CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

Preparing for a Post-Armed Conflict Strategic Environment

Michael P. Fischerkeller

About the author

Dr Michael Fischerkeller is a researcher in the Information, Technology and Systems Division at the Institute for Defense Analyses, a federally funded research and development centre in Alexandria, VA, United States. Michael has spent 25 years supporting the U.S. Office of the Secretary of Defense, Joint Chiefs of Staff, and Combatant and Multi-National Force commanders. His areas of expertise are cyber strategy, strategic/operational concept development, and assessment. Michael's dozens of single and co-authored publications on cyber strategy include essays in national media, articles in peer-reviewed journals, book chapters, and recently, *Cyber Persistence Theory: Redefining National Security in Cyberspace*, published by Oxford University Press in 2022. Dr Fischerkeller holds a PhD in international relations from the Ohio State University.

CCDCOE

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) is a NATO-accredited knowledge hub offering a unique interdisciplinary approach to the most relevant issues in cyber defence. The heart of the CCDCOE is a diverse group of international experts from military, government, academia, and industry, currently representing 39 nations.

The CCDCOE maintains its position as an internationally recognized cyber defence hub, a premier source of subject-matter expertise and a fundamental resource in the strategic, legal, operational, and technical aspects of cyber defence. The Centre offers thought leadership on the cutting edge of all aspects of cyber defence and provides a 360-degree view of the sector. The Centre encourages and supports the process of mainstreaming cybersecurity into NATO and national governance and capability, within its closely connected focus areas of technology, strategy, operations, and law.

The Tallinn Manual, prepared at the invitation of the CCDCOE, is the most comprehensive guide for policy advisers and legal experts on how international law applies to cyber operations carried out between and against states and non-state actors. Since 2010, the Centre has organized Locked Shields, the biggest and most complex technical live-fire cyber defence challenge in the world. Each year, Locked Shields gives cybersecurity experts the opportunity to enhance their skills in defending national IT systems and critical infrastructure under real-time attacks. The focus is on realistic scenarios, cutting-edge technologies, and simulating the entire complexity of a massive cyber incident, including strategic decision-making and legal and communication aspects.

The CCDCOE hosts the International Conference on Cyber Conflict, CyCon, a unique annual event in Tallinn, bringing together key experts and decision-makers from the global cyber defence community. The conference, which has taken place in Tallinn since 2009, attracts more than 600 participants each spring.

The CCDCOE is responsible for identifying and coordinating education and training solutions in the field of cyber defence operations for all NATO bodies across the Alliance. NATO-accredited centres of excellence are not part of the NATO Command Structure.

www.ccdcoe.org
publications@ccdcoe.org

Disclaimer

This publication is a product of the CCDCOE. It does not necessarily reflect the policy or the opinion of the Centre or NATO. The Centre may not be held responsible for any loss or harm arising from the use of information contained in this publication and is not responsible for the content of the external sources, including external websites referenced in this publication.

Table of Contents

1. Abstract

Policies in response to and trends in the Russia-Ukraine armed conflict portend a post-armed conflict strategic environment that will pose a strategic challenge in and through cyberspace to NATO and its member states. By considering Russia's unchanging motivation to manage the security architecture of Europe and the novel Russian capability profile that Western policies intend to influence, this paper posits two alternative cyber security futures, for both of which NATO is arguably not yet prepared. Recent calls for NATO to adopt a proactive cyber posture and descriptions of what that would entail are necessary but insufficient for preparing NATO for this forthcoming strategic challenge – NATO should also establish a proactive cyber operational element that continuously campaigns to ensure the security of its member states and partners. It is further proposed that this element would generate an additional benefit of addressing concerns raised by those who argue that the elevation of China in strategic guidance will distract from addressing the Russian strategic challenge.

2. Introduction

One year after Russia's invasion of Ukraine, scholars and policymakers are examining potential outcomes, including Russian victory, loss, or stalemate. No matter the outcome of the armed conflict, the North Atlantic Treaty Organization (NATO) and its member states will likely face significant strategic risk in the immediate post-armed conflict environment. The constancy of Russia's unrelenting ambition, the increase in Russia's operational tempo and intensity of cyber operations targeting NATO and its member states, and the ongoing attrition of Russia's conventional force capabilities portend dangerous cyber futures for the Western allies.

From the lens of cyber persistence theory, one can forecast two alternative cyber futures.[1] First, *because of* the resultant vacuum of conventional force capabilities, Russia will sustain or increase the current tempo and intensity of cyber campaigning targeting NATO and its member countries while taking care not to breach the tacit ceiling of cyber agreed competition – that is, Russia will not engage in cyber operations that cause armed-attack equivalent effects. Alternatively, *in spite of* the resultant vacuum of conventional force capabilities but because of its nuclear deterrent, Russia will be emboldened to breach the tacit ceiling of cyber agreed competition and target NATO and its member states with cyber campaigns or operations of armed-attack equivalence. Both futures rest on the same assumption – at the end of kinetic hostilities, Russia will not fold up its tent and go home but rather will continue its strategic competition with NATO through aggressive cyber campaigning.

Both futures should cause NATO and the West to pause and reassess current objectives, preparations for the post-armed conflict environment, and strategic shifts or tilts to China by some member states and NATO's strategic concept.[2] A post-armed conflict Russia that is more aggressive in and through cyberspace has the potential to weaken the democratic world and the transatlantic alliance and, in so doing, create an 'invaluable distraction dividend' and 'strategic running room' for China to exploit.[3] NATO and its member states should not make strategic decisions based on the presumption that when major combat operations abate in the Russia-Ukraine armed conflict, so too will an active strategic threat from Russia.

[1] Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett, *Cyber Persistence Theory: Redefining Security in Cyberspace* (Oxford: Oxford University Press, 2022). Cyber persistence theory is a structural theory of cyber security arguing that core structural features of cyberspace – interconnectedness, macro-resilience/micro-vulnerability, and mutability – designate conditions of constant contact and offence–defence fluidity to which all cyber actors are subject. The strategic logic for cyber security that flows from these conditions is initiative persistence in setting favourable conditions in and through cyberspace by exploiting others' vulnerabilities (technical and cognitive) while ensuring they cannot exploit yours.

[2] See e.g. White House, *2022 National Security Strategy*, October 2022, https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf;
H. M. Government, *Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy*, March 2021, https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy; H. M. Government, *Integrated Review Refresh 2023*, March 2023, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1145586/11857435_NS_IR_Refresh_2023_Supply_AllPages_Revision_7_WEB_PDF.pdf; NATO, *NATO 2022 Strategic Concept*, https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf. For a comprehensive review of all European countries, see Bernhard Bartsch and Claudia Wessling, eds., *From a China Strategy to No Strategy at All: Exploring the Diversity of European Approaches* (European Think-tank Network on China, July 2023), https://www.clingendael.org/sites/default/files/2023-07/ETNC_Report_2023_final_0.pdf.

[3] Hal Brands, 'Opposing China Means Defeating Russia', *Foreign Policy*, 5 April 2022, https://foreignpolicy.com/2022/04/05/china-russia-war-ukraine/.

In this paper, I review alternative outcomes of the armed conflict, consider Russia's military capability profile in a post-armed conflict environment, and posit alternative cyber security futures based on Russian motivation(s) and capabilities. I then address three policy questions: Is the current objective of weakening only Russia's conventional force generation functions prudent? How can NATO optimize its member states' aggregate cyber capabilities and capacities to prepare for these cyber futures? And might recent shifts and tilts to China distract from such preparations?

3. Potential Armed-Conflict Outcomes

Most observers predict one of three armed-conflict outcomes: Russian victory, Russian loss, or stalemate.[4] In every case, Russia's motivation(s) will fuel aggressive actions against NATO and its member states.

Russian Victory

There is consensus that a Russian victory would invite increased adventurism by Russia. Michael Miklaucic argues that a Russian victory would be 'very bad', as it would 'signal that armed force is the arbiter of sovereignty' and that 'armed aggression is not only permissible behavior but effective statecraft'.[5] Eliot Cohen similarly argues that Putin will be empowered to expand Russia's influence with 'unlimited violence'.[6] Noting that Putin has yet to halt his efforts to dominate the security structure in Europe, Anthony Cordesman argues that a Russian victory would leave Russia so divided from Europe that Russia would face a major ongoing confrontation with the West.[7] And Dov Zakheim argues that if Russia triumphs to any degree, including merely retaining control of Crimea, it could evoke in Moscow and across the country a sense of popular triumphalism to undermine or invade other states in the near-abroad.[8]

Russian Loss

Views also converge in discussions of a Russian loss. Liana Fix and Michael Kimmage propose that the most plausible Ukrainian victory would be 'winning small', where Russia is expelled from the western bank of the Dnieper River, and Ukraine establishes perimeters of defence around the Russian-controlled areas in Ukraine's east and south and secures its access to the Black Sea.[9] Justin Bronk argues that Moscow would 'feel very vulnerable' were this to be the outcome (because Russia's conventional force capabilities will be significantly degraded both in terms of their actual and perceived potential),[10] but Fix and Kimmage posit that a Ukrainian victory would 'only spur more Russian intransigence in its wake'

[4] Eugene Rumer, 'Putin's War Against Ukraine: The End of The Beginning', Carnegie Endowment for International Peace, 17 February 2023, https://carnegieendowment.org/2023/02/17/putin-s-war-against-ukraine-end-of-beginning-pub-89071.

[5] Michael Miklaucic, 'Taking War Seriously', *RealClear Defense*, 31 May 2023, https://www.realcleardefense.com/articles/2023/05/31/taking_war_seriously_902610.html.

[6] Eliot A. Cohen, 'It's Not Enough for Ukraine to Win. Russia Has to Lose', *Atlantic*, 19 May 2023, https://www.theatlantic.com/ideas/archive/2023/05/ukraine-victory-russia-defeat/674112/.

[7] Anthony H. Cordesman, 'How? (and Does?) the War in Ukraine End: The Need for a Grand Strategy', Center for Strategic and International Studies, 24 February 2023, https://www.csis.org/analysis/how-and-does-war-ukraine-end-need-grand-strategy.

[8] Dov S. Zakheim, 'Russia Will Remain a Threat, No Matter How the War in Ukraine Ends', *Hill*, 17 February 2023, https://thehill.com/opinion/international/3862054-russia-will-remain-a-threat-no-matter-how-the-war-in-ukraine-ends/.

[9] Liana Fix and Michael Kimmage. 'What if Ukraine Wins? Victory in the War Would Not End the Conflict with Russia', *Foreign Affairs*, 6 June 2022, https://www.foreignaffairs.com/articles/ukraine/2022-06-06/what-if-ukraine-wins. Fix and Kimmage also suggest that, over time, a 'winning small' victory could be expanded by Ukrainian forces breaking up the land bridge that Russia has established to Crimea and regaining the territory in southeastern Ukraine that Russia seized and annexed back in 2014. They also describe a 'winning big' victory that includes these same objectives but in a more compressed timeline.

[10] Justin Bronk (Royal United Services Institute), quoted in Barry Rosenberg, '3-to-5 Years from Now Is the Danger Time When the US Could Face Both China and Russia', *Breaking Defense*, 20 July 2023, https://breakingdefense.com/2023/07/three-to-five-years-from-now-is-the-danger-time-when-the-us-could-face-both-china-and-russia/.

and that Russia would use a narrative of humiliation to stir domestic support for a renewed effort to control Ukraine.[11] Additionally, they argue that Putin would continue to engage in 'active measures' to probe for Western vulnerabilities.[12] Zakheim argues that should Russia suffer defeat, Moscow would be 'consumed by revanchist irredentism' and thus a danger to its contiguous neighbours and to all of Europe for years to come.[13] Finally, Cohen argues that a defeated Russia will still be 'malevolent, angry, and vengeful' and that it will 'engage in subversion, political warfare, and malicious behavior of all kinds'.[14]

Russian and Ukrainian Stalemate

Rudolf Adam argues that a third potential outcome – a stalemate or 'frozen conflict' – is the likely result of the armed conflict, comprising an 'uneasy truce along a disputed and heavily armed line of demarcation'.[15] Both Eugene Rumer and Cordesman suggest that this outcome would be similar to the permanent standoff on the Korean Peninsula, where both sides would agree to stop fighting but remain deployed.[16] But Cordesman argues that, although this kind of unstable settlement has worked with the two Koreas, it has done so only at the cost of constantly being on the edge of another war. Thus, this outcome would do little or nothing to stabilize the overall security of Western Europe and particularly the European states along the Russian border. He claims it would create the equivalent of a 'rules-based disorder' where individual European states would secure their positions relative to Russia along different lines, with some bolstering a deterrent posture and others seeking to ease tensions. Joshua Huminski argues that, should the outcome be a stalemate, Russia would nonetheless continue to be 'determined to bring it [Ukraine] back into its orbit'.[17]

No matter the outcome of the fighting in Ukraine, the constancy of Russia's ambition to expand its power will continue to pose a strategic threat to NATO and its member states.[18]

[11] Fix and Kimmage, 'What If Ukraine Wins?'

[12] Fix and Kimmage.

[13] Zakheim, 'Russia Will Remain a Threat'.

[14] Cohen, 'It's Not Enough for Ukraine to Win'.

[15] Rudolf G. Adam, 'Beyond Russia's War Against Ukraine', *GIS*, 13 February 2023, https://www.gisreportsonline.com/r/ukraine-russia-stalemate/.

[16] See Rumer, 'Putin's War Against Ukraine'; Cordesman, 'How? (and Does?) the War in Ukraine End'.

[17] Joshua C. Huminski, 'Victory in Ukraine Could Mean a Stalemate', *Hill*, 28 June 2022, https://thehill.com/opinion/international/3539481-victory-in-ukraine-could-mean-a-stalemate/.

[18] Keir Giles, 'Russian Defeat Is More Dangerous than Russian Victory', in *How to End Russia's War on Ukraine* (London: Chatham House, 2023), 26–28, https://www.chathamhouse.org/2023/06/how-end-russias-war-ukraine.

4. Russia’s Post-Armed Conflict Capability Profile

Absent a severe escalation of the armed conflict, Russia’s nuclear arsenal and the strategic deterrent it provides will remain intact in the immediate post-armed conflict environment. Additionally, although open-source reporting offers some evidence of NATO member states disrupting and degrading deployed Russian or Russian-affiliated capability sets and command and control infrastructure,[19] no reporting points to the West directly targeting the cyber force generation functions of Russia’s military, intelligence services, contractors, and proxies. Therefore, Russia’s cyber capabilities will also remain largely intact after the kinetic conflict ends.

If the outcome is a stalemate, Cordesman argues that Russia would continue to build up its conventional capabilities,[20] although Russia would be motivated to do so no matter the outcome. But, importantly, Zakheim argues that ‘wartime losses and economic sanctions may set it [Russia] back in the immediate future’.[21] It may be the case, moreover, that the ‘immediate future’ is a period of several years. In September 2022, British officials remarked that some of Russia’s conventional forces had been ‘severely weakened’.[22] For example, ‘1 GTA [1st Guards Tank Army] suffered heavy casualties in the initial phase of the invasion and had not been fully reconstituted prior to the Ukrainian counter-offensive in Kharkiv’, said the UK Ministry of Defence. As one of the most prestigious of Russia’s armies, it is allocated for the defence of Moscow and intended to lead counterattacks in the case of a war with NATO.[23] The Ministry further concluded that ‘With 1GTA and other WEMD [Western Military District] formations severely degraded, Russia’s conventional force designed to counter NATO is severely weakened. It will likely take years for Russia to rebuild this capability.’[24]

Comments by U.S. Secretary of Defense Lloyd Austin III in April 2022 bolster this assessment. ‘We want to see Russia weakened to the degree that it can’t do the kinds of things that it has done in invading Ukraine,’ stated Secretary Austin, further noting that Russia ‘has already lost a lot of military capability, and a lot of its troops, quite frankly. And we want to see them not have the capability to very quickly

[19] For example, in April 2022, the U.S. Federal Bureau of Investigation disrupted communication between all US systems infected with Russia’s CYCLOPSBLINK malware and the malware’s command control infrastructure, and a U.S. Cyber Command (USCYBERCOM) ‘hunt forward’ team deployed in Ukraine reportedly discovered and made inert malware targeting the Ukrainian railway system. See, respectively, U.S. Department of Justice, ‘Justice Department Announces Court-Authorized Disruption of Botnet Controlled by the Russian Federation’s Main Intelligence Directorate (GRU)’, 6 April 2022, https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-disruption-botnet-controlled-russian-federation; Mehul Srivastava, Madhumita Murgia, and ND Hannah Murphy, ‘The Secret U.S. Mission to Bolster Ukraine’s Cyber Defences Ahead of Russia’s Invasion’, *Financial Times*, 9 March 2022, https://www.ft.com/content/1fb2f592-4806-42fd-a6d5-735578651471; Alexander Martin, ‘U.S. Military Hackers Conducting Offensive Operations in Support of Ukraine, Says Head of Cyber Command’, *Sky News*, 1 June 2022, https://news.sky.com/story/us-military-hackers-conducting-offensive-operations-in-support-of-ukraine-says-head-of-cyber-command-12625139.

[20] Cordesman, ‘How? (and Does?) the War in Ukraine End’.

[21] Zakheim, ‘Russia Will Remain a Threat’.

[22] Quoted in Sophia Sleigh, ‘It Will Take Years For Russia To Rebuild “Severely Weakened” Forces, Britain Says’, *Huffington Post*, 9 September 2022, https://www.huffingtonpost.co.uk/amp/entry/it-will-take-years-for-russia-to-rebuild-severely-weakened-forces-british-officials-say_uk_63201cf6e4b027aa405ebdcf/.

[23] Sleigh.

[24] Sleigh.

reproduce that capability.'[25] The reference to reproduction capacity is notable, as it suggests the United States is seeking to degrade Russia's conventional force generation functions (i.e. its defence-industrial base). This policy, if successful, would further increase the time necessary for Russia to reconstitute its conventional force capabilities.[26] The policy was clarified and expanded days later in remarks by then-press secretary of the White House Jen Psaki, who, when asked whether US policy was now to permanently degrade Russia's military, replied that Austin was talking about preventing Russia from taking Ukraine but admitted that 'we are also looking to prevent them from expanding their efforts and President Putin's objectives beyond that, too'.[27] This position underpinned a sanctions policy targeting G7-produced technology needed for Russia's technology, aerospace, and defence sectors.[28] Expressing similar goals, both the UK and the European Union have levied comparable sanctions against Russia.[29] Ukrainian assessments suggest that these policies are beginning to achieve their intended effects.[30]

In sum, for several years after major combat operations cease, Russia will remain a nuclear state with substantial cyber capability but likely without significant conventional capability. This capability profile has no precedent in the 21st-century international system. When coupled with Russia's post-armed conflict motivation(s), we are likely to see unprecedented Russian cyber behaviours in the immediate post-armed conflict period.

[25] Quoted in Olivier Knox and Caroline Anders, 'The U.S. Has a Big New Goal in Ukraine: Weaken Russia', *Washington Post*, 26 April 2022, https://www.washingtonpost.com/politics/2022/04/26/us-has-big-new-goal-ukraine-weaken-russia/.

[26] Russia claims that its factories are producing military equipment nonstop. 'Russian Defense Chief Says Military Factories Working "Around the Clock"', *Moscow Times*, 2 January 2023, https://www.themoscowtimes.com/2023/01/02/russian-gas-exports-outside-ex-soviet-states-fell-455-in-2022-a79863.

[27] Quoted in Knox and Anders, 'The U.S. Has a Big New Goal in Ukraine',

[28] 'Treasury Sanctions Impede Russian Access to Battlefield Supplies and Target Revenue Generators', U.S. Department of the Treasury, 20 July 2023, https://home.treasury.gov/news/press-releases/jy1636. The G7 comprises Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States.

[29] See 'UK Sanctions Relating to Russia', Foreign, Commonwealth and Development Office, 30 June 2023, https://www.gov.uk/government/collections/uk-sanctions-on-russia; 'Webinar: UK Sanctions Relating to Russia: Briefing by UK Government', Foreign, Commonwealth and Development Office, 21 September 2022, https://www.youtube.com/watch?v=0Mb5ZLFE9EY; 'EU Response to Russia's Invasion of Ukraine', European Council and Council of the European Union, https://www.consilium.europa.eu/en/policies/eu-response-ukraine-invasion/.

[30] For example, in a recent interview, Andrii Yusov, representative of the Ministry of Education and Culture, noted that '[o]pportunities for deep modernization of the production of new weapons have significantly decreased due to the introduction of sanctions. In fact, the Russians have serious problems with modern optics, electronics, chips and circuits. And today there is no unequivocal source that would enable them to solve these problems.' Quoted in Angelina Strashkulych, 'Russia Refuses to Hand Over Many Ukrainian Prisoners of War without Any Explanation', UKRINFORM, 6 September 2023, https://www.ukrinform.ua/rubric-ato/3757717-andrij-usov-predstavnik-gur-mou.html.

5. Alternative Cyber Security Futures

James Dubik argues that, after major combat operations cease, Russia will continue to 'fight' by other means, using, for example, cyber actions to pursue its strategic goals in Ukraine.[31] Such actions would also likely (continue) against NATO and its member states. Dubik implores Western leaders to avoid the mistake of believing that the conflict with Ukraine, and the larger conflict with NATO and its members, will be over when the fighting stops.[32] Thus, planning should begin now 'for the inevitable, post-major combat operations transition period', a view shared by Fix and Kimmage, who argue that the Western strategy must think through 'the day after' major combat operations end.[33] But what strategic challenges will 'the day after' present to NATO and its members?

No matter the outcome of the kinetic conflict, Russia will still seek to control the security architecture in Europe, fuelled by either euphoria or an increased sense of irredentist revanchism. Coupling these motivations with Russia's nuclear and cyber capability profile suggests a novel post-armed conflict strategic challenge for NATO and its member states. This is recognized in Latvian Minister of Defence Ināra Mūrniece's comment that, despite Russia's major losses in Ukraine, it is a mistake to think that Russia has been weakened by this armed conflict and is incapable of new strategic surprises. Consequently, she argues, countries have to prepare for Russia to continue using its hybrid and nuclear threat arsenal to intimidate NATO member states and weaken support for Ukraine.[34]

Regarding Russia's nuclear capabilities, Rumer argues that although Russia's conventional force military stature has been diminished, its actions during the armed conflict have reinforced its reputation as a 'dangerous and unpredictable neighbor brandishing nuclear weapons' to achieve its strategic objectives.[35] History has shown, however, that nuclear weapons are not effective instruments of compellence. Thus, absent notable conventional force capabilities, should Russia win the armed conflict, it is unlikely that its nuclear arsenal would successfully support a triumphalism-fuelled effort to expand its gains beyond Ukraine.[36] For the same reason, should Russia lose the armed conflict or if it results in stalemate, it is unlikely that Moscow will find that brandishing its nuclear capabilities will successfully support an irredentist, revanchist-fuelled effort to reclaim Ukraine or other former Soviet territories. However, no matter the outcome of the armed conflict, Russia will continue to lean on its nuclear weapons as a strategic deterrent against any perceived threat of NATO aggression.

What does this portend for how Russia might employ its cyber capabilities?[37] Starting in mid-2022, Russian state-sponsored and state-affiliated cyber actors increased the operational tempo and intensity of cyber campaigns/operations targeting NATO and its member states.[38] Over the first year of armed

[31] James M. Dubik, 'The War in Ukraine Won't End When the Fighting Is Over', *Hill*, 9 March 2023, https://thehill.com/opinion/national-security/3890975-the-war-in-ukraine-wont-end-when-the-fighting-is-over/.

[32] Dubik.

[33] Dubik; Fix and Kimmage, 'What If Ukraine Wins?'

[34] 'Latvian Minister: It's Wrong to Think Russia Is Weakened by War with Ukraine', Baltic News Network, 23 May 2023, https://bnn-news.com/latvian-minister-its-wrong-to-think-russia-is-weakened-by-war-with-ukraine-245962.

[35] Rumer, 'Putin's War Against Ukraine'.

[36] See Todd S. Sechser and Matthew Fuhrmann, *Nuclear Weapons and Coercive Diplomacy* (New York: Cambridge University Press, 2017); Todd S. Sechser and Matthew Fuhrman, 'Crisis Bargaining and Nuclear Blackmail', *International Organization* 67, no. 1 (Winter 2013): 173–195, 179, https://www.jstor.org/stable/43282156.

[37] These may be employed independently or as part of a 'hybrid threat' capability package.

[38] Gareth Corfield, 'Putin's Cyber Shock Troops Turn Their Sights on NATO', *Telegraph*, 9 April 2023, https://www.telegraph.co.uk/technology/2023/04/09/russia-cyber-attack-troops-target-nato/.

conflict, cyber phishing activity against NATO and its member states increased 300% over pre-armed conflict levels, with a primary emphasis reportedly on cyber-enabled espionage.[39] Additionally, cyber activities have included distributed denial-of-service (DDoS) campaigns,[40] information operations,[41] and destructive operations.[42] Whereas Russia's increase in conventional force operations is leading to the attrition of skilled conventional force operators,[43] the opposite is arguably true in and through cyberspace. An increased cyber operational tempo is improving the skills of Russia's cyber operators.

Given Russia's nuclear-cyber capability profile and its post-armed conflict motivation(s), cyber persistence theory suggests two alternative cyber futures.[44]

Cyber Security Future #1: Cyber Campaigning Short of Armed-Attack Equivalent Effects

Regardless of the post-armed conflict outcome, in an effort to keep NATO and its members on their heels, Russia sustains and even increases the current operational tempo and intensity of its cyber campaigns/operations.[45] Given severely degraded conventional force capabilities, Moscow abstains

[39] See Google Threat Analysis Group, 'Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape', Google, February 2023, https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf. That these operations were reportedly primarily for espionage put policymakers at ease. As Microsoft notes, 'For the past year, threat actors with known or suspected ties to the GRU, FSB, and SVR have targeted and potentially gained footholds in government, policy, or critical infrastructure sectors throughout the Americas, Europe, and elsewhere. Although most of the operations are probably espionage-focused, the GRU actors have already shown a willingness to use destructive tools outside Ukraine if instructed.' Microsoft Threat Intelligence, 'A Year of Russian Hybrid Warfare in Ukraine', Microsoft, 15 March 2023, https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/03/A-year-of-Russian-hybrid-warfare-in-Ukraine_MS-Threat-Intelligence-1.pdf.

[40] See EU-CERT, *Russia's War on Ukraine: One Year of Cyber Operations*, https://cert.europa.eu/static/MEMO/2023/TLP-CLEAR-CERT-EU-1YUA-CyberOps.pdf, 5, Tom Hegel and Aleksandar Milenkoski, 'NoName057(16) – The Pro-Russian Hacktivist Group Targeting NATO', Sentinel Labs, 12 January 2023, https://www.sentinelone.com/labs/noname05716-the-pro-russian-hacktivist-group-targeting-nato/; Mandiant Intelligence, 'KillNet Showcases New Capabilities While Repeating Older Tactics', Mandiant, 20 July 2023, https://www.mandiant.com/resources/blog/killnet-new-capabilities-older-tactics; 'Unraveling Russian Multi-Sector DDoS Attacks Across Spain', Radware, 2 August 2023, https://www.radware.com/security/threat-advisories-and-attack-reports/unraveling-russian-multi-sector-ddos-attacks-across-spain/?utm_source=substack&utm_medium=email; Daryna Antoniuk, 'Pro-Russian Hackers Claim Attacks on Italian Banks', *Record*, 2 August 2023, https://therecord.media/russian-hackers-claim-attacks-on-italy; 'Dutch Organizations Targeted by DDoS Attacks', Nationaal Cyber Security Centrum, 8 August 2023, https://www.ncsc.nl/actueel/nieuws/2023/augustus/8/nederlandse-organisaties-doelwit-van-ddos-aanvallen?utm_source=substack&utm_medium=email.

[41] 'Sweden Says It's Target of Russia-Backed Disinformation over NATO, Koran Burnings', *Reuters*, 26 July 2023, https://www.reuters.com/world/europe/sweden-says-its-target-russia-backed-disinformation-over-nato-koran-burnings-2023-07-26/.

[42] See Tim Starks and Aaron Schaffer, 'Russian Sandworm Hackers Deployed Malware in Ukraine and Poland', *Washington Post*, 11 November 2022, https://www.washingtonpost.com/politics/2022/11/11/russian-sandworm-hackers-deployed-malware-ukraine-poland/; Dan Goodin, 'Mystery Solved in Destructive Attack that Knocked Out >10k Viasat Modems', *ars TECHNICA*, 31 March 2022, https://arstechnica.com/information-technology/2022/03/mystery-solved-in-destructive-attack-that-knocked-out-10k-viasat-modems/.

[43] 'Secretary of Defense Lloyd J. Austin III and Joint Chiefs of Staff Chairman General Mark A. Milley Hold Press Conference Following Virtual Ukraine Defense Contact Group Meeting', U.S. Department of Defense, 18 July 2023, https://www.defense.gov/News/Transcripts/Transcript/Article/3462659/secretary-of-defense-lloyd-j-austin-iii-and-joint-chiefs-of-staff-chairman-gene/.

[44] Fischerkeller, Goldman, and Harknett, *Cyber Persistence Theory*.

[45] This view is shared by David Van Weel, Assistant Secretary General for Emerging Security Challenges at NATO, who recently stated: 'Russia has made ample use of cyber capabilities before invading Ukraine, during hostilities, and it will likely continue using them after the kinetic phase of this conflict.' Quoted in Alexander Martin,

from or significantly limits the number of campaigns/operations that cause armed-attack equivalent effects and focuses on damaging political parties and leaders it dislikes, undermining the internal stability of 'anti-Russian' countries, degrading the integrity of the transatlantic alliance, and disrupting the logistics infrastructure of states that support Ukraine's reconstitution. In essence, Russia sustains its ongoing cyber campaigns/operations against NATO and its member states in the current geopolitical condition of armed conflict into a post-conflict condition of competition with the intent of cumulating tactical gains to levels of strategic significance. As cyber persistence theory explains, exploitative cyber campaigning offers an alternative to threats and the use of force for maintaining or altering the international distribution of power.

Cyber Security Future #2: Escalating to Cyber Armed-Attack Equivalent Effects

In this alternative future, *in spite of* its severely degraded conventional force capabilities, Russia targets NATO and its members with cyber campaigns/operations that cause armed-attack equivalent effects. Not content with the time it takes to cumulate effects from campaigns short of armed-attack equivalence, Russia escalates its activities in and through cyberspace.

Cyber persistence theory posits that certain destabilizing conditions may encourage states to breach the tacit ceiling of armed-attack equivalent effects and escalate to activities centred on coercion or physical damage/destruction, injury, or loss of life.[46] For example, to arrest a loss of relative power due to cyber strategic competition, a state may deliberately decide to threaten the use of force or strike kinetically. A post-armed conflict, nuclear-armed Russia with significantly degraded conventional force capabilities arguably presents a novel destabilizing condition and a conundrum for NATO and its member states.

Whereas nuclear weapons as a compellent will not serve Moscow's adventurism, nuclear weapons as a strategic deterrent may encourage Russia to target some NATO member states with cyber campaigns/operations that cause armed-attack equivalent effects to stress test NATO's willingness to invoke Article 5. The absence of significant Russian conventional force capabilities may induce caution in NATO when considering invoking Article 5, because Russia's weakened conventional force effectively removes a buffer (or a medium) in and through which NATO could manage a coercive or use-of-force escalation dynamic before reaching the threshold of nuclear threats, a threshold that Russia has demonstrated an unsettling level of comfort in crossing. Additionally, in a post-armed conflict geopolitical condition of competition, a kinetic response by NATO triggered by cyber-induced armed-attack equivalent effects would be a first for a state or state-level entity and would set a perilous precedent. Alternatively, inaction by NATO (i.e. failure to invoke Article 5) might open a seam in the alliance that Russia could seek to exploit to reconstruct the pre-armed conflict relations it enjoyed with some NATO member states and further push the envelope regarding the threshold of Article 5.[47] Counterintuitively, the West's objective of significantly degrading Russia's conventional force generation functions (the defence industrial base) may place the West in an unenviable position when confronting a nuclear-armed, cyber belligerent, post-armed conflict Russia.

'NATO: Military Cyber Defenders Need to Be Present on Networks During Peacetime', *Record*, 5 June 2023, https://therecord.media/nato-peacetime-cyberdefense-david-van-weel-cycon?utm_medium=email&_hsmi=261219959&_hsenc=p2ANqtz-9U-ST14DVdNDbXkohb6Zz_4QR_R-gHLXSBqk7OpsYOgjUBhRUn8wU51FneD5bx9XbNEetmxCu4XpZLmlGOLW755CyR2Q&utm_content=261221009&utm_source=hs_email.

[46] Fischerkeller, Goldman, and Harknett, *Cyber Persistence Theory*, chapter 5.

[47] Bronk argues that all Russia needs to do to 'break NATO' is to show that Article 5 'is a bluff'. Quoted in Barry Rosenberg, '3-to-5 Years from Now Is the Danger Time'.

6. Optimizing NATO's Aggregate Cyber Capability and Capacity

To prepare for the post-armed conflict environment, Cordesman argues that NATO today 'needs to make a massive effort to rebuild its forces to deter Russia from any further military adventures'.[48] Gideon Rose argues that 'the fighting must continue until Moscow accepts that it cannot achieve territorial gains by military force'.[49] NATO member states should certainly sustain their support for Ukraine and increase their conventional force capabilities, but this paper argues that those efforts should be informed as follows: (a) Russia's conventional forces will likely be significantly degraded in the immediate post-armed conflict environment; (b) the most likely strategic threat to NATO and its member states will be in and through cyberspace; and (c) current (and additional) NATO conventional force capabilities will likely have no deterrent effect on Russia's efforts to destabilize the Alliance and its member states via cyber campaigns/operations.[50]

A more strategically salient effort would be to focus on Russia's threat in and through cyberspace. This effort could have two tracks. First, NATO member states with the cyber capability and capacity to do so ought to support any current Ukrainian efforts,[51] or engage in efforts themselves,[52] to target Russia's cyber force generation functions, including but not limited to tools – sets of code used to create, debug, maintain, or otherwise support programs or applications – and Russian domestic cyber force infrastructure. Doing so should reduce the likelihood of the potential post-armed conflict conundrum presented by a vacuum of Russian conventional force capability. Russia will more quickly and successfully reconstitute cyber force generation functions relative to conventional force generation

[48] Cordesman, 'How? (and Does?) the War in Ukraine End'.

[49] Gideon Rose, 'Ukraine's Winnable War', *Foreign Affairs*, 13 June 2023, https://www.foreignaffairs.com/ukraine/ukraines-winnable-war.

[50] States are gradually coming to accept that conventional force capabilities do not serve as effective deterrents for opponents' cyber exploitative campaigns short of armed-attack equivalence. To wit, the U.S. Department of Defense argues that '[c]ompetitors deterred from engaging the United States and our allies in an armed conflict are using cyberspace operations to steal our technology, disrupt our government and commerce, challenge our democratic processes, and threaten our critical infrastructure'. See U.S. Department of Defense, *Summary: Department of Defense Cyber Strategy 2018*, p. 1, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF. Further, the United Kingdom and the United States have commented, respectively, that 'evidence is limited for cyber operations being a primary contributor to deterrence' and '[t]he Department's experiences have shown that cyber capabilities held in reserve or employed in isolation render little deterrent effect on their own'. See U.S. Department of Defense, *Summary: 2023 Cyber Strategy of the Department of Defense*, https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF; National Cyber Force, *The National Cyber Force: Responsible Cyber Power in Practice*, March 2023, p. 10, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1148278/Responsible_Cyber_Power_in_Practice.pdf.

[51] Joe Tidy, 'Meet the Hacker Armies on Ukraine's Cyber Front Line', BBC News, 15 April 2022, https://www.bbc.com/news/technology-65250356.

[52] In response to comments by USCYBERCOM's General Paul Nakasone that the US has conducted a series of operations across the full spectrum of offensive, defensive, [and] information operations in support of Ukraine, White House press secretary Karine Jean-Pierre was asked whether the offensive cyber operations were contrary to the US position of avoiding direct engagement with Russia. Jean-Pierre responded, 'We don't see it as such. We have talked about this before. We've had our cyber experts here at the podium lay out what our plan is. That has not changed. So the answer is, just simply, no.' Quoted in Martin, 'U.S. Military Hackers Conducting Offensive Operations in Support of Ukraine'.

functions,[53] which should encourage capable Allied states to engage persistently in such cyber functions.[54] Second, to prepare for the immediate post-armed conflict environment, the transatlantic alliance ought to begin shifting to a proactive cyber operational posture that leverages the aggregate cyber capabilities and capacities of its member states to mitigate the strategic consequences of a hostile, post-armed conflict Russia primarily pursuing its strategic goals in and through cyberspace.[55]

The individual decisions of the most cyber-capable NATO member states to support any current Ukrainian efforts, or engage in efforts themselves, to target Russia's cyber force generation functions need not be made with the full backing of all NATO member states, but a NATO shift to a proactive cyber operational posture must. Thus, it is important to consider what this would entail for NATO, how such a posture might be authorized, and how it may be operationalized.

David Van Weel, Assistant Secretary General for Emerging Security Challenges at NATO, recently commented that NATO must take a more proactive approach to achieve security in the strategic competition playing out in and through cyberspace, which 'is contested at all times'.[56] To do so, he argues that NATO and its member states must 'foster an entirely new mindset regarding how to operate, compete, and, if necessary, fight in the cyber domain'.[57] Indeed, he argues that 'being proactive … means being responsible actors'.[58] Van Weel highlights three areas of emphasis: NATO 'requires a better integration of activities among numerous stakeholders at each of NATO's three cyber defense levels – political, military, and technical';[59] NATO member states must act coherently with other states and relevant actors, including industry, academia, the private sector, and other international organizations; and NATO and its member states must focus on 'getting the basics right and ensuring that defenders have the capabilities to detect, prevent, and mitigate malicious activity'.[60]

While Van Weel's priorities are necessary for improving the cyber security of NATO and its member states and supporting preparations to 'respond swiftly', they are not sufficient. What is missing is a proactive operational element that supports continuous campaigning 'forward' in space and time to anticipate, preclude, inhibit, or otherwise constrain adversaries' opportunities to realize strategic gains in and through cyberspace. Absent the adoption of a proactive, anticipatory operational element, NATO member states' aggregate cyber capabilities and their employment (or lack thereof) would, at best, support a 'response force' that is misaligned with the cyber strategic environment and, therefore,

[53] Russia could, for example, appropriate the infrastructure of some of the many Russian state-sponsored or state-affiliated cyber threat groups.

[54] Evidence shows that when cyber force generation functions are targeted, they can be reconstituted relatively rapidly. The technology-centred economic sanctions on Russia may slow this reconstitution effort somewhat, but not preclude it.

[55] By 2018, 23 NATO member states had active-duty military organizations possessing the capability and authority to conduct cyberspace operations. However, establishing a cyber command should not be equated with creating a robust military cyber capability needed to support a proactive operational posture, which may be considered as 'the ability to effectively execute and sustain a range of cyber operations that serve tactical or strategic purposes'. In this light, only a handful of NATO member states are capable of sustaining a proactive cyber operational posture. See Max Smeets, 'The Challenges of Military Adaptation to the Cyber Domain: A Case Study of the Netherlands', *Small Wars & Insurgencies* (2023): 1–20, https://doi.org/10.1080/09592318.2023.2233159.

[56] David Van Weel, 'A Proactive Approach to the Cyber Domain Strengthens NATO's Deterrence and Defense Posture', *Digital Front Lines*, 13 July 2023, https://digitalfrontlines.io/2023/07/13/proactive-approach-to-the-cyber-domain/.

[57] Van Weel.

[58] A similar position is taken by the United Kingdom in National Cyber Force, *The National Cyber Force: Responsible Cyber Power in Practice*.

[59] Van Weel, 'A Proactive Approach to the Cyber Domain'.

[60] Van Weel.

suboptimal for providing security in and through cyberspace for NATO and its member states and partners.[61]

Although a proactive operational element could, in exigent circumstances, leverage the cyber effects capabilities that have been volunteered by at least nine NATO members to date,[62] its primary focus ought to be leveraging non-exquisite capabilities that support operating forward to identify, for example, adversary tactics, techniques and procedures, malware, and other adversary signatures, and to set favourable security conditions should a crisis or armed conflict erupt. Operating forward would enable the anticipation of adversary operations, preclusion of adversary options, reduction in the number of attack vectors, and denial of cyber terrain. In this context, forward in space may be understood in two ways: first, as networks, systems, and devices beyond the technical boundaries of NATO's communication and information systems but within the national boundaries of NATO member states; second, as networks, systems, and devices positioned beyond those boundaries.[63]

In the first instance, a NATO proactive operational element would support 'hunting forward' on a member state's networks, systems, and devices with the permission of that NATO member state. This could take different forms – for example, one alliance member could 'hunt' alongside a host nation's cyber defenders, as the US has done with Albania,[64] Croatia,[65] Estonia,[66] Lithuania,[67] Montenegro,[68] and North Macedonia,[69] and as the US and Canada have done with Latvia.[70] However, not all member states

[61] General Paul Nakasone, Commander, USCYBERCOM has stated, 'If we are only defending in "blue space", we have failed.' Thus, '[s]hifting from a response outlook to a persistence force that defends forward moves our cyber capabilities out of their virtual garrisons, adopting a posture that matches the cyberspace operational environment.' Paul M. Nakasone, 'A Cyber Force for Persistent Operations', *Joint Force Quarterly* 92 (1st Quarter 2012): 10–14, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92.pdf. Quotes appear on pages 12 and 13, respectively.

[62] Shannon Vavra, 'NATO Cyber-Operations Center Will Be Leaning on Its Members for Offensive Hacks', *Cyberscoop*, 30 August 2019, https://cyberscoop.com/nato-cyber-operations-offensive-hacking-neal-dewar/.

[63] 'Forward in time' refers to the notion that operations and activities support an anticipatory posture.

[64] Cyber National Mission Force Public Affairs, '"Committed Partners in Cyberspace": Following Cyberattack, U.S. Conducts First Defensive Hunt Operation in Albania', 23 March 2023, https://www.cybercom.mil/Media/News/Article/3337717/committed-partners-in-cyberspace-following-cyberattack-us-conducts-first-defens/.

[65] Cyber National Mission Force Public Affairs and United States European Command, 'Partnership in Action: Croatian, U.S. Cyber Defenders Hunting for Malicious Actors', 19 August 2022, https://www.eucom.mil/article/42191/partnership-in-action-croatian-us-cyber-defenders-hunting-for-malicious-actors.

[66] US Cyber Command, 'Estonia, U.S. Conduct Joint Defensive Cyber Operation', 3 December 2020, https://www.defense.gov/News/News-Stories/Article/Article/2434474/estonia-us-conduct-joint-defensive-cyber-operation/.

[67] See Cyber National Mission Force Public Affairs, 'U.S. Conducts First Hunt Forward Operation in Lithuania', U.S. Cyber Command, 25 August 2023, https://www.cybercom.mil/Media/News/Article/3505610/us-conducts-first-hunt-forward-operation-in-lithuania/; '"Building Resilience": U.S. Returns from Second Defensive Hunt Operation in Lithuania', U.S. Cyber Command, 12 September 2023, https://www.cybercom.mil/Media/News/Article/3522801/building-resilience-us-returns-from-second-defensive-hunt-operation-in-lithuania/#:~:text=FORT%20GEORGE%20G.,the%20country%20in%20May%202022.

[68] 'US, Montenegro Work Together to Defend against Malicious Cyber Actors', DoD News, 30 October 2019, https://www.cybercom.mil/Media/News/News-Display/Article/2002939/us-montenegro-work-together-to-defend-against-malicious-cyber-actors/.

[69] US European Command Public Affairs, 'U.S. and Macedonia Participate in Cyber Defense Cooperation', U.S. Cyber Command, 12 October 2018, https://www.cybercom.mil/Media/News/Article/1660069/us-and-macedonia-participate-in-cyber-defense-cooperation/.

[70] Cyber National Mission Force Public Affairs, '"Shared Threats, Shared Understanding": U.S., Canada and Latvia Conclude Defensive Hunt Operations', U.S. Cyber Command, 10 May 2023,

may be comfortable with this model, so alternatives ought to be considered.[71] For example, after being made aware by the United States that China had compromised its classified defence networks, Japan was wary of the US offer to provide a 'hunt forward' team to assist in identifying the breadth and depth of the compromise.[72] A former senior US defence official commented that '[t]hey were uncomfortable having another country's military on their networks'.[73] Consequently, the US and Japan arrived at a compromise approach: the Japanese would use domestic commercial firms to assess the severity of the compromise, and a joint U.S. National Security Agency and USCYBERCOM team would review the results and provide guidance on how to mitigate the vulnerabilities.[74]

In the second instance, a cyber team or teams contributed by one or more NATO member states would operate beyond the national boundaries of NATO member states.

Fully specifying how NATO could authorize a proactive operational element is beyond the scope of this paper, but offering several broad notional frameworks is not. Some have offered a framework where NATO's Intelligence and Security division would gather intelligence on cyber threats, the Cyberspace Operations Center (CYOC) would outline ways to mitigate those threats, and the CYOC would share its analyses with threatened states, and those states would request assistance from Allies who have volunteered to support threatened target classes (or countries) by employing their own cyber capabilities against the identified threats.[75] However, this framework excludes important elements likely necessary to support a proactive operational element engaged in continuous campaigning – command and control by Supreme Allied Commander Europe (SACEUR) and a mandate to operate from the North Atlantic Council (NAC).

An alternative is to establish a cyber-focused Memorandum of Understanding (MOU) organization that specifies a framework for allies and partners to coherently, efficiently, and continuously campaign together in and through cyberspace under the command and control of SACEUR and by NAC mandate in competition, militarized crisis, and armed conflict.[76] As such a framework would place some cyber capabilities under the command of SACEUR, it would exceed the requirements of the Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA) mechanism. However, as it enables campaigning in strategic competition short of militarized crisis and armed conflict, it would also exceed the strategic utility of SCEPVA.[77] Additionally, the capabilities required to support a proactive operational element need not be the likely exquisite offensive cyber operations capabilities that member states volunteer through SCEPVA. To prepare for the post-armed conflict strategic environment(s), member states and partners ought to be more willing to contribute more 'mundane' but nonetheless important capabilities that are far less likely to potentially jeopardize their intelligence assets, means, and methods.[78] A model

https://www.cybercom.mil/Media/News/Article/3390470/shared-threats-shared-understanding-us-canada-and-latvia-conclude-defensive-hun/.

[71] Elise Vincent, 'France's Cyber Defense Force Questions Role of U.S. Support in Europe', *Le Monde*, 15 January 2023, https://www.lemonde.fr/en/international/article/2023/01/15/france-s-cyber-defense-force-questions-the-role-of-us-support-in-europe_6011684_4.html.

[72] Ellen Nakashima, 'China Hacked Japan's Sensitive Defense Networks, Officials Say', *Washington Post*, 8 August 2023, https://www.washingtonpost.com/national-security/2023/08/07/china-japan-hack-pentagon/.

[73] Nakashima.

[74] Nakashima.

[75] Franklin D. Kramer, Lauren Speranza, and Conor Rodihan, 'NATO Needs Continuous Responses in Cyberspace', *New Atlanticist*, 9 December 2020, https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-needs-continuous-responses-in-cyberspace/.

[76] A full listing of NATO Partners can be found at https://www.nato.int/cps/en/natohq/51288.htm.

[77] It is presumed that the SCEPVA mechanism holds relevance for only militarized crisis and armed conflict.

[78] Mikkel Storm Jensen, 'Five Good Reasons for NATO's Pragmatic Approach to Offensive Cyberspace Operations', *Defence Studies* 22, no. 3 (May 2022): 467, https://doi.org/10.1080/14702436.2022.2080661.

for this organization could be NATO's Allied Special Operations Forces Command under the command of SACEUR and sourced by cyber contributions from member states.

A proactive continuous campaign in substance could comprise the tasking contours of the ongoing, non-Article 5 Operation Sea Guardian, albeit adapted to the context of cyberspace.[79] For example, a named campaign could encompass tasks for cyberspace situational awareness; operations to anticipate, preclude, inhibit, and interdict/disrupt adversary cyber campaigns/operations, and defend and protect NATO and its member states against cyberspace-based malicious activities; identifying, locating, and disrupting the sharing of malware; and protecting critical infrastructure from adversary cyber activities. NATO allies and partners contribute to Operation Sea Guardian through 'direct support' by placing assets under NATO operational command and through 'associated support' with assets that remain under national command. Such an approach would align with the differential cyber capability sets and capacities of member states.

Given that NATO is a defensive alliance, some may argue that a proactive operational element and its associated activities and operations would not align with NATO's purpose. The *raison d'etre* of the Alliance, however, is to safeguard the freedom and *security* of all Allies, against all threats, from all directions.[80] Cyber persistence theory argues that security in and through cyberspace comes through seizing and sustaining the initiative in cyber strategic competition to set favourable conditions, tempo, and the decision-making cycle of operational action in order to place the adversary at a disadvantage and/or force the adversary to adjust to friendly action. Therefore, to act in alignment with the Alliance's stated purpose, to the degree that the Alliance has the capacity and capability to do so, it ought to incorporate into its overall cyber strategy an operational element to responsibly seize and sustain the initiative.

[79] For a description of Operation Sea Guardian, which has been ongoing since 2016, see 'Operation Sea Guardian', North Atlantic Treaty Organization, 26 May 2023, https://www.nato.int/cps/en/natohq/topics_136233.htm; 'Operation Sea Guardian', Allied Maritime Command, https://mc.nato.int/missions/operation-sea-guardian.

[80] 'Deterrence and Defence', North Atlantic Treaty Organization, 19 July 2023, https://www.nato.int/cps/en/natohq/topics_133127.htm#:~:text=NATO%20is%20a%20defensive%20alliance,one%20of%20NATO's%20core%20tasks.

7. Grand Strategy Shifts and Tilts

The most recent national security strategies of the United States and the United Kingdom speak of shifts and tilts to the Indo-Pacific region. Additionally, NATO's *2022 Strategic Concept* has elevated the importance of China.[81] Some have expressed concerns that these leanings ought to be reconsidered in light of the Russia-Ukraine armed conflict.

Cordesman says that US national defence strategy must be 'revised' to reflect the fact that US efforts during the Russia-Ukraine armed conflict and its strategy for a post-armed environment 'are just as important as its efforts to strengthen its forces and collective defense efforts in Asia'.[82] Similarly, Zakheim argues that many US politicians and policymakers 'seem to hope that whatever the outcome of Russia's invasion of Ukraine, the United States will be able to return to its main national security preoccupation –namely, the threat that China poses to American interests in the western Pacific and elsewhere around the globe'. Acting on this hope, however, 'would constitute a serious strategic error', Zakheim says. 'Whether it wins or loses the war with Ukraine, Russia's threat to European stability will not disappear.'[83]

Dan Sabbagh suggests that the emphasis on China in the UK's *Integrated Review Refresh 2023* is misguided. He argues that 'further boosting Britain's tiny military presence in the Indo-Pacific is not obviously good value for money for the UK's stretched armed forces – and for now, at least, the primary threat from Beijing to Britain is its ceaseless desire to steal intellectual property, not a military one'.[84] Therefore, he proposes that investments in British military capability 'ought to be focused on helping Ukraine and frontline Nato states protect themselves'.[85]

The frameworks offered in this paper for optimizing NATO's aggregate cyber capability and capacity for a post-armed conflict environment could, in different ways, satisfy those who call for a stark shift to the Indo-Pacific and also those who do not. If one accepts that Russia's primary strategic threat to NATO and its member states in the immediate post-armed conflict environment originates from cyberspace, the proposals address that threat, thereby satisfying the concerns of those arguing for elevating the priority of Russia. The proposals could also placate those who elevate China as the primary threat because, as Brands argues, the West 'can inflict severe strategic defeat on it [China] by ensuring that Russia loses its war in Ukraine'.[86] Moscow, Brands argues, 'weakens the democratic world through cyberattacks and information warfare; it helps Beijing make the global internet friendlier to dictatorial rule. Joint military exercises, defense technological projects, and other aspects of Sino-Russian cooperation fuel China's challenge to U.S. power.'[87] Brands' claim ought to be appended to include ensuring that Russia is precluded, inhibited, or otherwise constrained from threatening the West in and through cyberspace in a post-armed conflict environment.

Optimizing the aggregate capacity and capability of NATO member states through a proactive operational element would provide increased security against cyber campaigns/operations from *both*

[81] See *NATO 2022 Strategic Concept*, page 5.
[82] Cordesman, 'How? (and Does?) the War in Ukraine End'.
[83] Zakheim, 'Russia Will Remain a Threat'.
[84] Dan Sabbagh, 'Sunak's Focus May Be on China, but It's Europe's Security That Is Vital for the UK', *Guardian*, 12 March 2023, https://www.theguardian.com/politics/2023/mar/12/sunaks-focus-may-be-on-china-but-its-europes-security-that-is-vital-for-the-uk.
[85] Sabbagh.
[86] Hal Brands, 'Opposing China Means Defeating Russia'.
[87] Brands.

Russia and China, the latter of which also targets those states in and through cyberspace and operates globally to spread disinformation, illicitly acquire defence contractors' intellectual property and other sensitive government information, and compromise critical infrastructure.[88] Thus, it would assuage both those who argued that China ought to have been elevated in NATO's strategic concept and those who argued the contrary.

[88] See Laurens Cerulus, 'Von der Leyen Calls Out China for Hitting Hospitals with Cyberattacks', *Politico*, 22 June 2020, https://www.politico.eu/article/eu-calls-out-china-for-hitting-hospitals-with-cyberattacks/; Gordon Corera, 'China Accused of Cyber-attack on Microsoft Exchange Servers', *BBC News*, 19 July 2021, https://www.bbc.com/news/world-asia-china-57889981; Jonathon Greig, 'Multiple Chinese APTs Are Attacking European Targets, EU Cyber Agency Warns', *Record*, 17 February 2023, https://therecord.media/multiple-chinese-apts-are-attacking-european-targets-eu-cyber-agency-warns.

8. Conclusion

No matter the outcome of the Russia-Ukraine armed conflict, Russia will continue to be motivated to control the security architecture of Europe. The West's current objective of attriting Russia's conventional force generation functions could drive Russia to leverage its substantial cyber capability and capacity in the post-armed conflict environment. This may, counterintuitively, place NATO in a bind should Russia escalate in and through cyberspace to campaigns/operations that cause armed-attack equivalent effects. Even if Russia chooses to stay short of such effects, the trend of Russia's current cyber operational tempo, including groups affiliated with Russia, suggests that NATO and its member states will be subject to a significant, perhaps unprecedented, sustained volume of cyber intrusions in a post-armed conflict environment.

It would be prudent for NATO and its member states to start preparing now for these potential futures. Member states ought to support current Ukrainian efforts or engage in their own efforts to target Russia's cyber force generation functions, and NATO must adopt policies that optimize member states' and partners' aggregate cyber capability and capacity – policies that centre on a proactive operational posture inclusive of an operational element that can anticipate, preclude, inhibit, or otherwise constrain Russian cyber efforts in a post-armed conflict environment. Both of these efforts would satisfy the security concerns of those in the West who prioritize Russia over China and of those who hold opposing views.