Russian scholarly discussions of nonmilitary warfare as securitizing acts

Markus Balázs Göransson

Department of War Studies and Military History, Swedish Defence University, Stockholm, Sweden

ABSTRACT
The article examines Russian scholarly discussion of nonmilitary warfare with reference to securitization theory. Focusing on three main concepts of nonmilitary warfare that have featured in the Russian scholarly military and security debate in recent years – information war, color revolutions and hybrid war – it shows that Russian scholarly discussion of nonmilitary warfare, as it has evolved over time, has cast a widening range of phenomena as potential security threats, implying the need for an expanded state response to meet these threats. The broadened Russian understanding of security has some parallels in Western security discussions. However, a crucial distinction is that the Russian discussion has remained wedded to strong statist notion of security and a preponderant Western enemy image.

Introduction
In recent years, Western scholars have paid increasing attention to Russian military theorizing, which comes after a lull in interest in the 1990s and early 2000s, when Russia’s military, having suffered a dramatic decline following the collapse of the Soviet Union, was viewed by many in the West as a bygone threat. With Moscow’s new military assertiveness on the world – which reached a peak with Russia’s full-scale invasion of Ukraine in February 2022 – Western thinkers are increasingly turning their sights to Russian theorizing about war.

Part of the recent Western discussions about Russian military thinking has focused on ideas of nonmilitary warfare. Much ink has been spilled on “hybrid warfare”, “New Generation Warfare”, “subversion war”, “information war” and other concepts that center on the potential use of nonmilitary means in contemporary warfare. Mark Galeotti, Bettina Renz, Ofer Fridman, Oscar Jonsson and Jānis Bērziņš are some of the Western scholars who have written about the growing focus on nonmilitary means in Russian military discussions. As Jonsson notes:

The traditional Russian understanding of the nature of war as defined by armed violence has broadened to include nonviolent means of information-psychological warfare and color revolutions, which are now seen to be so effective that they are equivalent to violence, blurring the boundaries of war and peace.
Russian ideas of nonmilitary warfare have often been considered from two vantage points. On the one hand, research has focused on the extent to which the new Russian ideas have marked a break in Russian military thought or, alternatively, if they follow on older Soviet thinking about warfare. On the other, it has considered whether the new ideas have been operationalized in recent Russian military practice, particularly in Russia’s takeover of Ukraine’s Crimean Peninsula and in its political warfare against the West. Much of the focus, in other words, has been placed on the ideational content of the Russian military discussions and its impact on Russian war fighting.

The present article considers the Russian scholarly discussion of nonmilitary warfare as a discourse, and specifically the manner in which it represents threats. How are nonmilitary phenomena, including foreign diplomacy, political instability, social protests, religious organizations, NGOs, epidemics and migration, represented as threats in Russian scholarly military discussions? How can we understand the process through which certain phenomena traditionally outside the military domain become discursively represented as state security threats? In considering these questions, the article draws on securitization theory, which addresses the linguistic processes through which phenomena become constructed as threats.

The article is divided into three parts. First, it discusses securitization theory as expounded by the Copenhagen School and its relevance for understanding Russian academic discussions of nonmilitary warfare. Then, it considers Russian academic discussions on nonmilitary warfare, focusing on three concepts that have been salient in Russian scholarly military discussions in recent years: information war [informat-sionnaya voyna], color revolutions [tsvetnye revol'yutsii] and hybrid warfare [gibridnaya voyna]. Lastly, it reflects on the findings, including the implications of the academic discourse on nonmilitary warfare for Russian security policy.

The article draws on a range of Russian books and journal articles that address the three concepts studied in this article. Among them are articles from the two flagship journals of Russian military studies, Voennaya Mysl’ [Military Thought] and Vestnik Akademii Voyennykh Nauk [The Journal of the Russian Academy of Military Science], both of them published by the Russian Ministry of Defense, and Problemy natsional'noy strategii [Problems of national strategy], issued by the Russian Institute for Strategic Research (RISS), which is affiliated with the administration of the President of the Russian Federation. Articles on information war, color revolutions and hybrid warfare in other journals are also discussed. The books that are considered include Aleksandr I. Vladimirov’s three-volume opus Osnovy obshchey teorii voyny [The foundations of a general theory of war], Igor Panarin’s books on information war, Igor Popov and Musa Khamzatov’s Voyna Budushchego [War of the future] and Pavel Tsygankov’s “Gibridnye Voyny” V Khaotiziruyushchemsy mire XXI veka [“Hybrid wars” in the chaotizing world of the 21st century].

The article argues that Russian scholarly military discussions of information war, color revolutions and hybrid war broaden the range of conceivable security issues for Russia in Russian scholarly discourse, which, in turn, widens the horizon of legitimate political action. Importantly, the three terms are weakly conceptualized and frequently lack empirical substantiation, yet function discursively to recast social, political, diplomatic and other phenomena as potential security threats.
Axioms of Western enmity

The growing focus on nonmilitary warfare in Russian military discourse has been underpinned by assumptions of Western malevolence. This Western enemy image has been inherited from the Cold War, when the West and particularly the United States were (quite accurately) seen as major external threats to the Soviet Union. Today, that enemy image is again strong to the point of being treated axiomatically in Russian military and security scholarship. For example, Aleksandr Vladimirov, Aleksandr Bartosh, Marina Kuchinskaia and other scholars do not find it necessary to justify casting Western state actors as major threats to Russia but treat it as a given in their writings. The following passages from General Vladimirov’s three-volume opus, The Foundations of a General Theory of War, well illustrates this:

It is possible and necessary to conduct a dialogue with the West, but one should understand that in the West there is nothing sacred and nothing can be sacred (emphasis in the original); the West has no allies, no feelings, there is only the interests of the ruling minority of pathologically greedy, moral freaks; because of this, the West always behaves like a bandit, and will always behave as such as long as they are in charge.

Kuchinskaia, a senior researcher at the Russian Institute for Strategic Studies (RISS), similarly treats Western enmity as a given:

The political will and the availability of the combined resources of the United States and NATO permit it within the framework of its strategy, which is directed towards global domination, to successively conduct subversive operations within the framework of the hybrid war that is being conducted against the Russian Federation.7

It is in this context of assumed Western enmity that much of the Russian scholarly discussion of widening nonmilitary threats unfolds.

Securitization theory

Background

Securitization theory was originally developed by researchers associated with the so-called Copenhagen School and derives from the understanding that security is an essentially contested concept. As Michael J. Butler and Zena Wolf have noted, securitization theory emerged as part of a wider shift in security studies in the late 1980s and the early 1990s away from statist understandings of security to more eclectic notions.8 The post-Cold War period saw structural transformations in the global political system that “stimulated greater recognition of the possibility of a ‘new’ security environment in which security actors, threats, and responses alike are subject to an ongoing social and political process of definition, redefinition, and contestation.”9

Turning their sights to that process, Barry Buzan and Ole Waever, among others, sought to understand how certain issues become recognized as security issues while others do not. To answer this question, they drew on J.L. Austin’s speech act theory10 which maintains that language has both locutionary, illocutionary and perlocutionary functions.11 Language is locutionary because it performs an utterance, illocutionary when it seeks a communicative effect (for instance, through a promise or a warning);
Comparative Strategy

and perlocutionary in the sense that it may have effects beyond those that were intended.\(^{12}\)

Using Austin's framework, researchers have explored how issues become framed as security threats and why a particular framing may become accepted by an audience. They have argued that a key element in this process is the ability of a securitizing actor to convince an audience that a particular issue poses an existential threat to a valued referent object,\(^{13}\) for instance lives, livelihoods, cultural identity or the stability of the state. Acknowledgement of an issue as an existential threat paves the way for accepting the use of extraordinary measures to protect the threatened object. This elevates, they point out, the issue from ordinary politics to a level where extraordinary measures are deemed acceptable and necessary.\(^{14}\) As Michael C. Williams notes, securitization refers to processes whereby “the socially and politically successful speech act labels an issue a security issue, removing it from the realm of normal day-to-day politics, casting it as an existential threat calling for and justifying extreme measures.”\(^{15}\)

Securitization, thus, involves four elements: 1) a securitizing actor that claims that a particular issue needs to be treated as a security matter; 2) a claim that a particular phenomenon presents a threat; 3) the identification of a referent object that is being threatened; and 4) an audience that needs to be convinced that the identified phenomenon threatens the referent object. The theory is rooted in a constructivist view of security as contingent on linguistic action, and draws attention to the linguistic moves performed by the securitizing actor to recast something as a security threat.

Securitizing move vs securitization

In the classic elaboration of securitization theory the securitizing move is distinguished from securitization itself. While the former constitutes an effort to present an issue as a security threat, the latter arises when that issue is accepted as such by a relevant audience. Some scholars have argued that this distinction introduces a degree of confusion at the heart of the securitization framework. Thierry Balzacq has questioned whether it is at all possible to understand securitization as both a speech act and an intersubjective process that relies on the involvement of an audience,\(^{16}\) suggesting that securitization should instead be understood as the outcome of strategic discursive action conducted in a social context, i.e. “a field of power struggles in which securitizing actors align on a security issue to swing the audience's support toward a policy or course of action.”\(^{17}\) Sarah Léonard and Christian Kaunert, along with others,\(^{18}\) have argued that one must take into account multiple audiences, “characterized by different logics,” yet all “inter-linked as they are part of the same policy process.”\(^{19}\) Others have pointed out that the failure of securitizing moves often depends on the audience,\(^{20}\) insisting that special attention should be afforded to this element of securitization in securitization research.

In the present article it is assumed that the audience and the securitizing move can be kept analytically apart, like in the original Copenhagen School framework but in contrast to Balzacq. To be sure, it is acknowledged that the response of the audience to a securitizing move determines its outcome and may, as Balzacq points out, be
heavily implicated in the strategic deliberations of the securitizing actor. Yet, this does not preclude that the linguistic performances through which an issue is recast as a security threat can be analytically delineated and examined in isolation from the wider context in which those performances take part. The present article largely eschews the audience and focuses on the securitizing move itself, i.e. the linguistic process that recasts an issue as a security threat deserving of particular political attention. More specifically, it considers the manner in which the Russian scholarly discourse on non-military warfare presents a broadened threat perception, identifying a wider range of phenomena as potential security issues demanding expanded political action. Whether those security moves lead to successful securitization is beyond the scope of the study, which is not concerned with the success or failure of the securitizing moves but with the manner in which threat perceptions are constructed in Russian scholarly discourse.21

The following section considers Russian military and security researchers’ writings on three forms of nonmilitary warfare: information warfare, color revolutions and hybrid war. It examines how Russian scholars have addressed these topics, and pays particular attention to the manner in which the scholars use the concepts to construct particular threat imaginaries.

**Information war, color revolutions and gibridnaya voyna**

**Information warfare**

One of the major exponents of Russian thinking on information warfare is the political scientist Igor Panarin, who has written several books on the topic, including a number of historical overviews.22 His thinking, which draws on the Russian philosopher Sergey Rastorguev,23 has been influential in Russian scholarly writing on information war. According to war scholar Ofer Fridman, it has underpinned wider discussions about nonmilitary warfare, including about hybrid warfare.24

Panarin views information war as a comprehensive effort to use information to manipulate the decision-making process of the adversary. According to Panarin, it involves “the use of all available means to introduce necessary comments (kommentary) into the governing sphere of the opposing side”25 and may be conducted in the political, diplomatic, financial-economic and military domains.26 In his book *Informatsionnaya Voyna i Mir* (Information war and peace), Panarin defines information war as:

> A form of struggle between sides that represents the use of special (political, economic, diplomatic, military and other) methods, ways and means to influence the information environment of the opposing side and defend one's own attained goals.27

As emerges here, Panarin’s definition of information war is highly encompassing, covering not only the political, economic, diplomatic and military domains but also unspecified “other” spheres. Mere “influence” on the information environment of the adversary is understood as sufficient to qualify as information war. Information war may indeed be understood as comprising any attempt to use information to gain an advantage over an adversary. “War,” in Panarin’s definition, is made synonymous with “struggle” or even “competition.”
Elsewhere in his writings, Panarin describes the existence of a coordinating actor capable of directing actions in the information sphere to a nation's benefit. In reference to Western states, and particularly the United States, Panarin speaks of “specialized institutions or sub-divisions within various organizations that handle information analysis within their fields.” More specifically, he mentions the U.S.-operated Echelon system, which reportedly intercepts foreign communications. Panarin claims the system conducts a “round-the-clock scanning of all information in the world,” a grand and rather unlikely statement that attributes virtual omniscience to the United States.

The understanding of information war as all-embracing leads Panarin to claim that the Cold War was the first world information war, a struggle between the Soviet and the Western blocs that was waged largely in the information domain. According to Panarin, the United States used information means successfully to destabilize the Soviet elite, by targeting the transfer of power in particular.

According to Panarin, the Cold War information war has continued until the present day and remains “the major tool of contemporary world politics, [and] the dominant way to achieve political and economic power in the 21st century.” According to Panarin, the United States continues to weaponize information in pursuit of its interests.

Panarin notably draws little analytical distinction between information war and other forms of information activities that Russia and other adversaries of the United States may perceive as threatening to their interests. Information war remains a weakly delineated concept and therefore difficult to falsify. It also has questionable analytical value, even as it imputes an ostensible logic to Western actions vis-à-vis Russia over past decades.

Panarin is not the only Russian theorist of information war. Other theorists understand the concept with similar open-endedness. Aleksandr Vladimirov notes in Osnovy obshchey teorii voyny that information war has “a total character, that is it is conducted continuously in all the operating spheres of the state (and part of the social mind, sotsiuma).” Sergey Rastorguev defines it as: “the overt and covert purposive informational influence of one system on another with the goal of achieving a certain win in the material sphere.” Marina Danilova equates information war with the “manipulation of information.” Viktoriya Romanova understands it as consisting of “influence (vozdeystvie) on the information sphere of the adversary and influence on the consciousness of people.” S.S. Sulakshina, too, believes that information war “targets above all social consciousness.”

Thus information war in common Russian scholarly discourse denotes a wide range of phenomena linked to information dissemination as potential security threats to Russia. In terms of securitization theory, the designated threat (information influence) and the designated referent objects (information sphere and social consciousness) are vaguely defined, while the reader is told that information war holds immense destructive potential: “[Information war] touches (zatragivaet) all spheres and aspects of national existence, political and military activity, all levels of national government and different types of military technology and weapons.” Indeed, information war, Vladimirov notes, may lead to the adversary’s “ceasing to believe what he always used to believe, and forgetting that, which he always knew.”

Panarin is explicit about the implications of his theory for Russian policy making. To address the specter of information war, Panarin wants, as Fridman points out, a
“meaningful system of management” that would involve coordinating and integrating the activities of authorities, mass media, security services and state intelligence agencies. The purpose of this system would be to “organize defensive and offensive informational operations (on the territory of Russia and abroad).” Furthermore, Panarin argues for increased private-governmental information exchange, including by establishing a private-governmental intelligence agency that would coordinate information activities between the private and government spheres.

General-Major Igor Sheremet, a specialist on information technology, agrees with Panarin that information war requires a broadened political response from Russia. He advocates for an expanded role for the military establishment in combating information war. In a speech published in Vestnik Akademii Voyennykh Nauk in 2019 Sheremet held that Western information operations present a danger to Russian social consciousness. Providing an overview of Russian state departments charged with combating disinformation and other forms of pernicious informational influence, he concluded that “Of all possible options, apparently only the Ministry of Defense has sufficient possibilities to create a system for ensuring the security and stability of Russia’s technosphere.”

**Color revolutions**

Color revolutions were the largely peaceful uprisings that toppled or sought to topple authoritarian political leaders in post-Soviet and other post-socialist countries, including Ukraine, Georgia, Kyrgyzstan and Serbia. In wider usage, it has been applied also to the revolutionary movements of the Arab Spring, the Philippine “People’s Power” movement that overthrew Ferdinand Marcos’ autocratic regime in 1986 and the 2006 Lebanese “Cedar” Revolutions. As Jonsson points out, Russian elites did not originally see the color revolutions “as nonmilitary warfare by Western governments” but as spontaneous protest movements. From 2004 up until the 2007-8 Russian elections, however, “the threat of color revolutions was increasingly securitized” and in the 2010s, Russian leaders and military theorists openly blamed Western governments for instigating them.

The term color revolutions was used in political discourse before it was taken up by Russian academics in the sense of a particular species of warfare. Russian President Vladimir Putin used the term in speeches in the 2000s, well before theorists such as Aleksey Belsky, Andrey Manoylo and Aleksandr Bartosh wrote articles about color revolutions in 2013-2015. But with time, military theorists turned their minds to the concept and it became a feature of Russian academic discussions of nonmilitary warfare.

Russian military theorists view color revolutions as surrogates for military action, more specifically as a nonviolent method for engineering regime change in countries outside of the Western orbit, paving the way for the accession of pro-Western governments. The color revolutions that have taken place in the post-Soviet sphere (including a number of unsuccessful popular protests, for example in Moldova) are viewed as components of a concerted push to extend Western influence, particularly in the countries of the former Soviet Union. The Russian sociologist Vladimir Barsamov writes of a “not accidental” tendency to “destabilize” the post-Soviet space. Andrey Manoylo, a professor of political science at the Moscow State University and a member
of a scientific advisory body to the Security Council of the Russian Federation, writes that “the concept of ‘color revolutions’ comprises an entirety of scenarios of state overthrow and the dismantling of political regimes, successfully disguised as a popular uprising.” Manoylo and Oleg Karpovich (the latter a professor of political science and the director of the Russian Foreign Ministry’s Diplomatic Academy’s Institute for Current International Problems) contend in a book from 2015 that the concept, model and technologies of color revolutions play a role in the “dismantling of political regimes in contemporary states (of both authoritarian and democratic types).” Color revolutions are a replacement for lethal force, evading the danger of escalation and granting the movements legitimacy as popular uprisings.

Color revolutions allegedly involve a range of operation types by Western actors, including disinformation and ideological seduction, whereby Western-type liberalism is presented as an attractive alternative to existing rule. Key to successful color revolutions is the provision of support to local civil-society actors, particularly non-governmental organizations that espouse liberal and other Western values. Like the movement Otpor in Serbia and the organizers of the Orange Revolution in Ukraine in 2004-5, such organizations mobilize the masses, engage in protest tactics and provide unifying symbols and slogans to the protest movement. According to Russian theorists, the organizations may not themselves realize that they are acting on behalf of foreign interests and may engage in protests in earnest.

There was a change in Russian thinking about color revolutions over time. Initially, they were seen as largely peaceful, if hostile, events, but with time they were increasingly understood to constitute one phase in a destabilizing process that might lead to violent escalation. This change in thinking appears to have coincided with the Arab Spring uprisings, which resulted in widespread violence, particularly in Libya and Syria, where civil wars erupted. War scholar and retired Colonel Valery Kiselyov and war scholar and retired General-Major Ivan Vorobyov list the regime changes in Afghanistan in 2001, Libya in 2011 and Egypt in 2012 under the sobriquet of color revolutions. In Libya, for instance, according to the authors:

The first thing NATO did...was to raise armed internal opposition groups whose actions were coordinated by agents of the U.S., British, and French special services. The population and government agencies were exposed to a psychological information warfare campaign so unprecedented in scale that it actually wrenched control out of the government’s hands, forcing it to cease resisting outside interference.

Hence, color revolutions, much like information warfare, is a highly encompassing concept. It offers no means for distinguishing between genuine and orchestrated popular movements or between legitimate and illegitimate forms of foreign support to non-governmental organizations. All forms of protest may be subsumed under the term, which means that all popular protests can be identified as potential security threats, indeed as acts of nonmilitary warfare. The Ukrainian Orange Revolution, the Kyrgyz Tulip Revolution, the Georgian Rose Revolution, the 2011-13 protest movement in Russia and other mass protests are consequently viewed as hinging not on genuine popular dissatisfaction but on foreign interference. The concept of color revolutions imputes to the phenomenon of mass uprisings a logic rooted in ideas of Western instrumental and malevolent action.
Hybrid war (гібридна вона)
The term гібридна вона (hybrid warfare) was imported into Russian military discussions from Western discussions about hybrid warfare already in the late 2000s but has achieved salience in Russia only relatively recently with the publication of a number of articles and books about the concept after the beginning of the war in Ukraine in 2014. As in the West, the term гібридна вона is used eclectically in Russian military discourse to designate warfare that combines different forms of power projection, both military and nonmilitary. In Russia, the term at times has also taken on a distinct meaning that partially overlaps with the concepts of information warfare and color revolutions.

Ofer Fridman has contended that the Russian discourse on гібридна вона has little to do with the Western understanding of hybrid warfare. Russian scholars, Fridman writes, do not understand гібридна вона in U.S. military scholar Frank Hoffman's sense of a tactical-operational method that draws together multi-domain assets, but as a strategic assault on “the spirit of the adversary's nation by a gradual erosion of its culture, values and self-esteem.” 51 The concept of гібридна вона denotes warfare whose “main purpose…is to avoid the traditional battlefield and destroy the adversary via a hybrid of ideological, informational, financial, political and economic methods that dismantle the fabric of society, leading to its internal collapse.”

According to this argument, the Russian discourse on гібридна вона traces its intellectual pedigree not to Western scholars of hybrid war but to Igor Panarin's understanding of information warfare, Aleksandr Dugin's concept of net-centric warfare and especially the Russian émigré scholar Evgeniy Messner's idea of subversion warfare. Messner, who wrote during the Cold War, argued that the nuclear threat, global interconnectivity and new informational systems had made the risks of open warfare politically unacceptable, and had thereby incentivized states to instead seek to weaken their adversaries by sowing internal discord and exploiting existing divisions through covert and indirect means. Гібридна вона, according to Fridman, is the latest installment in a tradition in Russian military thought that contends that nonmilitary means of warfare may be powerful weapons in weakening the adversary from within.

As has been pointed out elsewhere,53 many Russian scholars of гібридна вона do not in fact draw on Panarin, Dugin and Messner explicitly (although some, like Vladimirov, do)54, but do cite major Western exponents of theories of hybrid warfare, including Hoffman and the International Institute for Strategic studies.1 While it is true that Russian thinkers of гібридна вона such as Marina Kuchinskaia, Aleksandr Bartosh and Aleksandr Vladimirov share with Panarin, Dugin and Messner a belief in the potential subversiveness of nonmilitary action, which may be considered a part of the paradigm of security thinking in contemporary Russia, this does not necessarily amount to a distinct Russian theoretical tradition of warfare. After all, it is a view embraced also by other authoritarian states fearful of foreign meddling in their internal affairs.

With that said, there is a duality in the Russian use of the concept of гібридна вона.55 When Russian scholars apply it to states other than Russia or the Soviet Union, the concept tends to be used in a sense that closely resembles the operational-tactical concept developed by Hoffman, Nathan Freier, Russel W. Glenn and others. That is, гібридна вона then denotes the synergistic combination of forces in multiple domains. But when Russian scholars (sometimes the very same individuals) discuss alleged Western hybrid warfare against Russia or the Soviet Union,
CoMpaRaTive STR aTeGy

The term is usually used in the broader sense of a targeting of the internal stability of the country. The concept then acquires a different meaning linked to what Fridman views as a Russian understanding of war as a “socio-political phenomenon.” Marina Kuchinskaia, a researcher at the Russian Institute for Strategic Studies, for instance, shifts between the two senses of the term when she, in one article, talks about the Western intervention in Libya as a case of operational-tactical hybrid warfare and in another article speaks of a hybrid campaign against Russia as involving the use of “traditional diplomacy and special operations forces, financial bodies, economic sanctions, non-governmental organizations and global mass media,” i.e. mostly nonmilitary means deployed at the strategic level. In the latter article, the focus on the operational-tactical level and the combined use of military and nonmilitary means to secure an advantage on the battlefield is missing and gibridnaya voyna is used to denote supposedly pernicious activities undertaken by a range of nonmilitary actors acting in combination with special operations forces.

Gibridnaya voyna in the latter sense of the term encompasses a very wide range of phenomena without an obvious delineation. Indeed, the spectrum of activities that potentially fall under it is even broader than for information warfare and color revolutions. Beyond information influence and protest movements, it may encompass also other phenomena that are conceivable as threats to Russia, including financial sanctions and traditional diplomacy. These activities are discursively elevated into potential acts of (hybrid) war. Aleksandr Neklessa, who is quoted at length in Aleksandr Vladimirov’s work, articulates gibridnaya voyna in the following broad terms:

Hybrid warfare is the sum of aggressive actions that broaden the possibilities of conventional politics, as well as the use of various instruments to subordinate or destroy an adversary, deconstruct undesirable circumstances and reorganize the existing order or establish a new order.

Neklessa’s definition is encompassing to the point of being catch-all, with vague words and phrases such as “instruments that broaden the possibilities of conventional politics.” His formulation leaves it difficult to determine what perceived pernicious actions could not be categorized under this definition.

Some Russian thinkers explicitly exclude military means from hybrid warfare, while others, like Neklessa, believe that the concept should comprise also military means. The Russian military thinkers, Viktor Popov and Musa Khamzatov note sardonically that the result of the wide usage of the term is that “[in Russia] the term gibridnaya voyna began to be understood as everything that did not fit into the notion of traditional armed struggle.” Indeed, in contrast to information war and color revolutions, which denote nonmilitary forms of warfare, gibridnaya voyna can integrate both nonmilitary and military threats to Russia and its spheres of influence. It makes this concept the broadest of the three concepts that are examined in this article and a virtually catch-all word that can potentially securitize a very wide range of phenomena as threats to Russia.

Concluding discussion

As has been pointed out in this article and elsewhere, recent Russian military theorizing has devoted special attention to nonmilitary warfare. This theorizing has been
underpinned by assumptions that nonmilitary means of power projection may inflict severe damage on an adversary by undermining it from within – damage that may be equal to, or even exceed, the damage that can be achieved through armed violence. Russian military thinkers such as Aleksandr Vladimirov, Aleksandr Bartosh, Evgeniy Messner and Makhmut Gareev have argued that modern conditions create disincentives for military warfare and incentives for nonmilitary warfare. The major disincentive for military warfare is the nuclear threat, which deters actions that may lead to military escalation. The main incentives for nonmilitary action is the existence of multiple entry points and vectors for weakening states from within, afforded by increased global connectivity and information systems of unprecedented power and reach. Russian theorists argue that Western states – above all the United States – exploit the new possibilities by undertaking subversive actions against Russia and its partner states.

The Russian academic discourse on nonmilitary warfare revolves around a number of concepts. Three of these have been considered in this article: information war, color revolutions and hybrid war (gibridnaya voyna), which overlap with each other and may, in certain respects, be seen as representing different stages of an evolving and expanding line of thinking about nonmilitary warfare. Gibridnaya voyna can comprise methods associated with color revolutions while color revolutions usually involve information warfare. Gibridnaya voyna can comprise methods associated with color revolutions while color revolutions usually involve information warfare. Gibridnaya voyna is the most encompassing of the three concepts, denoting an almost limitless range of nonmilitary actions that are construed as pernicious to Russia (and in some elaborations of the term, it includes military action, too). Indeed, gibridnaya voyna has become a catch-all term for any harmful action toward Russia. One interesting aspect of gibridnaya voyna is that it offers a conceptual manner of integrating military and nonmilitary threats. Aleksandr Bartosh and Marina Kuchinskaia, for instance, see hybrid warfare as a potentially escalatory method of warfare. It may begin with nonmilitary action in the form of “discriminatory sanctions, information warfare [and] the activation of ‘fifth columns’” that pave the way for color revolutions but may thereby increase tension to the point that armed violence breaks out. For Kuchinskaia, the use of arms represents the “final stage” of hybrid warfare.

Stephen J. Blank, writing in 2010, noted that many of the threat assessments that were made by Russian military specialists such as the chairman of the Russian Academy of Military Sciences Makhmut Gareev and Chief of the Russian General Staff Yuri Baluyevsky in the mid-2000s exaggerated the scope of nonmilitary threats. According to Blank, this represented a “neo-Soviet securitizing move” and an “all-encompassing securitization” that had a clear political purpose in making “the military the supreme arbiter of national defense.” The broadened threat assessment, in Blank’s words, was “based on the presupposition of enemies everywhere and pervasive threats to Russia’s government, identity, territory, and economy.” Residual Soviet threat imaginaries were dusted off and used to advocate for an expanded role for Russia’s military establishment in the country’s security policy.

The Russian scholarly discussions of information warfare, color revolutions and hybrid warfare fulfill a similar securitizing role as the security discussions that Blank considered. Information warfare, color revolutions and hybrid warfare are highly encompassing concepts that cast a wide range of actions as potential security threats. Under these terms, non-governmental organizations, foreign media outlets, diplomats, economic sanctions and other nonmilitary actors and actions may all be understood as security
threats, with the implication that they should be addressed outside of the realm of ordinary politics. In 2010, Blank wrote: “Russia sees an enormous range of subjects as constituting the elements that comprise national security and considers them as fit subjects for state leadership if not control.”67 This applies to the use of information war, color revolutions and hybrid warfare, which greatly broadens the security horizon. Russian military and security scholars are securitizing actors that contend that an increasingly large range of phenomena should be conceived as potential forms of warfare and therefore treated as subjects for extraordinary response.

Thus the discussions about information war, color revolutions and hybrid warfare imply a need for the state to widen its role in countering the security threats, including by setting up new agencies or delegating tasks to the Ministry of Defense, as was explicitly suggested by Igor Panarin and Igor Sheremet. Securitization implies politicization. The designation of new security threats entails a need for novel political action in response.

Russian scholarly discussions of nonmilitary warfare hold weak analytical power, turning on concepts that are poorly delineated and weakly substantiated. But they have an obvious discursive function in their widening of the spectrum of conceivable threats to Russia. They also form a kind of skewed mirror image to security discussions in the West, which too have grown more encompassing in recent decades. Like Western security discussions, the Russian discussions are based on a broadened notion of security that transcends traditionalist military conceptions and includes also nonmilitary and nonviolent forms. The Russian discussions involve an increased number of referent objects. National identity, social cohesion and social consciousness are all designated as referent objects alongside state military security. This parallels Western security discussions that have diversified their understanding of security threats and referent objects.68 Yet, the Russian security discourse is bounded by a persistent Western enemy image that identifies Western state actors and particularly the United States as the wellspring of threats against Russia, as well as a residual statist conceptualization of security evident in notions like national identity and social cohesion. Domestic instability, economic crisis and socio-cultural change are all securitized as the work of Western state actors and as threats against primarily the strength and sovereignty of the Russian state. It may be understood as an attempt to shoehorn an increasingly diversified security landscape into the rigid enemy images and security conceptualizations of yore. Russian hybrid war discourse, not least, may be understood as an attempt to integrate a spectrum of nontraditional security issues under the statist and national umbrellas, linking phenomena as wide-ranging as epidemics and political contestation to issues of national security.

Notes

1. Marina Kuchinskaia, “Fenomen gibridizatsii sovremennykh konfliktov: otechestvennyi i zapadny voenno-politicheskii diskurs,” (The phenomenon of the hybridization of contemporary conflicts: national and Western military-political discourse) Problemy natsional’noi strategii 6, no. 51 (2018): 122-43; A.A. Bartosh, “Smysly gibridnoy voyny,” (The meanings of hybrid war), Vestnik akademii voennykh nauk 59, no. 2 (2017), 165-172. Another Russian researcher who explicitly bases himself on a Western definition of ‘hybrid warfare’
is Yuri Alekseevich Popkov who cites Frank Hoffman’s definition of hybrid war as the “best definition” of the phenomenon. Yu. A. Popkov, “Tactical Reconnaissance in Hybrid Warfare”, *Military Thought* 3, no. 26 (2017), 120.

**Notes**

1. Sandor Fabian, “The Russian Hybrid Warfare Strategy – Neither Russian nor Strategy,” *Defense & Security Analysis* 35, no. 3 (2019): 308–25, doi: [https://doi.org/10.1080/14751798.2019.1640424](https://doi.org/10.1080/14751798.2019.1640424); Ofer Fridman, *Russian 'Hybrid Warfare'. Resurgence and Politicization* (London: Hurst & Company); Alexander Lanoszka, “Russian Hybrid Warfare and Extended Deterrence in Eastern Europe,” *International Affairs* 92, no. 1 (2016): 175–95, doi: [https://doi.org/10.1111/1468-2346.12509](https://doi.org/10.1111/1468-2346.12509); Bettina Renz, “Russia and 'Hybrid Warfare,” *Contemporary Politics* 22, no. 3 (2016): 283–300, doi: [https://doi.org/10.1080/13569775.2016.1201316](https://doi.org/10.1080/13569775.2016.1201316); Mark Galeotti, “Hybrid, Ambiguous, and Non-Linear? How New Is Russia’s 'New Way of War'? "*Small Wars & Insurgencies* 27, no. 2 (2015): 282–301 doi: [https://doi.org/10.1080/09592318.2015.1129170](https://doi.org/10.1080/09592318.2015.1129170); Mark Galeotti, “‘Hybrid War’ and ‘Little Green Men’: How It Works and How It Doesn’t,” in *Ukraine and Russia: People, Politics, Propaganda and Perspectives*, ed. Agnieszka Pikulicka-Wilczewska and Richard Sakwa (Bristol: E-international relations publishing, 2015), 156–64; Jānis Bērziņš. “Russian New Generation Warfare Is Not Hybrid Warfare,” in *The War in Ukraine: Lessons for Europe*, ed. Artis Pabriks and Andis Kudors (Riga: University of Latvia Press, 2015), 40–51; András Rác, *Russia’s Hybrid War in Ukraine: Breaking the Enemy’s Ability to Resist* (Helsinki: Finnish Institute of International Affairs, 2015).

2. Peter A. Mattsson, “Russian Military Thinking – A New Generation of Warfare,” *Journal of Baltic Security* 1, no. 1 (2017): 61–70; Timothy Thomas, “The Evolution of Russian Military Thought: Integrating Hybrid, New-Generation, and New-Type Thinking,” *The Journal of Slavic Military Studies* 29, no. 4 (2016): 554–75, doi: [https://doi.org/10.1080/13518046.2016.1232541](https://doi.org/10.1080/13518046.2016.1232541); Jānis Bērziņš, “Russia’s New Generation Warfare in Ukraine: Implications for Latvian Defense Policy” (Policy Paper no. 2, National Defense Academy of Latvia, 2014): 5; Bērziņš, “Russian New Generation Warfare”.

3. Katri Pynnöniemi & Minna Jokela, “Perceptions of Hybrid War in Russia: Means, Targets and Objectives Identified in the Russian Debate,” *Cambridge Review of International Affairs* 33, no. 6 (2020): 828–45, doi: [https://doi.org/10.1080/09557571.2020.1787949](https://doi.org/10.1080/09557571.2020.1787949); Ofer Fridman, “Hybrid Warfare or Gibrindnaya Voyna? Similar, but Different,” *The RUSI Journal* 162, no. 1 (2017); Ofer Fridman. 2017. “The Russian Perspective on Information Warfare: Conceptual Roots and Politicisation in Russian Academic, Political, and Public Discourse,” *Defense Strategic Communications* 2: 61–86, doi: 10.30966/2018.riga.2.3.

4. Fridman, “Russian 'Hybrid Warfare',” 75–90.

5. Oscar Jonsson, *The Russian Understanding of War. Blurring the Lines between War and Peace* (Washington, DC: Georgetown University Press, 2019), 152.

6. Cf. Bērziņš, “Russia’s New Generation Warfare in Ukraine”; see also Rod Thornton, “The Changing Nature of Modern Warfare,” *The RUSI Journal* 160, no. 4 (2015): 40–8, doi: [https://doi.org/10.1080/03071847.2015.1079047](https://doi.org/10.1080/03071847.2015.1079047); Mark Galeotti, *Russian Political War. Moving beyond the Hybrid* (Abingdon: Routledge, 2019), 50–7; Bettina Renz, *Russia’s Military Revival* (Cambridge and Medford MA: Polity Press, 2018), 161; Kristin Ven Bruusgaard, “Crimea and Russia’s strategic overhaul,” Parameters 44 (2014): 81–90; Carl Plöen and Markus Balázs Göransson, “Kontinuitet och förändring i rysk militär vilseledning. En jämförande studie av Afghanistan 1979 och Krim 2014” [Continuity and Change in Russian Military Deception. A Comparative Study of Afghanistan 1979 and Crimea 2014], *Kungliga krigsvetenskapsakademin's handlingar & tidskrift* 2 (2021): 58–77.

7. Marina Evgen'evna Kuchinskaia, “Politika Sderzhivaniya Rossii: ‘Novaya Norma’ dlya NATO,” [The Politics of Deterrence against Russia: A New Normal’ for NATO], *Problemy Natsional’noy Strategii* 1, no. 40 (2017): 147–62.
8. Michael J. Butler & Zena Wolf, “Revisiting Securitization and the ‘Constructivist Turn’ in Security Studies,” in *Securitization Revisited. Contemporary Applications and Insights*, ed. Michael J Butler (London and New York: Routledge, 2020), 3–27.

9. Butler & Wolf, "Revisiting Securitization," 4.

10. Ole Waever, “The Theory Act: Responsibility and Exactitude as Seen from Securitization,” *International Relations* 29: 1 (2015): 121–7, doi: https://doi.org/10.1177%2F0047117814526606d.

11. J. L. Austin, *Doing Things With Words* (Cambridge, MA: Harvard University Press, 1975).

12. Ibid.

13. Ole Waever, "Securitization and desecuritization," in *On Security*, ed. Ronnie D. Lipschutz (New York: Columbia University Press, 1993), 46–86. See also Juha A. Vuori, “A Timely Prophet? The Doomsday Clock as a Visualization of Securitization Moves with a Global Referent Object,” *Security Dialogue* 41, no. 3 (2010): 255–77, doi: https://doi.org/10.1177%2F0967010610370225.

14. Paul Roe, “Is Securitization a ‘Negative’ Concept? Revisiting the Normative Debate over Normal Versus Extraordinary Politics,” *Security Dialogue* 43, no. 3 (2012): 249–66, doi: https://doi.org/10.1177%2F0967010612443723; Michael C. Williams, “Securitization as Political Theory: The Politics of the Extraordinary,” *International Relations* 29, no. 1 (2015): 114–20, doi: https://doi.org/10.1177%2F0047117814526606c; Rita Floyd, “Extraordinary or Ordinary Emergency Measures: What, and Who, Defines the ‘Success’ of Securitization?” *Cambridge Review of International Affairs* 29, no. 2 (2016): 677–94, doi: https://doi.org/10.1080/09557571.2015.1077651.

15. M. C. Williams, “Modernity, Identity and Security: A Comment on the Copenhagen Controversy,” *Review of International Studies* 24, no. 3 (1998): 435, doi: https://doi.org/10.1017/S0260210598004355.

16. Thierry Balzacq, “The Three Faces of Securitization: Political Agency, Audience and Context,” *European Journal of International Relations* 11, no. 2 (2005): 171–201, doi: https://doi.org/10.1177/1354066105052960. See also Sarah Léonard and Christian Kaunert, “Reconceptualizing the Audience in Securitization Theory,” in *Securitization Theory. How Security Problems Emerge and Dissolve*, ed. Thierry Balzacq (London: Routledge, 2011), 60.

17. Balzacq, “The Three Faces of Securitization,” 173.

18. Constantinos Adamides, “Securitization,” in *Securitization and Desecuritization Processes in Protracted Conflicts*, ed. Constantinos Adamides (Cham: Springer, 2020), 1–14; Stina Fredrika Wassen, “Where Does Securitisation Begin? The Institutionalised Securitisation of Illegal Immigration in Sweden: REVA and the ICFs,” *Contemporary Voices: St Andrews Journal of International Relations* 1, no. 1 (2018): 78–103, doi: http://doi.org/10.15664/jtr.1468.

19. Léonard and Kaunert, “Reconceptualizing the Audience,” 74.

20. Tasos Karafoulidis, “Audience: A Weak Link in the Securitization of the Environment?” in *Climate Change, Human Security and Violent Conflict. Challenges for Societal Stability*, ed. Jürgen Scheffran, Michael Brzoska, Hans Günter Brauch, Peter Michael Link, and Janpeter Schilling (Heidelberg: Springer, 2012), 259–72.

21. To be sure, Russian military scholars address themselves to various audiences, including fellow scholars, security and military practitioners, and the political establishment. It is an elite discourse conducted in a particular military-academic setting. There is evidence that it has had an impact on Russian defense policy and rhetoric. Roger McDermott, “Russia’s Military Scientists and Future Warfare,” *Eurasia Daily Monitor*, June 5, 2019, https://jamestown.org/program/russias-military-scientists-and-future-warfare/ (accessed November 24, 2020). Russian Chief of the General Staff Valeriy Gerasimov also embraced the concept of *gibridnaya voyna* (hybrid warfare), which had found its way into Russian academic debate from Western discussions in the late 2000s. Michael Kofman, “Gibridnaya Voyna, Kotoroy Net,” *Vedomosti*, April 20, 2016, https://www.vedomosti.ru/opinion/articles/2016/04/20/638380-gibridnaya-voyna (accessed November 24, 2020).
22. Igor Panarin, *SMI, Propaganda i informatsionnye voiny* [Mass Media, Propaganda and Information War] (Moscow: Pokolenie, 2012); Igor Panarin, *Pervaya Mirovaya Informatsionnaya Voyna. Razval SSSR* [The First World Information War. The Collapse of the Soviet Union] (Saint-Petersburg: Izdatel’stvo ‘Piter’, 2010); Igor Panarin, *Informatsionnaya Voyna i Mir* [Information War and Peace] (Moscow: Olma-Press, 2003).

23. See S. P. Rastorguev, *Informatsionnaya Voyna* [Information War] (Moscow: Radio i svyaz, 1998). Among other things, Panarin recapitulates Rastorguev’s analysis of the *Protocols of the Elders of Zion*, the author of which Rastorguev calls the “first serious theoretician” of information warfare. Panarin, *Informatsionnaya Voyna i Mir*, 18.

24. Fridman, *Russian ‘Hybrid Warfare’*.

25. Panarin, *Pervaya Mirovaya Informatsionnaya Voyna*, 23. According to Panarin, it comprises three broad elements: 1) strategic political analysis, that is the collection and processing of information about the adversary; 2) information influence, which is the “introduction of negative comments and disinformation in the information field of the adversary”; and 3) information resistance (defense), which is counter-information warfare where an actor seeks to block disinformation spread by an adversary.

26. Ibid.

27. Panarin, *Informatsionnaya Voyna i Mir*, 20.

28. Ibid., 21.

29. Ibid., 26.

30. Igor Panarin, *Informatsionnye voyny i kommunikatsii* (Moscow: Goryachaya liniya – Telekom, 2014), 118. Cited in Fridman, *Russian ‘Hybrid Warfare’*, 87–8.

31. Ibid., 116. Cited in Fridman, *Russian ‘Hybrid Warfare’*, 88.

32. Vladimiriv, *Osnovy Obshchey Teorii Voyny*, 526.

33. Sergey Rastorguev, “Informatsionnaya Voyna kak Tselenapравленное Informatsionnnoe Vozdeystvie Informatsionnykh Sistem” [Information War as the Purposive Informational Influence of Informational Systems], *Problemy Informatsionnoy Voyny* 1, no. 4 (1997): 2.

34. Marina Danilova, “Informatsionnaya Voyna kak Real’nost’” [Information War as Reality], *Istoricheskaya I Sotsial’no Obrazovatel’naya Mysl* 3: 1.

35. Viktoriya Romanova, “Informatsionnaya Sostavlyayushchaya Gibridnykh Voyn Sovremennosti,” *European Journal of Social Sciences* 8, no. 1 (2014): 442.

36. S. S. Sulakshina, “Kognitivnoe Oruzhie – Novoe Pokolenie Informatsionnogo Oruzhiya” [Cognitive Weapons – The New Generation of Information Weapons], *Vestnik Akademii Voyennykh Nauk* 1, no. 46 (2019): 58.

37. Vladimiriv, *Osnovy Obshchey Teorii Voyny*, 526.

38. Ibid., 528.

39. Cited in Fridman, *Russian ‘Hybrid Warfare’*, 88–9.

40. Ibid., 89.

41. I. A. Sheremet, “Ugrozy Tekhnosfere Rossii i Protivodeystvie im v Sovremennykh Usloviyakh” [Threats to the Technosphere of Russia and Countermeasures to them in Contemporary Conditions], *Vestnik Akademii Voyennykh Nauk* 1, no. 46 (2019): 27–34.

42. Ibid., 33.

43. Jonsson, *The Russian Understanding of War*, 125.

44. Ibid., 125.

45. A. N. Belsky and O. V. Klimenko, “Political Engineering of Color Revolutions: Ways to Keep Them in Check,” *Military Thought* 3, no. 23 (2014): 20–9; Aleksandr Bartosh, “Model Upravlyayemogo khaosa v Sfere Voyennoy Bezopasnosti” [The Model of Controlled Chaos in the Sphere of Military Security], *Vestnik Akademii Voyennykh Nauk* 46, no. 1 (2013): 69–77; Aleksandr Bartosh, “Razrushitelniy Tandem: Tsvetnaya Revolyutsiya; Gibridnaya Voyna” [Destructive Tandem: Color Revolution; Hybrid War], *Nezavisimoye Voyennoye Obozreniye*, July 24, 2015. Some, like the sociologist Vladimir Barsamov, however, used the term already in 2006, as referenced in the note below.

46. V. A. Barsamov, “‘Tsvetnaya Revolyutsiia’: Teoreticheskiy i Prikhodnuyu Aspekty,” *Politicheskaya Sotsiologiya* (2006), 57.
47. A. V. Manoylo, “Informatsionniy faktor tsvetnykh revolyutsiy i sovremennykh tekhnologiy demontazha politicheskikh rezhimov,” Vestnik MGIMO Universiteta (2014): 61–6.
48. O. G. Karpovich and A. V. Manoylo, Tsvetnye Revolyutsii. Teoriya i Praktika Demontazha Sovremennykh Politicheskikh Rezhimov (Moscow: Obshchestvo s Ogranichennoy Otvetstvennost’yu "Izdatel’stvo Yuniti-Dana," 2015), 3.
49. Andrew Korybko, Hybrid Wars: The Indirect Adaptive Approach to Regime Change (Moscow: People’s Friendship University of Russia, 2015), 79. Cited in Jonsson, The Russian Understanding of War, 143.
50. V. A. Kiselyov and I. N. Vorobyov, “Hybrid Operations: A New Type of Warfare,” Military Thought 2, no. 24 (2015): 29.
51. Ibid., 92.
52. Ibid., 93.
53. Markus Balázs Göransson, “The Russian Discussion of Gibridnaya Voyna,” in Hybrid Warfare. Security and Asymmetric Conflict in International Relations, ed. Mikael Weissmann, Niklas Nilsson, Björn Palmertz, and Per Thunholm (London: I.B. Tauris, 2021), 83–94.
54. Vladimir I. Popov and Khamzatov, Voyna Budushchego, 343–4.
55. Ibid., 343.
56. Makhmut Gareev, “Predchustvovat’ izmeneniya v kharaktere voyny” [A Premonition of Changes in the Character of War], Voenno-Promyshlennyi Kur’er 47 (2013), 515.
57. Aleksandr Bartosh, “Primenenie gibridnykh metodov v sovremennykh konfliktax,” (The Use of Hybrid Methods in Contemporary Conflicts), Problemy national’noi strategii 6, no. 39 (2016): 160.
58. Ibid., 46.
59. Stephen J. Blank, “’No Need to Threaten Us, We Are Frightened of Ourselves,’ Russia’s Blueprint for a Police State, the New Security Strategy,” in The Russian Military Today and Tomorrow: Essays in Memory of Mary Fitzgerald, ed. Stephen J. Blank and Richard Weitz (Washington, DC: The Strategic Studies Institute, 2010), 48.
60. Ibid.
61. Ibid., 46.
62. Since the end of the Cold War, much of the security scholarship in the West has sought to decenter the state and the nation from security discourses, favoring concepts such as human security, economic security and environmental security. Michael J. Butler and Zena Wolf speak of a growing recognition in the Western academe since the 1980s that “the utility of a cognitive lens that places a premium on states, material interests, and military capabilities seems limited at best.” Butler & Wolf, “Revisiting securitization,” 4. One implication of this is that in mainstream Western security thinking, the state may only partially be understood as a proxy for other important referent objects, which renders new conceptualizations of security necessary. In contrast, the state and the nation have remained key referent objects in Russian security discussions. For instance, in the 1990s, Russia faced an economic crisis, political instability and a growing AIDS epidemic, yet these issues were by and large not securitized by a security establishment that maintained a mostly traditional understanding of security. As Roxanna Sjöstedt has pointed out, it took until 2006 before Russia’s President Vladimir Putin declared the country’s AIDS...
epidemic, among the worst in the world, a national security threat, Roxanna Sjöstedt, "Exploring the Construction of Threats: The Securitization of HIV/AIDS in Russia,” Security Dialogue 39, no. 1 (2008): 7–29.

**Disclosure statement**

The authors report there are no competing interests to declare.

**Funding**

The article has been made possible with a grant from the Swedish Armed Forces.

**Notes on contributor**

Markus Balázs Göransson (markus.goransson@fhs.se) is an Assistant Professor in War Studies at the Swedish Defence University. He holds a PhD in International Politics from Aberystwyth University. His research focuses on Russian military debates, Soviet military veterans and violent conflict more broadly. LinkedIn: https://www.linkedin.com/in/markus-g%C3%B6ransson-5450b72/