Cyber Strategy in Practice The Evolution of US, Russian and Ukrainian National Cyber Security Strategies through the Experience of War

Article *in* The RUSI Journal · August 2024

DOI: 10.1080/03071847.2024.2377544

3 authors, including:

Tom Johansmeyer
University of Kent
15 PUBLICATIONS **5** CITATIONS

SEE PROFILE

Jason R. C. Nurse
University of Kent
209 PUBLICATIONS **4,966** CITATIONS

SEE PROFILE

The RUSI Journal

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

Cyber Strategy in Practice

The Evolution of US, Russian and Ukrainian National Cyber Security Strategies through the Experience of War

Tom Johansmeyer, Gareth Mott & Jason R C Nurse

To cite this article: Tom Johansmeyer, Gareth Mott & Jason R C Nurse (01 Aug 2024): Cyber Strategy in Practice, The RUSI Journal, DOI: 10.1080/03071847.2024.2377544

To link to this article: https://doi.org/10.1080/03071847.2024.2377544

Published online: 01 Aug 2024.

Research Article
RUSI Journal

Cyber Strategy in Practice

The Evolution of US, Russian and Ukrainian National Cyber Security Strategies through the Experience of War

Tom Johansmeyer, Gareth Mott and Jason R C Nurse

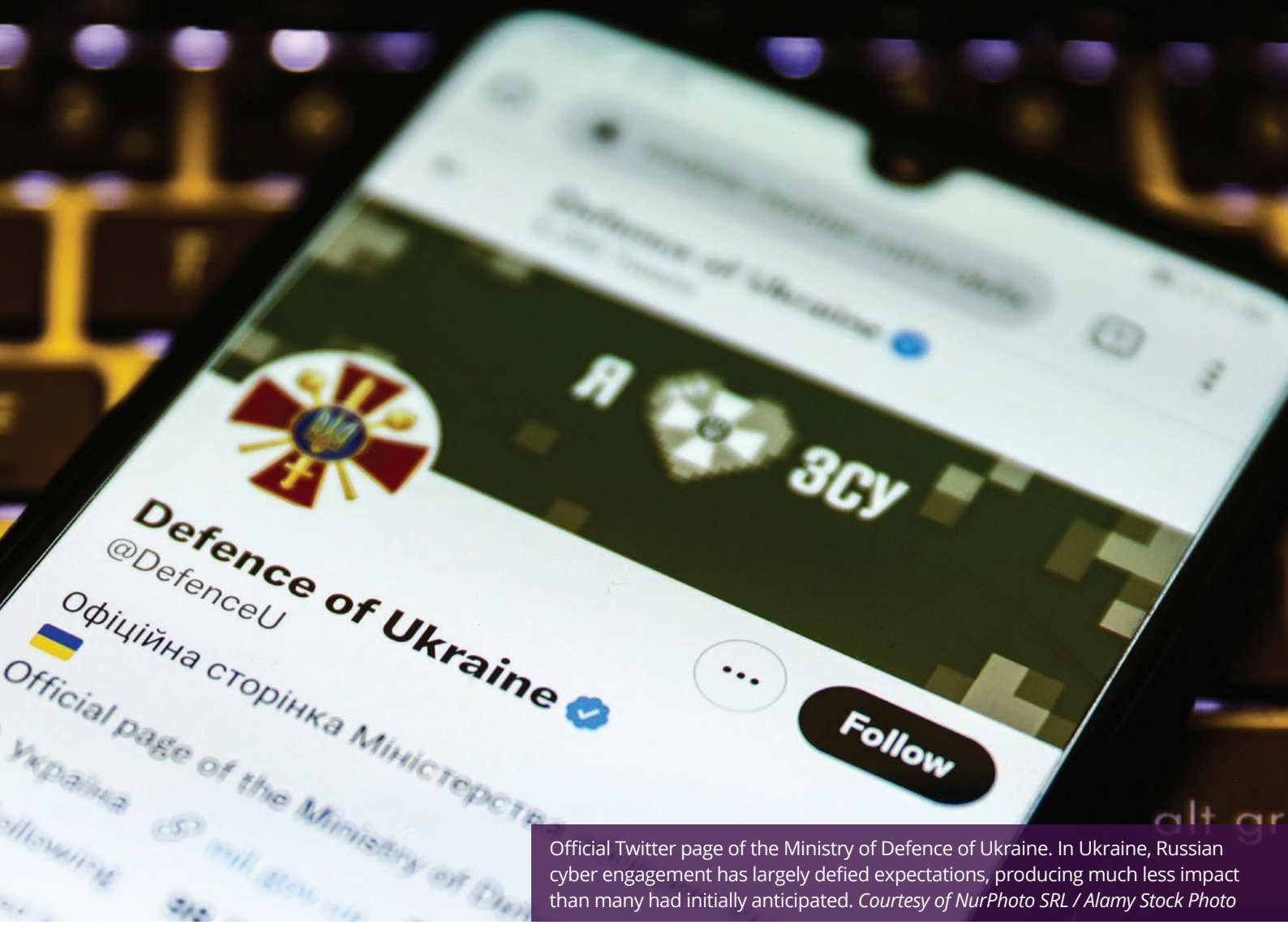
National cyber security strategies had already undergone a period of evolution before Russia's 2022 invasion of Ukraine, ostensibly in preparation for just such a catalyser of major cyber conflagration. But the cyber war never came. Tom Johansmeyer, Gareth Mott and Jason R C Nurse analyse the national cyber security strategies (NCSS) of the US, Ukraine and Russia – as significant cyber domain stakeholders in the conflict – and how aligned these strategies were for the cyber component of the Ukrainian war. In addition, they consider areas of reflection for the future evolution of NCSS documents, particularly in light of the current state of play with cyber operations.

The conflict in Ukraine offers a pertinent opportunity to evaluate, critique and challenge the role of cyber strategy in broader national security strategy. The tripartite cyber domain of operations involving the US, Russia and Ukraine has seen its constituent national cyber security strategies (NCSS) tested. The heavy integration of cyber security into broader national security strategy over the past decade created an expectation for what cyber warfare might look like, and the conflict offers the first opportunity to scrutinise those assumptions. This article explores the fitness for purpose of the three NCSS; particularly with regard to how they have held up since the full-scale Russian invasion of Ukraine in February 2022. It will further explore what changes may be necessary for these strategies to become more effective.

The article develops a comparative analysis of multiple strands of narratives that have been emblematised in public-facing NCSS – as opposed to the private, confidential or otherwise sensitive materials that inform security strategy at a more granular, actionable level. The research is underpinned by a qualitative research methodology, broadly situated within 'interpretative' approaches to security studies. Narratives, and the interplay between narratives, form 'discourse', enabling security stakeholders to convey complex intersubjective knowledge.[1] The authors identify the narratives and themes underpinning the national security strategies (NSS) and attendant strategies of the US, the Russian Federation and Ukraine and the relevance of those security strategies to the cyber aspects of the Russia/Ukraine conflict. By assessing the interplay between these narratives and the present conflict environment, the authors identify how the strategies responded to the conflict and what future iterations should contemplate.

The article proceeds in three parts, starting with a brief review of the historical literature and NSS materials from the US, Russia and Ukraine, followed by the comparison and analysis of the relevant strategy documents from each of the three states. The analysis and comparison lead to a discussion section, which reviews the outcomes of the comparison relative to the current state of play, as well as how those views of cyber security strategy could change as a result of how the conflict in Ukraine has proceeded.

1. Marianne Jorgensen and Louise Phillips, *Discourse Analysis as Theory and Method* (London: Sage, 2002).



Official Twitter page of the Ministry of Defence of Ukraine. In Ukraine, Russian cyber engagement has largely defied expectations, producing much less impact than many had initially anticipated. *Courtesy of NurPhoto SRL / Alamy Stock Photo*

Literature Review

The extent to which cyber threats are securitised is evident through the development of the NSS and NCSS, as well as other related and adjacent security strategy statements. Experience shows that the effectiveness of cyber warfare may be inconsistent with prevailing cyber security strategy. NSS materials have focused largely on hypothetical scenarios and state capacity for action rather than lessons learned or an approximation of what a range of realistic impacts could be. In Ukraine, however, Russian cyber engagement has largely defied expectations, producing much less impact than many had initially anticipated.[2] The cyber domain has not been a significant aspect of the conflict up to this point. The lessons of Ukraine may not call for a revolution in military affairs because of the cyber experience so far, but they should perhaps trigger an evolution in them.

Cyber security can be split into 'hard' and 'soft' cyber, a distinction particularly evident in Russian cyber security strategy thinking, which affirmatively includes both and even favours the latter, which includes information and influence operations, as this article discusses. This article focuses on hard cyber, which consists of the direct weaponisation of cyber capabilities in a manner consistent with the Clausewitzian tradition of war.[3] Soft cyber is increasingly becoming the more widely visible form of cyber operations, but it sits outside the Clausewitzian tradition. While this research focuses on 'hard' cyber, further research could analyse the interplay between 'soft' cyber and destructive cyber operations vis-à-vis public-facing strategies.

The benefits of strategic thinking have become particularly evident since 24 February 2022, when Russia's full-scale invasion of Ukraine began. Cyber activity began even before soldiers crossed the

2. Jon Bateman, 'Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications', Carnegie Endowment for International Peace, 16 December 2022, <https://carnegieendowment.org/research/2022/12/russias-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications?lang=en>, accessed 4 June 2024.
3. George Dimitriu, 'Clausewitz and the Politics of War: A Contemporary Theory', *Journal of Strategic Studies* (Vol. 43, No. 5, 2020), p. 652.

DOI: 10.1080/03071847.2024.2377544

border, with increased adversarial cyber engagement in late 2021 and early 2022.[4] However, the efforts of both sides failed to advance from minor breaches to conflict-altering cyber attacks. In fact, one could reasonably argue that no effort at cyber warfare has achieved that end yet. Whether one claims that the world has yet to see a 'cyber Pearl Harbor' or simply that cyber operations have failed to change tactical or strategic circumstances,[5] the net effect is the same: cyber security strategies have largely remained as theoretical as the magnitude of threat they contemplate.[6]

The smaller-scale engagements often cited in support of a historical precedent of emergent cyber war[7] – such as Estonia in 2007, Georgia in 2008, Stuxnet in 2009/2010,[8] and the wave of cyber attacks on Ukraine from 2014 to 2021[9] – demonstrate state interest in disruptive cyber activity outside armed conflict, but are not akin to tactical operations within a state of war. The 2015 attack on the Ukrainian power grid, for example, which left 230,000 people without power for six hours was certainly a hostile act, and it appears to have been the most impactful of such attacks in the decade-long hostilities between Russia and Ukraine. However, it hardly represents a compelling impact. In recalling the Clausewitzian tradition, it is clear that the worst cyber attack against Ukraine's power grid failed to achieve any meaningful strategic result. However, that did not slow efforts to turn to the cyber domain again ahead of the 24 February 2022 invasion.

War in the Wires

The war in Ukraine not only features the first use of cyber operations in a conventional and traditional major European land war, but it also follows a decade of focused cyber conflict alongside lower-intensity fighting in Ukraine's Donbas region.[10] The frequent and significant cyber attacks by Russia from 2014–23 summarised non-exhaustively by the Council on Foreign Relations' Cyber Operations Tracker may only be the tip of the iceberg, but it is nonetheless indicative of the activity that preceded the February 2022 invasion.[11] In addition to foreshadowing the cyber attacks that would accompany the kinetic war, the early activity provides important context for understanding the cyber components of the broader war (starting in 2022), how this experience interacts with pre-existing cyber security strategy, and how all this could inform future strategic planning.

Cyber attacks intensified ahead of, and shortly after, the 24 February 2022 invasion and sought to help reshape the battlefield.[12] This may have been ambitious, though, because it is generally difficult to integrate cyber capabilities into combined arms operations.[13] Of course, the limited effectiveness of Russia's cyber attacks involves more than just the difficulties involved in coordinating cyber and kinetic assets. Theories abound, and it is likely that there is a range of possible factors, including target hardening in Ukraine, the transitory nature of cyber weapons,[14] and the ease with which the damage from

4. James A Lewis, 'Cyber War and Ukraine', Center for Strategic and International Studies, 16 June 2022, <https://www.csis.org/analysis/cyber-war-and-ukraine>, accessed 2 November 2023.
5. Joe R Reeder and Tommy Hall, 'Cybersecurity's Pearl Harbor Moment: Lessons Learned from the Colonial Pipeline Ransomware Attack', *Cyber Defense Review* (Vol. 6, No. 3, 2021), p. 15.
6. Thomas Johansmeyer, 'What Everyone Misses when it Comes to Cyber Attacks', World Economic Forum, 25 January 2023, <https://www.weforum.org/agenda/2023/01/theres-one-key-advantage-when-it-comes-to-cyber-attacks/>, accessed 9 July 2023.
7. Carmen-Cristina Cirlig, 'Briefing: Cyber Defence in the EU: Preparing for Cyber Warfare?', European Parliament, October 2014, p. 2, <https://www.europarl.europa.eu/EPRS/EPRS-Briefing-542143-Cyber-defence-in-the-EU-FINAL.pdf>, accessed 18 June 2024.
8. Council on Foreign Relations, 'Cyber Operations Tracker', 2023, <https://www.cfr.org/cyber-operations/>, accessed 23 May 2024.
9. Jakub Przetacznik and Simona Tarpova, 'Russia's War on Ukraine: Timeline of Cyber-attacks', European Parliamentary Research Service, June 2022, pp. 2–4.
10. Council on Foreign Relations, 'Cyber Operations Tracker'.
11. *Ibid*.
12. Bateman, 'Russia's Wartime Cyber Operations in Ukraine'.
13. Matthias Schulze and Mika Kerttunen, 'Cyber Operations in Russia's War Against Ukraine', *SWP Comment* (No. 23, April 2023), p. 2.
14. Max Smeets, 'A Matter of Time: On the Transitory Nature of Cyberweapons', *Journal of Strategic Studies* (Vol. 41, Nos 1–2, 2018), pp. 10–11.

cyber attacks can be reversed.[15] Moreover, there is room for a range of interpretations. One could argue that impact as measured in the Clausewitzian sense is not needed for cyber domain engagement to help a state advance its kinetic objectives.[16]

The sheer fact that Ukraine had sustained cyber attacks for over a decade likely helped the state deal with Russia's attacks. Ukraine had plenty of opportunity to learn from experience, although this article will discuss how much of that learning translated into a planned reliance on foreign support.[17] To this point, Ukraine did receive considerable support from Western states – including the US and NATO – and the private sector[18] in hardening its technology infrastructure in the closing months of 2021. The role of such external support warrants reflection regarding agency and responsibilities in the context of NSS/NCSS design and implementation.

While it would be tempting to assume that the lessons from a decade of cyber engagement would have informed and framed Ukraine's NCSS, this article shows that few lessons were digested during this crucial period. Despite having sustained attacks from a more powerful and sophisticated neighbour, Ukraine neglected to implement much of its 2016 NCSS, and by its update in 2021, the strategy appears to have morphed into an expectation of help from states whose interests would presumably align with those of Ukraine.[19] In fairness, the expectation was not only realistic but actually came to pass, yet this evolution does not equate to disciplined strategic planning. The same is true of contributions by the private sector – which echoes the deputisation of that same constituency under the US NCSS.[20] The US government, having ascertained that the private sector has skills, resources and expertise that may not be available in the public sector – at least not at the same scale – has noted a strategic role for the technology sector with regard to national cyber security. Relying on alignment of interest can be risky, particularly where there is no formal framework or expectation that support would come. In fact, Ukraine's expectation that the US and NATO will rush to its aid is called into question – if not significantly undermined – by increasing pro-Russia (or at least anti-Ukraine) sentiment in places like Hungary,[21] Poland[22] and Slovakia,[23] not to mention reluctance to support Ukraine in parts of the US government.[24]

Although there is strong support in the historical literature for the belief that cyber war is destined to be (at best) narrowly effective in supporting broader kinetic activity,[25] the cyber domain still requires strategic security planning. The following analysis of US, Russian and Ukrainian NCSS illustrates not just the strategic state of play before the invasion, but also the gaps relative to how the war unfolded in the cyber domain.

Comparison of Cyber Security Strategies

The extent to which cyber threats are securitised – and how such securitisation is intertwined with other sectors, particularly economic security – is generally evident through the development of NSS

15. Tom Johansmeyer, 'How Reversibility Differentiates Cyber from Kinetic Warfare: A Case Study in the Energy Sector', *International Journal of Security, Privacy, and Trust Management* (Vol. 12, No. 1, 2023), p. 5.
16. David Cattler and Daniel Black, 'The Myth of the Missing Cyberwar', *Foreign Affairs,* 6 April 2022.
17. National Security and Defense Council of Ukraine, 'The Working Group at the NCCC at the NSDC of Ukraine Approved the Draft Cybersecurity Strategy of Ukraine', March 2021, p. 4, <https://www.rnbo.gov.ua/en/Diialnist/4838.html>, accessed 18 July 2024.
18. Przetacznik and Tarpova, 'Russia's War on Ukraine', p. 5.
19. National Security and Defense Council of Ukraine, 'The Working Group at the NCCC at the NSDC of Ukraine Approved the Draft Cybersecurity Strategy of Ukraine'.
20. White House, 'National Cybersecurity Strategy', March 2023, pp. 4–5, <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>, accessed 18 July 2024.
21. Amanda Coakley, 'Putin's Trojan Horse Inside the European Union', *Foreign Policy*, 3 August 2022.
22. Mateusz Mazzini, 'How the Polish Anti-War Movement's Message Entered Mainstream Politics', *Balkan Insight,* 1 February 2024, <https://balkaninsight.com/2024/02/01/how-the-polish-anti-war-movements-message-entered-mainstream-politics/>, accessed 23 May 2024.
23. Tomas Valasek, 'Handle with Care: The Risks of Punishing Slovakia's New Government', European Council on Foreign Relations, 14 May 2024, <https://ecfr.eu/article/handle-with-care-the-risks-of-punishing-slovakias-new-government/>, accessed 23 May 2024.
24. Kori Schake, 'The Case for Conservative Internationalism', *Foreign Affairs,* 4 December 2023.
25. Schulze and Kerttunen, 'Cyber Operations in Russia's War Against Ukraine', p. 3.

and NCSS. The reasons why countries develop and publish NSS – including the US,[26] Russia[27] and Ukraine[28] – include the legal requirement to do so as well as making a statement to allies and adversaries as much as to the country's citizenry.

US: Ambivalent Leadership

The continuum from presidents George W Bush to Barack Obama to Donald Trump to Joe Biden covers almost the entire history of US cyber security strategy, and the frequency of the appearance of dramatic change highlights the primary challenge that allies and adversaries alike face with regard to US security strategy in general. The 2023 cyber security strategy[29] is quite detailed, particularly when compared with its counterpart in the Russian Federation, with specific views on securing federal networks, funding for federal projects, and information sharing and incident reporting. Partnership with the private sector features prominently as well. Most interesting, though, is that cyber security is clearly shifted closer to a desecuritised status vis-à-vis prior strategies. The US narrows its focus and relies more on commercial technology providers, who are effectively deputised as a first line of defence.[30]

The 2023 cyber security strategy benefits from historical perspective. The Biden administration's view of borderless security threats was undoubtedly shaped by such developments as the Covid-19 pandemic, the Intergovernmental Panel on Climate Change's 'Code Red' on climate change,[31] and of course ongoing cyber attack activity. Competing crises always shape the narrative, though, as evidenced by the prominence given to 'global pandemic, a crushing economic downturn, a crisis of racial justice, and a deepening climate emergency' in the 2021 National Security Guidance.[32] The publication of the 2023 NCSS certainly advances the US focus on cyber strategy itself, but it is important to put it into context by seeing the other threats with which it competes for executive branch attention. Cyber appeared to receive more specific attention in the Trump-era NSS, the strategy published at the end of 2017, likely due in large part to that year's ongoing major cyber attacks, including WannaCry and NotPetya.[33] Crucially, they did not have to compete with the worst global pandemic in a century for headlines or impact. For example, Covid-19 had an estimated economic impact of $14 trillion in the US,[34] compared to $14 billion for WannaCry and NotPetya combined.[35]

The result is a mixed bag of cyber security strategy and practice, in which tone and character can whipsaw from one administration to the next – a feature or flaw of liberal democracies – but practice

26. Barry Pavel and Alex Ward, 'Purpose of A National Security Strategy', *Atlantic Council*, 28 February 2019, <https://www.atlanticcouncil.org/content-series/strategy-consortium/purpose-of-a-national-security-strategy/>, accessed 9 April 2022.
27. Russian Federation, 'Russian National Security Strategy, December 2015 – Full-text Translation', December 2015, <https://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf>, accessed 18 June 2024.
28. Taras Kuzio, 'The Long and Arduous Road: Ukraine Updates Its National Security Strategy', *RUSI Commentary*, 16 October 2020.
29. US Department of Defense, 'Summary: 2023 Cyber Security of The Department of Defense', 12 September 2023, <https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF>, accessed XX.
30. Tom Johansmeyer, 'If Cyber Is Uninsurable, the United States Has a Major Strategy Problem', *Lawfare*, 26 July 2023, <https://www.lawfaremedia.org/article/if-cyber-is-uninsurable-the-united-states-has-a-major-strategy-problem>, accessed 3 November 2023; see also Andrea Barinnha and Louise Hurel, 'The Hybrid Place: Civil Society in The Open-ended Working Group', in Fabio Cristiano and Bibi Berg (eds), *Hybridity, Conflict and The Global Politics of Cybersecurity* (London: Rowman and Littlefield, 2023).
31. UN News, 'IPCC Report: "Code Red" for Human Driven Global Heating, Warns UN Chief', 9 August 2021, <https://news.un.org/en/story/2021/08/1097362>, accessed 6 May 2023.
32. White House, 'Interim National Security Strategic Guidance', March 2021, <https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf>, accessed 14 November 2023.
33. Michael Sulmeyer, 'Cybersecurity in the 2017 National Security Strategy', *Lawfare*, 19 December 2017, <https://www.lawfaremedia.org/article/cybersecurity-2017-national-security-strategy>, accessed 18 June 2024.
34. Jakub Hlavka and Adam Rose, 'COVID-19's Total Cost to the U.S. Economy Will Reach $14 Trillion by End of 2023', USC Schaeffer, 16 May 2023, <https://healthpolicy.usc.edu/article/covid-19s-total-cost-to-the-economy-in-us-will-reach-14-trillion-by-end-of-2023-new-research/>, accessed 1 March 2024.
35. Tom Johansmeyer, 'Surprising Stats: the Worst Economic Losses from Cyber Catastrophes', *The Loop: ECPR's Political Science Blog*, 12 March 2024, <https://theloop.ecpr.eu/surprising-stats-the-worst-economic-losses-from-cyber-catastrophes/>, accessed 18 June 2024.

shows little evolution, with limited or incremental steps taken in the public-facing domain. Relative to the US desire for leadership in cyber geostrategy worldwide, the published security strategies have matured but still pale in comparison to the sheer size and scale of the US presence and the extent to which it can be resourced. US cyber security strategy was prepared for a US role in a strategically significant conflict involving non-NATO partner(s), such as that which has arisen in Ukraine. Further, it addressed the adversarial relationship the US has in the cyber domain with the Russian Federation – for which the feeling is mutual.

Russia: Expansionist Ambitions

The Russian Federation has established itself as one of the most powerful states operating in the cyber domain. With robust capabilities that have been deployed to sometimes meaningful effect – to include the attacks on Estonia, Georgia and Ukraine mentioned earlier in this article, not to mention hacking the US Democratic National Committee[36] and a number of US politicians and candidates for elected office[37] – the Russian Federation's cyber operators have become synonymous with offensive cyber capabilities and a willingness to use them. Given its global prominence and demonstrated capabilities, Russia remains a key concern for Western states, their allies and other states of strategic significance (for instance, Ukraine). Russia's NSS reflects this, as do those of its adversary states, such as the US. In fact, an imbalance has emerged in the adversarial relationship Russia has cultivated with the West, and this imbalance has not only evolved since 2015, but has also become a useful lever in justifying assertive behaviour in the cyber domain.

Unlike the importance of collaboration and cooperation among allies in the US NCSS (and those of its allies), the Russian NSS appears to be ready to 'go it alone'.[38] This strategic posture feeds the need for both capabilities and strategy, particularly strong and reliable allies that are currently absent.

In 2015, the Russian Federation had clearly positioned itself as an aggrieved party in an increasingly hostile world, in which the country had to strengthen itself 'against a backdrop of new threats to national security that are multifarious and interconnected'.[39] Strength and threat vacillate across the 2015 NSS, with Russia seeking to show itself as a continually threatened 'leading world power'.[40] Published between the 2014 Ukraine invasion[41] and the 2016 US election,[42] it reflects Russia's increasing assertiveness and its dissatisfaction 'with its current place in the world'.[43]

Foundational to the view of state-level risk and security in the Russian Federation's strategy infrastructure is the notion of 'interstate contradictions',[44] an expression that features regularly and at least as far back as 2000.[45] While the term seemingly refers to disagreement between states – it is used that way by Arseni

36. Sinan Ulgen, 'A Lack of Cybernorms Threatens Western Democracies', Carnegie Endowment for International Peace, 14 December 2016, <https://carnegieendowment.org/europe/strategic-europe/2016/12/a-lack-of-cybernorms-threatens-western-democracies?lang=en&center=europe>, accessed 18 June 2024.
37. Center for Strategic and International Studies, 'Significant Cyber Incidents Since 2006', <https://theloop.ecpr.eu/surprising-stats-the-worst-economic-losses-from-cyber-catastrophes/>, accessed 18 June 2024.
38. Elizabeth Buchanan, 'Russia's 2021 National Security Strategy: Cool Change Forecasted for the Polar Regions', *RUSI Commentary*, 14 July 2021, <https://rusi.org/explore-our-research/publications/commentary/russias-2021-national-security-strategy-cool-change-forecasted-polar-regions>, accessed 9 April 2022.
39. Russian Federation, 'Russian National Security Strategy', p. 3.
40. *Ibid.*, p. 30.
41. David J Kramer, 'The Ukraine Invasion: One Year Later', *World Affairs* (Vol. 177, No. 6, 2015), p. 10.
42. Robert S Mueller III, 'Report on the Investigation into Russian Interference in the 2016 Presidential Election, Volume I of II', US Department of Justice, March 2019, p. 9.
43. Olga Oliker, 'Unpacking Russia's New National Security Strategy', Center for Strategic and International Studies, 7 January 2016, <https://www.csis.org/analysis/unpacking-russias-new-national-security-strategy>, accessed 17 December 2021.
44. Russian Federation, 'Russian National Security Strategy', p. 5.
45. Vladimir Putin, 'The Foreign Policy Concept of the Russian Federation', 28 June 2000, p. 2. For an indicative recent use of the term, see Gennady Gatilov, 'Statement by Ambassador Gennady Gatilov at the Conference on Disarmament - International Security and Disarmament', Permanent Mission of the Russian Federation to the United Nations Office in Geneva, 18 May 2023, <https://geneva.mid.ru/web/geneva_en/international-security-and-disarmament/-/asset_publisher/Gx3Med4zxBAF/content/statement-by-ambassador-gennady-gatilov-at-the-conference-on-disarmame-2?inheritRedirect=false>, accessed 19 June 2024.

Sivitski, director of the Minsk-based Centre for Strategic and Foreign Policy Studies, for instance[46] – the expression reaches deeper. Andrey Volodin, Senior Research Fellow at the Centre for Eurasian Studies in the Diplomatic Academy of the Russian Foreign Ministry, clarifies, referring to the need for a 'global collective security system' with an underlying impediment consisting of 'inter and intrastate conflicts, originating in cultural, ethnic, historical and religious contradictions'.[47]

Such 'contradictions' have in recent history provided a useful foundation for the Russian Federation in advancing its agenda for regional hegemony, as evidenced in its 2015 NSS document's sections on culture and language, which are echoed in the 2021 document: '[T]he decline in the role of the Russian language' and 'attempts to falsify Russian and world history' are counterbalanced with plans to 'support the study of the Russian language and culture' among Commonwealth of Independent States members to accelerate 'Eurasian integration'.[48] The nakedly expansionist objective links to 'regional and sub regional integration and coordination', including, controversially, South Ossetia and Abkhazia[49] – and also, clearly, Ukraine.

The 2015 NSS provides crucial context for Russia's NCSS, published in 2016 as the Doctrine of Information Security of the Russian Federation. The doctrine clearly treats cyber as a broadly existential threat, from 'enhancing the secure and safe operation of weapons, military and special equipment and automated control systems' to protecting infrastructure, preventing domestic instability (generally instigated by external actors), and defending against economic threats.[50] The inclusion of economic security is noteworthy, particularly as it relates to foreign threats. The doctrine mentions only 'mass media' rather than foreign businesses, emphasising the primacy of soft cyber in Russian strategic thinking.[51] The intuitive link is to the use of information operations to affect society, to include influencing adversaries' elections. To stop at this point, though, is to miss the doctrine as an important point in the evolution through 2021 of Russia's cyber security strategy thinking.

The NSS evolution from 2015 to 2021 is evident in a comparison by analyst Nivedita Kapoor, Research Fellow at the National Research University Higher School of Economics, a sentiment echoed by historian Mark Galeotti. Russia's dissatisfaction with its place in the world, so to speak, became a central strategic tenet. According to Kapoor, 'almost every priority area in the 2021 document contains criticism of Western actions that purportedly undermine Russian interests'.[52] Galeotti observes that 'the new strategy paints a more alarming picture about the threats Russia faces from the West and also conceptualizes those threats in wider terms'.[53] Although the 2015 document was not short on criticism of the Russian Federation's adversaries, the 2021 version is more specific and pointed, signalling not just a continuation of prior sentiment but also their ongoing intensification.

The 2021 Russian Federation's NSS opens with a more assertive narrative than the 2015 NSS. The two strategies were published between Russia's two major engagements in Ukraine (2014 and 2021), and while the former looks like a statement of current effort to attain future potential, the latter communicates a more confident and assertive posture, particularly ahead of the invasion. Information (including cyber) security, only sparingly present in the 2015 NSS, pervades the 2021 update. The 2021 NSS recognises the use of information (and disinformation) as a tool of assertive engagement (and even hard power).[54] The 2021 NSS establishes the cyber domain as a relevant area of operations and advances sophistication with which it can be used. This is particularly evident in the discussion of the role of non-state actors. The Russian Federation acknowledges several important

46. Arseni Sivitski, 'The Belarus-Russia Conflict Through the Lens of the Gerasimov Doctrine', *BelarusDigest*, 6 March 2017, <https://belarusdigest.com/story/the-belarus-russia-conflict-through-the-lens-of-the-gerasimov-doctrine/>, accessed 19 July 2022.
47. Andrey Volodin, 'The Return of History', *World Affairs: The Journal of International Issues* (Vol. 24, No. 2, 2020), p. 35.
48. Russian Federation, 'Russian National Security Strategy', pp. 21–22.
49. *Ibid.*, p. 24.
50. Russian Federation, 'Doctrine of Information Security for the Russian Federation', December 2016, p. 8, <http://www.scrf.gov.ru/security/information/DIB_engl/>, accessed 18 June 2024.
51. *Ibid.*, p. 5.
52. Nivedita Kapoor, 'Russia's New National Security Strategy', Observer Research Foundation, 7 July 2021, <https://www.orfonline.org/expert-speak/russias-new-national-security-strategy>, accessed 23 May 2024.
53. 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.
54. Russian Federation, 'On the National Security Strategy of the Russian Federation', 2021, p. 5.

blended cyber-economic security risks in the 2021 NSS. It specifically identifies Russia's dependence on imported technology,[55] a concern echoed in external analysis of the strategy by Dmitri Trenin[56] and Elizabeth Buchanan,[57] signalling a practical problem that would arise only a year later.

If one accepts that the conflict in Ukraine results at least in part from Russia's concerns about sharing land borders with hostile nations, then the use of cyber capabilities as part of a broader security strategy begins to make sense.

While both the US and the Russian Federation have characterised cyber security as a borderless matter, the prospect of physical manifestation should not be ignored, particularly given its relevance to Russia and Ukraine. It may seem counterintuitive to link cyber measures to geographic security considerations. The conflict in Ukraine – in all its incarnations since 2014, physical and otherwise – shows, however, that Russia's concerns over its land borders actually manifest directly in its cybersecurity strategy and engagement. Cyber operations have become a means for managing both territorial security and expansion to further ensure that security. If one accepts that the conflict in Ukraine results at least in part from Russia's concerns about sharing land borders with hostile nations,[58] then the use of cyber capabilities as part of a broader security strategy begins to make sense. This context frames the role of cyber in broader Russian security strategy, which differentiates between the accusation that 'Russia has shown itself to be a reckless cyber actor', and the nuanced, integrated and (from the Russian Federation's perspective) preventive posture given the historical threats the country has endured.[59]

The Russian Federation's physical security concerns provide a seeming justification for an integrated security strategy that places itself at the centre of a risky world, requiring broad interlocking security strategies for its survival, including cyber. Yet, the territorial grounding of the Russian view of cyber security pivots back to the borderless with regard to non-state actors. Its efforts to secure physical and territorial security – from the Russian strategic perspective – ultimately results in vulnerability through its dependence on imported technology,[60] as also highlighted by Trenin[61] and Buchanan.[62] The consequences of this dependence on technology from foreign – and sometimes adversary – states have become particularly evident with 2022 sanctions related to the conflict in Ukraine, which include the cessation of new system sales by Microsoft in Russia, among many other technology providers.[63] In fact, it became clear that the Russian Federation relied rather heavily on technology providers outside its borders and headquartered in adversary states, as evidenced by the impact noted by the Yale University Chief Executive Leadership Institute.[64]

55. *Ibid.*, p. 25.
56. Dmitri Trenin, 'Russia's National Security Strategy: A Manifesto for a New Era', Carnegie Moscow Center, 7 June 2021, <https://carnegiemoscow.org/commentary/84893>, accessed 9 April 2022.
57. Buchanan, 'Russia's 2021 National Security Strategy'.
58. Kataryna Wolczuk and Rilka Dragneva, 'Russia's Longstanding Problem with Ukraine's Borders', Chatham House Explainer, 13 October 2022, <https://www.chathamhouse.org/2022/08/russias-longstanding-problem-ukraines-borders>, accessed 23 May 2024.
59. Franklin Holcomb, 'Countering Russia and Chinese Cyber-Aggression: Prospects for Transatlantic Cooperation', Center for European Policy Analysis, December 2020, <https://cepa.org/comprehensive-reports/countering-russian-and-chinese-cyber-aggression/>, accessed 18 June 2024.
60. Russian Russian President's Decree, 'About National Security Strategies', 2021, p. 25, <https://rusmilsec.blog/wp-content/uploads/2021/08/nss_rf_2021_eng_.pdf>, accessed 19 June 2024.
61. Trenin, 'Russia's National Security Strategy'.
62. Buchanan, 'Russia's 2021 National Security Strategy'.
63. Brad Smith, 'Microsoft Suspends New Sales in Russia', Microsoft on the Issues, 4 March 2022, <https://blogs.microsoft.com/on-the-issues/2022/03/04/microsoft-suspends-russia-sales-ukraine-conflict/>, accessed 9 April 2022.
64. Yale University Chief Executive Leadership Institute, 'Over 1,000 Companies Have Curtailed Operations in Russia – But Some Remain', 10 July 2023, <https://som.yale.edu/story/2022/over-1000-companies-have-curtailed-operations-russia-some-remain>, accessed 10 July 2023.

Ukraine: Caught Between World Powers

The security situation at the inception of Ukraine's first NCSS in 2016 was understandably grim.[65] It reflects the cyber threats associated with its neighbour, a known cyber power, against the backdrop of its own problems with cyber modernisation and resilience. Despite the annexation of Crimea and ongoing threat from Russia, the strategy spends at least as much time on cyber crime and terrorism.

The 2016 strategy mentions Russia only twice, one of which is the specific acknowledgement of the 'ongoing aggression of the Russian Federation'.[66] This comes despite heavy attacks, including the 2015 and 2016 attacks on its power grid.[67] While this may possibly be an instance of cautious diplomatic messaging – again, NCSS documents are for external as well as domestic consumption – this phrasing arguably downplays the scale of the objective threat. This is particularly notable, given the significant and sustained cyber engagement by Russia in 2014 and 2015 in conjunction with the invasion and attendant Donbas and Crimea occupation. Russian aggression contributed to the inception of the document itself, with the 'political will' for the cyber strategy spurred by the 2015 energy grid attack.[68]

Ukraine's national cyber security in 2016 comes across as the ante in a wager on broader international support. What is more prominent is Ukraine's focus on achieving relationships with the EU and NATO, as well as reaching their cyber security standards,[69] although there are nods to system and security modernisation and efforts to improve digital literacy.[70] The 2016 strategy mentions NATO five times, making it much more a fixture than the Russian Federation.

The implied prioritisation of foreign support with regard to cyber strategy materialised in late 2021 and early 2022, with NATO members providing security support ahead of the Russian invasion.[71] As to the rest, it has been described as 'opaque', and relying on 'outdated standards for cybersecurity',[72] and reflecting 'a low level of cyber-risk awareness'.[73] Execution was largely seen as disappointing as well, with implementation impeded by the fact that nobody seems to be in charge.[74]

Ukraine's 2020 NSS provides a broader context for the major and subtle objectives of the 2016 cyber security strategy. Built on three pillars – deterrence, resilience and interaction – the NSS formed a new basis for strategy across domains and disciplines.[75] Deterrence, of course, did not work, as evidenced by the magnitude and cadence of cyber attacks during the period covered by the first NCSS. This aligns with broader debates regarding the limitations of deterrence in cyber security.[76] However, the resilience and interaction pillars have shown more promise. Interaction materialised before the 2022 invasion by the Russian Federation, and indeed it speaks to the 'big bet' mentioned above.

Unlike Ukraine's 2016 cyber security strategy, the 2021 draft cyber security strategy update emphasises both the adversary on its border and the role that

65. Natalia Spînu, 'Ukraine Cybersecurity: Governance Assessment', DCAF Geneva Centre for Security Sector Governance, November 2022 <https://www.dcaf.ch/sites/default/files/publications/documents/UkraineCybersecurityGovernanceAssessment.pdf>, accessed 19 June 2024.
66. Russian Federation, 'Doctrine of Information Security for the Russian Federation'.
67. Przetacznik and Tarpova, 'Russia's War on Ukraine', p. 3.
68. Tom Stoelker, 'Ukraine Cybersecurity Officials Describe Defense Against Cyber War', *Fordham News*, 21 July 2022, <https://news.fordham.edu/university-news/ukraine-cybersecurity-officials-describe-threats/>, accessed 9 October 2023.
69. For instance, see Russian Federation, 'Doctrine of Information Security for the Russian Federation', p. 4.
70. *Ibid.*, p. 6.
71. NATO, 'NATO Agency and Ukraine Reaffirm Commitment to Technical Cooperation', 17 January 2022, <https://www.ncia.nato.int/about-us/newsroom/nato-agency-and-ukraine-reaffirm-commitment-to-technical-cooperation.html>, accessed 1 March 2024.
72. Vera Zimmerman, 'Ukraine's Finally Got a Cybersecurity Strategy. But is it Enough?', Atlantic Council, 20 April 2016, <https://www.atlanticcouncil.org/blogs/ukrainealert/ukraine-s-finally-got-a-cybersecurity-strategy-but-is-it-enough/>, accessed 9 October 2022.
73. Nataliya Tkachuk, 'National Cyber Security System of Ukraine: Perspectives of Policy Development and Capacity Building', *Internauka* (November 2019), p. 2, <https://journals.indexcopernicus.com/api/file/viewByFileId/1037327>, accessed 18 June 2024.
74. *Ibid*., p. 19.
75. Spînu, 'Ukraine Cybersecurity', pp. 6–7.
76. James Lewis and Chris Painter, '2021 in Review: All Things Cyber', *Inside Cyber Diplomacy Podcast*, 17 December 2021.

cyber could play in conflict with that adversary – an update that came almost a year prior to the invasion.[77] Further, the notion of cyber threats being linked to 'armed aggression' as well as resilience finally gains prominence, although Ukraine still prioritises relationships with the EU and NATO as fundamental to cyber security strategy.[78] However, the draft strategy does acknowledge that 'cooperation with international partners ... is insufficient'.[79] The major shift from 2016 to 2021, therefore, is from an emphasis on foreign reliance (that is to say, NATO) to an emphasis on an adjacent foreign threat (that is to say, Russia). This turn reflects a greater focus on the nearby adversary and the likelihood of engagement (which ultimately occurred).

The 2021 draft strategy includes Russia's use of 'information confrontation' up front,[80] links it to ongoing hybrid warfare in areas occupied by Russia prior to the 2022 invasion, and focuses on the threat to critical infrastructure.[81] Despite the focus on the heightened threat, little was accomplished between the release of the 2016 cyber security strategy and the 2021 draft update. Yet, the swift delivery of significant foreign support (both within the cyber domain and on the ground) does suggest that the backbone of the 2016 strategy was foretelling. In fact, it was reiterated in 2021 with the mention of '[c]ooperation with foreign partners', particularly NATO.[82]

One could argue that, if not for the relationships Ukraine had developed with Western powers, the cyber component of the 2022 invasion could have been very different. After all, the level of resilience Ukraine would have been able to achieve on its own would most likely have been substantially lower than that achieved with foreign assistance. However, it is important to keep context in mind with regard to the original risk Ukraine would have faced without NATO and other support. The 2015 cyber attack against the Ukrainian power grid remains an apt and useful reference point. While the potential usefulness of cyber warfare as part of a broader effort cannot be ignored, it must be tempered by clear limitations, particularly because of difficulties in coordination with conventional forces.[83] While the enduring lesson for the US and NATO may involve the preventive value of supporting an adversary's adversary, the impact of attack prevented needs to be balanced against the potential that cyber war would have brought absent support for Ukraine from NATO and other Western states.

A Spectator Sport for a While

US support for Ukraine is consistent with what the US sees as the need for an 'open, interoperable, reliable, and secure Internet to ... protect and ensure economic security for American workers and companies'.[84] The broad, shepherd-type mission declared in US national cyber security documents has been sufficient to cover support for Ukraine (and presumably other states that could be affected in the future) without resulting in direct involvement in a conflict in the cyber domain. In this regard, the US cyber security strategy has demonstrated relevance in the context of the recent and generally unexpected military conflict in Ukraine. However, broad, non-specific commitments may not be enough in the future, especially if heightened risk of conflict becomes the norm.

Cyber activity throughout the conflict in Ukraine suggests that the flexibility the US has enjoyed in the recent past may not convey sufficient support for allies and aligned states that they can count on US help if digitally attacked. This is not to say that the US and other Western bloc members fell short in their support for Ukraine in the cyber domain. In fact, the contrary is visibly true. The cyber barrage that came early in the conflict was generally ineffective

77. National Security and Defense Council of Ukraine, 'The Working Group at the NCCC at the NSDC of Ukraine Approved the Draft Cybersecurity Strategy of Ukraine'.
78. *Ibid*., p. 6.
79. *Ibid*., p. 9.
80. *Ibid*., p. 2.
81. Janne Hakala and Jazlyn Melnychuk, *Russia's Strategy in Cyberspace* (Riga: NATO Strategic Communications Centre of Excellence, 2021).
82. National Security and Defense Council of Ukraine, 'The Working Group at the NCCC at the NSDC of Ukraine Approved the Draft Cybersecurity Strategy of Ukraine', p. 4.
83. Schulze and Kerttunen, 'Cyber Operations in Russia's War Against Ukraine', p. 2.
84. White House, 'National Cyber Strategy of the United States of America', September 2018, p. 2, <https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>, accessed 18 July 2024.

due to the significant support Ukraine received from Western states in hardening its technology systems.[85] Now that the US has answered the call – as have other NATO members – a firmer strategic statement of support might be necessary. A commitment to act is crucial when the need to act has already arisen.

If the US were to adopt a more forward-looking cyber security strategy, it would have profound implications for Russia's NCSS. An early indicator of this can be found in the 2023 US cyber security strategy with regard to what amounts to the deputisation of the technology industry – a development almost predicted by Russian security strategies from 2015 to 2021. Via the cyber domain, Russian economic vulnerability comes at least in part from its dependence on foreign technology.[86] According to the Council on Foreign Relations' Cyber Operations Tracker, which dates back to 2005, Russia was the victim of 11 cyber operations by state actors. The decisions by US technology companies such as Alphabet (Google's parent), Microsoft and Sabre (airline systems) [87] to curtail their business activity in Russia have arguably had more impact than the 11 cyber operations perpetrated against Russia by state actors.[88] For Russia, the enduring cyber security lesson from the conflict in Ukraine likely has less to do with attacks on Sberbank and more to do with foreign technology – not to mention foreign manufactured components and capital.[89] The outcome could go in one of two directions: diplomacy or self-reliance.

Diplomacy would take considerable time and effort, but Russia has done it before. The international engagement culminating in the 2014 Winter Olympics in Sochi is largely recognised as a masterful effort in soft power.[90] Isolating itself from Western trading partners, on the other hand, would effectively require Russia to develop its own technology alternatives to Western standards while coping with a technology 'brain drain'.[91] Self-reliance – pejoratively, 'going it alone' – has little in the way of successful precedent.

> A commitment to act is crucial when the need to act has already arisen.

While Russia is faced with a choice for the future, Ukraine is not. Although it will spend the years after the eventual cessation of fighting focused on both physical and societal reconstruction, it will also have to rethink its overall security strategy. Much of that, of course, will be pointed at the 2,000 km border it shares with its adversary to the east, and cyber will certainly play a role. In addition to refining the draft cyber strategy from 2021, Ukraine will need to commit to (and invest in) execution. Given the scale of the protracted present conflict, Ukraine may need substantive material support. This speaks to the independence of security that is narrated in the NSS/NCSS documents of Ukraine and its allies. The factor of interdependency – particularly with respect to cyber – could become an increasingly prominent element of security strategies, moving forward.

Conclusion

What has been called the largest land war in Europe since the Second World War is also the first major conflict of the digital age.[92] As such, it has offered the first possibility to see cyber operations alongside kinetic warfare at scale. The conflict has tested the strategic planning not just of the principal adversaries – Ukraine and the Russian Federation – but of adjacent states that may have an interest in the

85. Ariel Levite, 'Integrating Cyber into Warfighting: Some Early Takeaways from the Ukraine Conflict', Carnegie Endowment for International Peace, 18 April 2023, <https://carnegieendowment.org/2023/04/18/integrating-cyber-into-warfighting-some-early-takeaways-from-ukraine-conflict-pub-89544>, accessed 10 July 2023.
86. Russian Federation, 'Doctrine of Information Security for the Russian Federation', p. 6.
87. Yale University Chief Executive Leadership Institute, 'Over 1,000 Companies Have Curtailed Operations in Russia – But Some Remain'.
88. Council on Foreign Relations, 'Cyber Operations Tracker'.
89. *Ibid.*
90. Jonathan Grix and Nina Kramareva, 'The Sochi Winter Olympics and Russia's Unique Soft Power Strategy', *Sport in Society* (Vol. 20, No. 4, 2015), <https://www.tandfonline.com/doi/full/10.1080/17430437.2015.1100890?needAccess=true>, accessed 10 July 2023.
91. Cade Metz and Adam Satariano, 'Russian Tech Industry Faces "Brain Drain" as Workers Flee', *New York Times*, 13 April 2022.
92. Matt Fitzpatrick, 'Remembering the Past, Looking to the Future: How the War in Ukraine is Changing Europe', *The Conversation*, 2 March 2002, <https://theconversation.com/remembering-the-past-looking-to-the-future-how-the-war-in-ukraine-is-changing-europe-178151>, accessed 4 November 2023.

outcome of the conflict, particularly the US, given its role as both the Russian Federation's primary adversary and as the pre-eminent ally in NATO. The nature and impact of the cyber conflict that has unfolded alongside the conventional conflict has shown mixed results for the fitness of pre-existing cyber security strategies.

Activity in the cyber domain has failed to become a material driver of the conflict, with some attempts failing and those that succeeded demonstrating a distinct ineffectiveness. Matthias Schulze and Mika Kerttunen note that where malware failed to impact the Ukrainian power grid in 2022, 'conventional bombings were able to shut down 40 per cent' of it.[93] Preventive measures contributed to some of Ukraine's successful defence, although it seems that cyber impact was never going to rise to the levels initially contemplated.

A miss on potential impact, though, should not be permitted to obscure where NSS and NCSS have been both prescient and useful. The 2021 draft Ukrainian NCSS pivoted to salient reliance on support from aligned but non-allied Western powers, successfully anticipating that they would respond to an attack on Ukraine as an increase in the threat to adjacent NATO members. Moreover, the threat to Ukraine was telegraphed for years through the Russian NSS and NCSS apparatus, particularly with regard to its own history of physical security. The US, of course, sees the nexus of cyber and military security more in adjacent threats than those directly against itself – for example, the escalation of security problems through threats to NATO members in Central and Eastern Europe rather than direct war-like attacks on the US and its citizens.

There is plenty of room for strategic refinement across the US, the Russian Federation and Ukraine. This article has shown that the manifestation of cyber war as part of a larger effort is not what state NSS and NCSS expected, offering the opportunity to improve such strategy for the future. If the purpose of cyber war was to achieve the dream of bloodless conflict, the events of the Russian invasion of Ukraine has reminded the world to accept the reality: 'War never changes. It only becomes more bloody and brutal'.[94] ■

Tom Johansmeyer is a Pol&IR 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 the 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 insurance, security risk management, corporate communications and cyber security, insider threat, cybercrime and the psychology of cyber security.

93. Schulze and Kerttunen, 'Cyber Operations in Russia's War Against Ukraine', p. 6.
94. US Congress, 'Hearings Before the Committee on Foreign Affairs', 11 April–2 May 1939, p. 62.