a target audience, whether an individual leader, members of decision-making group, military organizations and personnel, specific population subgroups, or mass publics" (Larson et al., 2009: 2). Influence operations are therefore an umbrella term covering all operations in the information domain, including soft power activities (Cohen & Bar'el, 2017).[8]

While is not the purpose of this work to give a definition of these terms—which do not have any commonly accepted or legally binding—for the scope of this essay we adopt the following comprehensive definition of IO set forth in the monograph by Porche et al. (2013, xx), to which we refer for a discussion: "efforts to inform, influence, or persuade selected audiences through actions, utterances, signals, or messages". A similar definition is provided by some scholars (see, e.g., Hollis 2007, 1023; Brangetto & Veenendaal, 2016, 114). Information operations are generally understood as intended to influence decisions, perceptions, and behaviour of political leaders, the population or particular target groups with the objective of achieving security policy objectives (Schmidt-Felzmann, 2017; Cohen & Bar'el, 2017; Pamment et al., 2018; Cordey, 2019).

The Russian strategy, which deeply incorporates IOs within IW (Blank, 2017: 93), proved to be crucial to win every war in which Moscow has participated in the second millennium (Blank, 2017: 85), particularly in Ukraine and Crimea (Jaitner, 2015, 87; Bakshi, 2018, 181). In this context, Renz and Smith (2016, 12) point out that there are no wars in history that were won by non-military means, or by the use of information, alone (Renz & Smith, 2016 12).

Kuehl (2002, 36) explains clearly the difference between IO and IW: the former are "actions taken to affect adversary information and information systems while defending one's own information and information systems"; the latter consists of "information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries". Giles (2016a, 18–19, 24, b, 9), to which we refer for a discussion on the cognitive and technical aspects of the Russian IO, finds that information-psychological warfare affects the personnel of the armed forces and the population of the adversary. Zhaohong (2016, 5) sceptically argues that information operations are probably overrated, to the point that they are supposed to exercise a "disproportionate influence" over population and to undermine the legitimacy and morality of the military. Anyway, regardless of their pivotal role, effectiveness of IO is not questioned.

All these activities, although currently carried out with the use of modern technology, are not new: they are widely described as a simply a modern, digital-age version of well-established Soviet tactics and strategies (Thomas, 1996b, 31–32; Darczewska, 2014, 34, 2015, 7, 33; Snegovaya, 2015, 7; Arold, 2016, 26; Giles,

[8] For a meaningful list of information operations, see Schreier (2015), 19–23.

2016a, 33–36, b: 4; Renz & Smith, 2016, 6; Blank, 2017, 83, 89; Ajir & Vailliant, 2018, 75; Beehner et al., 2018, 35–36). Darczewska (2014, 34) pictures them effectively as "an old product in new packaging". Indeed, "Disinformation" is the English transliteration of the Russian word *dezinformatsiya*, a KGB black propaganda department (Jowett & O'Donnell, 2012, 23–24). This term can be defined as "the deliberate creation and sharing of false and/or manipulated information that is intended to deceive and mislead audiences, either for the purposes of causing harm, or for political, personal or financial gain" (Digital, Culture, Media and Sport Committee [DCMS], 2018, 2, 2019, 10, 12). On the opposite, misinformation is "the inadvertent sharing of false information" (DCMS, 2018, 2, 2019, 10, 12). The same distinction can be found in a fresh report on IO drafted for the U.S. Congress (Theohary, 2020). Libicki (2007, 50) thinks that the expected outcome of misinformation is believing what is not true, while disinformation is aimed to lead the audience to being unable to believe what is true.[9]

In the changed nature of conflict, the manipulation of information became an essential function and a high priority goal for political and military leaders (Bishop & Goldman, 2003, 116; Hutchinson, 2006, 213). The control of information is therefore deemed critical to military success and PSYOP are regarded to have a fundamental role to influence the decision-making of possible adversaries (Wilson, 2006).

PSYOP gained a central importance for insurgency and counterinsurgency operations, starting from international tension and going through all pre-conflict, conflict, and post-conflict phases (Lord & Barnett, 1988, xix). In the IW context, denial and deception support the construction of an "artificial reality" that may prove useful to gain advantage over the adversary: this combination became a mantra (Godson & Wirtz, 2002).

Propaganda is included in the bouquet of techniques used in psychological warfare and is widely used to influence public opinion and to support the government's hardline (Marsili, 2015). According to the definition of Jowett and O'Donnell (2012, 7): "Propaganda is the deliberate, systematic attempt to shape perceptions, manipulate cognitions, and direct behaviour to achieve a response that furthers the desired intent of the propagandist". Through the intentional dissemination of false claims, fictitious or based on facts, propaganda aims to support or justify political actions or ideologies by creating a false image in the mind of the audience (Marsili, 2015). Although it is information, propaganda is not impartial—neither should tell the truth—but it often presents facts selectively, thus possibly lying by omission, to produce an emotional rather than rational response to the information presented (Marsili, 2015). Propaganda also has much in common with public information campaigns by governments or political groups, which are intended to encourage or discourage certain forms of behaviour, including a nationalist discourse, but also covert interests (Marsili, 2015).

[9] For a definition of disinformation and misinformation, see Theohary (2018, 4), Arold (2016, 25–26).

## 3 The Russian Information Strategy

Lord & Barnett (1988, 17) thinks that psychological-political operations should target everybody: not only adversaries, but also neutral, allied, and semi-allied countries. Accordingly, Moscow's information strategy is aimed to present the behaviour of the RF as "fair and just", to demonize the adversaries and to frighten its neighbours, from the Baltic to the Black Sea (Blank, 2017, 87). To accomplish its geopolitical objectives, Russia relies on social media tools to disseminate a blend of propaganda, misinformation, and disinformation (Darczewska, 2014, 2015; Snegovaya, 2015; Arold, 2016, 25–26; Müür et al., 2016, 30–31; Iasiello, 2017, 51, 61; Theohary, 2018, 9; Vertuli & Loudon, 2018).

Thomas (1996a, 84, 87) finds that information warfare—*informatsionnaya voyna*—emerged in the Russian military strategy after the end of the Cold War and considers the RF to be the forefront of this array of techniques. On a Russian standpoint IW is a strategy of resolving a conflict through information and psychological influence on a nation's decision-making system and on its population that includes a variety of military activity/operations (Thomas, 1996, 26–27; Giles, 2016a, 18–19, 24; Renz & Smith, 2016, 11–18; Beehner et al., 2018; Tashev et al., 2019, 139).

The Russian doctrine has adopted a concept of offensive IW that includes physical attacks and the use of CNO, EW, PSYOP, STRATCOM, and MILDEC (Thomas, 1996b, 33; Cilluffo & Gergely, 1997, 85; Heickerö, 2010, 9; Darczewska, 2015; Vertuli & Loudon, 2018).[10] Although the Russian tradition of propaganda and (dis)information comes from afar (Iasiello, 2017, 51), the Moscow authorities started framing doctrine organically since 2000 and now information superiority in considered instrumental for a successful military strategy (Iasiello, 2017, 61; Sazonov et al., 2017a, b, 7).

The *Information Security Doctrine* approved by the President of the Russian Federation in September 2000, jointly with the *Russian Federation Armed Forces' Information Space Activities Concept,* underlines the role of the information war and the global importance of information space in all spheres of the vital activity of the society. The *Conceptual Views on the Activity of the Armed Forces of the Russian Federation in Information Space*, adopted in the end of 2011 by the Russian Ministry of Defence, presents the updated vision of aims, priorities, and methods of activities of the Russian armed forces in information space. The *Russian Military Doctrine*, approved in December 2014, lists the key features of modern conflict that include information operations, "protest potential" of local populations, and the use of special forces (Darczewska, 2015, 27; Charles, 2016). Lastly, the Russian *National Security Strategy 2020* further emphasizes the significance of the "global information struggle" against nationalists and separatists (Jaitner, 2015, 88). In this way, IW concepts were integrated into the Russian national security and foreign policy agenda. Nevertheless, the Russian IW approach is to be considered a "developing process", rather than "a static situation" (Giles, 2016b, 2).

[10] For a discussion on the IIO Russian strategy, concepts and doctrine, see Arold (2016).

The Russian strategy employs (dis)information to affect adversary's decision-making process and to guide the opponent into making pre-determined decisions favourable to Moscow (Thomas, 2004, 253; Heickerö, 2010, 21; Giles, 2016a, 18–19; Beehner et al., 2018, 35; Tashev et al., 2019, 139). Therefore, IIO are means (or weapons, if you want to consider them as such) to impose limited sovereignty upon allies and neighbours (Darczewska, 2015, 7, 35). Tabansky (2017, 3) and Giles (2016a, 18–19, 24) believe that Russian IO are planned to manipulate public opinion, political debate, and decision-making in its neighbouring countries, while it is questioned whether IO should be considered an instrument of hard or soft power, according to the original definition if the term by Joseph Nye (Tabansky, 2017, 5).

A deep study conducted in 2009 by Kivirähk investigates the Russian influence operations on six former USSR counties (Latvia, Lithuania, Estonia, Georgia, Moldova, and Ukraine) through the analysis of soft power means, including IO. The research concludes that the RF uses the promotion of culture and language and the use of media as tools for achieving foreign policy objectives and as means of persuasion to threaten neighbouring countries. Likewise, Winnerstig (2014, 143) assumes that soft power seems to be a preferred option for Russian policymakers to have weak and domestically unstable neighbouring states.

A report published by the Swedish Defence Research Agency (FOI) concludes that the Russian soft power strategy towards the Baltic states consists only of non-military means of influence as tools of destabilization whose effects can be "devastating" (Winnerstig, 2014, 4, 10, 12, 143). On this point the scientific community offers different interpretations. Brangetto and Veenendaal (2016, 114) infer that Russia considers IW as an instrument of hard power, while Darczewska (2015, 29) and Bakshi (2018, 181) think that Moscow views IW as a soft power tool. We disagree with both these assumptions and we explain why. Hard power is based on military intervention, coercive diplomacy, and economic sanctions, while "soft power is the capacity to persuade others to do what one wants" (Wilson, 2008, 114) using various means, including IIO. Armitage and Nye made clear that hard power combined with soft power combined gives birth to "smart power" (2007, 7), hence using a mix of resources that fits better with the concept of hybrid warfare (Blank, 2017, 86–87). Hudson (2015), who investigated the extent of Russian soft power in contemporary Ukraine, offers a different interpretation: she gathers that, while Moscow is convinced to use soft power, the Kremlin strategy is seen by the audience as "hard". Probably this ambiguity is due to the fact that Russia's understanding of IW does not distinguish between war and peace activities (Heickerö, 2010; Darczewska, 2015, 31; Giles, 2016a, 4, 10–11; Gorkowski, 2018, 23; Cordey, 2019, 9; Tashev et al., 2019, 133, 141). Soft power therefore seems to be not a form of warfare per se, but "something that is done for purposes that might be useful both in peacetime and in a future traditional conflict" (Winnerstig, 2014, 143).

The Russian leaders are not only questioning the post-Cold War order in Europe, but they are also employing hybrid instruments to blur the boundaries between war and peace (Meister, 2016; Renz & Smith, 2016, 12; Värk, 2017, 46; Tashev et al., 2019, 134). The vast majority of the analysts (Darczewska, 2014, 2015; Winnerstig, 2014, 11; Vilson, 2016; Blank, 2017, 88, 91; Cullen & Reichborn-Kjennerud, 2017,

28; Sazonov et al., 2017a, b: 8; Sliwa, 2017, 21–22; Anastasov, 2018; Ajir & Vailliant, 2018; Beehner et al., 2018, 35, 39; Rugge, 2018) argue that, in the context of the strategic confrontation with the Euro-Atlantic bloc and its Eastern partners, the RF makes an extensive use of (dis)information techniques as a strategy to undermine the trust in Western institutions and to disrupt the process of integration into the latter of the nations once included into the Soviet Union's sphere of influence: the Baltic states, Georgia, and Ukraine. Beehner et al. (2018, 32) assumes that the Russian IW is aimed, inter alia, to prevent countries in its desired sphere of "privileged interest" from Western alliances like NATO by keeping these areas in perpetual conflict, regardless of the national state of cooperation or hostility between the opposing sides (Giles, 2016a, 10).

Indeed, IW can be used as a means of coercion to persuade an adversary to reverse or stop (deterrence) an action (Bishop & Goldman, 2003, 133–134). While deterrence is aimed at dissuading an adversary from undertaking a damaging action, coercion is used to persuade an adversary to stop or reverse an action. Coercion does not require the use of force; it may be executed entirely through diplomacy and persuasion (Bishop & Goldman, 2003, 134).

Some researchers (Fridman, 2018) believe that hybrid warfare is the Kremlin's main strategy in the twenty-first century, while some others contest this interpretation (Renz & Smith, 2016: 14; Fabian, 2019) but they all agree the RF employs widely a mix of techniques, methods, technologies, and tactics that we can cluster under the umbrella concept of "hybrid warfare" (Pakhomenko & Tryma, 2016; Renz & Smith, 2016, 1).[11] Lanoszka (2016) thinks that the Russian hybrid warfare strategy has made other former Soviet republics, such as the Baltic countries, fear that Moscow would use subversion rather than conventional military means against them. Thus, we can infer that the RF is not only threatening but is also blackmailing its neighbours.

Information warfare is considered a critical component of Russia's hybrid warfare strategy (Snegovaya, 2015, 21; Beehner, et al., 2018; Tashev et al., 2019, 138) intended to achieve combat superiority (Thomas, 1996b, 27; Heickerö, 2010, 25) and to accomplish results that are usually gained with the use of military means (Giles, 2016a, 16; Blank, 2017, 83). Russia sees superiority in this broad application of IW as a key enabler for victory in current and future conflict (Giles, 2016a, 6). This does not mean that Moscow gave up traditional means: the RF has simply embodied information capabilities into conventional ones (Beehner et al., 2018; Thompson, 2018, 5) and resorts to armed force when non-military measures fail (Darczewska, 2015, 30; Renz & Smith, 2016, 18; Kofman et al., 2017; Tashev et al., 2019, 140). Indeed, the Russian concept of IW does not fit the conventional notion of war but is instead a mix of traditional, old and modern methods, open and covert means, military and non-military, conventional and unconventional, lethal and non-lethal (Darczewska, 2015, 14–16, 38; Giles, 2016a, 6; Sliwa, 2017, 21). The conflicts in Estonia, Georgia, and Ukraine served as test beds for Russian forces to fully integrate new capabilities into traditional military operations (White, 2018, 155).

[11] For a discussion on hybrid warfare Russian strategy, concepts and doctrine, see Renz and Smith (2016).

The attack on Estonia in 2007, that the government of Tallinn has equated to a conventional attack or an act of war (Hollis, 2007, 1025–1026; 1028), can be considered an "exercise" of the effectiveness of IW. The lack of specific provisions on cyberwarfare, as well as the difficulty in identifying the perpetrators with certainty, makes this option profitable for the perpetrators, with the Kremlin that easily denied any participation in the attacks against Estonia (Heickerö, 2010, 42, 50; Schreier, 2015, 79, 110).

In Summer 2008 hundreds of government and corporate websites in another Baltic state, Lithuania were hacked by Russian nationalists nostalgic for the Soviet era (Schreier, 2015, 111). Kyrgyzstan suffered a similar cyberattack in January 2009, in which the Russian authorities denied any involvement (Schreier, 2015, 113). Until then, just non-kinetic actions.

Schreier (2015, 23–24) infers that IO are a good strategic viaticum, but at operational-tactical level they are not enough to achieve conflict resolution. Accordingly, Russia made a quantum leap one year later, when Georgia was the first country to experiment the combination of IO and PSYOP with traditional kinetic attacks (Heickerö, 2010, 43, 46; Schreier, 2015, 112; Blank, 2017, 88–89; Iasiello, 2017, 52; Gorkowski, 2018, 22). IO against Georgia were part of a "coordinated and synchronized kinetic and non-kinetic campaign" which appeared to be orchestrated with military and political operations (Murphy, 2010, 95).

After the war in Georgia, Moscow was forced to rethink how to conduct IO and adjusted its strategy 6 years later against Ukraine (Müür et al., 2016, 33; Iasiello, 2017, 51, 54, 59) when the Russian Federation conducted (dis)information operations to influence the audience and to destabilize entire communities and districts (Boyte, 2017, 93). The RF made extensive use of IIO to regain dominance in the Black Sea region (Darczewska, 2014; Giles, 2016b; Anastasov, 2018). Moscow reshaped its strategic influence in Crimea and Georgia by creating a hybrid approach to conventional warfare that makes a large use of strategic IO (Hatch, 2019, 69; Iasiello, 2017, 55).

Russia has been using an advanced form of hybrid warfare in Ukraine since early 2014 that relies heavily on an element of IW (Snegovaya, 2015, 7). In Ukraine, the Russian hybrid warfare was characterized by a mix of IO and PSYOP carried out jointly and integrated with military operations (Müür et al., 2016: 28–29; Renz & Smith, 2016, 22–23; Sazonov, 2017, 75; Sazonov & Müür, 2017, 11; Beehner et al., 2018: 42). In Crimea the RF combined a variety of means and tactics—military and irregular forces, IO and CO (Scheipers, 2016, 47)—but IO and PSYOP played a key role and were more important than the use of conventional means (Renz & Smith, 2016, 11).

IO were used to blanket covert operations (Giles, 2016a, 6; Kofman et al., 2017). From case to case the Russian Federation used military force openly or unofficially, like the military support offered to separatists (Kivirähk et al., 2009; Kofman et al., 2017, 55 et seq.; Sazonov, 2017, 75) but the open intervention in Eastern Ukraine in August 2014 transformed the nature of the conflict from hybrid war into a conventional, but limited, interstate conflict (Rácz, 2015, 14, 67, 73–4; Kofman et al., 2017, 2).

A report released in May 2019 by CNA, a non-profit research and analysis organization located in Arlington, VA, argues that Russia turned its attention to unconventional warfare by supplementing its conventional forces with proxies and mercenaries and conducting influence operations in Ukraine via proxies from the Donbass region (Graja, 2019, 11), even if these strategy and techniques have resulted employed less successfully in Eastern Ukraine (Tabansky, 2017, 26). The report concludes that, in doing so, Moscow is moving away from conventional battlefield operations.[12]

Distinguishing kinetic operations from IO or IW, like in Georgia and Ukraine, is virtually impossible: in the Russian strategy they are fully integrated in military operations (Giles, 2016a, 68, b, 4, 15; Blank, 2017, 81–82). In Ukraine the RF combined lawfare with kinetic and non-kinetic means to achieve its objectives, manipulating international law and using it as a weapon (Värk, 2017, 46). Information warfare is deemed to be convenient for Russia, as it remains below the threshold of conventional war and therefore it does not trigger a military response (Thomas, 1996b, 29; Giles, 2016a, 5; Gorkowski, 2018, 23).

Although Moscow won the battle on the field, the information war in Georgia was not successful (Heickerö, 2010, 50; Giles, 2016b, 4; Müür et al., 2016, 33; Iasiello, 2017, 52, 54, 59). As the result of the new strategy tested in Estonia and Georgia, the RF increased the use of social media to support military offenses in hybrid warfare (Boyte, 2017, 93). After the intervention in Crimea the Kremlin undertook measures to destabilize the compact Russian-speaking Eastern Ukrainian regions using, inter alia, IO, PSYOP, and CO (Sazonov et al., 2016, 10; Sazonov & Mölder, 2017, 30). Crimea has been assessed to be the only "completely successful case" of hybrid war conducted by the RF, even if unexpected (Renz & Smith, 2016, 2), being Eastern Ukraine a "partially successful case" (Rácz, 2015, 73). Kofman et al. (2017, 26) believes that the Russian information campaign in Crimea was not planned in advance, had several shortcomings and eventually was "of little influence".

Anyhow, the Russian global influence campaign through Internet and social media has been assessed to be the most successful in history (Hatch, 2019, 69). IO in Georgia and Ukraine marked a turning point in the use of IW within Russian traditional military activities (Giles, 2016a, 35). Has been reported (Iasiello, 2017, 61; Bakshi, 2018, 181) that, following the success of its IIO, the Russian military is expected to make a greater use of coordinated EW and PSYOP in the future, even if some scholars (Rácz, 2015, 90) believe that Russia can make a limited resort to hybrid warfare. Is therefore questioned whether the successful operation in Crimea can be repeated elsewhere in the former Soviet republics (Kofman et al., 2017, 74–76); Russia's operations in the peninsula benefited from a series of highly favourable circumstances that makes it difficult to replicate: political, historical, geographical (the proximity of Crimea to Russia), linguistic and military advantages.

[12] The collective volume *The Crisis in Ukraine and Information Operations of the Russian Federation*, edited in 2016 by Sazonov et al. provides a wide-ranging discussion on the attempts of the RF to control the neighbouring territories and analyses the information warfare and hybrid war in the context of the Ukrainian-Russian conflict.

## 4 The Nationalist Discourse and the Pro-Russia Narrative

The Russian speech blew over nationalism in Moldova, Georgia, and Ukraine (Popa, 2019, 347–348) where Moscow maintains military bases and troops in the occupied territories (NATO, 2018) to keep up the pressure on those countries (Blank, 2017, 87; 88). Indeed, the fear of a new intervention of the Russian soldiers in defence of Abkhazia proved successful in forcing the government of Tbilisi to step back from collaboration with NATO (Blank, 2017, 90; Popa, 2019, 360) and is perceived as a threat by the Baltic states (Winnerstig, 2014, 11). In Moldova and Armenia, the RF may be unlikely engaged in a hybrid war due to the lack of direct border, and hence the small Russian bases far away from mainland are not suitable for supporting the military like in Ukraine and Georgia (Rácz, 2015, 90). Nevertheless, the Russian support of separatism in Transnistria indicates the desire of the Kremlin to play an important role in events in Moldova (Kivirähk et al., 2009, 13). Eventually, the Kremlin took advantage of the conflict that re-flamed in Fall 2020 in Nagorno-Karabakh between Armenia and Azerbaijan to deploy a peacekeeping force of about 2,000 servicemen in the region and thereby increasing its influence in the region.

The use of media to impact society, national ethnic, or religious groups is a distinctive characteristic of IW (Wetoszka, 2016, 55). Hybrid warfare aims non only to traditional political and material objectives, but also as symbolic ones (Bishop & Goldman, 2003, 115). Information operations are not limited to the military context but form part of a broader strategy to exert power over adversaries by putting in place coercive economic means or exploiting ethnic, linguistic, regional, religious, and social tensions in society (Pamment et al., 2018). The Russian information strategy aims to lead to a climate of confusion among the masses of the target state and perpetuates distrust in the government and political system, in an attempt to subvert local authorities (Blank, 2017). If we reverse the reasoning of Bishop and Goldman (2003, 120) we can infer that information can facilitate inflammatory nationalist rhetoric and ethnic clashes.

An early report prepared in 1996 by RAND for the Office of the Secretary of Defence warns that the Russian IW effort increased that year as a strong "nationalist regime" came to power in Moscow and moved to consolidate influence in the near abroad (Molander et al., 1996, 5). In the post-Soviet linguistic tradition, the term "nation", as well as its derivative concept "national identity", has strong ethnic connotations (Pakhomenko & Tryma, 2016, 43). The conflicts between breakaway territories in former Soviet Union republics are rooted in the incorporation of Russian-speaking nationalities, which enjoyed a certain autonomy within the USSR, in ethnically, linguistically, and culturally different states (Marsili, 2016, 162, 163). To fill the vacuum caused by the breakup of the USSR, the Russian government committed itself to build a new national identity that puts together the many ethnic, religious, and national communities that once were incorporated into the Soviet state (Darczewska, 2014, 33; Sakwa, 2006, 412–6).

The Moscow authorities developed therefore a narrative that relies on belonging to the "glorious" Soviet era and therefore to Russia as a nation-state, thus creating

a common historical narrative (Breslauer & Dale, 1997, 315–17; Winnerstig, 2014, 143; Darczewska, 2015, 34–35; Sazonov et al., 2016, 11; Mölder, 2016, 105; Kofman et al., 2017, 80–81; Sazonov et al., 2017a, b, 55; Beehner et al., 2018, 31).

The RF uses national identity as a propaganda tool (Pakhomenko & Tryma, 2016). Indeed, the *Information Security Doctrine* (2000) discusses also how to strengthen national identity and preserve the cultural heritage to develop shared moral values, patriotism for the sake of the motherland (Heickerö, 2010, 18; Darczewska, 2015, 20, 24). Information operations orchestrated by Moscow, whether they are in the service of a conventional military attack or not, target extra-territorial Russian-speaking population (Kivirähk et al., 2009, 41 et seq.; Iasiello, 2017, 54; Beehner et al., 2018, 32) but they are successful only where there is a strong pro-Russia sentiment Renz and Smith (2016, 6).

Russian state and non-state actors have exploited history, culture, language, and nationalism (Giles, 2016b, 2) that seems to be the motivation that in Summer 2008 drove Russian patriotic hackers to perpetrate cyber-attacks against hundreds of government and corporate websites in Lithuania (Schreier, 2015, 111), Georgia and later in Ukraine (Cordey, 2019, 22).

In the Baltic region the Kremlin fully supported a strategy aimed not only to promote the Russian-speaking minorities in the area but also to undermine the local institutions (Winnerstig, 2014, 11, 142). The ethno-nationalist discourse supported by IO was experimented in Estonia in 2007 (Heickerö, 2010, 5; Hollis, 2007, 1024) with the goal to influence the "not friendly" government of Tallinn (Blank, 2017, 85–86). The complaint that the Russian population Estonia is discriminated (Kivirähk et al., 2009, 51, 141 et seq.) serves as excuse for a "fair and just" intervention to protect the Russian compatriots living in these countries but was not successful to warm the situation to the point of triggering military intervention like in Ukraine (Blank, 2017, 86). The FOI report concludes that in the Baltic region the Russian influence strategy that relies on cultural and linguistic the ties with the motherland was a flop (Winnerstig, 2014, 12, 143). The failure is due to integration and cultural policies that the three Baltic states have directed at their own minorities, especially in Estonia but also in Latvia and Lithuania.

The massive presence of ethnic Russian minorities in the target country, such as Ukraine, who are not completely satisfied with their treatment by the central government, is a precondition for a successful hybrid offensive (Rácz, 2015, 89; Kivirähk et al., 2009, 275; Kofman et al., 2017, 20). In the context of the Russo-Ukrainian confrontation IO were used to disorganize governance, organize anti-government protests, delude adversaries, influence public opinion, and reduce an opponent's will to resist (Jaitner, 2015, 89).

According to some observers (Hudson, 2015, 334; Malyarenko & Wolff, 2018) the reasons of the tensions between Kiev and Moscow reside in logic of competitive influence-seeking that the latter considers as the opportunity for a re-integration. Other analysts (Darczewska, 2014, 33; Wetoszka, 2016, 63; Herb & Kaplan, 2017) argue that the annexation of Crimea follows the political ambitions of the Kremlin

but also comes from a multifaceted Russian nationalism.[13] Ukraine has always been an essential part of narratives related to Russian nation-building, at the extent that the exit of Kiev from the geopolitical sphere of influence of the Moscow was perceived by Russia as its major geopolitical defeat, a catastrophe (Müür et al., 2016, 30–31; Kofman et al., 2017, 1).

In Ukraine, the Kremlin build a cultural narrative, targeting pro-Russian, that goes far beyond a simple ethno-national narrative, including native language and religious discourse (Hudson, 2015) and selects not just Russian citizens but the entire Russian-speaking population of the planet (Darczewska, 2015, 13; Jaitner, 2015, 92; Vilson, 2016, 120–121; Kofman et al., 2017, 81). The concept of Russian identity is multi-ethnic and international (Riistan, 2016, 220) and the so-called "compatriots' policy" supports all Russian-speaking people outside the motherland, thus emphasizing on language rather than ethnicity (Winnerstig, 2014, 142).

Ethnic or separatism and language-related elements have been present both in Crimea and in the Donbass (Rácz, 2015, 78, 80; Riistan, 2016, 222). The same name *Novorossiya* (New Russia), an historical region of the Russian Empire which now identifies a confederation of the self-proclaimed Donetsk People's Republic and Luhansk People's Republic, reveals the nationalism that underlies the conflict in Easter Ukraine (Marsili, 2016, 163, 170; Pakhomenko & Tryma, 2016, 45–46; Kofman et al., 2017, 51–54). In an attempt to legitimize the Russian intervention in the Donbas, propagandists sought to characterize the participation in the conflict in terms of language, culture, history, as a support to protect the just claims of the ethnic Russian separatists (Pakhomenko & Tryma, 2016, 52; Kofman et al., 2017: 49; Sazonov, 2017, 75; Popa, 2019, 349; Tashev et al., 2019, 130).

Russia's actions in its near abroad include the protection of Russian-speaking minorities through information and soft power means (Kivirähk et al., 2009, 13; Winnerstig, 2014, 11–12). Indeed, Moscow's military intervention in Georgia was justified as a defence of Russian citizens in South Ossetia (Kivirähk et al., 2009, 13). The Kremlin pushed on information to make believe that the intervention in Crimea and Eastern Ukraine was necessary to protect ethnic Russians and Russian native speakers (Renz & Smith, 2016, 6; Iasiello, 2017, 56; Kofman et al., 2017, 21; Värk, 2017, 46). The Russian language was used to keep cultural and emotional links with the fatherland and contributed to the successful of the operation (Darczewska, 2014, 34; Kofman et al., 2017, 16, 49–50). From this perspective, Eriksson (1999, 58) finds that IW tools are "weapons of *cultural* disruption".

During the secession of Crimea, local ethno-nationalists used the periphrasis "Russia's Kosovo" to underline the parallel with the independence of Pristina from Belgrade and the reasons underpinning (Blakkisrud & Kolstø, 2017). To legitimize their claims to Crimea, the authorities of Moscow presented the annexation with a national irredentist terminology, using ethno-lingual or ethno-cultural terms (Teper, 2016). The Ukranian experience proved to be so successful in mobilizing pro-Russian

[13] For a discussion on the direct impact of nationalism on the likelihood of disputes, see Ciorciari and Chen Weiss (2016).

sentiment that it becomes a landmark for future influence operations (Kalpokas, 2017, 53).

Information operations have blown nationalism, and created the political (and pseudo-legal) conditions for Russia's intervention beyond its borders, to the extent that Italy's interior minister and deputy Prime Minister, Matteo Salvini, head of the right-wing League party, backed the annexation of Crimea, due to the fact that there are "some historically Russian zones with Russian culture and traditions which legitimately belong to the Russian Federation" (Weymouth, 2018)—the Kremlin portrayed Crimea as being historically belonged to Russia (Kofman et al., 2017, 28, 52; Sazonov et al., 2017a, b, 57–58; Beehner et al., 2018, 40).

Kalpokas (2017, 53) has summarized effectively the Ukraine conflict characterizing it not only as a kinetic action, but also as a "battle of narratives". Much of the work produced in the area of IW is concerned with descriptive narrative (Martinus, 2001, 12), no matter whether it is truthful, and IO are intended to reinforce these narratives (Zhaohong, 2016, 49). As its IW strategy has proven successful, the RF is making an extensive use aggressive narrative to support the legitimacy of its Arctic sovereignty claims (Darczewska, 2015, 35; Carr, 2019) and is likely that the Kremlin will continue to make extensive use of this strategy in the conduct of its foreign policy.

## 5 Conclusions

Information superiority is considered essential to achieving victory on the physical battlefield in modern war. Information operations, for which it is difficult to attribute responsibility and which are not specifically regulated by international law, fall below the threshold of armed conflict and are convenient to be used to destabilize a government or to try to legitimize a (unlawful) action.

The Kremlin has developed information capabilities, clustered under the umbrella concept of "hybrid warfare", that make a fundamental contribution to accomplish foreign policy goals. Disinformation, propaganda, and cyber capabilities have been employed in Russian influence campaigns to support a new nationalist ideology. The Russian strategy makes a large use of media outlets to inspire nationalist Russian sentiment and identify loyalists and supporters.

Through flag propaganda operations, the Russian Federation has caused political instability and poisoned bordering countries with the purpose to regain regional dominance and counteract the enlargement of Western powers. It is expected that Moscow will continue to use this strategy that, so far, was successful to weaken neighbouring nations and increase its regional influence.

To be effective the hybrid strategy of Moscow, which makes extensive use of information and psychological operations, requires a combination of favourable circumstances: the presence of ethnic Russian and Russian-speaking population on foreign soil and the border with Russia, that is necessary for military intervention. Without

both requirements Moscow's strategy is ineffective and represents neither a deterrent nor a real threat.

**Acknowledgements** The author gratefully acknowledges the European Social Fund (ESF) and the Fundação para a Ciência e a Tecnologia (FCT), Portugal, for supporting this work through grant SFRH/BD/136170/2018.

## References

Ajir, M., & Vailliant, B. (2018). Russian information warfare: Implications for deterrence theory. *Strategic Studies Quarterly, 12*(3), 70–89.

Anastasov, P. (2018). The Black Sea Region: A Critical Intersection. NATO Review. Retrieved May 18, 2020, from https://www.nato.int/docu/review/2018/Also-in-2018/the-black-sea-region-a-critical-intersection-nato-security/EN/index.htm.

Andregg, M. (2019). Ultimate causes of wars (long-term, strategic causes) and differing roles for intelligence practitioners, academics, and policy makers. *Romanian Intelligence Studies Review, 19–20*(2018), 237–256.

Armitage, R. L., & Nye, J. S. (2007). *CSIS commission on smart power: A smarter, more secure America*. Washington, DC: CSIS Press.

Arold, U. (2016). Peculiarities of Russian information operations. *Sõjateadlane, 2,* 16–40.

Aspin, L. (1994). Annual Report to the President and the Congress. Washington, DC, Government Publishing Office.

Bakshi, B. (2018). Information warfare: Concepts and components. *International Journal of Research and Analytical Reviews, 5*(4), 178–185.

Beehner, L. M., Collins, L. S., & Person, R. T. (2018). The fog of Russian information warfare. In M. D. Vertuli & B. S. Loudon (Eds.), *Perceptions are reality: Historical case studies of information operations in large-scale combat operations* (pp. 31–50). Fort Leavenworth, KS: Army University Press.

Bishop, M., & Goldman, E. O. (2003). The strategy and tactics of information warfare. *Contemporary Security Policy, 24,* 113–139.

Blakkisrud, H., & Kolstø, P. (2017). Stavropol as "Russia's Kosovo"? Nationalist mobilization and public response in a Russian region. *Post-Soviet Affairs, 33*(5), 370–388. https://doi.org/10.1080/1060586X.2017.1355716.

Blank, S. (2017). Cyber war and information War à la Russe. In G. Perkovich & A. E. Levite (Eds.), *Understanding cyber conflict: Fourteen analogies* (pp. 81–98). Washington, DC: Georgetown University Press.

Boyte, K. J. (2017). An analysis of the social-media technology, tactics, and narratives used to control. Perception in the propaganda war over Ukraine. *Journal of Information Warfare, 16*(1), 88–111.

Brangetto, P., & Veenendaal, M. A. (2016). Influence cyber operations: The use of cyberattacks in support of influence operations. In N. Pissanidis, H. Rõigas, & M. Veenendaal (Eds.), *8th International Conference on Cyber Conflict* (pp. 113–126). Tallinn: NATO CCD COE. http://dx.doi.org/10.1109/CYCON.2016.7529430.

Breslauer, G., & Dale, C. (1997). Boris Yel'tsin and the invention of a Russian nation-state. *Post-Soviet Affairs, 13*(4), 303–332.

Carr, H. (2019). Arctic sovereignty and information warfare. *The Three Swords Magazine, 34,* 83–89.

Charles, K. B. (2016). Russia's indirect and asymmetric methods as a response to the new western way of war. *Special Operations Journal, 2*(1), 1–11.

Chekinov, S. G., & Bogdanov, S. A. (2013). The nature and content of a new-generation war. *Military Thought, 4*.

Cilluffo, F. J., & Gergely, C. H. (1997). Information warfare and strategic terrorism. *Terrorism and Political Violence, 9*(1), 84–94.

Ciorciari, J. C., & Chen Weiss, J. (2016). Nationalist protests, government responses, and the risk of escalation in interstate disputes. *Security Studies, 25*(3), 546–583. https://doi.org/10.1080/09636412.2016.1195633.

Cohen, D., & Bar'el, O. (2017). *The use of cyberwarfare in influence operations.* Tel Aviv: Yuval Ne'eman Workshop for Science, Technology and Security Tel Aviv University.

Cordey, S. (2019). *Cyber influence operations: An overview and comparative analysis.* Zurich: Center for Security Studies (CSS), ETH Zurich. Retrieved May 18, 2020, from https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-10-CyberInfluence.pdf.

Creţu, V., & Ardeleanu, D. (2019). The revival of the Intermarium geopolitical project—The Three Seas Initiative and Bucharest 9 Format. *Romanian Intelligence Studies Review, 19–20*(2018), 331–344.

Cullen, P. J., & Reichborn-Kjennerud, E. (2017). Understanding Hybrid Warfare. Multinational Capability Development Campaign (MCDC): Countering Hybrid Warfare Project. Retrieved August 10, 2010, from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf.

Darczewska, J. (2014). *The anatomy of Russian information warfare. The Crimean operation, a case study* (OSW Point of View No. 42). Warsaw: Ośrodek Studiów Wschodnich im. Marka Karpia/Centre for Eastern Studies. Retrieved May 18, 2020, from https://www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_information_warfare.pdf.

Darczewska, J. (2015). *The devil is in the details. Information warfare in the light of Russia's military doctrine* (OSW Point of View No. 50). Warsaw: Ośrodek Studiów Wschodnich im. Marka Karpia/Centre for Eastern Studies. Retrieved May 13, 2020, from https://www.files.ethz.ch/isn/191967/pw_50_ang_the-devil-is-in_net.pdf.

Denning, D. E. (1999). *Information warfare and security.* New York, NY: Addison Wesley Longman.

EEAS. (2016a). Eastern Europe. Retrieved May 14, 2020, from https://eeas.europa.eu/regions/eastern-europe/341/eastern-europe_en.

EEAS. (2016b). Eastern Partnership. Retrieved May 14, 2020, from https://eeas.europa.eu/diplomatic-network/eastern-partnership/419/eastern-partnership_en.

Eriksson, E. A. (1999). Information warfare: Hype or reality? *The Nonproliferation Review* (Spring-Summer) 57–64.

Fabian, S. (2019). The Russian hybrid warfare strategy—Neither Russian nor strategy. *Defense and Security Analysis, 35*(3), 308–325. https://doi.org/10.1080/14751798.2019.1640424.

Fridman, O. (2018). *Russian "hybrid warfare": Resurgence and politicization.* London: Hurst and Company.

Giles, K. (2016a). *Handbook of Russian information warfare* (Fellowship Monograph 9). Rome: NATO Defense College. Retrieved May 18, 2020, from http://www.ndc.nato.int/news/news.php?icode=995.

Giles, K. (2016b). *The next phase of Russian information warfare.* Riga: NATO Strategic Communications Centre of Excellence. Retrieved May 18, 2020, from https://www.stratcomcoe.org/next-phase-russian-information-warfare-keir-giles.

Godson, R., & Wirtz, J. J. (Eds.). (2002). *Strategic denial and deception: The twenty-first century challenge.* New Brunswick: Transaction Publishers.

Gorkowski, J. B. (2018). US information operations in large-scale combat operations: Challenges and implications for the future force. In M. D. Vertuli & B. S. Loudon (Eds.), *Perceptions are reality: Historical case studies of information operations in large-scale combat operations* (pp. 17–30). Fort Leavenworth, KS: Army University Press.

Graja, C. (2019). *SOF and the future of global competition.* Arlington, VA: CNA. Retrieved May 13, 2020, from https://www.cna.org/CNA_files/PDF/DCP-2019-U-020033-Final.pdf.

Gruffydd-Jones, J. (2017). Dangerous days: The impact of nationalism on interstate conflict. *Security Studies, 26*(4), 698–728. https://doi.org/10.1080/09636412.2017.1336393.

Hatch, B. (2019). The future of strategic information and cyber-enabled information operations. *Journal of Strategic Security, 12*(4), 69–89. https://doi.org/10.5038/1944-0472.12.4.1735.

Heickerö, R. (2010). *Emerging cyber threats and Russian views on information warfare and information operations* (Report No. FOI-R–2970—SE). Stockholm: FOI, Swedish Defence Research Agency. Retrieved September 7, 2020, from https://www.foi.se/rest-api/report/FOI-R–2970–SE.

Herb, G. H., & Kaplan, D. H. (2017). *Scaling identities: Nationalism and territoriality*. Lanham, MD: Rowman and Littlefield.

Hildreth, S. A. (2001). *Cyberwarfare* (CRS Report RL30735). Washington, DC: Congressional Research Service. Retrieved July 15, 2020, from https://www.hsdl.org/?viewanddid=123.

Hoffman, F. G. (2007). *Conflict in the 21st century: The rise of hybrid war*. Arlington, VA: Potomac Institute for Policy Studies. Retrieved May 18, 2020, from https://potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf.

Hollis, D. B. (2007). Why states need an international law for information operations. *Lewis and Clark Law Review, 11*(4), 1023–1061.

Hudson, V. (2015). Forced to friendship? Russian (mis-)understandings of soft power and the implications for audience attraction in Ukraine. *Politics, 35*(3), 330–346. https://doi.org/10.1111/1467-9256.12106.

Hutchinson, W. (2006). Information warfare and deception. *Informing Science, 9,* 213–223.

Iasiello, E. J. (2017). Russia's improved information operations: From Georgia to Crimea. *Parameters, 47*(2), 51–63.

Jaitner, M. (2015). Russian information warfare: Lessons from Ukraine. In K. Geers (Ed.), *Cyber war in perspective: Russian aggression against Ukraine* (pp. 87–94). Tallinn: NATO CCDCOE. Retrieved July 16, 2020, from https://ccdcoe.org/uploads/2018/10/CyberWarinPerspective_full_book.pdf.

Jensen, R. M. (1997). *Information war power: Lessons from air power* (P-97-2). Cambridge, MA: Program on Information Resources Policy, Harvard University, Center for Information Policy Research. Retrieved May 13, 2020, from http://www.pirp.harvard.edu/pubs_pdf/jensen/jensen-p97-2.pdf.

Johnson, S. L. (1997). Major intelligence challenge: Toward a functional model of information warfare. *Studies in Intelligence, 1*(1), 49–56.

Jones, A. (1999). Information warfare—What it is? *Information Security Technical Report, 4*(3), 12–19.

Jowett, G. S., & O'Donnell, V. (2012). *Propaganda and persuasion* (5th ed.). London: Sage Publications.

Kalpokas, I. (2017). Information warfare on social media: A brand management perspective. *Baltic Journal of Law and Politics, 10*(1), 35–62. https://doi.org/10.1515/bjlp-2017-0002.

Kanet, R. E. (2011). From the "new world order" to "resetting relations": Two decades of US–Russian relations. In R. E. Kanet (Ed.), *Russian foreign policy in the 21st century* (pp. 204–227). London: Palgrave Macmillan. https://doi.org/10.1057/9780230293168.

Khan, K. (2013). Understanding information warfare and its relevance to Pakistan. *Strategic Studies, 32–33*(4 and 1), 138–159. Retrieved May 13, 2020, from http://issi.org.pk/wp-content/uploads/2014/06/1379480610_58047454.pdf.

Kivirähk, J., Maliukevičius, N., Yeremeev, O., et al. (2009). *The 'humanitarian dimension' of Russian foreign policy towards Georgia, Moldova, Ukraine and the Baltic states* (2nd ed.). Riga: Centre for East European Policy Studies. Retrieved September 14, 2020, from https://er.nau.edu.ua/bitstream/NAU/24661/1/The%20"Humanitarian%20Dimension"%20of%20Russian%20Foreign%20policy%20Toward%20Georgia%2c.PDF.

Kofman, M., Migacheva, K., Nichiporuk, B., et al. (2017). *Lessons from Russia's operations in Crimea and Eastern Ukraine* (RR-1498-A). Santa Monica, CA: RAND Corporation. https://doi.org/10.7249/RR1498.

Kuehl, D. T. (2002). Information operations, information warfare, and computer network attack: Their relationship to national security in the information age. *International Law Studies, 76,* 35–58.

Lanoszka, A. (2016). Russian hybrid warfare and extended deterrence in Eastern Europe. *International Affairs, 92*(1), 175–195. https://doi.org/10.1111/1468-2346.12509.

Larson, E. V., Darilek, R. E., Gibran, D., et al. (2009). *Foundations of effective influence operations: A framework for enhancing army capabilities* (MG-654-A). Santa Monica, CA: RAND Corporation.

Libicki, M. C. (2007). *Conquest in cyberspace: National security and information warfare*. New York, NY: Cambridge University Press.

Lord, C., & Barnett, K. R. (Eds.). (1988). *Political warfare and psychological operations: Rethinking the US approach*. New York, NY: National Strategy Information Center. Retrieved May 19, 2020, from https://www.files.ethz.ch/isn/139664/1989-01_Political_Warfare_8-Chap.pdf.

Malyarenko, T., & Wolff, S. (2018). *The dynamics of emerging de-facto states: Eastern Ukraine in the post-Soviet space.* Abingdon: Routledge.

Marsili, M. (2015). Propaganda and International Relations: An Outlook in Wartime. Vozes dos Vales, 7 (pp. 1–38). https://doi.org/10.5281/zenodo.32424. Reprinted in ArtCiencia.com, 19 (pp. 1–26). https://doi.org/10.25770/artc.11095.

Marsili, M. (2016). The birth of a (fake?) Nation at the aftermath of the decomposition of USSR. The unsolved issue of post-Soviet 'frozen conflicts'. *Proelium, 7*(10), 167–174. http://doi.org/10.5281/zenodo.44945.

Marsili, M. (2019). The war on cyberterrorism. *Democracy and Security, 15*(2), 172–199. https://doi.org/10.1080/17419166.2018.1496826.

Marsili, M. (2020). An update of democracy's third wave. *Political Reflection, 6*(1), 44–48. https://doi.org/10.5281/zenodo.3626970.

Martinus, I. (2001). Small business in the new battlefield: Government attempts at providing a secure environment. In W. Hutchinson, M. Warren, & J. Burn (Eds.), *Survival in the e-conomy: 2nd Australian Information Warfare and Security Conference 2001* (pp. 12–20). Churchlands, Australia: School of Management Information Systems, Edith Cowan University. https://ro.ecu.edu.au/ecuworks/6758.

Meister, S. (2016). The "Lisa case": Germany as a Target of Russian Disinformation. NATO Review. Retrieved July 15, 2020, from https://www.nato.int/docu/review/articles/2016/07/25/the-lisa-case-germany-as-a-target-of-russian-disinformation/index.html.

Merrick, K., Hardhienata, M., Shafi, K., & Hu, J. (2016). A survey of game theoretic approaches to modelling decision-making in information warfare scenarios. *Future Internet, 8*(34). https://doi.org/10.3390/fi8030034.

McGovern, E. A. (Ed.). (2003). Military Intelligence Professional Bulletin, 29(3).

Molander, R. C., Riddile, A. S., & Wilson, P. A. (1996). *Strategic information warfare: A new face of war (MR-661-OSD).* Santa Monica, CA: RAND Corporation. https://doi.org/10.7249/MR661.

Mölder, H. (2016). The war of narratives—Putin's challenge to international security governance in Ukraine. *Sõjateadlane, 2,* 88–113.

Murphy, D. M. (2010). Attack or defend? Leveraging information and balancing risk in cyberspace. *Military Review* 88–96.

Müür, K., Mölder, H., Sazonov, V., & Pruulmann-Vengerfeldt, P. (2016). Russian information operations against the Ukrainian state and defence forces: April-December 2014 in online news. *Journal on Baltic Security, 2*(1), 28–71. https://doi.org/10.1515/jobs-2016-0029.

NATO. (2018, July). Russia's top five myths about NATO. Factsheet. Retrieved May 19, 2020, from https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_07/20180702_1807-russia-top5-myths-en.pdf.

NATO. (2020a). Partners. Retrieved May 19, 2020, from https://www.nato.int/cps/en/natohq/51288.htm.

NATO. (2020b, March). NATO-Russia Relations: The Background. Media Backgrounder. Retrieved May 19, 2020, from https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/2003-NATO-Russia_en.pdf.

Pakhomenko, S., & Tryma, C. (2016). Identity and propaganda in Russian-Ukrainian hybrid warfare. *Sõjateadlane, 2,* 42–53.

Pamment, P., Nothhaft, H., Agardh-Twetman, H., & Fjällhed, A. (2018). *Countering information influence activities: The state of the art*. Lund: Lund University.

Pompeo, M. R. (2020, July 22). Message on the 80th Anniversary of the Welles Declaration. Retrieved July 23, 2020, from https://www.state.gov/message-on-the-80th-anniversary-of-the-welles-declaration.

Popa A. V. (2019). Reconfiguring the balance of power in the wider Black Sea region: the Romanian proposal for an allied naval cooperation. *Romanian Intelligence Studies Review, 19–20*, 345–374 (2018).

Porche, I. R., Paul, C., York, M., et al. (2013). *Redefining information warfare boundaries for an army in a wireless world* (MG-1113-A). Santa Monica, CA: RAND Corporation. Retrieved May 18, 2020, from https://apps.dtic.mil/dtic/tr/fulltext/u2/a575268.pdf.

Rácz, A. (2015). *Russia's hybrid war in Ukraine: Breaking the enemy's ability to resist* (FIIA Report 43). Helsinki: Finnish Institute of International Affairs. Retrieved July 16, 2020, from https://www.fiia.fi/wp-content/uploads/2017/01/fiiareport43.pdf.

RAND Corporation. (n.d.). Information Operations. Retrieved May 18, 2020, from https://www.rand.org/topics/information-operations.html.

Renz, B., & Smith, H. (Eds.) (2016). *Russia and hybrid warfare—Going beyond the label* (Aleksanteri Papers No. 1/2016). Helsinki: Kikimora. Retrieved May 19, 2020, from https://helda.helsinki.fi//bitstream/handle/10138/175291/renz_smith_russia_and_hybrid_warfare.pdf?sequence=1.

Riistan, A. (2016). The Moscow patriarchate and the conflict in Ukraine. *Sõjateadlane, 2,* 206–231.

Rugge, F. (2018). "Mind Hacking": Information Warfare in the Cyber Age (ISPI Analysis No. 319). Retrieved May 13, 2020, from https://www.ispionline.it/sites/default/files/pubblicazioni/analisi319_rugge_11.01.2018_2.pdf.

Russian Federation. (2000). Russian Federation Armed Forces' Information Space Activities Concept, approved by the President of the Russian Federation on 9 September 2000. Retrieved July 17, 2020, from https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle.

Russian Ministry of Defense. (2011). Conceptual Views on the Activity of the Armed Forces of the Russian Federation in Information Space. Retrieved July 17, 2020, from http://www.pircenter.org/media/content/files/9/13480921870.pdf.

Sakwa, R. (2006). Nations and nationalism in Russia. In G. Delanty & K. Kumar (Eds.), *The SAGE handbook of nations and nationalism.* London: SAGE.

Sazonov, V. (2017). In V. Sazonov et al. (Eds.), *Conclusion: The Russian information operations in 2014–2015* (pp. 75–76).

Sazonov, V., Mölder, H., Müür, K., et al. (Eds.). (2017a). *Russian information operations against Ukrainian armed forces and Ukrainian countermeasures (2014–2015)*, ENDC Occasional Papers, 6. Tartu: Estonian National Defence College.

Sazonov, V., Müür, K., & Kopõtin, I. (2017b). In V. Sazonov et al. (Eds.), *Methods and tools of Russian information operations used against Ukrainian armed forces: The assessments of Ukrainian experts* (pp. 52–66).

Sazonov, V., & Müür, K. (2017). In V. Sazonov et al. (Eds.), *Introduction: Russian hybrid and information warfare* (pp. 9–12).

Sazonov, V., & Mölder, H. (2017). In V. Sazonov et al. (Eds.), *Why did Russia attack Ukraine?* (pp. 28–33).

Sazonov, V., Mölder, H., & Saumets, A. (2016). Introduction: The role of Russian information warfare. *Sõjateadlane, 2,* 7–12.

Scheipers, S. (2016). Winning wars without battles: Hybrid warfare and other 'indirect' approaches in the history of strategic thought. In B. Renz & H. Smith (Eds.), *Russia and hybrid warfare—Going beyond the label* (Aleksanteri Papers No. 1/2016) (pp. 47–51). Helsinki: Kikimora.

Schmidt-Felzmann, A. (2017). More than 'just' disinformation: Russia's information operations in the Nordic region. In T. Čižik (Ed.), *Information warfare. New security challenge for Europe* (pp. 32–67). Bratislava: Centre for European and North Atlantic Affairs.

Schreier, F. (2015). On Cyberwarfare. DCAF Horizon 2015 Working Paper No. 7. Geneva Centre for the Democratic Control of Armed Forces (DCAF). Retrieved May 13, 2020, from https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf.

Sliwa, Z. (2017). In V. Sazonov et al. (Eds.), *"Hybrid warfare"—The military security domain's considerations* (pp. 13–27).

Snegovaya, M. (2015). *Russia report 1—Putin's information warfare in Ukraine: Soviet origins of Russia's hybrid warfare.* Washington, DC: Institute for the Study of War. Retrieved August 10, 2020, from http://www.understandingwar.org/sites/default/files/Russian%20Report%201%20Putin%27s%20Information%20Warfare%20in%20Ukraine-%20Soviet%20Origins%20of%20Russias%20Hybrid%20Warfare.pdf.

Socor, V. (2018). NATO summit puts Black Sea strategy on hold for another year (part two). *Eurasia Daily Monitor, 15*(118). Retrieved May 19, 2020, from https://jamestown.org/program/nato-summit-puts-black-sea-strategy-on-hold-for-another-year-part-two.

Tabansky, L. (2017). *Cybered influence operations: Towards a scientific research agenda* (Security Policy Library SPL 2-17). Oslo: The Norwegian Atlantic Committee. Retrieved May 13, 2020, from https://www.atlanterhavskomiteen.no/files/dnak/Documents/SPL2-17.pdf.

Tashev, B., Purcell, M., & McLaughlin, B. (2019). Russia's information warfare. Exploring the cognitive dimension. *MCU Journal, 10*(2), 129–147. https://doi.org/10.21140/mcuj.2019100208.

Teper, Y. (2016). Official Russian identity discourse in light of the annexation of Crimea: National or imperial? *Post-Soviet Affairs, 32*(4), 378–396. https://doi.org/10.1080/1060586X.2015.1076959.

Theohary, C. A. (2018). *Information warfare: Issues for congress* (CRS Report No. R45142), Version 5 Updated. Washington, DC: Congressional Research Service. Retrieved May 13, 2020, from https://crsreports.congress.gov/product/pdf/R/R45142/5.

Theohary, C. A. (2020). *Defense primer: Information operations* (IF10771), Version 6 Updated 14 January 2020. Washington, DC: Congressional Research Service. Retrieved May 13, 2020, from https://crsreports.congress.gov/product/pdf/IF/IF10771.

Thomas, T. L. (1996a). Deterring information warfare: A new strategic challenge. *Parameters, 26*(4), 81–91.

Thomas, T. L. (1996b). Russian views on information-based warfare. *Airpower Journal* (Special Edition) 25–35.

Thomas, T. L. (2004). Russia's reflexive control theory and the military. *Journal of Slavic Studies, 17*(2), 237–256. https://doi.org/10.1080/13518040490450529.

Thompson, M. (2018). Information Warfare—A New Age? Speech at the iWar Five Eyes Principals Forum, 31 October–1 November 2018, Canberra. Retrieved May 13, 2020, from https://www.defence.gov.au/JCG/docs/Head_Information_Warfare-iWar_Five_Eyes_Principals_Forum_Speech-Canberra.pdf.

Tsymbal, V. I. (1995, September 12–14 ). Kontseptsiya "informatsionnoy voyny" (Concept of Information War). In *Speech at the Russian-U.S. Conference "Evolving Post-Cold War National Security Issues"*, held at the Russian Academy of Civil Service in Moscow.

U.S. Department of Defense. (2016). Strategy for Operations in the Information Environment. Retrieved May 13, 2020, from https://dod.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf.

U.S. Department of the Army. (1995). Military Operations Other Than War. In *Decisive force: The army in theater operations* (FM 100-7). Retrieved May 23, 2020, from https://www.hsdl.org/?viewanddid=437411.

UN General Assembly. (1998). Developments in the field of information and telecommunications in the context of international security (A/RES/53/70).

United Kingdom. Parliament. House of Commons. Digital, Culture, Media and Sport Committee. (2018, October 23). Disinformation and 'fake news': Interim Report: Government Response to the Committee's Fifth Report of Session 2017–19 (HC 1630 17/19). 5th Special Report of Session 2017–19. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1630/1630.pdf.

United Kingdom. Parliament. House of Commons. Digital, Culture, Media and Sport Committee. (2019, February 18). Disinformation and 'fake news': Final Report (HC 1791 17/19). 8th Report of Session 2017–19. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf.

Värk, R. (2017). In V. Sazonov et al. (Eds.), *Legal element of Russia's hybrid warfare* (pp. 45–51).

Vertuli, M. D., & Loudon, B. S. (Eds.) (2018). *Perceptions are reality: Historical case studies of information operations in large-scale combat operations*. Fort Leavenworth, KS: Army University Press. Retrieved May 13, 2020, from https://www.armyupress.army.mil/Portals/7/combat-studies-institute/csi-books/perceptions-are-reality-lsco-volume-7.pdf.

Vilson, M. (2016). The Europeanization of foreign policy. *Sõjateadlane, 2,* 113–140.

Wetoszka, A. (2016). An attempt to identify hybrid conflict. *Sõjateadlane, 2,* 54–75.

Weymouth, L. (2018, July 19). Italy has done a lot—Maybe too much. *The Washington Post*. Retrieved May 19, 2020, from https://wapo.st/2mvIgym?tid=ss_mailandutm_term=.3b7320fab8be.

White, W. P. (2018). The cyber crucible: Eastern Europe, Russia, and the development of modern warfare. In M. D. Vertuli & B. S. Loudon (Eds.), *Perceptions are reality: Historical case studies of information operations in large-scale combat operations* (pp. 151–162). Fort Leavenworth, KS: Army University Press.

Wilson, C. (2006). *Information operations and cyberwar: Capabilities and related policy issues* (CRS Report No. RL31787). Washington, DC: Congressional Research Service. Retrieved May 25, 2020, from https://fas.org/irp/crs/RL31787.pdf.

Wilson, E. J., III. (2008). Hard power, soft power, smart power. *ANNALS of the American Academy of Political and Social Sciences, 616*(1), 110–124. https://doi.org/10.1177/0002716207312618.

Winnerstig, M. (Ed.) (2014). *Tools of destabilization: Russian soft power and non-military influence in the Baltic states* (Report No. FOI-R–3990–SE). Stockholm: FOI, Swedish Defence Research Agency. Retrieved July 16, 2020, from https://www.stratcomcoe.org/mike-winnerstig-ed-tools-destabilization-russian-soft-power-and-non-military-influence-baltic-states.

Zhaohong, J. N. (2016). Information warfare—The challenges and opportunities for militaries in the information age. *Pointer, 42*(3), 49–57.

Zhou, V. (2020, March 23). Coronavirus barbs help nobody, China's Washington ambassador says after 'US army' tweets. *South China Morning Post*.