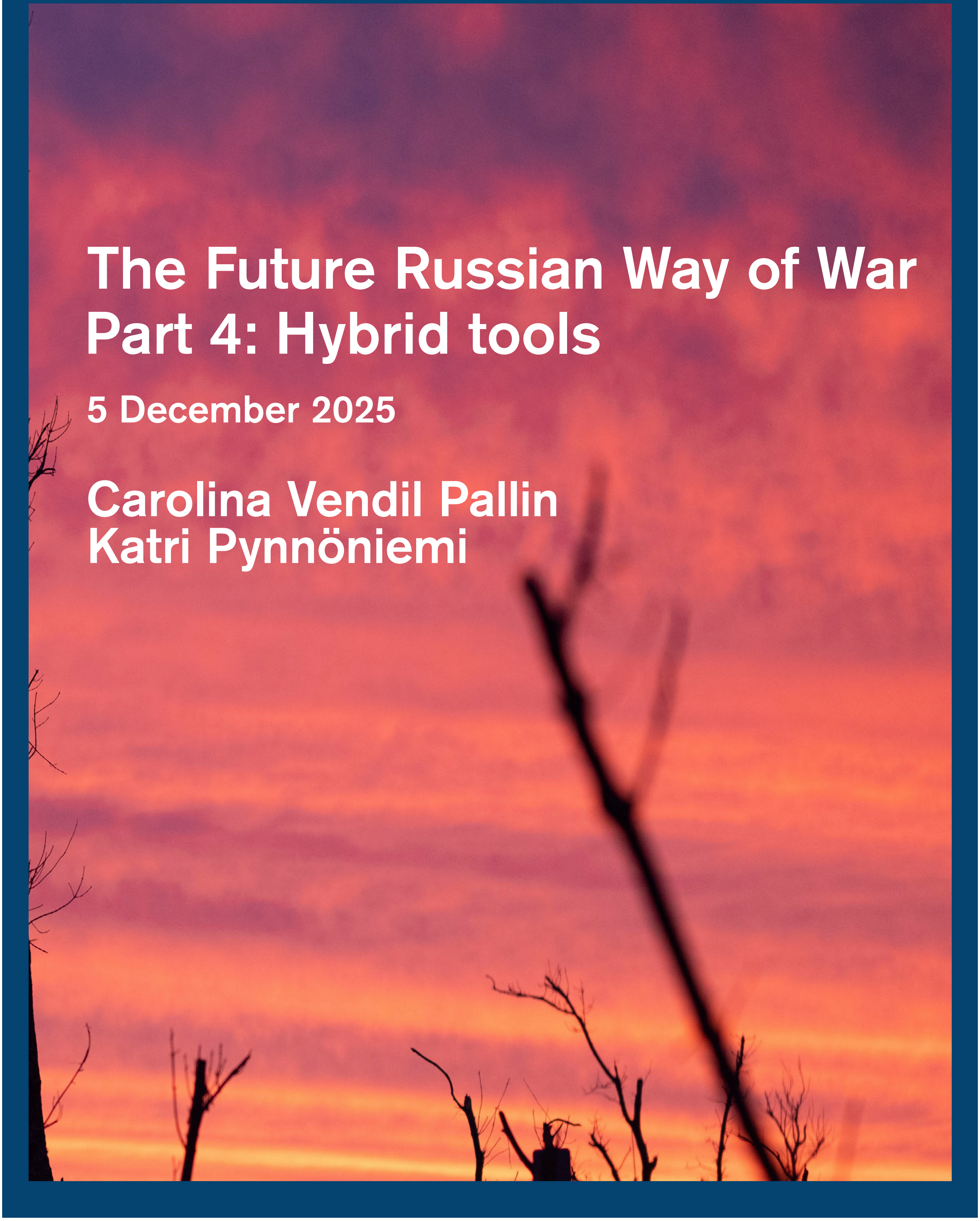
SCEEUS GUEST REPORT
NO. 6 2025

SCEEUS STOCKHOLM CENTRE FOR
EASTERN EUROPEAN STUDIES



The Future Russian Way of War Part 4: Hybrid tools

5 December 2025

Carolina Vendil Pallin
Katri Pynnöniemi

Introduction

In May 2025, the Stockholm Center for Eastern European Studies (SCEEUS) at the Swedish Institute of International Affairs gathered a group of leading specialists and researchers focusing on various dimensions of Russian security and military affairs. The conference, “The Future Russian Way of War,” was organized around four broad themes: 1) state mobilization; 2) military reform; 3) nuclear deterrence; and 4) hybrid tools.

Part 4: Hybrid tools

This is the fourth installment to be published from the conference, centered around its second theme, hybrid tools. It contains two papers.

The first paper, by Carolina Vendil Pallin, a researcher with the Swedish Defence Research Agency, deals with Russia’s approach to cyber warfare. She describes how cyber warfare is part of Russia’s broader thinking on information security, the vulnerabilities that Russian authorities have identified within this area, and how threats to Russian information security can be countered also with offensive tools.

The second paper, by Katri Pynnöniemi, Professor of Russian Security Studies at the University of Helsinki and the Finnish National Defence University, describes Russian thinking on the future of warfare. She describes what has been labelled a ‘revisionist’ approach to warfare, where non-traditional and indirect means are prioritised over traditional armed struggle, and non-military measures play an increasingly important role.

Russian Cyber Strategy and Hybrid Warfare

Carolina Vendil Pallin

Tracing a Russian cyber strategy

While Russia does not have a formal cyber strategy, a cyber command or even "cyber troops", it is a cyber power, it conducts cyber operations and it needs a cyber defence. Russia's thinking on cyber issues is part of its overall information strategy and military thinking. There is something of an orthodoxy in Russian information warfare terminology. In the early 2010s, the upper house of Russia's parliament, the Federation Council, initiated development of a cyber strategy. The initiative petered out, however, as it went through a round of consultations within Russia's National Security Council and the security services ("Kontseptsiia Strategii kiberbezopasnosti" 2014).

Russia has a wealth of strategic documents or policies on information security. There is an Information Security Doctrine from 2016, the Russian Armed Forces has a concept for its activities in the information sphere from 2013 and there are paragraphs on information warfare in everything from Russia's National Security Strategy (2021) to its most recent Foreign Policy Concept (2023). However, the word cyber, кибер, never appears. When Russia singles out technical and network aspects of information security, it does so by dividing these into psychological information security and technical information security. The latter amounts to what comes closest to "cyber security", dealing with IT and network security (see also Moore 2024: 6–7).

Departing from this definition of the prefix "cyber", I divide Russia's cyber strategy into five main themes. First, Russia has legislation that defines its critical information infrastructure and how to protect it. Second, Russia is keenly aware that one of its most critical vulnerabilities is its dependence on IT imports. Before 2022, Russia still imported everything from operating systems to servers and electronic components, primarily from the West and China.

Third, the Russian government wishes to establish control over what it terms "a Russian segment of the internet", to create a national information sphere. This somewhat blurs the distinction between psychological and technical aspects, but is at the heart of Russia's cyber strategy and anchored in finding technical solutions to establishing information control. This is where Russia's efforts to create a so-called sovereign internet fits in. Creating a kill switch was always primarily about being able to close down the internet in case of protests inside Russia rather than internet functionality. The main concerns are control over the content available to the Russian population, as well as internet surveillance.

The fourth component comprises Russia's efforts to influence how the global internet infrastructure is governed. Moscow has been a stern proponent in the UN of governments deciding this, rather than the current multistakeholder approach. Russia, like China, always refers to the need for an "information security agreement" rather than a cyber one. The main concern is to control the content that is available to their respective populations.

Finally, even in the absence of any publicly available documents on an offensive component to Russia's cyber strategy, there is ample evidence of Russian cyber operations against other countries. Russia is active along the entire spectrum, from relatively simple distributed denial-of-service (DDoS) attacks to more sophisticated cyber espionage and sabotage, such as entering and taking over the industrial control systems of electricity supply grids. Russia always denies being behind a cyber operation and there is an element of recklessness in how they are executed. Not Petya is a prime example, as the most costly cyber operation ever carried out in terms of the economic losses incurred. Authoritarian systems, such as Russia, have no qualms about using offensive cyber operations against their own citizens, primarily the independent press and political opposition.

Russia’s War against Ukraine

There had been expectations that cyber operations would play a role in Russia’s war against Ukraine, and Russia is known to have planned and executed cyber operations as part of its invasion in 2022. Per-Eric Nilsson (2023) identifies a number of reasons why they did not play the major role many analysts predicted. One of the more important factors is probably that Ukraine was prepared. It had been something of a testbed for Russian cyber operations since at least 2014. Russia underestimated Ukraine, which also received help from outside, from multinational giants such as Microsoft, Amazon and Google. Perhaps also, the expectation that it might turn into something of a cyber-Armageddon was always inflated and Russian cyber power overestimated. Furthermore, we probably do not know the whole story. As Lucas Kello (2018: 41) has noted, cyber warfare is a research topic where there is an abundance of data but it is difficult to draw conclusions. You rarely have complete datasets and you need to assume that many cyber operations are never disclosed or even detected. The parties involved – both attacker and target – often have a vested interest in keeping exploits secret, not least when it comes to the most advanced operations. In addition, it is inherently difficult to integrate offensive cyber operations with kinetic ones (Bateman 2023; Schulze and Kerttunen 2023).

Cyberattacks are a strategic resource typically conducted by the intelligence and security services, in Russia’s case the Military Intelligence Service (GRU), the Foreign Intelligence Service (SVR) and the Federal Security Service (FSB). Advanced malicious code and zero-day vulnerabilities are expensive and, unlike artillery shells, cannot be mass-produced and reused. You use them once and, once detected, they are out there, known not only to the target, but also, for example, to criminal ransomware groups.

Russian offensive cyber operations played an important role for Russia in shaping the battlefield. They were instrumental in gathering intelligence, mapping Ukraine’s military and society, and attempts to undermine Ukrainian resistance and establish a malign presence in critical information infrastructure. There was a surge in Russian offensive cyber operations at the start of the invasion. As the invasion developed into an attritional war, however, the importance of cyber operations diminished.

Importantly, Russia also experienced a wave of cyber operations from the outset of the war. In fact, Russia probably became the most attacked country in cyberspace on 24 February 2022. This began with relatively unsophisticated cyberattacks, such as DDoS attacks, but in time became more advanced. The so-called IT Army of Ukraine encouraged and coordinated hacker networks internationally to strike at Russian targets. An analysis of the main sectors targeted in Russia in the first year of the war suggests that the surge in attacks was politically motivated. For Russia, the situation was compounded by western sanctions, but also the fact that its business sector, government agencies and regular internet users could no longer update their security software or other software, such as Windows (Vendil Pallin 2024).

Moreover, the unofficial truce that had long existed between the Russian government and cyber criminals from the former Soviet republics broke down. Whereas formerly, criminal hacker networks were allowed to conduct their activities in peace as long as they did not attack Russian assets, many of the hackers now turned against Russia as bands of Ukrainian and Russian hackers ceased cooperation. Cybercrime in Russia increased and remains a pressing problem. Together with the surge in politically motivated cyberattacks, cyber criminality has created a noise of war. One fear in Russia is that this fog of cyberwar will make it more difficult to detect the most advanced and dangerous attacks (Vendil Pallin 2024).

Cyber operations as a hybrid tool?

There was no cyber-Armageddon but offensive cyber operations served as a reconnaissance and influence tool, and as a way of arranging the battlefield before the invasion. They were also used to increase the effect of the full-scale invasion's kinetic warfare. Cyber operations like these are often described as examples of Russian hybrid warfare, as tools that Russia resort to in order to test and weaken the opponent without invoking NATO's Article 5 within the alliance. According one of Russia's most influential military thinkers, the former deputy minister of defence and former chair of the Defence Council, Andrei Kokoshin, the only novelty in so-called hybrid warfare is the cyber measures. Just as we in the West only think of measures directed against us as hybrid measures, however, Russian thinkers only write about hybrid warfare as something that the West does to Russia. Following this logic, Russia regards the cyberattacks against it as part of Western hybrid warfare to undermine Russian resilience and defence capability, albeit spear-headed by Ukraine as a western proxy.

At first glance, it would seem that the cyber operations that Russia engaged in to form the battlefield in Ukraine are different from the activities it directs towards other European countries. However, if we take into account Russia's strategic goals of establishing and gaining recognition for a sphere of interest in Europe, this is what stands behind the overused phrase "changing the European security order". Russia's offensive cyber operations are thus part of a larger strategic goal to weaken European unity, and its resilience and will to support Ukraine. If successful, such efforts will indeed shape Russia's battlefield for the better in Ukraine, but also attain the political goal of being able to leverage more power against individual European countries.

References

Concept of the Foreign Policy of the Russian Federation [unofficial translation], Presidential Decree no. 229, 31 March 2023 (https://mid.ru/en/foreign_policy/fundamental_documents/186058).

Conceptual Views on the Activity of the Armed Forces in the Information Sphere (in Russian), Ministry of Defence, 2011 (https://info.publicintelligence.net/RU-CyberStrategy.pdf.

Information Doctrine of the Russian Federation (in Russian), Presidential Decree No. 646, 5 December 2016, http://scrf.gov.ru/security/information/document5/.

Kello, Lucas. The Virtual Weapon and International Order. London: Yale University Press, 2018.

"Kontseptsiia Strategii kiberbezopasnosti", Voprosy kiberbezopasnosti, No. 12 (2014): 2–4. https://cyberrus.info/wp-content/uploads/2014/03/2-4.pdf

Moore, Daniel. Offensive Cyber Operations: Understanding Intangible Warfare. London: Hurst & Company, 2024.

National Security Strategy of the Russian Federation (in Russian), Presidential Decree no. 400, 2 July 2021 (http://kremlin.ru/acts/bank/47046).

Nilsson, Per-Erik. Unraveling the Myth of Cyberwar - Five Hypotheses on Cyberwarfare in the Russo-Ukrainian War (2014–2023). FOI-R--5513--SE, Stockholm: Swedish Defence Research Agency (FOI), December 2023.

Schulze, Matthias & Mika Kerttunen. "Cyber Operations in Russia's War Against Ukraine", SWP Comment, No. 23, April 2023.

Vendil Pallin, Carolina. Rysslands cyberberedskap på hemmaplan [Russia's Cyber Preparedness at Home], FOI-R--5611--SE, Stockholm: Swedish Defence Research Agency (FOI), August 2024.

Reflections on the model of future military conflicts

Katri Pynnöniemi

Introduction

A report published by the Military Institute of the Russian General Staff Academy in late 2021argued that "it is necessary to create a 'security zone' around the borders of the Russian Federation – that is, to ensure a secure external environment, which will make it possible to address tasks aligned with national interests and Russia's role on the global stage" (Korzhevskii 2021: 60). The report epitomizes a shift from a classical definition of war to a revisionist vision where non-traditional and indirect means are prioritised over traditional armed struggle (Minic 2023: 2; Clark 2020: 21–22). In accordance with the revisionist vision of a "new type of war" (Serzhantov, Smolovyj and Dolgopolov 2021), the creation of Russia's "security zone" is seen as a process of eight phases, which combine the use of non-military measures with those of the armed forces. An analysis of the eight-phase scheme highlights important nuances in the Russian debate that have practical relevance for western policy.

Future military conflict in eight phases

The eight-phase model integrates different positions, aligning revisionist and traditionalist ideas of war in a single scheme. It represents war as a process where different forms of violence are used in combination until the final objectives are achieved. Similar ideas have been presented earlier (Shalamberidze 2011) and discussed at length after publication of Gerasimov's 2013 article on combination of military and non-military means in resolution of interstate conflicts (Kukkola 2022; Baumann and Pynnöniemi 2025). The model presented briefly below first appeared in 2021 (Serzhantov, Smolovyj and Dolgopolov 2021). It is also discussed in the above-mentioned report, in a section about 'contemporary forms of interstate conflict' (Korzhevskii 2021). A third version was published in late 2022 in an article by the then director of the Centre for Military-strategic Research at the Russian General Staff Academy, A. V. Smolovy (2022).

In the model, military conflict is divided into eight phases. The first four phases can be conceptualised as revolutionary,[1] or political (hybrid), warfare targeting the military-political leadership of the country. Thus, the conflict begins with the "creation of favourable conditions for the outbreak of aggression", through support for opposition forces and political destabilisation (phase 1). This is followed by strategic disinformation (phase 2), corruption and blackmail of the political and military leadership (phase 3), and activation of non-military and indirect (but violent) measures such as assassination of key stakeholders, sabotage and support for irregular forces at the phase 4. The aim is to paralyse resistance, create an artificial crisis with pseudo-political agencies that are used to legitimise intervention and, ultimately, secure the interests of the attacking state (Smolovy 2021: 83). If the attacker fails to attain its objectives during the first four phases, the conflict transforms into a traditional military conflict. The subsequent three phases are an air and sea blockade (phase 5), a military attack on critical military and political targets (phase 6) and a full-scale military invasion (phase 7) (Serzhantov, Smolovyj and Dolgopolov 2021: 27; Smolovy 2022: 83; Korzhevskii 2021: 51–53).

[1] A recent report suggests: 'the Russian theory of change is not premised on convincing a majority, but rather on empowering politicians in the target country who will spearhead the implementation of policy favourable to Russia. The objective is elite capture' (Watling et al. 2024: 13).

In both versions published before the full-scale invasion of Ukraine, priority is assigned to the first four phases. Importantly, the role of 'non-classical actors', such as irregular armed groups, terrorists and criminal organizations, as well as groups used for the purposes of sabotage and rioting, is emphasized at the expense of regular armed forces (Korzhevskii 2021: 52–53). The report argues:

> These non-classical actors are ideally suited for conducting new-type hybrid wars – a special kind of mobile, sabotage-terrorist, quasi-insurgent warfare, three-quarters of which consists of covert operations and operational combinations by intelligence services (including the intelligence networks of drug cartels, transnational criminal organizations, etc.), in which traditional armies prove too unwieldy and therefore powerless. (Korzhevskii 2021: 53)

The same point is made in the concluding section of the report, where it is argued that "in the context of modern conflicts, traditional methods of warfare associated with the use of regular forces are being eroded", as it becomes more difficult to distinguish between civilians and military participants in the conflict, wars are not formally declared and are no longer fought only on the territory of one country, and the international legal norms and rules of warfare are not observed (Korzhevskii 2021: 555). This sets the stage for the final phase of military conflict: complete liquidation of resistance and the creation of a new political system subordinate to the interests of the attacker (phase 8) (Smolovy 2022: 83; Korzhevskii 2021: 53; Serzhantov, Smolovyj and Dolgopolov 2021: 27).

The article published following Russia's full-scale invasion of Ukraine interprets the original scheme anew and introduces "a model of future military conflict" (Smolovy 2022: 83). Unlike the earlier versions, it emphasises that the sequence of phases can vary, and that not every phase is essential. Furthermore, it underlines that although the role of non-military measures has increased, the key element in all phases of an interstate conflict remains "sufficient and necessary use of military force" (Smolovy 2022: 83). The emphasis that "winning the war" requires "a completely new way of waging war" is also noteworthy (Smolovy 2022: 86; also Serzhantov and Muzyakov 2023: 37). In this "combination war", there are no clearly demarcated boundaries between combatants and civilians, battlefield and rear or political entities waging war and the neutral states. Smolovy declares that "Nothing is forbidden" (2022: 86), with a fervour reminiscent of Clausewitz's formulation of absolute war. Absolute war, wrote Clausewitz, "is an act of violence pushed to its utmost bounds" and fought until the complete submission of the enemy to the will of the attacker (Clausewitz 1968: 103–104). What is left out of the analysis in this and other versions of the model is what Clausewitz called "friction", a set of cultural, physical and emotional constraints that limit and derail the conduct of war (Clausewitz 1968: 164–167).

Conclusion

Analysis of the model and the discussion around it highlight a set of key assumptions about future military conflicts. First, there is an expectation of coordinated use of diverse actors (criminal networks, terrorists, local irregular armed groups and private military companies) that are not under direct government control, while the role of the armed forces in this network is not really addressed. Second, there are no legal, moral or spatial boundaries to action, and thus the war has no clear ending. It is perceived as a process in which different phases alternate. This can be interpreted as a tacit acknowledgement that the suggested objective of war – complete subordination of the target country – is unattainable. Finally, although the model can be used to explain Russian strategy and behaviour, inherent in it is an assumption of threat to Russia. In other words, the model legitimises "active defence" against threats to the Russian state and its idea of a presumed right to a "security perimeter" beyond its internationally recognised borders.

In conclusion, it can be argued that the model explains Russian strategy (strategic objectives) in terms of three parallel types of war: revolutionary, traditional and degenerate. The revolutionary war is fought by irregular, secret and criminal networks and aims to create a dual power as a cover for regime change. Traditional war is a means for securing the success of the first phase. Finally, degenerate war is inherent in the model, as it sets no legal, moral or spatial boundaries for action. An analysis of Russian debates about future military conflict is important as it may provide more clarity on key assumptions guiding Russia's strategy during the war as well as peacetime.

References

Baumann, Mario and Katri Pynnöniemi (2025). European Security in the Era of Hybrid Warfare. Active Measures in Russia's Confrontation with Europe. DGAP Policy Brief, 20. European Security in the Era of Hybrid Warfare | DGAP

Clausewitz, Carl Von (1968). On War. Edited with an introduction by Anatol Rapoport. London: Penguin Books.

Clark, Mason (2020). Russian Hybrid Warfare. ISW. URL: https://www.understandingwar.org/sites/default/files/Russian%20Hybrid%20Warfare%20ISW%20Report%202020.pdf.

Serzhantov, A. V., A. V. Smolovyi, and I. A. Terent'ev (2022). Transformatsiya soderzhaniya voinu: kontury voyennykh konfliktov budushchego. Voennya Mysl 6, pp. 19–30.

Serzhantov, A. V., A. V. Smolovyi, and A. V. Dolgopolov (2021). Transformaciâ soderžaniâ vojny: ot prošlogo k nastoâŝemu — tehnologii gibridnyh vojn. Voennya Mysl 2, pp. 20–28.

Serzhantov, A. V. and S.I. Muzyakov (2023). Mezgosudarstvennoe protivoborstvo v sovremennyh usloviyah: factornyi analiz. (interstate confrontation in current conditions: factor analysis). Vestnik Akademii Voennyih Nauk 4(85), 33–40.

Smolovyi, A.V. (2022). Voennie konflikti buduschevo: sovremennyi bzglyad. Vestnik Akademii Voennyih Nauk, 3(80), 80–87.

Korzhevskii, A. S. (Ed.). (2021). Прогнозируемые вызовы и угрозы национальной безопасности Российской Федерации и направления их нейтрализации. RGGU. URL: https://vagsh.mil.ru/upload/site17/document_file/Hoyla2YLpO.pdf.

Kukkola, J. (2022). The Promise of Cunning: Asymmetry, Indirectness, and Non-Military Measures as Focal Points of New Russian Military Art. [in Finnish] Research Reports 22, Department of Warfare, National Defence University: https://www.doria.fi/bitstream/ handle/10024/186010/Oveluuden%20lupaus_Kukkola_verkkoversio.pdf?sequence=1&isAllowed=y (accessed October 23, 2025);

Minic, Dimitri (2023). How the Russian army changed its concept of war, 1993–2022, Journal of Strategic Studies, DOI: 10.1080/01402390.2023.2199445.

Watling, Jack, Oleksandr V. Danylyuk and Nick Reynolds (2024). The Threat from Russia's unconventional warfare beyond Ukraine, 2022-2024. RUSI Special Report. URL: https://static.rusi.org/SR-Russian-Unconventional-Weapons-final-web.pdf.

Carolina Vendil Pallin

Researcher, Swedish Defence Research Agency.

Katri Pynnöniemi

Professor, Russian Security Studies at the University of Helsinki and the Finnish National Defence University.

About SCEEUS

The Stockholm Centre for Eastern European Studies (SCEEUS) at the Swedish Institute of International Affairs (UI) is an independent Centre, funded by the Swedish Government, established in 2021. The Centre conducts policy relevant analysis on Russia and Eastern Europe and serves as a platform and meeting place for national and international discussions and exchanges on Russia and Eastern Europe. Any views expressed in this publication are those of the author.

Cover Photo: AP/ Iryna Rybakova

Previous SCEEUS Publications

Unequal partners: Consequences of the power shift in Sino-Russian relations by Hugo von Essen and Patrik Andersson
SCEEUS-NKK Report No.6

What would security guarantees for Kyiv mean? by Andreas Umland
SCEEUS Report No. 11, 2025

SCEEUS STOCKHOLM CENTRE FOR EASTERN EUROPEAN STUDIES

THE SWEDISH INSTITUTE OF INTERNATIONAL AFFAIRS