The RUSI Journal

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/rusi20

Invisible Lines, Visible Impact: How Territorial Security Influences Russian Cyber Security Strategy

Tom Johansmeyer, Gareth Mott & Jason R C Nurse

To cite this article: Tom Johansmeyer, Gareth Mott & Jason R C Nurse (2025) Invisible Lines, Visible Impact: How Territorial Security Influences Russian Cyber Security Strategy, The RUSI Journal, 170:1, 20-31, DOI: 10.1080/03071847.2025.2458143

To link to this article: https://doi.org/10.1080/03071847.2025.2458143

Published online: 19 Feb 2025.

Research Article
RUSI Journal

How Territorial Security Influences Russian Cyber Security Strategy

Invisible Lines, Visible Impact

Tom Johansmeyer, Gareth Mott and Jason R C Nurse

The characterisation of the cyber domain as 'borderless' downplays the important relationship between cyber security and concerns over territorial integrity. The evolution of Russia's national security strategy since 2015 has shown that the two are tightly connected, and grounded in the country's history. Tom Johansmeyer, Gareth Mott and Jason R C Nurse show how Russian cyber security strategy sees the cyber domain as a strategic environment that interlocks with concerns over territorial integrity and physical security while also providing implicit justification for pursuing a strategy of regional hegemony.

Cyber threats may be seen as borderless, but that is only superficially true. The imaginary lines on the map become quite real when states contemplate the threats to their normal function and very existence. Although cyber attacks can be launched without actors having to cross them physically, borders do have direct links to the motivations associated with cyber security strategy. Territorial security can inform cyber security strategy – and even be used to justify controversial objectives and concerns. That borders may not be completely discernable and delineatory within the cyber domain does not mean they are not influential. They influence factors such as the motivation to attack (or spy) and can drive behaviour that is focused on protection both in the cyber domain and with regard to territorial security. Russia's views on cyber security exemplify this perspective, leading to a clear and direct research question: How do Russia's territorial concerns influence the state's cyber security strategy?

From 2015 through to the present, the cyber and information security elements of the Russian national security strategy (NSS) have clear links back to the vulnerabilities associated with long land borders. These borders naturally abut adversaries and strategic threats,[1] directly revealing the connection between territorial security and cyber strategy. This connection has become amplified over a period bookended by Russia's invasions of Ukraine (2014 and 2022). The threats chronicled in the 2015 NSS[2] indicate further institutionalisation of cyber security concerns than in the edition published six years later. This article makes a unique contribution to the historical literature by showing how the evolution of Russia's cyber security strategy from 2015–21 drew from the initial invasion and culminated in the recent invasion, and draws from a rich history of border-related anxiety.

1. Monica Kello, 'Russia's Strategic Culture Drives its Foreign Hacking', Binding Hook, 15 January 2024, <https://bindinghook.com/articles-hooked-on-trends/russias-strategic-culture-drives-its-foreign-hacking/>, accessed 2 April 2024.
2. 'Russian National Security Strategy, December 2015 – Full-text Translation', <https://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf>, accessed 16 January 2025.

The threat felt by Russia is intensified by its aggregate land borders; these are among the longest in the world and, collectively, are inherently vulnerable. *Courtesy of Amina Abdovic / Alamy*

Russia's contemporary ambitions are more nuanced than a reconstitution of the Soviet Union[3] or the 18th century Russian Empire.[4] Rather than simply reaching to reaccumulate territory, Russia's strategy, and indeed actions, over the past 15 years are indicative of a state that merges aggressive tendencies with meaningful fears with regard to its territorial integrity. Adjacency to adversaries calls for careful security strategy, even if the threat posed by those adversaries may be exaggerated to facilitate a broader agenda of self-interest. Within Russian strategic thinking, an ongoing tension between expansionism and defensiveness – with each feeding the other[5] – has yielded the strategic need for capabilities that provide for the protection of its borders across domains, including those that are not physical. Further, this has manifested in a way that prioritises offensive activity as a buffer to keep conflict outside its borders, which, although aggressive, has some foundation in Russia's history of being invaded.

The evolution of Russia's views on cyber security through its NSS documents since 2015 is inextricably linked with its longstanding fears of adversaries on, or near, its borders. Consequently, this article explores the extent to which Russia's territorial concerns influence its cyber security strategy. It proceeds with a review of the historical literature on both territorial security and cyber strategy, an analysis of the interplay between cyber security and territorial integrity, and a discussion of how they influence each other. Ultimately, the notion that cyber is 'in the wires'[6] is misleading. What happens in the cyber space is shaped by Russia's territorial 'container',[7] and concerns over the durability of that container manifest in the cyber domain. Ultimately,

3. Gabriel Gavin, 'Putin's Push for a New USSR Reawakens the Bloody Chaos of Soviet Collapse', *Politico*, 19 September 2022.
4. Mark Temnycky, 'Putin's Dreams of a New Russian Empire are Unraveling in Ukraine', *UkraineAlert*, blog of the Atlantic Council, 25 April 2023, <https://www.atlanticcouncil.org/blogs/ukrainealert/putins-dreams-of-a-new-russian-empire-are-unraveling-in-ukraine/>, accessed 23 June 2024.
5. Tom Johansmeyer, Gareth Mott and Jason R C Nurse, 'Cyber Strategy in Practice: The Evolution of US, Russian, and Ukrainian National Cyber Security Strategies through the Experience of War', *RUSI Journal* (Vol. 169, No. 3, 2024), p. 6.
6. Johansmeyer, Mott and Nurse, 'Cyber Strategy in Practice', p. 3.
7. John Agnew, 'The Territorial Trap: The Geographical Assumptions of International Relations Theory', *Review of International Political Economy* (Vol. 1, No. 1, 1994), p. 68.

DOI: 10.1080/03071847.2025.2458143

Russia's cyber security strategy draws heavily from the state's history and experience, reaching back to decades and centuries of history that predates the internet age. The future may not be bound by the past, but is certainly shaped by it.

Conceptualising Russian Territoriality

Territoriality is more than merely a container for a society and state, according to political geographer John Agnew.[8] It is, rather, a dynamic entity influenced by and engaging with economic activity, other states and societies, and even the people within its borders. In fact, those borders, much more than mere 'container boxes' of nation states,[9] define the interactions between states at their most fundamental level, simply by delineating where each ends, and the rest of the world begins. Borders can broadly be considered 'meeting points' among states for a wide range of activities, including economic activity, cultural engagement and, of course, 'clash'.[10]

Agnew's observation that the end of the Cold War reopened the question of spatiality regarding the identity of the state (and by extension, sovereignty),[11] was well-timed, given that the dissolution of the Soviet Union came at approximately the same time as the advent of commercial and popular internet use. The main political wedge between the state and dependence on territoriality came alongside an economic, social and technological lever for exacerbating the effects of that wedge. The notion that the internet has somehow made the world smaller and heightened multidirectional interactions by states and individuals across longer distances is true, but it follows a trajectory in which scholar Paul Virilio has observed, that place matters less than it has in the past, because technology effectively shortens physical distance. Specifically he writes that 'the strategic value of the non-place of speed has definitely supplanted that of place'.[12]

It would be hasty to deprive the state of a significant connection to territoriality. One can use the notion of geography as shorthand for a collection of characteristics – from technology stack to language and business customs associated with a country or region[13] – but this only captures the characteristics of the population within borders without addressing attendant issues of sovereignty.

Territoriality and Sovereignty

Even with the perceived erosion of the dependence of the state on the physical ground it occupies, the connection between territoriality and sovereignty remains strong. Although there are cases where states are beginning to contemplate how they would exist without territory – as climate change is forcing Tuvalu to do[14] – the notion that a state can exist, survive and thrive strictly in the wires and without its own physical location is difficult to imagine, even if there is some limited precedent in the notion of 'governments in exile'.[15] The state may not be the sum of its borders, as Agnew argued, but it is certainly influenced by those borders, if for no other reason than that those borders define the parameters by which a state interacts with other states (and the rest of the world in general), as Vladimir Kolossov and James Scott contend.[16]

A lack of clear, traditional borders (or some sort of digital equivalent) does not necessarily constrain state activity in the cyber domain. States exert influence over the borderless domains in which they operate. According to Forrest Hare, 'the relevance of a nation's borders in each domain is related to a nation's willingness and ability to assert their

8. *Ibid.*
9. Vladimir Kolossov and James Scott, 'Selected Conceptual Issues in Border Studies', *Belgeo* (Vol. 1, 2013), pp. 3, 6.
10. Marco Mogiani, 'Studying Borders from the Border: Reflections on the Concept of Borders as Meeting Points', *Geopolitics* (Vol. 28, No. 3, 2023), p. 1324.
11. Agnew, 'The Territorial Trap', p. 55.
12. Paul Virilio, *Speed and Politics* (Los Angeles, CA: Semiotext(e), 2007), p. 149.
13. Frank Cremer, Barry Sheehan, Martin Mullins, Michael Fortmann, Stefane Materne, and Finbar Murphy; 'Enhancing Cyber Insurance Strategies: Exploring Reinsurance and Alternative Risk Transfer Approaches', *Journal of Cybersecurity* (Vol. 10, No. 1, 2024), p. 8.
14. Delf Roth et al., 'Digital Tuvalu: State Sovereignty in a World of Climate Loss', *International Affairs* (Vol. 100, No. 4, 2024), pp. 1491–509.
15. Alex Green, 'UK Small Island Developing States Strategy', evidence submitted to the International Development Committee, UK Parliament, 16 June 2023, <https://committees.parliament.uk/writtenevidence/121909/html/#_Toc137564410>, accessed 15 October 2024.
16. Kolossov and Scott, 'Selected Conceptual Issues in Border Studies', pp. 3, 6.

sovereignty in them'.[17] It is at this point that territorial integrity and cyber security (and operations) begin to interact.

At the same time, however, cyberspace is not strictly a 'borderless' domain in the way that states (and other actors) interact with and within it. Actions – for instance, offensive operations or target hardening – will still take place against physical devices and within identified borders. Thus, notably, the term 'borderless', as used in the context of interactive agency in cyberspace, relates to the ability of actors to act in a less geographically constrained way than traditional means of conflict. Cyberspace, as an artificial 'fifth sphere' of power projection, is simultaneously a physical infrastructure and 'information' ecosystem. The two are inextricably linked.[18]

The Territorial Integrity of Russia and its Neighbours

Russia's perception of its sovereignty and territorial integrity – and thus its borders – is grounded in the same simultaneous sentiments of victimhood and strength that have vacillated throughout its NSS for nearly all of the past decade.[19] The state wants to be recognised as 'a great power, which involves maintaining influence in its immediate region', yet it is also sufficiently concerned about its own direct security that defending its own territory is Russia's '[f]irst and foremost' priority.[20] For a state that is perpetually in fear of its neighbours and the blocs with which they align, this should come as no surprise. The ongoing threat that Russia believes that the US and NATO poses, particularly in and among the former Soviet bloc states that are now NATO members, has clearly been identified as a vulnerability for Russia and contributes to its perceived need for asymmetric self-defence capabilities.[21]

Russian cyber security strategy involves a series of nested priorities and domains, with information security forming the overarching priority, and the focus of the strategy on dominating the overarching 'information landscape', which itself 'is regarded as a warfare domain'.[22] Within this environment, one sees a split between information operations (for example, foreign influence and disinformation) and what Western states would call cyber, such as activity intended to disrupt the function of technological systems. In the Russian view of cyber and information warfare, however, it is clear that the use of cyber is in large part to assert broader information domain dominance than to disrupt technology or systems operations.

The broad theme of information threats from the West goes back at least to the 2000 NSS[23] and was expressed by Russian military scholar M Prysiazhniuk, who recalls that '[f]rom the early 1970s to the late 1990s, the Americans were the absolute leaders in the field of information confrontation'.[24] In fact, noted Russian cyber security scholar and former KGB officer Igor Panarin claims that Western use of information warfare tools twice led to the collapse of the Russian state – first with the end of the Russian Empire in 1917 and again with the fall of the Soviet Union.[25] This ultimately led Panarin to advocate for 'the mechanisms of

17. Forrest Hare, 'Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security?', in Christian Czosseck and Kenneth Geers (eds), *The Virtual Battlefield: Perspectives on Cyber Warfare* (Amsterdam: IOS Press, 2009), pp. 88–105.
18. Daniel T Kuehl, 'From Cyberspace to Cyberpower: Defining the Problem', in Franklin D Kramer, Stuart H Starr and Larry K Wentz (eds), *Cyberpower and National Security* (Dulles, VA: Potomac Books, 2009).
19. Johansmeyer, Mott and Nurse, 'Cyber Strategy in Practice', p. 6.
20. Andrew Radin, Alyssa Demus and Krystyna Marcinek, 'Understanding Russian Subversion: Patterns, Threats, and Responses', RAND, February 2020, p. 3, <https://apps.dtic.mil/sti/pdfs/AD1096326.pdf>, accessed 9 July 2024.
21. Peter A Mattsson, 'Russian Military Thinking – A New Generation of Warfare', *Journal on Baltic Security* (Vol. 1, No. 1, 2015), pp. 64–65.
22. Michael Connell and Sarah Vogler, 'Russia's Approach to Cyber Warfare', CNA Analysis and Solutions, September 2016, p. 3, <https://apps.dtic.mil/sti/pdfs/AD1019062.pdf>, accessed 18 October 2024.
23. See Janne Hakala and Jazlyn Melnychuk, *Russia's Strategy in Cyberspace* (Riga: NATO Strategic Communications Centre of Excellence, 2021), p. 9.
24. M Prysiazhniuk, 'Peculiarities of the Modern Period of Informational-Psychological Confrontation: Global Confrontation of a New Type', in Michelle Grisé et al., *Russian and Ukrainian Perspectives on the Concept of Information Confrontation: Translations 2002-2020* (Santa Monica, CA: RAND, 2022), p. 41, <https://www.rand.org/content/dam/rand/pubs/research_reports/RRA100/RRA198-7/RAND_RRA198-7.pdf>, accessed 10 December 2024.
25. Ofer Fridman, 'The Russian Perspective on Information Warfare: Conceptual Roots and Politicisation in Russian Academic, Political, and Public Discourse', *Defence Strategic Communications: The Official Journal of the NATO Strategic Communications Centre of Excellence* (Vol. 2, Spring 2017), pp. 75–76.

the UN and the mechanisms of Russian-American consultations to create new rules of the game, rules of information balance and rules for protecting our sovereign national information space'.[26] Essentially, Panarin sees the use of information operations as the adoption of a form of warfare already pioneered by Russia's principal adversary rather than as an innovation intended to attack an unwitting victim. This sentiment is echoed by Andrei Ilnitsky, an adviser to the Russian defence minister, who sees Russian activity in the information domain as matching NATO's capabilities rather than taking a fundamentally different approach.[27]

Gregory Tulchinsky provides insight into the advantages of the asymmetric nature of information warfare. These would clearly benefit Russia, given its economic and military disadvantages compared with the capabilities of the US and NATO. Specifically, Tulchinsky speaks not just to the ability to evade attribution and bask in ambiguity, but also to the 'mythicisation of "information wars"'.[28] However, the reach of the information domain is intended to extend to the territorial. Russian military strategy scholar Vladimir Slipchenko sees victory in the information and cyber domain as enabling 'the capture of [adversary] territory', along with the achievement of economic and political objectives.[29]

The result of Russia's views on information warfare (cyber and otherwise) has been a carefully balanced approach to security, even if some may characterise it as 'reckless'.[30] The use of technology and information capabilities has allowed Russia to engage in security activity, informed by its strategy, in a manner that maximises its ability to defend itself (or operate in a more forward manner without retribution or meaningful response) without having to contend with NATO's traditional overmatch capabilities. As General Valery Gerasimov observes, technology can help to close the gap, and 'contactless actions' can be used to achieve military goals without risking exposure to traditional conflict.[31] Gerasimov's perspective, and his broader views on information warfare, provide a foundation for the expansion of Russia's influence beyond its physical borders while remaining in the spirit of sovereignty.

> An expansion of Russia's sphere of influence over its neighbours – which were overtly within its sphere of influence during the Soviet era – would provide security to Russians abroad and also form a layer of physical protection relative to the country's borders

Russia has been quite candid about its security concerns. It takes a more contemporary view of security that spans societal, economic and technological domains (among others) to discuss what it sees as the greatest threats to its existence and normal function. The temptation to ascribe the disclosure of those vulnerabilities as a justification for aggressive behaviour – which is consistent with the notion of influence and control over neighbouring states in the name of one's own security – must be counterbalanced with the recognition of the longstanding and important historical security concerns of a country with long land borders that have a history of being violated. This includes but is not limited to the devastation that Russia sustained during the Great Patriotic War – its conflict with Germany as part of the Second World War.[32] Again, the history of victimhood due to incursion by foreign powers continues to

26. Keir Giles, '"Information Troops" – A Russian Cyber Command?', in C Czosseck, E Tyugu and T Wingfield (eds), '3rd International Conference on Cyber Conflict', Tallinn, 2011, p. 50, <https://ccdcoe.org/uploads/2018/10/InformationTroopsARussianCyberCommand-Giles.pdf>, accessed 18 October 2024.
27. Marina Miron and Rod Thornton, 'The Use of Cyber Tools by the Russian Military: Lessons from the War Against Ukraine and a Warning for NATO?', *Applied Cybersecurity and Internet Governance* (Vol. 3, No. 1, 2024), p. 150.
28. Fridman, 'The Russian Perspective on Information Warfare', p. 77.
29. Vladmir Slipchenko, quoted in Keir Giles, *Handbook of Russian Information Warfare*, *Fellowship Monograph No. 9* (Rome: NATO Defence College, 2016), p. 17.
30. Eugene Rumer, 'The Primakov (Not Gerasimov) Doctrine', Return of Global Russia, Carnegie Endowment for International Peace, June 2019, p. 5.
31. Wesley P White, 'The Cyber Crucible: Eastern Europe, Russia, and the Development of Modern Warfare', in Mark D Vertuli and Bradley S Loudon (eds), *Perceptions are Reality: Historical Case Studies of Information Operations in Large-Scale Combat Operations* (Fort Leavenworth, KS: Army University Press, 2018), p. 31.
32. Kello, 'Russia's Strategic Culture Drives its Foreign Hacking'.

feed into the 'national paranoia' noted by Monica Kello, which itself is supercharged by 'the notion of Russian exceptionalism'.[33]

That exceptionalism, in fact, links Russia's cyber security strategy to its traditional territorial security considerations. The war in Ukraine – as it has evolved since 2014 and which Vladimir Putin links to Russian exceptionalism and regional hegemony[34] – demonstrates this. An expansion of Russia's sphere of influence over its neighbours – which were overtly within its sphere of influence during the Soviet era – would provide security to Russians abroad and also form a layer of physical protection relative to the country's borders. Moreover, as observed by Slipchenko, the asymmetric and non-kinetic capabilities associated with cyber operations could provide the means to enact such a strategy focused on territorial integrity. The asymmetric nature of cyber and information operations can help to 'achieve information supremacy without crossing borders' and, more generally, from a point of disadvantage relative to its adversaries.[35] In Russian security strategy thinking, this is both an opportunity and a vulnerability, as Russia spends considerable time focused on the threats of foreign information violating its own information space and consequently affecting its citizens.

Methodology

This article evaluates how Russia's territorial security concerns influence its approach to cyber security strategy. It looks primarily at how the focus on cyber security and societal security has evolved from 2015–21, as presented in Russia's two NSS documents of that period, and contemplates additional security strategy materials published during the period as well as outside analysis. The focus on these two specific NSS documents comes from the fact that they cover a pivotal period in recent relations between Russia and Ukraine, specifically the eight-year period (2014–22) covering the lower-intensity conflict in Ukraine and rise of cyber operations by Russia. The 2015 NSS directly follows the 2014 invasion, and the 2021 NSS directly precedes the 2022 invasion, thus interlocking with a pivotal period in recent relations between the two states.

The analysis below compares several narratives released by states in the form of NSS (and other related strategy) documents with regard to cyber security, specifically excluding materials that are private, confidential or otherwise sensitive and intended to support cyber security strategy on a more actionable basis. This study again uses 'interpretive' approaches to security studies, identifying and evaluating the themes in Russian NSS thinking from 2015–22 – which addresses the 2014 low-intensity invasion of Ukraine and the 2022 large-scale invasion – relevant to the interplay between territorial integrity and cyber security. Ultimately, the study shows that Russia's views on the security of its borders and its cyber security strategy are indeed interconnected.

How Territorial Security Concerns Shape Cyber Strategy

Russia has declared itself exposed to a wide range of traditional and unorthodox security threats from a large bloc of adversaries. Some of them are territorial, such as the prospect of Ukrainian NATO membership.[36] Some are intangible – ranging from economic warfare in the form of sanctions,[37] to an ongoing information assault on 'Russia's traditional values and historical legacy'.[38] Importantly, Russia states explicitly the threats to its borders via the cyber domain, ruing the 'use of information and communications technology to interfere in the internal affairs of states, [and] undermine their territorial integrity'.[39] Treated separately, they show

33. *Ibid.*
34. Vladimir Putin, 'On the Historical Unity of Russians and Ukrainians', Kremlin.ru, 12 July 2021, <http://en.kremlin.ru/events/president/news/66181>, accessed 19 July 2024.
35. Bilyana Lilly and Joe Cheravitch, 'The Past, Present, and Future of Russia's Cyber Strategy and Forces', in T Jančárková et al. (eds), *12th International Conference on Cyber Conflict* (Tallinn: NATO CCDCOE Publications, 2020), p. 137.
36. Ronald Suny, 'Ukraine War Follows Decades of Warnings that NATO Expansion into Eastern Europe Could Provoke Russia', *The Conversation*, 28 February 2022.
37. Russian Federation, 'О Стратегии национальной безопасности Российской Федерации' ['On the National Security Strategy of the Russian Federation'], 2021, p. 38.
38. Dmitri Trenin, 'Russia's National Security Strategy: A Manifesto for a New Era', Commentary, Carnegie Moscow Center, 6 July 2021, <https://carnegiemoscow.org/commentary/84893>, accessed 9 April 2022.
39. Russian Federation, 'О Стратегии национальной безопасности Российской Федерации' ['On the National Security Strategy of the Russian Federation'], p. 19.

concerns in one domain that manifest as security problems (or perceived solutions) in another. Together, they provide a holistic view of how Russia feels threats on its borders and – at least in part – turns to the cyber domain for remediation.

Historical Border Threats and Today's Security

Russia has experienced a long history of foreign threats and territorial invasion, some of which remains part of its societal memory, with the Great Patriotic War leaving a cultural imprint. Although the generation that fought is passing and those who know them ageing,[40] the sacrifices made during the war continue to be remembered and celebrated,[41] particularly within the context of Soviet nostalgia.[42] The losses sustained on its own soil are still used to justify a more forward-leaning strategic posture, and the effects experienced by the Soviet Union (rather than just Russia itself) imply a shared history that can be used to justify expansion as part of a historical obligation to protect the former Soviet republics victimised during the war.[43] The notion of threats on the border appears to be intertwined with the DNA of the Soviet Union itself, given that its first 20 years as a state were nestled between two world wars, both of which had had profound security implications for the budding nation. This has contributed to the persistence of the state's perception of insecurity. Such perceptions have been sustained since the dissolution of the Soviet Union by the growth of NATO through former Warsaw Pact member states, and the recent additions of Sweden[44] and Finland.[45]

The threat felt by Russia is intensified by its aggregate land borders; these are among the longest in the world and, collectively, are inherently vulnerable. Moreover, Russia's territorial security is frustrated by the fact that few of those borders are natural.[46] This suggests a decrease in perceived security, not just due to the obstacles provided by natural boundaries, but also because a 'legitimate state's border depends on international legal recognition and its geographical location with respect to bordering states'.[47] Natural borders – such as rivers and mountain ranges – can reduce the ambiguity of where borders lie and why their locations have been chosen. The existence of borders relies on the consent of adjacent states, and that exercise is more negotiated where nature has not done the heavy lifting already.

Further, Russia's vast land borders have a history of being compromised. The state 'has repeatedly had to mobilize its society to counter foreign aggressions',[48] and even the memory of that can be compelling. Setting aside whether the dissolution of the Soviet Union could be seen as such an event – potentially over the objections of President Putin[49] – it is perilously easy to lose sight of the territorial risks Russia faces, given that it has not experienced such an incursion in approximately 50 years. Yet, to say that several decades should be enough to dull the national paranoia Kello mentions is to overlook an important part of Russia's cultural memory. Even if one fails to trust the source, the experiences of Putin's family (and others across Russia) during

40. Vladimir Putin, 'Vladimir Putin: The Real Lessons of the 75th Anniversary of World War II', *National Interest*, 18 June 2020.
41. Miriam J Dobson, 'Russia: Victory Day 2022 and Why Commemoration of the End of WWII Matters Today', *The Conversation*, 29 April 2022.
42. David Masci, 'In Russia, Nostalgia for Soviet Union and Positive Feelings about Stalin', Pew Research Center, 29 June 2022, <https://www.pewresearch.org/short-reads/2017/06/29/in-russia-nostalgia-for-soviet-union-and-positive-feelings-about-stalin/>, accessed 23 June 2024.
43. For example, see Simone Benazzo, Martina Napolitano and Marco Carlone, 'Gagauz Resist Moldova's Embrace of West', *Balkan Insight*, 3 January 2018, <https://balkaninsight.com/2018/01/03/gagauz-resist-moldova-s-embrace-of-west-01-01-2018-1/>, accessed 30 June 2024.
44. NATO, 'Sweden Officially Joins NATO', 7 March 2024, <https://www.nato.int/cps/en/natohq/news_223446.htm>, accessed 31 July 2024.
45. NATO, 'Secretary General Makes First Visit to Helsinki since Finland Joined NATO, Welcomes Strong Support to Ukraine', 6 June 2024, <https://www.nato.int/cps/en/natohq/news_226143.htm?selectedLocale=en>, accessed 31 July 2024.
46. Hakala and Melnychuk, *Russia's Strategy in Cyberspace*, p. 9.
47. J Kukkola and M Ristolainen, 'Projected Territoriality: A Case Study of the Infrastructure of Russian Digital Borders', *Journal of Information Warfare* (Vol. 17, No. 2, 2018), p. 85.
48. Hakala and Melnychuk, *Russia's Strategy in Cyberspace*, p. 9.
49. For example, see Katie Sanders, 'Did Vladimir Putin Call the Breakup of the USSR "The Greatest Geopolitical Tragedy of the 20th Century?"', PolitiFact, 6 March 2014, <https://www.politifact.com/factchecks/2014/mar/06/john-bolton/did-vladimir-putin-call-breakup-ussr-greatest-geop/>, accessed 5 June 2024.

the Great Patriotic War demonstrate the lingering memory of occupation and war across generations.

The 2022 invasion of Ukraine fits neatly into this context. If one accepts that the conflict results – at least in part – from Russia's concerns over sharing land borders with hostile states,[50] then the use of cyber capabilities as part of a broader, holistic security strategy begins to make sense, at least as part of a broader approach to territorial security. In addition to generally being a domain to be secured – which has been well established[51] – cyber operations enable the ability to lean forward into adversary states to prevent the risk of future incursion, whether real or imagined, in a manner consistent with that expressed by General Gerasimov.[52]

The flow of the territorial into the cyber domain is evident in Russian strategic thinking, with Russia seeing the information space as a 'continuation of territorial borders', which, Russia believes, are 'constantly being violated by foreign intrusions'.[53] There are clear indications of this sentiment in the Russian NSS tradition, as this article explores. The extension of traditional borders via the cyber domain and the anxious strategic posture noted above naturally lead to the conclusion that territorial concerns are bound to extend to the digital environment. To be insecure on the border, therefore, means to be insecure in the cyber domain.

Territorial Security as Fuel for Hegemonic Ambitions

Foundational to understanding the role of territorial security in shaping Russian cyber security strategy is the position in the 2015 NSS that Russia is 'an aggrieved party' in what it believed to be 'an increasingly hostile world'.[54] The strategy ascribes strength to Russia's adversaries, a belief with roots in the post-Soviet malaise rued by President Putin.[55] In its 2015 NSS, Russia declared that it had to strengthen itself 'against a backdrop of new threats to national security that are multifarious and interconnected'.[56] By claiming a disadvantaged position in the 2015 NSS, Russia sets up a dynamic in which it has a salient need for strong, decisive – if controversial – action as a weaker but righteous actor surrounded by existential threats from a large, unified bloc. What emerges tonally is a vacillation between strength and insecurity – the former being formidable but requiring clear action relative to the sheer magnitude of its adversaries.[57] Russia seeks to show itself as a continually threatened 'leading world power', a nation to be taken seriously but not so strong that it can take the role of confident spectator.[58]

To this end, in 2015, Russia expressed the need for regional hegemony as key to its territorial security. Because it is strong but vulnerable, and with a history of border security issues, the state would naturally see an existential need to strengthen and buffer its borders, recalling a strategy it used for most of the Soviet era. Simply asserting a security need and claiming ground, however, would not be accepted by more powerful adversaries and lacks any broader justification for such an aggressive strategy. This constructs hegemony through shared culture and values as a more powerful expression of cohesive state identity, as suggested in Putin's 2021 essay on the historical linkages between Russia and Ukraine.[59] Extending the concept of shared culture and language to former Soviet republics and other states once in that sphere of influence, however, turns the concept of conquest into one, effectively, of reunification.

Through 2021, culminating in Putin's essay, mentioned above, the sentiment of bringing together the Russian people of the world – through shared culture, language and values – matured in Russia's strategic thinking. In the NSS published that year, Russia lamented the 'decline in the role of the Russian language', blaming foreign 'attempts to falsify Russian and world history'. [60] The 2021 NSS offers

50. Kataryna Wolczuk and Rilka Dragneva, 'Russia's Longstanding Problem with Ukraine's Borders', Explainer, Chatham House, 13 October 2022, <https://www.chathamhouse.org/2022/08/russias-longstanding-problem-ukraines-borders>, accessed 30 June 2024.
51. NATO, 'Cyber Defence', 14 September 2023, <https://www.nato.int/cps/en/natohq/topics_78170.htm>, accessed 5 June 2024.
52. Lilly and Cheravitch, 'The Past, Present, and Future of Russia's Cyber Strategy and Forces', p. 132
53. Hakala and Melnychuk, *Russia's Strategy in Cyberspace*, p. 6.
54. Johansmeyer, Mott and Nurse, 'Cyber Strategy in Practice', p. 6.
55. Putin, 'On the Historical Unity of Russians and Ukrainians'.
56. Russian Federation, 'Russian National Security Strategy, December 2015—Full Text Translation', p. 3.
57. Johansmeyer, Mott and Nurse, 'Cyber Strategy in Practice', p. 6.
58. Russian Federation, 'Russian National Security Strategy, December 2015—Full Text Translation', p. 30.
59. Putin, 'On the Historical Unity of Russians and Ukrainians'.
60. Russian Federation, 'Russian National Security Strategy, December 2015—Full Text Translation', pp. 21–22.

efforts to propagate Russian culture and language across the former Soviet republics as a possible remedy.[61] The NSS's claims to protect Russia from extremism, propaganda and 'racial, religious, and interethnic intolerance' quickly yield to aims of regional hegemony.[62] The roots of this need for hegemony run deep, and they provide at least some justification for the country's expansionist aims.

While it is easy to adopt a refreshed Western view of imperialism that simply substitutes 'Russia' for the 'Soviet Union', doing so is to misunderstand fundamentally the historical context of Russian territorial security. In fact, how the West sees the human and societal costs of the Second World War is far different from that of Russia, where the Great Patriotic War is a stark reminder of what foreign aggression can entail. During that conflict, Russia sustained horrific losses on its own soil, and the war was followed by the emergence of a bipolar order which pitted a new, nuclear-enabled adversary right in its backyard. One solution was to extend this 'yard', by seizing territory further into Eastern Europe.

Reflecting on this critical formative period, Nikita Khrushchev claimed that 'American foreign policy was calculated to provoke and bully us from a position of strength ... [the US Air Force] was the best in the world ... I would even say the Americans were invincible at that time'.[63] In contrast, in the aftermath of 1945, the Soviet Union needed to undertake the reconstruction of 91,000 km of main roads, 930 km of bridges,[64] and 35,000 km of railway track.[65] Even by 1950, half of Red Army transportation was horse-drawn.[66] As a result of this sharp juxtaposition, the notion of expansion for self-defence, which may seem like a convenient excuse for territorial expansion in general, can be seen as grounded in a foundational and relevant territorial security issue. In fact, this aligns with Russia's concerns about a West-leaning Ukraine on its border.[67]

In this regard, the 2015 NSS can be read as a preamble to the 2021 edition. This is evident in the significant change in tone from the 2015 NSS to its 2021 refresh. By 2021, the regionally (and globally) assertive posture evident in the 2015 NSS became the focus of the strategy. Needless to say, it represents 'more than an update of the previous paper', in that it offers a fundamental change from token grievance to outright adversarial posturing.[68] This stands in stark contrast to the lack of update from 2009 to 2015, in which the 'strategy remains largely the same'.[69]

Discussion: The Intersection of Cyber and Border Security in Russian Strategy

Among the important changes from the 2015 to 2021 NSS is a shift towards less orthodox security sectors,[70] which interlock effectively with the cultural and economic issues involving adjacent states and ethnic Russians abroad and the state's hegemonic ambitions.[71] However, NSS is a mere statement if not put into practice, and one can see from the implementation of the NSS from 2015–22 that it was intended to be actionable, given the 'big hunt' for programmers and related talent by the GRU, Russia's defence intelligence organisation. Information confrontation has become a military priority, with cyber security strategy gaining importance throughout 2021.[72]

Russia had identified that the information space is very much a domain of operations, alongside

61. Putin, 'On the Historical Unity of Russians and Ukrainians'.
62. Russian Federation, 'Russian National Security Strategy, December 2015—Full Text Translation', p. 22.
63. Nikita Khrushchev, *Khrushchev Remembers: The Last Testament*, edited and translated by Strobe Talbott (London: Andrew Deutch, 1974), p. 356.
64. Matthew Evangelista, 'Stalin's Postwar Army Reappraised', *International Security* (Vol. 7, No. 3, 1982–83), p. 122.
65. Office of Strategic Services, Research and Analysis Branch, 'Capabilities and Intentions of the U.S.S.R. in the Post-war Period', p. 11. Note that Soviet calculations of damage to the Soviet railway system have suggested a figure of 65,000 km. See Vasilii Vysotskii, *Tyl Sovetskoi Armii* [*The Rear Services of the Soviet Army*] (Moscow: Voenizdat, 1968).
66. Edgar O'Ballance, *The Red Army* (London: Faber and Faber, 1964), p. 192.
67. Wolczuk and Dragneva, 'Russia's Longstanding Problem with Ukraine's Borders'.
68. Trenin, 'Russia's National Security Strategy'.
69. Mark Galeotti, 'Russia's New National Security Strategy: Familiar Themes, Gaudy Rhetoric', *War on the Rocks*, 4 January 2016.
70. Galeotti, 'Russia's New National Security Strategy'.
71. Mark Galeotti, 'New National Security Strategy is a Paranoid's Charter', *Moscow Times*, 5 July 2021, <https://www.themoscowtimes.com/2021/07/05/new-national-security-strategy-is-a-paranoids-charter-a74424>, accessed 23 May 2024.
72. Lilly and Cheravitch, 'The Past, Present, and Future of Russia's Cyber Strategy and Forces', p. 141.

space as an emerging area of global competition.[73] Yet the NSS proceeds to review the psychological, cultural and moral threats to Russia,[74] indicating a concern more focused on the transmission of information itself (for example, through 'mass media'[75]) than the sorts of incisive cyber attacks that Western states have come to equate with Russian cyber aggression (for example, NotPetya). The development of cyber capabilities and issuance of a focused national cyber security strategy in 2015 and 2016 clearly established a foundation for both thinking and action, as evidenced by the accumulation of talent, refinement of strategy, and execution in the form of increased cyber operations (as discussed earlier in this article). By the time of the 2021 NSS's publication, execution was in progress and justified by Russia's broad territorial concerns to include the protection of Russians abroad, a category that focuses on ethnic Russians rather than citizens.

The thread connecting these concepts can be found at the end of the 2021 NSS, which includes a handful of clustered 'goals of the foreign policy of the Russian Federation' that delineate not just the impact between cyber security strategy and territorial integrity in Russian thinking but the priority assigned to proper and effective execution.[76] Points 18–26 lay out a clear line of thinking with profound consequences for the global community, as demonstrated only eight months after its publication. The collection of objectives can be viewed in three parts: definition of the Russian people; establishment of the information threat; and the use of international relationships to counter those and other cross-border threats culminating in the information space.[77]

First, the 2021 NSS establishes the scope of Russian cultural reach, consisting of 'the role of the Russian Federation in the global humanitarian, cultural, scientific, and educational space', with priority ascribed to 'strengthening the position of the Russian language as a language of international communication'.[78] The sentiment is then bolstered by defining what is meant by the Russian people, consisting of 'compatriots living abroad' and the right to 'maintain an all-Russian cultural identity'.[79] The NSS uses the connection of language, culture and ethnicity to expand the scope of the strategy to include states on its borders, by 'strengthening the fraternal ties between the Russian, Belorussian, and Ukrainian peoples'.[80]

> Russia had identified that the information space is very much a domain of operations, alongside space as an emerging area of global competition

Second, Russia establishes the nature of the information domain threat. This is done briefly, with only three objectives: points 19; 20; and 22.[81] The first harkens back to culture, calling for Russia to counter 'attempts to falsify history', to include 'protecting historical truth' and 'preserving historical memory'.[82] This point establishes an important pivot from the cultural and social levers for justifying the integration of foreign territory for border security to the importance of cyber and information domain security. This is followed by an emphasis of the importance of improving Russia's 'mass media and

73. Russian Federation, 'О Стратегии национальной безопасности Российской Федерации' ['On the National Security Strategy of the Russian Federation'], 2021, p. 5.
74. Russian Federation, 'О Стратегии национальной безопасности Российской Федерации' ['On the National Security Strategy of the Russian Federation'], 2021, p. 8.
75. Russian Federation, `О Стратегии национальной безопасности Российской Федерации' ['On the National Security Strategy of the Russian Federation'], 2021, p. 6.
76. Russian Federation, 'О Стратегии национальной безопасности Российской Федерации' ['On the National Security Strategy of the Russian Federation'], 2021, p. 39.
77. Russian Federation, `О Стратегии национальной безопасности Российской Федерации' ['On the National Security Strategy of the Russian Federation'], 2021, pp. 41–42.
78. Russian Federation, `О Стратегии национальной безопасности Российской Федерации' ['On the National Security Strategy of the Russian Federation'], 2021, p. 41.
79. *Ibid.*
80. *Ibid.*
81. Russian Federation, `О Стратегии национальной безопасности Российской Федерации' ['On the National Security Strategy of the Russian Federation'], 2021, p. 42.
82. *Ibid.*

mass communications in the global information space',[83] the sort of asymmetric advantage that Russia could establish, per Slipchenko,[84] as a way to counter a more powerful adversary. Of course, the discussion of mass media comes within the context of a broader approach to information conflict evident during the period, combining both Russia's offensive cyber activity[85] and other forms of information warfare, such as the spread of disinformation for election manipulation and societal disruption.[86]

Third, the NSS's establishment of the scope of the information domain flows naturally into Russia's plan for controlling such threats. The next four points in the 2021 NSS (points 23–26) culminate in the need for 'international cooperation for the formation of a secure and equitable global information space'.[87] The four points cover diplomatic, military, anti-crime, and general information space security cooperation. The ostensible purpose is to demonstrate Russian leadership in attempts at compromise, even when documentation may not be consistent with historical precedent, as this article has discussed. The focus, of course, is on inbound foreign influence along these dimensions, from information warfare to the establishment of a large bloc against Russia (that is, NATO) to the threat of reduced access to systems delivered by foreign vendors[88] – a vulnerability that manifested following the 2022 invasion of Ukraine.[89] Russia has raised what it perceives to be a threat, essentially, and offers leadership to address the overarching problem.

To take a purely cynical view – that Russia simply seeks to use its NSS to mask its true intentions[90] – is to claim that Russia itself has no vulnerability to the perceived threats it references. This is demonstrably untrue, given the fact that it recognises that its adversary is more powerful and that it is at the mercy of 'transnational corporations [desiring to] consolidate their monopoly position in the Internet and control all information resources',[91] which itself was deputised by the US government in its most recent national cyber security strategy.[92] Russia's fears of a cyber threat to its territorial integrity, expressed explicitly in the 2021 NSS, are legitimate,[93] even if partially of its own making.

The interplay between Russia's security concerns on its border with Ukraine and cyber domain engagement is particularly insightful in this regard. That border is only Russia's fourth largest, but it is the largest land border it shares with a country abutting NATO members. In fact, that border is longer than the aggregate length of Russia's borders with NATO member states, yet the historical relationship between Ukraine and Russia, as laid out by Putin, offers context for the heightened security posture.[94] Moreover, it exemplifies the sense of border insecurity felt by the Russian state and expressed through its NSS materials. For the concept of border security to extend into the cyber and information domain should come as no surprise. Further, if physical borders – particularly those not reinforced by natural features – are subject to the consent of abutting states, then the notion of consent in cyber border recognition is even firmer, given that the cyber domain is a space that is 'novel, man-made, imaginary, malleable, and transitory'.[95]

83. *Ibid.*
84. Slipchenko, quoted in Giles, *Handbook of Russian Information Warfare*, p. 17; Russian Federation, 'On Spyware and its Use by US Intelligence Services', unofficial translation with input of the Russian Federation, 2021, p. 2, <https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Spyware_and_its_use_by_US__intelligence_services_ENG_0.pdf>, accessed 11 July 2024.
85. For example, see Council on Foreign Relations, 'Cyber Operations Tracker', 2024, <https://www.cfr.org/cyber-operations/>, accessed 10 December 2024.
86. Johansmeyer, Mott and Nurse, 'Cyber Strategy in Practice', p. 7.
87. Russian Federation, 'О Стратегии национальной безопасности Российской Федерации' ['On the National Security Strategy of the Russian Federation'], 2021, p. 42.
88. Russian Federation, `О Стратегии национальной безопасности Российской Федерации' ['On the National Security Strategy of the Russian Federation'], 2021, p. 13.
89. Johansmeyer, Mott and Nurse, 'Cyber Strategy in Practice', p. 8.
90. *Ibid.*
91. Russian Federation, 'О Стратегии национальной безопасности Российской Федерации' ['On the National Security Strategy of the Russian Federation', 2021, p. 12.
92. Johansmeyer, Mott and Nurse, 'Cyber Strategy in Practice', p. 5.
93. Russian Federation, 'О Стратегии национальной безопасности Российской Федерации' ['On the National Security Strategy of the Russian Federation'], 2021, p. 19.
94. Putin, 'On the Historical Unity of Russians and Ukrainians'.
95. Kukkola and Ristolainen, 'Projected Territoriality', p. 85.

Ultimately, action defines the purpose, intent and usefulness of an NSS. Although cyber and information operations have been flagged as threats to territorial integrity via assaults on both Russia and Russianness (for example, the culture and language dimensions), it is the execution of cyber operations, particularly in Ukraine, from the early days of the 2014 invasion that demonstrates the utility of asymmetric cyber and information capabilities in using an offensive approach to border defence and the security of territorial integrity. The campaigns conducted in Ukraine over the past decade have demonstrated how the intersection of territorial security and cyber strategy within the NSS context in Russia has influenced its approach to cyber and border security strategy.

Conclusion

Russia's cyber security and operational capabilities are firmly grounded in the state's territorial concerns. Although one could contend that cyber engagement necessarily involves a borderless domain, the Russian NSS and its execution clearly show the nexus of the physical and the virtual. Not merely a digital shooting gallery, the information space is rather a strategic environment with security ramifications that interlock with those of Russia's territorial considerations. Like the land borders that do not benefit from reinforcement by physical features, such as rivers and mountains, the demarcation in the cyber domain necessarily requires assertion and action, which the Russian NSS supports and which the implementation of its strategy demonstrates.

Russia's physical security concerns provide a seeming justification, if not a foundation, for an integrated security strategy that places the country at the centre of a risky world, requiring broad interlocking security strategies for its survival. Cyber security forms a meaningful and influential part of this framework. What began as 'informational pressure' alongside economic, military and political concerns and 'intensifying confrontation in the informational region' in 2015, has eventually matured to the point in 2021 where the cyber domain as a whole is an area of clear strategic priority. It now includes the role of non-state actors,[96] which itself becomes a foundation for the cyber operations that Russia has conducted to protect its territorial integrity.

The intersection of the physical and the virtual may seem soft and theoretical, but it becomes real in the Russian NSS and tangible in the execution of that strategy. The evolution of information and cyber security from 2015–21, surrounded by kinetic (if irregular) warfare in 2014 and since 2022, reinforces the importance of planning and conducting offensive cyber operations – justified by a broad view of Russia's security domain (to include Russian speakers outside Russia) and cultural imperatives – to ensure the integrity of its borders. Vulnerability on the border – and of the border – has become a crucial element to Russia's cyber security strategy, as the 2021 NSS revealed.[97] Physical borders require non-physical security from foreign threats, and sometimes the prevention of those threats requires offensive action.

What the Russian approach to the nexus of cyber security and territorial integrity reveals is a more global concern about the use of the cyber domain for the purposes of territorial security. Russian strategic thinking reveals that the days of distinction between cyber and physical domains – or even the notion of hybrid approaches that fuse the separate – are over. Instead, a fluidity is emerging, in which a holistic view of security entails the physical and virtual, each informing the whole, with interplay between the two evident and necessary to ensure the survival of the state. ■

Tom Johansmeyer is a Politics and International Relations PhD candidate at the University of Kent, Canterbury, where he is researching the role of insurance in cyber security strategy. He is also a reinsurance broker based in Bermuda, where he focuses on alternative forms of risk transfer.

Gareth Mott is a Research Fellow at RUSI. His research interests include governance and cyberspace, novel technologies, developments in the cyber risk landscape, and the evolution of security and resilience strategies at micro and macro levels.

Jason R C Nurse is a Reader in Cyber Security at the University of Kent and an Associate Fellow at RUSI. His research interests include cyber policy, cyber security risk management, cybercrime and the psychology of cybersecurity.

96. Russian Federation, 'Russian National Security Strategy, December 2015—Full Text Translation', pp. 3, 5.
97. Russian Federation, 'О Стратегии национальной безопасности Российской Федерации' ['On the National Security Strategy of the Russian Federation'], 2021, p. 19.