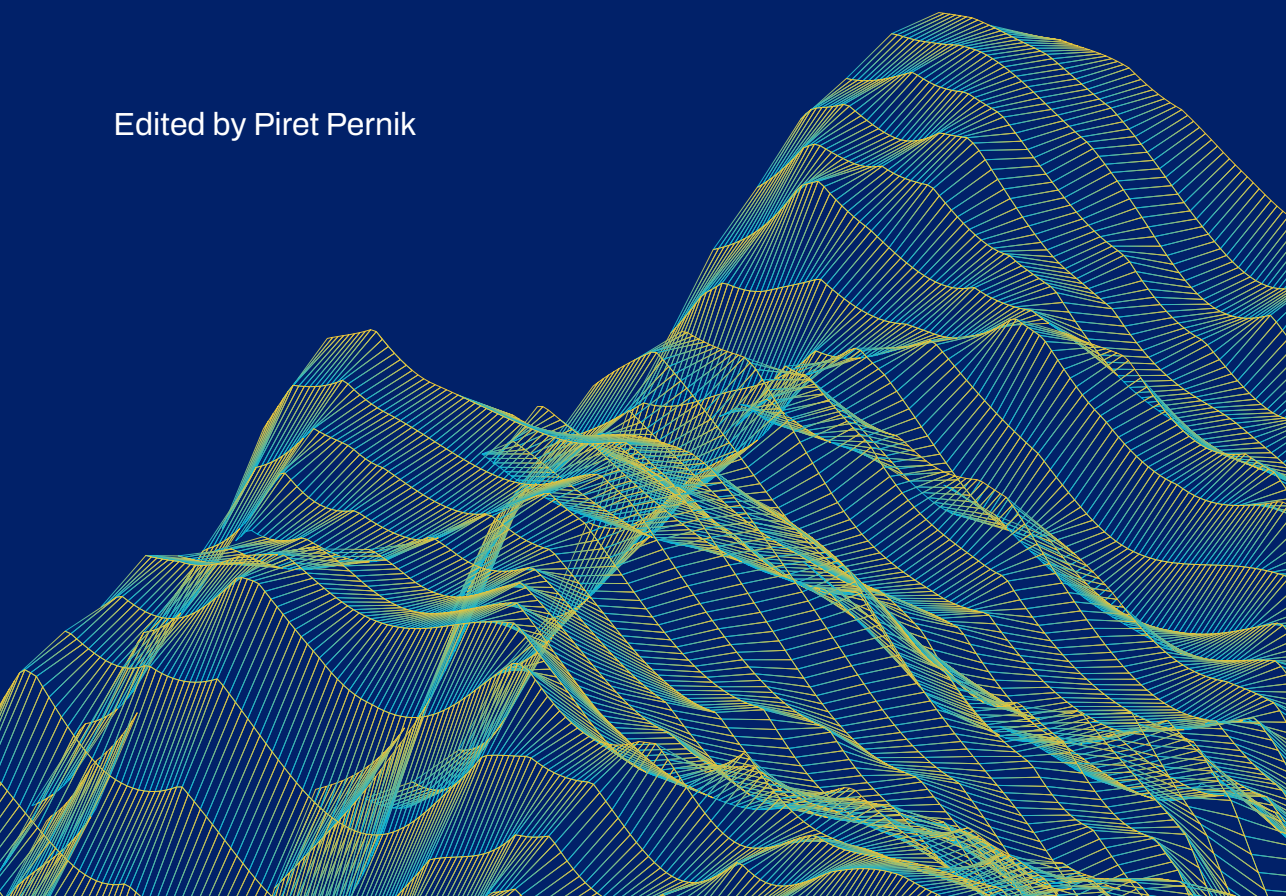
Published by CCDCOE

# Cyberspace Strategic Outlook 2030

## Horizon Scanning and Analysis

Edited by Piret Pernik



Published by CCDCOE

# Cyberspace Strategic Outlook 2030

## Horizon Scanning and Analysis

Edited by Piret Pernik

# Cyberspace Strategic Outlook 2030
# Horizon Scanning and Analysis



ISBN (print): 978-9916-9565-8-8
ISBN (pdf): 978-9916-9565-9-5

## COPYRIGHT AND REPRINT PERMISSIONS



2022 © NATO CCDCOE Publications
NATO CCDCOE Publications
Filtri tee 12, 10132 Tallinn, Estonia
Phone: +372 717 6800
Fax: +372 717 6308
E-mail: publications@ccdcoe.org
Web: www.ccdcoe.org
Cover design and content layout: Erkin Antov
Language editing: Refiner Translations, Chris Springer

## 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 34 nations.

The CCDCOE (also referred to as the Centre) maintains its position as an internationally recognised 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 Centre is staffed and financed by Austria, Belgium, Bulgaria, Canada, Croatia, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Montenegro, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, South Korea, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States.

The CCDCOE produces the Tallinn Manual 2.0, the most comprehensive guide for policy advisors and legal experts on how international law applies to cyber operations carried out between and against states and state actors. Since 2010 the Centre has organised Locked Shields, the biggest and most complex technical live-fire challenge in the world. The CCDCOE hosts the International Conference on Cyber Conflict, CyCon, a unique annual event in Tallinn, bringing together key experts and decision-makers of 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

# Contents


| | | |
|---|---|---|
| | **Foreword**<br>David van Weel | **6** |
| | **Introduction to Cyberspace Strategic Outlook 2030: Horizon Scanning and Analysis**<br>Piret Pernik | **7** |
| **Chapter 1** | **A Strategic Outlook for Cyberspace Operations**<br>James A. Lewis | **10** |
| **Chapter 2** | **Situational Cyber Stability and the Future of Escalating Cyber Conflict**<br>Jason Healey and Virpratap Vikram Singh | **19** |
| **Chapter 3** | **Do Joint All-Domain Operations Increase Cyber Vulnerabilities in Nuclear Command, Control, and Communications Systems within the NATO Alliance?**<br>Franz-Stefan Gady | **32** |
| **Chapter 4** | **NATO's Role in Responding to China's 'Cyber Superpower' Ambitions**<br>Laura G. Brent | **42** |
| **Chapter 5** | **Drivers of Change Impacting Cyberspace in 2030**<br>Piret Pernik | **56** |
| **Chapter 6** | **NATO Cyber Policies in Relation to the International Stability Framework**<br>Berend Valk | **80** |
| | **Contributors** | **102** |

# Foreword

International stability has been challenged in recent days. Peace on the European continent has been fundamentally shattered. The Alliance's foundational commitment to the principles of individual liberty, democracy, human rights, and the rule of law also fully applies in the realm of emerging technological challenges. These evolving threats include those within the cyber domain, which increasingly challenge the NATO Alliance as part of the growing strategic competition in international security.

This volume of edited papers is intended to help inform decision-makers so they better understand the critical features of, and differences among, the various cyber threats we face. Threat actors are increasingly seeking to destabilise the Alliance through the cyber domain by employing malicious cyber activities and campaigns below the threshold of an armed attack.

Early in the decade of the 2000s, NATO developed its cyber capabilities as a purely technical issue. Cyber defence first became part of NATO's core task of collective defence in 2014. Allied heads of state and government endorsed NATO's Comprehensive Cyber Defence Policy in June 2021, further incorporating cyber defence into NATO's broader approach of deterrence and defence. These changes build upon the important understanding that the cyber domain must properly align with NATO strategic decision-making.

In the 2021 policy, NATO acknowledged that only a comprehensive approach to cyberspace could respond to a domain that is contested at all times by threat actors. A proactive approach requires a coordinated effort between the distinct cyber mandates and activities at the political, military, and technical levels.

NATO's core role is to defend its own networks while also using its entire toolbox – political, diplomatic, and military measures – to respond to the full spectrum of cyber threats. Lower-impact malicious cyber campaigns over time by the same threat actor are understood to be potentially as destructive as a single high-impact cyberattack. Allies recognise that the impact of significant and cumulative malicious cyber activities might, in certain circumstances, be considered as amounting to an armed attack.

NATO must and will enhance its role as a platform for political consultation among Allies, to share concerns about malicious cyber activities, possible collective responses, and the option to impose costs on those who harm Alliance security. Increased information and intelligence-sharing supports political consultations. Resilience remains a priority and Allies must be continuously prepared to detect, prevent, mitigate, and respond to vulnerabilities and intrusions. Future efforts in this area will continue to build on the Cyber Defence Pledge that Allies adopted in 2016 to maintain robust defences that also harness partnerships and leverage technological innovation.

Cyber defence is a strategic issue, not just a technical matter to be left to specialists. Malicious cyber activity presents an immense challenge, as it blurs the lines between the traditional thresholds of peace, crisis, and conflict. Preserving security now requires taking into account the constant competition that is taking place in cyberspace. This volume is intended to help leaders and policymakers as they consider the way forward.

# Introduction

NATO deputy secretary general Mircea Geoană has stated: 'The coming decade will be dominated by the need to combat hybrid and cyber threats.'[1] NATO's new Strategic Concept, which will be adopted at the Madrid Summit in June 2022, will guide Allies to address these threats, along with threats emerging from emerging and disruptive technologies (EDTs). The Strategic Concept sets the Alliance's strategy and fundamental security tasks, and guides its future political and military development.[2] In order to stay relevant, NATO should 'capitalize on what the Alliance needs to do and does well' rather than focusing on new tasks that could dilute its primary military role.[3]

NATO's strategic thinking about cyber threats seems to be evolving towards more assertive and proactive collective responses. A shift in NATO's response to cyber threats occurred in June 2021 when the Alliance, endorsing a new Comprehensive Cyber Defence Policy, recognised for the first time that 'the impact of significant malicious cumulative cyber activities might, in certain circumstances, be considered as amounting to an armed attack'.[4] In other words, the Alliance declared it could respond to malicious cyber activities below the threshold of use of force causing significant harm with, among other things, conventional military or offensive cyberspace operations. At the same time, NATO's cyber defence mandate remains defensive – and as an organisation, it does not possess or seek to develop offensive cyber capabilities.[5] In regards to cyberspace operations, NATO performs roles confined to the defence side of the equation as follows: preventing, defending, and recovering from cyberattacks against the Alliance; maintaining cyberspace situational awareness; and planning cyberspace operations and command and control (C2) of cyberspace operations.[6]

While retaining its defensive mandate in the cyber domain, the Alliance could, through the Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA) mechanism, carry out offensive cyber effects (which themselves can reach the threshold of use of force), if authorised to do so by the North Atlantic Council. However, given the secrecy and political sensitivity concerning the possession and use of cyber capabilities among Allies, it is questionable whether the 30 Allies could reach consensus in the short time necessary for any meaningful response to a cyberattack. To retain strategic ambiguity around thresholds that would trigger possible counter-responses (thus reinforcing deterrence in the cyber domain), NATO has not disclosed what cyber threats it considers to be triggers for offensive cyber effects.[7] This ambiguity seems aligned with the national approaches as NATO Allies are also

---

1 'Future-Proofing the NATO Alliance', North Atlantic Treaty Organisation, 4 February 2022, https://www.nato.int/cps/en/natohq/news_191388.htm?selectedLocale=en.

2 'Strategic Concepts', North Atlantic Treaty Organisation, https://www.nato.int/cps/en/natohq/topics_56626.htm.

3 Thierry Tardy, 'The Future of NATO', *NATO Defence College Policy Brief,* No. 20, November 2021, https://www.ndc.nato.int/news/news.php?icode=1634.

4 'Brussels Summit Communiqué: Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Brussels', NATO, 14 June 2021, https://www.nato.int/cps/en/natohq/news_185000.htm.

5 In July 2016, the Allies reaffirmed NATO's defensive mandate. See 'Cyber Defence', North Atlantic Treaty Organisation, 2 July 2021, https://www.nato.int/cps/en/natohq/topics_78170.htm; Steven Hill, 'NATO and International Law of Cyber Defence', in *Research Handbook on International Law and Cyberspace,* 2nd edition, eds. Nicholas Tsagourias and Russell Buchan, Elgaronline, DOI: https://doi.org/10.4337/9781789904253, page 513.

6 'Request for Information RFI-ACT-SACT-22-22', Headquarters Supreme Allied Commander Transformation, February 2022, https://www.act.nato.int/application/files/7916/4436/5772/rfi022022.pdf.

7 In addition, there are concerns that use of offensive cyber effects escalates conflict, risks miscalculation and exposes tactics, techniques, and procedures to a potential adversary, thereby decreasing deterrence in the cyber domain. See Jan Kallberg, 'Demilitarize Civilian Cyber Defense, and You'll Gain Deterrence', *DefenceNews*, 9 February, https://www.defensenews.com/opinion/commentary/2022/02/09/demilitarize-civilian-cyber-defense-and-youll-gain-deterrence/.

secretive concerning their intentions to engage in cyber activities short of war.[8]

Yet others have called for greater transparency about the use of force in cyberspace.[9] They point out that political and public debate about how to respond to malicious cyber activity 'short of war' would be beneficial.[10] They suggest Allies should formulate a strategy of response options and establish a framework to classify cyber incidents and attacks, as well as formulate specific thresholds and trigger points for counteractions.[11] The need for the Alliance to address cyber activities in the so-called grey zone seems to be supported by empirical evidence of present and past cyberattacks.[12] Contrary to popular belief, analysis shows that authoritarian opponents' cyberspace operations are run primarily below the threshold of use of force.[13] Cyberspace operations are not been used as 'substitutes or complements to military operations' and their strategic effects are negligible.[14] This observation underlines the need to address cumulative cyber activities and identify possible counter-responses in the grey zone.

The present volume focuses upon NATO responses to cyber threats in 2022–2030, addressing EDTs, evolving cyber threats, strategies and tactics of cyberspace actors, and other drivers of change. It is the second edited book about cyberspace horizon scanning and analysis published by the CCDCOE, contributing to the NATO 2030 discussions about how to strengthen the Alliance militarily and politically against cyber threats. The volume addresses conceptual debates and practical requirements contributing constructively to the NATO 2030 Agenda.

The book consists of six chapters that elucidate the evolution of cyber threats and nation-state competition in the new decade. The chapters draw implications for NATO strategy and policies. All the chapters in this book have undergone peer review to ensure their academic quality of the research.

In the opening chapter, **James A. Lewis** argues that cyber norms and old concepts such as deterrence are insufficient for achieving international stability in cyberspace. He recommends that NATO develop a new conceptual framework and a set of proportional response options to respond to cyberattacks. He observes that political consensus needs to be established in order to exercise these options.

In Chapter Two, **Jason Healey and Virpratap Vikram Singh** consider the likelihood of geopolitical and cyber tensions escalating into a larger conflict. They develop a matrix of high and low geopolitical and cyber tensions and find that in high-tension contexts, there is an increased likelihood of cyber

8 A recent study shows that several European Allies are ambiguous about when, how, and to what extent offensive cyber capabilities could be deployed. See Tobias Liebetrau, 'Cyber Conflict Short of War: A European Strategic Vacuum', *European Security*, 4 February 2022, DOI: 10.1080/09662839.2022.2031991.

9 Some Five Eyes countries are relatively transparent about their offensive cyber capabilities and cyberspace operations. See Josh Gold, 'The Five Eyes and Offensive Cyber Capabilities: Building a "Cyber Deterrence Initiative"', CCDCOE, 2020, https://ccdcoe.org/library/publications/the-five-eyes-and-offensive-cyber-capabilities-building-a-cyber-deterrence-initiative/.

10 Liebetrau, 'Cyber Conflict Short of War'.

11 Ibid.

12 Lennart Maschmeyer and Nadiya Kostyuk, 'There Is No "Shock and Awe": Plausible Threats in the Ukrainian Conflict', War on the Rocks, 8 February 2022, https://warontherocks.com/2022/02/there-is-no-cyber-shock-and-awe-plausible-threats-in-the-ukrainian-conflict/. As Maschmeyer and Kostyuk note, there is a political and scholarly debate about the empirical lack of cyberwar, the questionable strategic value of cyberattacks, and the understanding of cyber conflict as mainly an intelligence contest.

13 Ibid.

14 Ibid.

incidents and escalation of cyber conflict.

In Chapter Three, **Franz-Stefan Gady** examines the Joint All-Domain Operations (JADO) concept of the NATO future operational doctrine, which could link conventional command and control with the nuclear ones. Gady identifies cybersecurity risks related to that development, addresses the possibility of miscalculation in times of crisis, and draws three implications on the deployment of cyberspace operations.

In Chapter Four, **Laura G. Brent** posits that NATO must act to counter China's ambitions to become a 'cyber superpower' by treating China as a strategic challenge and requiring improved resilience from the Allies in cooperation with the European Union. She draws attention to collective security, which she defines as 'coordinated and consensus approaches to the broad spectrum of security challenges below the threshold of armed conflict'.

In Chapter Five, **Piret Pernik** explores global drivers of change relevant to cyberspace that NATO should consider in looking at the 2030 horizon. She contends that the cyber domain is best understood as part of all-domain shaping, contesting, and fighting actions. She says that NATO should study how authoritarian opponents are likely to deploy EDTs and what their strategic thinking and tactical innovations will look like in the new decade. She closes by suggesting avenues for future research for the NATO community.

In the last chapter, **Berend Valk** illustrates how NATO has implemented cyber norms and confidence- and capability-building measures. The Alliance's role in norms-building is limited. Valk describes how NATO implements its cyber defence and the SCEPVA mechanism, and recommends integrating the latter into collective defence. He calls for starting discussions on Allied responses to cyberattacks in the grey zone.

Chapter 1

# A Strategic Outlook for Cyberspace Operations

**James A. Lewis**
Senior Vice President and Director
Strategic Technologies Program
Center for Strategic and International Studies

## Abstract

Global agreement on international cybersecurity norms in the United Nations was an important first step in increasing stability in cyberspace. However, norms alone are insufficient to achieve this. Powerful state actors seek to restructure international relations to better serve their own interests, and they have very different views of the nature of state sovereignty and the rule of law. Changing this requires a new, more active strategy. Twentieth-century strategic concepts like deterrence are no longer an adequate guide for strategy or effective in ensuring peace. The nature of military conflict has changed, given technological advances. This changes the defensive mission of NATO, which faces very capable opponents in cyberspace and raises the question of how to create accountability when a hostile state fails to observe the globally agreed norms. While most NATO members now see the benefit of imposing consequences in a way consistent with international law, they would prefer these be limited to measures that do not entail force or the threat to use force. Fears that a more forceful response could lead to escalation are exaggerated, but there is not an agreed-upon menu of proportional response options. NATO members need to create a new conceptual framework for action, developing a menu of proportional responses and then building the political consensus to use them.

**Keywords**: *accountability, norms, strategy*

# Introduction

On the 100th anniversary of the founding of the Chinese Communist Party, Xi Jinping proclaimed that the West was in irreversible decline, that China's rise to dominance was unstoppable, and that anyone who opposed it would find their 'heads bashed and bloody'.[1] A few days earlier, Vladimir Putin gave a similar speech, noting that Russia 'considers it legitimate to take symmetrical and asymmetric measures' in response to threats to Russia's traditional values (presumably autocracy, although he did not say so explicitly).[2] These statements provide the broad framing for the strategic context NATO faces in cyberspace.

NATO is on the defensive. For more than a decade, Russia and China have held the initiative, not just in cyberspace but regionally. Cyberspace is the focal point for conflict today. Much of the blame for these setback goes to the three previous American administrations. The US and its NATO allies have been preoccupied with campaigns in the Middle East, but now they must develop strategies for this new strategic conflict.

This poses difficult strategic problems. Our opponents cannot be deterred from pursuing their objectives, which is to restructure the global order to better serve their own interests while diminishing American power. There is no easy or painless solution to this challenge, and democracies have been reluctant to recognise that the international environment has become more conflictual. Relations among the great powers are no longer peaceful but confrontational. We are already in conflict with powerful authoritarian opponents, but it is not primarily a military conflict, and this complicates the development of strategies for defence.

The most pressing need for democracies today is to rethink their global strategies. Invocations of 20th-century strategic concepts like deterrence will not achieve this. Paul Kennedy, whose work on the British Empire's decline is instructive, wrote that great powers do not decline because they fail to recognise problems; they decline because they apply outdated solutions to new problems.[3] The problem is more acute for an intangible battlefield shaped by covertness.

The hardest question for reconceptualisation revolves around deterrence. NATO is a defensive organisation. It exists to deter attacks on democracies, and after a long period of struggle, it had remarkable success in the 20th century. But by either design or luck, our opponents have developed strategies that allow them to circumvent deterrence, to act coercively in pursuit of their goals while minimising the risk of retaliation. This is the core strategic problem: how does NATO defend itself in a situation of calculated aggression where the nature of conflict has changed significantly?

Armed conflict will not follow the patterns of the 20th century. New technologies have reshaped conflict in ways that make cyberspace operations increasingly important. Dramatic parallels between nuclear weapons and cyberattack are unrealistic – the former would have an incomparably greater effect than the latter. Nuclear weapons make the nations that possess them cautious about entering

1 Editorial Board, 'China's Xi Promises the World "Heads Bashed Bloody". He Should Be Taken Seriously', *Washington Post*, 5 July 2021, https://www.washingtonpost.com/opinions/2021/07/05/chinas-xi-promises-world-heads-bashed-bloody-he-should-be-taken-seriously/.

2 Russia: Putin Approves Strategy to Counter Western Influence', Deutsche Welle, 3 July 2021, https://www.dw.com/en/russia-putin-approves-strategy-to-counter-western-influence/a-58151622.

3 Paul Kennedy, *The Rise and Fall of British Naval Mastery* (Scribner, 1976).

into armed conflict against peers, so they have found new ways to coerce. Armed conflict has also been reshaped by emerging technologies and their military applications, since these allow for achieving strategic effects (e.g. effects that provide decisive advantage over an opponent) without nuclear weapons or massive, prolonged conventional action. Given the improved performance of advanced conventional weapons, even conventional war between major powers can be too damaging and too expensive to be sustained for long.

We can test this hypothesis by looking at major conflicts over the last decade. These have tended to be short and limited in scope (America's misadventures in the Middle East are not counterexamples, as these were against lightly armed irregular opponents). The Falklands War (23 days from UK landings to Argentine surrender),[4] the Yom Kippur War (10 days),[5] and the Armenia-Azerbaijan conflict (42 days)[6] are precedential. These were short, intense conflicts, often accompanied by diplomatic efforts by the international community to bring hostilities to an end. Yet in most cases, such diplomatic efforts ended only combat, not the underlying enmity.

Among military powers, precision-guided munitions (PGM), unmanned aerial vehicles (UAV), and cyberspace operations allow states to create strategic effects at long range and without using nuclear weapons. These technologies, guided by greatly improved reconnaissance and intelligence capabilities and using dynamic new forms of electronic warfare (that go beyond jamming set frequencies), will increase lethality and destructiveness.[7] A Turkish media source notes that 'the drones quickly made traditional [military] tactics useless'.[8] Future developments in hypersonic delivery vehicles and AI-enhanced weaponry (including cyberattack tools) will further expand this capacity for non-nuclear strategic effect.

The result of these changes is not that nations have renounced war; it is that they have found other ways to fight. If the effect of nuclear weapons in the Cold War was to incentivise the avoidance of conflict, cyber and new technologies have the opposite effect. The most immediately applicable of the new strategic capabilities for NATO's opponents is cyberspace operations, especially as it has expanded to include politically damaging information operations conducted over networks. If anything, the level of conflict (though not violence) between democratic and authoritarian states has increased. Inter-state conflict is focused on competition over political and economic influence, and over technological leadership, which can provide foreign policy benefits. Countering these intangible actions is much more difficult than responding to an armed incursion.

NATO and its main opponents have thus far managed to avoid direct armed clashes between each other's forces. There is, of course, the risk that one side could miscalculate, but authoritarian states have developed less provocative techniques for coercion and the exercise of force, including cyber

---

4 Imperial War Museum, 'A Short History of the Falklands War', https://www.iwm.org.uk/history/a-short-history-of-the-falklands-war.

5 Ministry of Foreign Affairs, 'The Yom Kippur War (October 1973)', https://www.mfa.gov.il/mfa/aboutisrael/history/pages/the%20yom%20kippur%20war%20-%20october%201973.aspx.

6 'Armenia-Azerbaijan: Why did Nagorno-Karabakh Spark a Conflict?' BBC, 12 November 2020, https://www.bbc.com/news/world-europe-54324772.

7 Robyn Dixon, 'Azerbaijan's Drones Owned the Battlefield in Nagorno-Karabakh – and Showed Future of Warfare', *Washington Post*, 12 November 2020, https://www.washingtonpost.com/world/europe/nagorno-karabkah-drones-azerbaijan-aremenia/2020/11/11/441bcbd2-193d-11eb-8bda-814ca56e138b_story.html; Seth Frantzman, 'Israeli Drones Used by Azerbaijan under Spotlight in New TV Report', *Jerusalem Post*, 13 March 2021, https://www.jpost.com/middle-east/israeli-drones-used-by-azerbaijan-under-spotlight-in-new-tv-report-661804.

8 'All Eyes on Turkish Drones after Azerbaijan's Victory', TRT, 5 January 2021, https://www.youtube.com/watch?v=S_X_9oWLmfU.

and cognitive warfare, the use of proxies, and territorial manoeuvres that provide advantage while controlling the risk of open warfare. These new operational modes were likely shaped by a desire to circumvent traditional deterrence by staying below the threshold of hostile action that would provoke retaliation.

The Cold War is not a useful precedent; nor are conflicts today likely to resemble the total war of the Second World War, with tanks rolling into the opponent's capital and the toppling of the opponent's government. Since neither side is likely to 'defeat' the other, major power conflict today will be interspaced with periods of inactivity and perhaps negotiation. To call this new kind of conflict a 'grey zone'[9] is misleading. It is not a grey zone; it has become one of the principal venues for hostile engagement. It does not fall between war and peace, because these old distinctions do not map well to today's circumstances and can be unhelpful.

Cyberspace operations are ideal for conflict in this new environment for several reasons, most of which are well known. Any rules governing their use can be safely ignored. Their effect is corrosive, offering the ability to damage an opponent without engaging their military forces, but the effect is not so sudden or violent as to justify retaliation. Social media technologies create new avenues for coercive affect. Covertness is required only for insertion, since increasingly, it appears that Russia and China no longer mind being caught. Cyberspace operations are best used not as a replacement for kinetic action but to create the cognitive and political effects that erode an opponent's will to resist, providing the political means for victory without defeating armies.

This competition can also, as we have seen, take the form of propaganda and influence campaigns enhanced by social media to create consequences that undercut political foundations and weaken opponent resistance. The objective is to produce a political effect using technologies and tactics that, enabled by the internet, create cognitive manipulation. Russian campaigns have been successful in expanding discontent in the West.[10] China has also begun to use these tactics.[11] These influence campaigns can be a violation of sovereignty and can be coercive, but they do not involve force. Existing international humanitarian law (with its protections for non-combatants) is not easily applied to this kind of digital conflict.

How is this different from what NATO faced in the past? The chief difference is that cyberspace operations enable both the routine violation of sovereignty, greater political effect, and a larger scope of coercive cyber and informational operations. The risks of an cyberattack on critical infrastructure or command and control are not that different from an attack using conventional weapons. This makes it easier to plan the appropriate response. The problem arises from a new and more difficult unconventional challenge, a 'continuation of politics by other means' (to use Clausewitz's phrase) using cyberspace operations.

This means that the strategic challenge for NATO is to find new ways to blend its traditional deterrence functions based on the Alliance's conventional military forces, with new strategies and coordination mechanisms for cyber action. NATO has made good progress in adapting to the risk of cyber

9 L. J. Morris et al., 'Gaining Competitive Advantage in the Gray Zone', RAND, 2019, https://www.rand.org/content/dam/rand/pubs/research_reports/RR2900/RR2942/RAND_RR2942.pdf.

10 See, for example, Heather Conley, 'The Kremlin Playbook', CSIS, October 2016, an early example of the extensive research effort on Russian information operations: https://www.csis.org/analysis/kremlin-playbook.

11 Joshua Kurlantzick, 'How China Ramped up Disinformation Efforts during the Pandemic', Council on Foreign Relations, 10 September 2020, https://www.cfr.org/in-brief/how-china-ramped-disinformation-efforts-during-pandemic.

warfare when it follows conventional formats and targets (e.g. an attack on critical infrastructure, but using cyber- rather than kinetic attacks). The recent agreement on ransomware that targets critical infrastructure is a further step in this direction. But if war is a continuation of politics by other means, cyberspace operations provide a new way to produce political effects, and our strategies will need to adapt. Effective cyber defence requires more than making it more difficult for opponents to penetrate networks, disrupt services, or exfiltrate data. Hardening targets is not enough. Our opponents are persistent, well-resourced, and determined. We cannot expect to defeat them, but must instead change their calculations of benefits and risks if the number of cyber incidents is to decrease NATO's ability to send a collective message of resistance and a credible threat of response may be one of its most valuable assets in this new conflict. A new cyber strategy must be embedded in NATO's larger approach to China and Russia, and NATO's actions must support the larger objective of creating an uneasy stability in its relations with Russia and China, rather than being simply reactive.

# What Risks Does NATO Face?

If the malicious cyber actions fall outside the conventional definitions of the use of force or an armed attack, they complicate the politics of deciding on a response. If Russian cyberspace operations were part of a larger conventional attack, the targets would include NATO's command-and-control networks, advanced weaponry held by member states, and perhaps critical infrastructure, if the Russians calculated that disrupting or destroying it would improve their chances of success.

While it is in the Russian interest to probe these network and digital targets and perhaps pre-position cyber tools for later use, an actual attack on these targets is unlikely outside of armed conflict between NATO and Russia. Cyberspace operations are likely to remain below this threshold, as they provide political and perhaps military advantage at low risk. There are opportunities for use outside of larger hostilities, but each opportunity comes with different degrees of risk and potential advantage.

Russia could disrupt services provided by critical infrastructure (as it did in Ukraine with electricity), but it could not hope to do this covertly. This makes attacks on critical infrastructure risky for Russia, an extreme step only to be taken at the onset of a larger conflict. Russia could disrupt digital infrastructure, and the denial-of-service attacks against Estonia was an early (and primitive) example of this. Again, covertness would be difficult to maintain. As NATO makes progress in refining the applicability of Article 5 for cyberattack,[12] an opponent attack on digital infrastructure using cyber means could potentially become as risky as kinetic actions or damage to or disruption of critical infrastructure.

Russia can continue to exploit its ability to access NATO networks and infiltrate state and private networks for intelligence purposes. Espionage is generally accepted as a legitimate (if hostile) act by sovereign states, and Russia faces no immediate penalty for continuing to engage in it. Russia can continue its campaign of political interference using cyber means. The effect should not be overstated, but it has been enough (and the risks to Russia for undertaking such actions so low) that Russia has no incentive to stop. The public discontent in democracies that provides Russia with the ammunition for its disinformation derives from domestic political issues in member states and falls

12 Libby Cathey, 'How NATO Is Updating Its Common Defense Pact to Deal with Global Cyberattacks', 14 June 2021, ABC News, https://abcnews.go.com/Politics/nato-updating-common-defense-pact-deal-global-cyberattacks/story?id=78271735.

largely outside NATO's purview.

Cyberspace operations make it easy for China to reach Europe and the United States for coercive and strategic effect while preserving a degree of deniability. China will accompany aggressive cyber espionage campaigns with forays by its naval forces into the margins of NATO's sphere of interest. Where possible (as in Djibouti[13]), China will establish a military presence, but its primary mode of operation will be political, seeking to use its economic power to recruit European nations as supporters.

If this assessment is correct, it points to a Russian strategy of preparing for highly disruptive cyber actions in the event of conflict and continuing espionage, political actions, and low-level disruption in the meantime. The wider conflict may never arrive; Russia's internal problems could be an obstacle to escalation, and it may feel its preparatory actions are sufficient to achieve its political goals, but NATO's planning should anticipate more aggressive and disruptive cyber actions from Russia. By contrast, China will pursue a steady course of increasing economic, informational, and cyber pressure on NATO nations (given that, for domestic political reasons, China may take steps that lead to armed conflict with the US, Japan and others over Taiwan). Although the strategic objectives for China and Iran differ somewhat, the same constraints apply to them (although Iran may have a higher tolerance for risk than China). Despite differences in intent and operations, the same response can be applied to these three opponents.

# Element of a Response

Precedent suggests that authoritarian opponents are opportunistic. They may have been surprised at their success and the lack of a response. Similarly, if they encounter resistance or perceive unacceptable risk in continued action, they will adjust their strategies. This is where NATO has an opportunity to reduce risk if it can develop appropriate responses to coercive cyber action.

There are three sets of actions NATO can take to improve its cyber defences and prevent attacks on its members. First, NATO should persuade its opponents that they cannot expect to be covert in their operations. Surprise is easy in cyberspace, but covertness is difficult. Two NATO members (the US and the UK) have exceptional capabilities to attribute the source of a cyber action, and several other members have strong and improving attribution capabilities. The goal for attribution is to persuade opponents that covertness is not just difficult but impossible. This will shape their assessment of risk as they consider coercive actions.

Deception is a normal part of warfare and honesty not always the best policy. NATO does not need perfect attribution capabilities; it merely needs to persuade its opponents that it has perfect capabilities. Both Russia and China already overestimate some NATO members' ability to attribute the source of an attack. Persuading them of the difficulty of covertness raises the risk of cyber action for them and decreases the likelihood of opponent action.

Second, NATO needs to develop a menu of proportional responses to malicious cyber actions. This

13 Sam LaGrone, 'AFRICOM: Chinese Naval Base in Africa Set to Support Aircraft Carriers', U.S. Naval Institute, 20 April 2021, https://news.usni.org/2021/04/20/africom-chinese-naval-base-in-africa-set-to-support-aircraft-carriers.

is not a linear process. It is not apparent, for example, what would constitute a proportional response to electoral interference – interfering in Russian and Chinese elections, for example, would be pointless as outcomes are pre-ordained. Proportionality is much clearer in the physical domain, and work could usefully begin to explore how to create similar clarity in the cyber domain. Developing this response menu would give more credibility to NATO's cyber defence. Making clear that the response to a malicious cyber action need not be confined to cyberspace, as Secretary General Stoltenberg did recently,[14] is a valuable step that can be expanded. In applying such responses, however, responses should draw upon the full range of diplomatic, economic and coercive actions available to states. Of course, no options from this menu can be implemented automatically; any action will require discussion in the North Atlantic Council.

Third, NATO needs to demonstrate that it and its members will be resilient in the event of an attack. Resilience means continuing to operate despite a successful attack. There has been much useful discussion of the benefits of resilience in changing opponents' calculations of risk and benefit. NATO has done good work in hardening its command-and-control networks, and member states have also made some progress in improving their cybersecurity. Political resilience is a more difficult topic, since it falls outside the scope of military defence, but it is necessary for member states to be aware of this as a vulnerability.

This combination of attribution, response and resilience is best not described as deterrence. Deterrence is a Cold War concept in need reassessment. This is not the place for an extended critique of Cold War strategic thinking, but the pursuit of deterrence is a handicap in the new domain of conflict. Russia and China have continued to use cyberspace operations against NATO and its members while disregarding NATO's deterrent effort. NATO's new strategy should attempt to shape and limit such attacks, and unlike traditional deterrence, which implies a degree of passivity, any member state will need to consider the use of its own intrusive cyber actions against opponents and their possible coordination within NATO.

This is an important question to consider as NATO further develops policies for collective cyber defence and determines the responsibilities of the Alliance. In September 2019, in a joint statement on advancing responsible state behaviour in cyberspace, 28 nations agreed to 'work together on a voluntary basis to hold states accountable when they *act contrary to* this framework, including by taking measures that are transparent and consistent with international law'.[15]

Other Cold War concepts deserving examination include escalation and miscalculation. These concepts are not useful guides to policy. Escalation and miscalculation in the cyber context remain hypothetical constructs: there are no examples of either having occurred despite the high level of malicious action in cyberspace.[16] These risks can be managed through diplomatic action and engagement with adversaries.

It could be argued that retaliatory action is best left to NATO member states acting on their own.

---

14 'NATO: Cyber-Attacks "As Serious as Any Other Attacks" to Allies', BBC, 15 June 2021, https://www.bbc.com/news/av/world-57478561.

15 U.S. Department of State, 'Joint Statement on Advancing Responsible State Behavior in Cyberspace', 23 September 2019, https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/.

16 'Russian Military Was behind NotPetya Cyberattack', *Washington Post*, 12 January 2018, https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html.

Alternatively, it could be argued that retaliatory actions could be used by opponents to justify their own actions or set unfortunate precedents. Counsels of caution are one reason we find ourselves in the current situation, since they are essentially an argument for inaction and are perceived by opponents as a green light. Our opponents are already taking action. They will not stop if we exercise self-restraint. Our goal is to shape and constrain their actions, building on NATO's success in the conventional sphere. This will require creating a new conceptual framework for action, developing a menu of proportional responses, and then building the political consensus to use them. These tasks will strain the Alliance, but it is making progress in developing a cyber defence policy for this century. These are delicate times as we have entered a new era of conflict, but collective defence remains the best tool to protect democracy by countering Chinese and Russian aggression in cyberspace.

Chapter 2

# Situational Cyber Stability and the Future of Escalating Cyber Conflict

**Jason Healey**
Senior Research Scholar
School of International and Public Affairs
Columbia University

**Virpratap Vikram Singh**
Research and Program Coordinator
School of International and Public Affairs
Columbia University

## Abstract

This paper builds on the concept of situational cyber stability by tackling the underlying context that creates geopolitical and cyber tensions which allow for the use of one of the four stabilising and destabilising mechanisms identified by Healey and Jervis. Using a 2x2 matrix of high and low geopolitical and cyber tensions, we explore the likelihood of cyber conflict escalating into a kinetic conflict, an observation that is made pertinent by the growing ineffectiveness of stabilising pressure-release cyber actions. This paper examines prevailing trends of increasing geopolitical friction, an intensification of cyber actions, and the dependence on technology. We argue that there is an increased likelihood of cyber incidents commencing within a context of high tensions, creating a tinderbox for escalating cyber conflict.

**Keywords**: *escalation, cyber intensification, situational cyber stability, cyber conflict*

# Introduction[1]

The stabilising or destabilising effect of offensive cyber operations cannot be determined without the context of the underlying state of geopolitical and cyber tensions between states. Yet the amplifying or dampening role of such pre-existing tensions has often been overlooked in international relations and practitioner literature, even though it is not unique to cyber conflict (since, for example, large military exercises or naval deployments take on a more ominous character when rivals' blood is up).

This article builds on earlier work by Jason Healey and Robert Jervis on 'situational cyber stability'. That work proposed four mechanisms of escalation, depending on geopolitical circumstances, but was unable to delve deeper into how changes in geopolitical or cyber tensions might affect the escalatory risk caused by offensive cyberspace operations and how this could change over time.[2]

Accordingly, this paper uses the four mechanisms to examine the escalatory effects of cyber conflict in four situations, forming a 2x2 matrix of high and low geopolitical tension (the overall relations between rivals) and cyber tension (relations specifically within cyberspace). Looking towards 2030 and beyond, it then discusses three prevailing trends: an increase in geopolitical friction, the intensification of cyber conflicts, and dependence on technology. These trendlines are used to explain the anticipated ratcheting intensification of cyber conflict, as well as a set of potentially stabilising tools to forego these effects.

# Situational Cyber Stability

Though cyber conflict has intensified over the last three decades,[3] with especially intense cyber incidents in the last few years (such as NotPetya,[4] SolarWinds,[5] and Colonial Pipeline[6]), no incidents or campaigns have escalated into a larger kinetic conflict. The cyber fight has stayed in cyberspace. This evidence supports the scholarly assessment that cyberspace operations can be non-escalatory, providing a stabilising release of pressure.[7]

But this is, at best, half of the story. Almost the entirety of cyber conflict has happened since the end

---

1 This paper was submitted for publication in December 2021, before Russia's invasion of Ukraine in February 2022.

2 Jason Healey and Robert Jervis, 'The Escalation Inversion and Other Oddities of Situational Cyber Stability', Texas National Security Review 3, no. 4 (2020).

3 Jason Healey and Robert Jervis, 'How to Reverse Three Decades of Escalating Cyber Conflict', Atlantic Council, 24 March 2021, https://www.atlanticcouncil.org/blogs/new-atlanticist/how-to-reverse-three-decades-of-escalating-cyber-conflict/.

4 Ellen Nakashima, 'Russian Military Was behind "NotPetya" Cyberattack in Ukraine, CIA Concludes', Washington Post, 12 January 2018, https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html.

5 Christopher Bing, Joseph Menn, Raphael Satter, and Jack Stubbs, '"Powerful Tradecraft": How Foreign Cyber-Spies Compromised America', Reuters, 19 December 2020, https://www.reuters.com/article/us-global-cyber-usa-insight-idUSKBN28T0XV.

6 Christopher Bing and Stephanie Kelly, 'Cyber Attack Shuts down U.S. Fuel Pipeline "Jugular", Biden Briefed', Reuters, 8 May 2021, https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/.

7 Brandon Valeriano, Benjamin Jensen, and Ryan C. Maness, Cyber Strategy: The Evolving Character of Power and Coercion (New York: Oxford University Press, 2020); Joshua Rovner, 'Cyber War as an Intelligence Contest', War on the Rocks, 16 September 2019, https://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest/.

of the Cold War, a time of relative peace and geopolitical stability which has seen relative restraint between major powers. It is, therefore, no wonder that even substantial cyber disruptions have not been enough to tempt states into a larger conflict with a nuclear-capable rival. However, the growing risk of conflict between major powers - after Russia's second invasion of Ukraine - means that states may be more willing to throw even harder punches and less likely to turn the other cheek.

Healey and Jervis accordingly tackle the question, 'under what conditions are cyber capabilities escalatory?' Healey and Jervis outlined four major mechanisms of cyber stability – one stabilising mechanism and three destabilising mechanisms – that can lead to a larger conflict, depending on the geopolitical context.[8]

## Stabilising Mechanism

→ **Pressure Release:** In periods of relative peace and stability, cyber actions have provided decision-makers with a non-threatening, non-kinetic option. In this context, cyber actions have created negative feedback for conflict, providing an off-ramp for great powers and geopolitical rivals.

## Destabilising Mechanisms

In each case, the contested parties no longer see cyberspace operations through the lens of an intelligence contest or pressure release.

→ **Spark:** 'As cyberspace becomes increasingly existential for economies and societies, states compete more aggressively over the same cyber terrain and treasure. In such circumstances, cyber capabilities add positive feedback, intensifying conflict within cyberspace.'[9]

→ **Pull out the Big Guns:** When acute geopolitical crises are more prevalent, states will be less willing to abide by the tacit agreements of peacetime. Growing geopolitical stakes can translate to more risk-seeking, including the more provocative use of cyber capabilities. Rivals targeted by these freshly aggressive attacks, in the midst of a crisis, will feel even less restraint towards using harsh, possibly kinetic, responses.

→ **Escalation Inversion:** If states suspect war is increasingly possible, they may believe their best (or indeed, only) chance of success is a surprise, large-scale cyber offensive, if only to 'keep the victim reeling when his plans dictate he should be reacting'[10] in the early stages of a conflict. 'Cyber capabilities may be to World War III as mobilisation timelines were to World War I.'[11]

The mechanisms outlined by Healey and Jervis provide a starting point from which to understand how prevailing changes in geopolitical or cyber tensions over time are more likely to trigger larger conflicts.

8 Healey and Jervis, 'The Escalation Inversion'.

9 Ibid.

10 Richard K. Betts, Surprise Attack: Lessons for Defense Planning (Washington, DC: Brookings Institution, 2010), 5.

11 Healey and Jervis, 'The Escalation Inversion'.

# Conditional Escalation

A simple 2x2 matrix contrasts differing escalatory dynamics of high and low geopolitical and cyber tensions.

## Understanding 'Tensions'

In this paper, the term 'geopolitical tension' is shorthand for an existing state of stress or crisis. States in circumstances of low geopolitical tension are generally at peace with their neighbours; any rivalries are not acute and can be expected to be resolved diplomatically. States in circumstances of high geopolitical tension are in a crisis or pre-crisis with a rival and might expect economic trade restrictions and sanctions, election and political interference, military actions and border disputes, or the like. This variable is generally dyadic (as with the low tension between France and Germany or the high tension between Armenia and Azerbaijan). As with cyber tension, this is a very fuzzy metric only meant to be used as a relative guide. Further work might more clearly define the terms and find more precise metrics (such as a tracking metric of tension, perhaps by a political-risk consultancy).

Cyber tensions are the simply the subset of geopolitical tensions dealing with cyberspace, mostly but not entirely cyber conflict (such as cybercrime, disruptions, and espionage). States in circumstances of low cyber tensions perceive little danger. While they may suffer or initiate relatively minor cyber incidents, no wrath results; the incidents are written off as nuisances or part of an 'intelligence contest'.[12] States in circumstances of high cyber tension feel the fangs of existential crises around them. This can be a dyadic variable: for instance, the United States blames Russia for harbouring cyber criminals, conducting norm-breaking and reckless operations, and bullying neighbours, while Russia fears US-based information that might undermine regime stability and cause a new 'colour revolution'. However, high or low cyber tensions may also be an environmental variable, affecting all or most states. This might be driven by ubiquitous cybercrime, widespread vulnerabilities and failures, or perceptions of a global arms race and lack of restraint.

The degree of historical rivalry and tension between states naturally dampens or amplifies perceptions of tension. A non-rival caught in an audacious act of cyber espionage will likely have less impact than a strategic competitor caught in the same act. If, for example, Pegasus spyware was produced by a Chinese company and not the Israeli NSO group, the US reaction would likely have been even more pronounced.[13]

## Cyber Escalation and Global Tension

Table 1 displays which of the four Healey-Jervis escalation mechanisms are active in each quadrant of the tension 2x2 matrix. The sole stabilising mechanism, 'Pressure Release', is likely only operative

12 Rovner describes the five elements of intelligence contest as: 1) a race among adversaries to collect more and better information, 2) a race to exploit that information to improve one's relative position, 3) a reciprocal effort to covertly undermine adversary morale, institutions, and alliances, 4) a contest to disable adversary capabilities through sabotage, and 5) a campaign to preposition assets for intelligence collection in the event of a conflict.

13 Joseph Menn and Joel Schectman, 'U.S. Lawmakers Call for Sanctions against Israel's NSO, Other Spyware Firms', Reuters, 15 December 2021, https://www.reuters.com/world/us/exclusive-us-lawmakers-call-sanctions-against-israels-nso-other-spyware-firms-2021-12-15/.

in low geopolitical tension (Quadrants 2 and 3). Destabilising mechanisms are more likely during high tension: 'Spark' in high cyber tension (Quadrants 1 and 2) and 'Pull Out the Big Guns' and 'Escalation Inversion' in high geopolitical tension (Quadrants 1 and 4).

**Table 1:** Escalation Mechanisms in Times of Tension

| | **Low Geopolitical Tension** | | **High Geopolitical Tension** | |
|---|---|---|---|---|
| **High Cyber Tension** | Q2 | Spark, Pressure Release | Q1 | Spark, Escalation Inversion, Pull out the Big Guns |
| **Low Cyber Tension** | Q3 | Pressure Release | Q4 | Pull out the Big Guns, Escalation Inversion |

Quadrant 3 (low,low) is the safest, as all sorts of compensating mechanisms dampen the escalatory impact of cyberspace operations. Policymakers simply have little reason to respond forcefully. Cyber operations would have to be especially aggressive or unprecedented to cause more than a medium-term blip in relations, as happened with the revelations by Edward Snowden about US espionage, which tangled US-European relations but did not lead to escalation.[14]

Quadrant 1 (high,high) is the most dangerous quadrant, more at risk of cyberspace operations into war as rivals are starting from high,high. It is not a certainty, of course, but it does create a challenge for diplomacy and decision-making, which may only have hours to succeed rather than days or weeks.

The rest of this section will explore each quadrant in turn.

1. **Pressure Release:** This mechanism is characterised by negative feedback damping down instability, when states on both sides are either at relative peace or want to limit escalation. The best example is President Trump's 2019 decision to forgo punitive airstrikes on Iran in lieu of disruptive cyberattacks.

   In Quadrant 3 (low,low), even quite substantial attacks can be brushed aside. Cyber capabilities, seen as a less-threatening, non-kinetic mechanism, can stop brewing crises, keeping states in Quadrant 3.

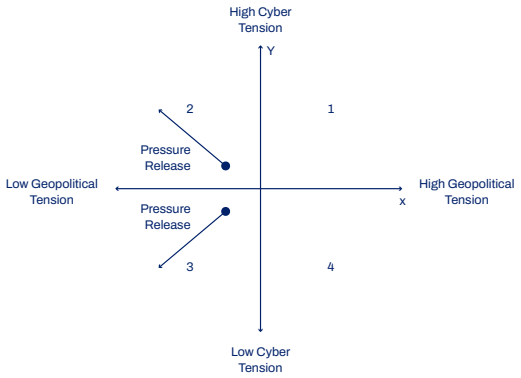



**Figure 1:** Pressure Release

   In Quadrant 2 (low,high), states might use cyber capabilities to reduce geopolitical tension, but

14 European Union Center of North Carolina, 'The NSA Leaks and Transatlantic Relations', 2014, https://europe.unc.edu/wp-content/uploads/sites/314/2016/11/Brief_NSA_Leaks_Transatlantic_Relations_2014.pdf.

this can exacerbate cyber tension, moving higher on the Y axis on Figure 1. For example, the United States and Israel disrupted Iranian nuclear enrichment with a covert, offensive cyber capability, only to have Iran conduct its own disruptive cyber operations in response.

The feature of the Pressure Release mechanism is largely determined by a desire to retain a status quo of peace and stability, or at least to avoid an all-out conflict.

2. **Spark:** This destabilising mechanism is characterised by the struggle faced by nations to exert dominance in cyberspace. As cyber conflict is fought over increasingly existential issues (i.e. pipelines), states may choose to further escalate rather than treat them as a relatively inoffensive pressure release. Stuxnet, the destructive 2010 cyberattack, served as a destabilising mechanism that pushed Iran to commit resources towards its cyber capabilities to become a 'force to be reckoned with'.[15]

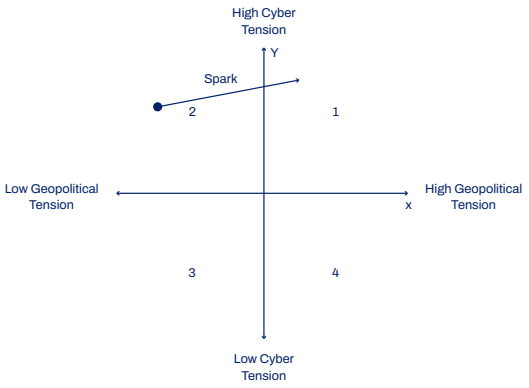



**Figure 2:** Spark

States in Quadrant 2 (low,high) may be more likely to lean into the fight, akin to spiral escalation, and invest in resources and policies to improve their cyber capabilities. Potential adversaries may then feel a need to respond, which pushes parties into Quadrant 1 (high,high).

States in Quadrant 1 (high,high) may perceive any fresh cyber campaign by a rival (or some mischief-maker posing as a rival) as a surprise military attack, even if the campaign is similar to those that have acted as pressure releases in the past or is a proportional response to their own operations. Especially states lacking advanced defensive capabilities – such as India and Pakistan or Azerbaijan and Armenia – may not have the time or inclination to wait for better attribution or attack assessment and may feel the need to respond with their own counteroffensive.

The next two destabilising mechanisms, 'pulling out the big guns' and 'escalation inversion', remain theoretical possibilities. This is largely, Healey and Jervis argue, because cyber competitions have been occurring during a time of relative peace and stability between major powers, a trend that appears to be shifting in a dangerous direction.

3. **Pulling out the Big Guns:** As crises become more frequent, such as under great power competition, states are more willing to take risks, including more provocative cyber operations. For example, since the annexation of Crimea, Russia has been far more willing to undertake extreme and reckless cyber operations, especially against Ukraine, though not so much as to

15 Andrea Shalal-Esa, 'Iran Strengthened Cyber Capabilities after Stuxnet: U.S. General', Reuters, 17 January 2013, https://www.reuters.com/article/us-iran-usa-cyber-idUSBRE90G1C420130118.

spark a larger war.

States in Quadrant 4 (high,low) use their stockpiled cyber capabilities to match the perceived dangers of the geopolitical crisis. This abandonment of past restraint (perceived or actual) can push parties towards Quadrant 1 (high,high) as the geopolitical tension invites cyber tension.

(Figure 4:) When applied to Quadrant 1 (high,high), there is no longer a desire to avoid escalation, and when coupled with a decay of geopolitical stability, this can create worsening cyber competition.

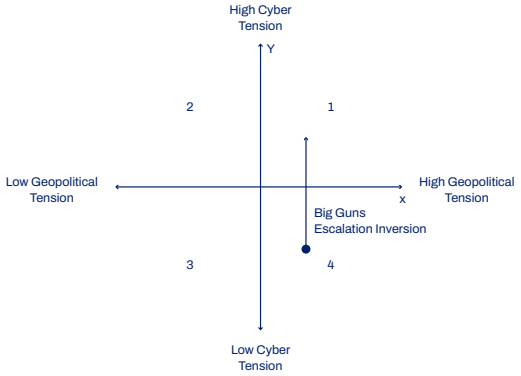



**Figure 3:** Big Guns & Escalation Inversion in low cyber tension

4. **Escalation Inversion:** This destabilising mechanism occurs when an intensifying crisis, with states in Quadrant 1 (high,high), tempts states to utilise cyberattacks in an effort to gain a first-mover advantage with substantial intelligence and the disruptive use of cyber capabilities against an adversary. Regardless of whether a perception of impending conflict is shared by both sides, such cyber first strikes are likely to be destabilising.

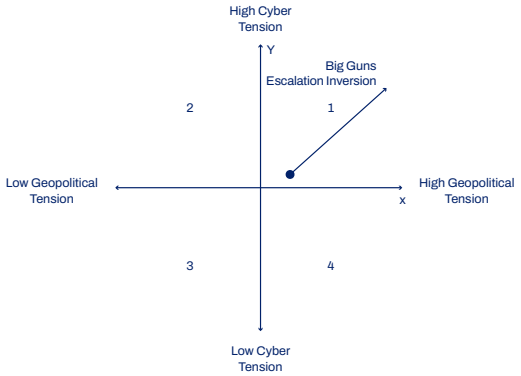



**Figure 4:** Big Guns & Escalation Inversion in high cyber tension

(Figure 3:) For states in in Quadrant 4 (high,low), the cyberspace operations occur in the absence of prior cyber tension. Perhaps regardless of the success of the operation, the cyber potshot pulls parties towards Quadrant 1 (high,high) unless the target's leadership is willing to shrug off a pre-emptive cyberattack.

# Trends towards Increasing Tension

It is likely the case that cyber conflict has been an intelligence contest and that offensive cyberspace operations act as a pressure release that has not escalated into warfare. However, these findings, being empirical, only inform on what has happened and not what might happen if the future looks mostly like the past. Many such assessments ignore changes to underlying assumptions that contribute to ongoing trends in geopolitical and cyber tensions. Unfortunately, three trends suggest increased tensions, making those assumptions exceedingly suspect.

## Increasing Geopolitical Friction

Cyber competition grew and developed in a period of relative peace and stability, owing to the relative restraint of post-Cold War adversaries. As Healey and Snyder explain: 'The desire to avoid escalation, and cyber-as-pressure-release, may not be inherent to cyber competition but merely be an inherited characteristic from the global balance of power during the entire period under consideration.'[16]

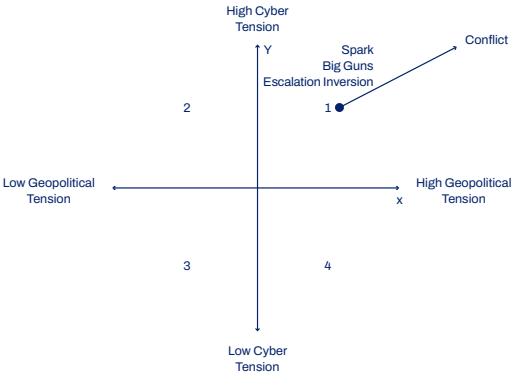



**Figure 5:** Jump to Conflict

Unfortunately for the trends between 2021 and 2030, the trendline for geopolitical tension for many states is rising into Quadrants 1 and 4 in Figure 5. This is clear from the growing reality of 'great power competition', from a rising China seeking to shape the world order to a risk-seeking Russia happy to destabilise its neighbours and perceived rivals. The breakdown of the international liberal order and a breakdown in global governance could expand this to all states, not just great powers.

By 2030, substantial crises are likely to increase geopolitical tension: the climate crisis, the Covid-19 pandemic, the continued migration of refugees from conflicts and economic inequality, and domestic extremist movements within democracies will all contribute to this friction.[17] The breakdown of the international liberal order and deterioration in global governance means there are fewer ways to manage these crises and counterbalance increased geopolitical tensions.

## Intensification of Cyber Conflicts

Tension is also growing in cyberspace, pushing towards Quadrants 1 and 2: whether gauged by the size and magnitude of incidents, the perception of participants, or the operational size and technical sophistication of committed military and intelligence forces, there has been a relentless intensification of cyber activities as nations build their organisations and employ them in more frequent and more dangerous incidents.[18]

With major campaigns and vulnerabilities like SolarWinds, the Microsoft Exchange campaign by Hafnium,[19] and ransomware attacks on gas pipelines and other US critical infrastructure,[20] there is little evidence of any change to this decades-long trend, which could easily continue into the 2020s

16 Jason Healey and Jack Snyder, 'Strategic Equilibrium and Persistent Engagement in Cyberspace', draft paper, June 2020.

17 Mathew Burrows, 'Global Risks 2035 Update: Decline or New Renaissance?' Atlantic Council, 30 October 2019, https://www.atlanticcouncil.org/in-depth-research-reports/report/global-risks-2035-update/.

18 Healey and Jervis, 'How to Reverse Three Decades of Escalating Cyber Conflict'.

19 Patrick Howell O'Neill, 'How China's Attack on Microsoft Escalated into a Reckless Hacking Spree', MIT Technology Review, 10 March 2021, https://www.technologyreview.com/2021/03/10/1020596/how-chinas-attack-on-microsoft-escalated-into-a-reckless-hacking-spree/.

20 Lily Hay Newman, 'Ransomware Hits a Food Supply Giant – and Underscores a Dire Threat', Wired, 1 June 2021, https://www.wired.com/story/jbs-ransomware-attack-underscores-dire-threat/.

and well into 2030.

If cyberspace operations follow a normal distribution, as simplified in Figure 6 (with the number of incidents on the y-axis and impact on the x-axis), then intensification of cyber conflict shifts the mean well to the right. Severe incidents, which had been quite rare in a slender right tail, are now closer to the mean, which is a far higher severity. The most severe incidents, on that slender tail, are now orders of magnitude worse than those that came before.

This worrying assessment aligns with the observation that the problems 'faced in 2008 seem minor compared to today and the organisations seem small and limited, while the cyber incidents from 1998 and 1988 seem trivial. Operations considered risky twenty years ago are now routine.'[21]

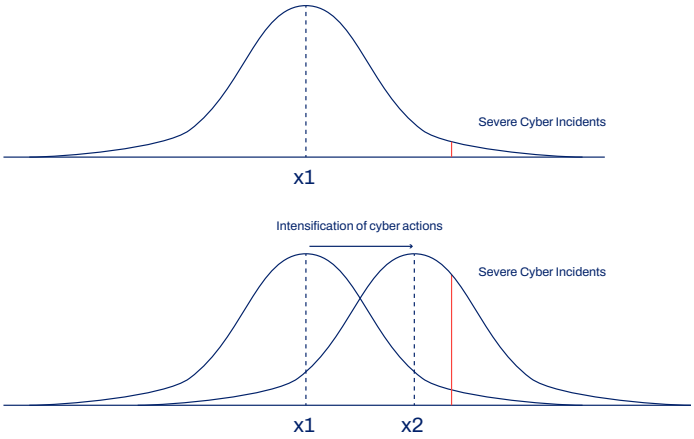



**Figure 6:** Intensification of Cyber Events

A number of other developments may accelerate this trend:

→ Improvements to AI and machine-learning technologies which might improve the efficiency and effectiveness of offensive cyberspace operations more than defence;[22]
→ The arrival of quantum computing to unravel conventional encryption protection;
→ The continued lack of regulation around cryptocurrency, allowing further monetisation of cyberattacks at Internet scale;
→ Continued increase in the number of states with offensive cyber capabilities and commands;
→ Failure to reaffirm or enforce internationally agreed cybersecurity norms.[23]

## Dependence on Technology

The rapid deployment of insecure industrial control systems (ICS) and Internet-of-Things (IoT) devices, in particular, increase the societal damage by any particular adversary while decreasing the level of sophistication any particular adversary needs in order to have a substantial effect. As Healey wrote in 2013, 'Cyber incidents have tended to be either widespread but fleeting, or persistent but

21 Healey and Jervis, 'How to Reverse Three Decades of Escalating Cyber Conflict'.
22 Burrows, 'Global Risks 2035 Update'.
23 Josh Gold, 'Unexpectedly, All UN Countries Agreed on a Cybersecurity Report. So What?' Council on Foreign Relations, 18 March 2021, https://www.cfr.org/blog/unexpectedly-all-un-countries-agreed-cybersecurity-report-so-what.

narrowly focused', because attacks only generally destroy things made of bits and bytes or silicon.[24]

With the growth of ICS and IoT, such attacks can disrupt things made of concrete and steel, and year after year, more adversaries have the capability to do so.[25] These less-capable adversaries are less likely to be able to understand the damage their attacks are doing, making it more likely they will cascade messily into an incident to which a targeted state must respond, especially if cyber or geopolitical tensions are already high.

As such, this trend does not itself push tensions more towards Quadrant 1 (high,high) but is an exacerbating factor that makes such intensification more likely.

## Tying Trends to Escalation

Increasing geopolitical and cyber tensions make it likely that more and more cyber incidents commence in Quadrant 1 (high,high), where offensive cyberspace operations are more likely to escalate to outright armed attack. These forces hinder efforts to remove tension. Modest incidents become more severe over time. Severe events are more likely to get out of hand.

Healey and Jervis described aggression as ratcheting up the overall nature of cyber conflict, building towards a precipice from which de-escalation becomes increasingly harder. Figure 7 illustrates this occurrence by highlighting that even if two parties have a dynamic that is within Quadrant 3 (A1), a cyber incident (S1) can shift tensions to a new point (X1). If the affected party opts to utilise their cyber capabilities to apply a Pressure Release action (S2) it can shift tensions to a lower point of stability (A2) within Quadrant 3. This new point of stability (A2) may remain consistent for a time, until a future cyber incident occurs (S3), shifting tensions to an even higher point (X2), with the cycle repeating until tensions break into Quadrant 1, where overall tensions are high. In such a position, and due to prevailing trends contributing to heightened tensions, future Pressure Release actions may no longer be viable or seen as effective in relieving tensions – especially as states view previous incidents as a reason to improve their own capabilities (as outlined by Spark), or begin to view cyberspace operations as provocative (as outlined by Big Guns and Escalation Inversion.)

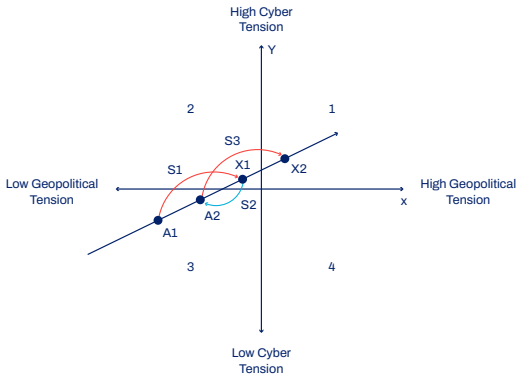



**Figure 7:** Ratcheting of Cyber Tensions

24 Jason Healey, A Fierce Domain: Conflict in Cyberspace, 1986 to 2012 (Cyber Conflict Studies Association, 2013), 21.

25 Vitali Vitaliev, 'Interview with Jason Healey'. Engineering and Technology, 16 December 2013, https://eandt.theiet.org/content/articles/2013/12/interview-with-jason-healey/.

# Potential Stabilising Options

There are a number of events that could blunt the intensification of cyber conflict and inevitable shift towards Quadrant 1:

→ **Increased global governance:** Reinvigoration of global governance – such as through the United Nations, the G-7, the G-8, and the G-20 – and bilateral trust and agreements could slow, reverse, or mitigate growing geopolitical tension.

→ **Comity between great powers:** A Sino-American rapprochement seems unlikely anytime soon but has happened before. Likewise, a post-Putin Russia might be more willing to step back from confrontation with the West, reducing geopolitical tensions.

→ **International cooperation towards peace in cyberspace:** Respect for the cyber norms agreed to in two separate UN processes, as well as those created in other forums, could reduce cyber tension by reducing the number of, and impact of, the most extreme and brazen events.[26]

→ **Splintering the Internet:** It has long been US policy to have an Internet that is 'open, interoperable, secure, and reliable'. However, it may no longer be possible to achieve the other goals while keeping it open.[27] Harder virtual boundaries might make the Internet more defensible, making it less likely that cyberspace operations will increase tensions.

→ **Revolutionary cyber defence innovations:** Defenders have long been outpaced by attackers.[28] It is possible that future innovations in policy, operations, or technology could substantially improve defences across the entire Internet, which could decrease tensions and reduce the chances that offensive capabilities will appear as an existential threat.

→ **Involvement of the private sector:** A select group of cybersecurity and technology companies have unique cyber defence capabilities that outstrip even those of the United States and other top-tier cyber powers. These companies might further strengthen their capabilities to reduce cyber tensions.

# Further Research

Building on Healey and Jervis's four mechanisms of situational cyber stability, this paper has sought to expand the contextual landscape in which these mechanisms will come into play. With trends

26 Michael Schmitt, Steven Katz, Richard Goldstone, Jameel Jaffer, Ryan Goodman, Rebecca Barber, Justin Hendrix et al., 'The Sixth United Nations GGE and International Law in Cyberspace', Just Security, 10 June 2021, https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/; Gold, 'Unexpectedly, All UN Countries Agreed on a Cybersecurity Report'.

27 White House, 'International Strategy for Cyberspace', May 2011, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

28 New York Cyber Task Force, 'Building a Defensible Cyberspace', Columbia University, School of International and Public Affairs, 2017, https://www.sipa.columbia.edu/ideas-lab/techpolicy/building-defensible-cyberspace.

pointing towards increased geopolitical and cyber tensions, it is critical to better understand the impacts on stability and escalation and question the underlying assumptions of academic theories and government strategies.

More work needs to be done to better understand situational cyber stability. States have found themselves in Quadrant 1 (high,high) yet have managed to find off-ramps to avoid conflict. Applying situational cyber stability to existing academic and policy work on off-ramps will yield important insights. Second, there is also a role for political psychology, as 'tension' and 'escalation' are in the minds of the beholder, and little has been done to apply these concepts to cyber escalation. Third, as noted above, this paper has not fully developed the concepts of geopolitical and cyber 'tension', which can be better defined and perhaps tied to existing proxy measures, such as those possibly developed by political risk consultancies.

Lastly, this paper suggested some ways tension and escalation apply not just to the major cyber powers but also to others, not least regional rivals like India and Pakistan, Armenia and Azerbaijan, China and Taiwan, and Russia and Ukraine. Many of the existing theories seem to anchor their analysis in assumptions that the United States is one of the parties to the conflict. Especially as increasingly dangerous capabilities are available to more and more states, more research needs to focus on these regional conflicts.

Chapter 3

# Do Joint All-Domain Operations Increase Cyber Vulnerabilities in Nuclear Command, Control, and Communications Systems within the NATO Alliance?

**Franz-Stefan Gady**
Research Fellow for Cyber, Space and Future Conflict
Institute for International Strategic Studies

## Abstract

The Joint All-Domain Operations (JADO) concept, mandating the integration of capabilities and synchronisation of operations and fires across all warfighting domains, is to be integrated into NATO operational doctrine in the coming months and years. Likely to be underpinned by the Joint All-Domain Command and Control (JADC2) system(s) linking 'sensors to shooters' from across the various armed services of NATO member states, the JADO concept will probably lead to the deeper entanglement of conventional and nuclear command, control, and communications (NC3) systems within the Alliance. This may result in a significant proliferation of real or perceived cybersecurity risks to NC3 systems, thus increasing the possibility of leadership miscalculation in times of crisis. As a result, JADO is liable to bring about changes in crisis dynamics that impact leadership behaviour in multiple ways, including: (1) increasing reluctance among policymakers and military commanders to order attacks against conventional C2 targets for fear of escalation; (2) raising the appeal of cyberattacks against the civilian critical information infrastructure of nuclear states in lieu of conventional military C2 systems; and (3) raising the appeal of the utilisation operations in cyberspace principally for cyber espionage, information operations, and the targeting of specific weapon systems and platforms.

# Introduction

NATO is in the process of adopting a new warfighting capstone concept based on Joint All-Domain Operations (JADO).[1] This brief discussion paper explores the degree to which JADO and the corresponding US concept, Joint All-Domain Command and Control (JADC2), increase the risk posed by real or perceived cyber vulnerabilities in NATO nuclear forces. More specifically, the paper seeks to examine the potential vulnerabilities of nuclear command, control, and communications (NC3) systems within NATO to intrusions from cyberspace. The paper will first present a foresight scenario set in 2031, followed by a brief discussion of how JADO and JADC2 integrate with cyberspace. Following this, the relationship between the two concepts and NC3 systems will be discussed. Finally, the potential cyber vulnerabilities of NC3 systems will be outlined. The paper will conclude by setting forth a series of likely implications for the future conduct of offensive cyberspace operations between nuclear-armed states.

# 2030s Scenario: Exercise 'Spring Storm 2031'

May 2031, Estonia. It is the third day of the major annual military exercise 'Spring Storm 2031', led by the Estonian Defence Forces with the participation of two of NATO's four Enhanced Forward Presence battlegroups. The US-led battalion-size battlegroup, which includes a Recon Scout troop from the US Army's First Squadron, 91st Cavalry Regiment equipped with half a dozen intelligence, surveillance, and reconnaissance (ISR) unmanned aerial vehicles, is operating in the southeastern part of the country near the Russian border. Its mission is to conduct a reconnaissance-in-force operation and delay any potential Russian incursions. For the first time, all deployed NATO forces are equipped with the new advanced battle management system (ABMS), which links 'sensors to shooters' in the internet of military things (IoMT) and fuses vast amounts of information with the aid of machine learning (ML) algorithms, thereby providing decision support to Allied commanders. It has taken over a decade to deploy this new system and make it interoperable with similar NATO systems. The ABMS is made possible by the NATO Joint Warfighter Cloud Capability (NJWCC), which integrates hundreds of smaller military clouds from NATO member countries which previously did not connect with one another, and which also took almost 10 years to complete. Thanks to the NJWCC, the ABMS is now feeding the head of US Strategic Command real-time battlespace updates enhanced with ML algorithms which assess the impact of battlespace updates on nuclear threats during the exercise.

Due to a persistent stalemate in arms reduction talks, the deployment by both NATO and Russia of more sophisticated missile defence systems, and a prevailing perception in the US and Europe of a more aggressive Russian nuclear doctrine and posture, for the past five years, Spring Storm has included a nuclear component. The real-time fusion and quick redistribution of data across domains and all levels of command is a key technical requirement of the 2021 NATO Warfighting Capstone Concept (NWCC), operationalised with the help of a joint all-domain operations (JADO) 'roadmap'. This roadmap was developed in the early 2020s by NATO's Allied Command Transformation (ACT) to support the transformation of Alliance militaries into multi-domain forces. Both ABMS and NJWCC

1 The NATO Warfighting Capstone Concept (NWCC) was endorsed in 2021 by NATO leaders. 'NWCC: NATO Warfighting Capstone Concept', fact sheet, NATO Allied Command Transformation [undated], https://www.act.nato.int/nwcc.

have multiple cyber defence layers, a series of defensive mechanisms ranging from advanced biometrics to more traditional system and network security. For years, Russian hackers from the Main Intelligence Directorate of the General Staff of the Armed Forces of the Russian Federation (commonly referred to as the GRU) have been trying to compromise the ABMS in a sustained effort to discredit the NWCC and sow distrust between the US and its European partners (as the latter remain deeply sceptical of the new warfighting concept and reluctant to invest in new technology enabling interoperability with the US systems).

In 2031, a group of specialist GRU tactical cyber warfare experts embedded in a small Spetsnaz GRU unit are finally about to succeed in breaching the ABMS by targeting its weak perimeter rather than its strong core. Shadowing the US Recon Scout troop from the Russian side of the border, the Spetsnaz GRU specialists aimed to succeed not by targeting the troop itself but by targeting the cloudlets, servers, and communications equipment installed on the unit's ground vehicles that serve as a collection point for ISR data heading to the NJWCC-enabled cloud. Thus far, the Spetsnaz GRU unit has been able to track the troop and determine its geolocation with ease thanks to lax electronic signature discipline (one US trooper even smuggled his cell phone to the exercise, occasionally turning it on to share updates with his girlfriend). Unbeknownst to the troop, for three days the Spetsnaz GRU specialists have been attempting to break the relatively weak cryptographic security of one of the vehicle's cloudlets. For many months, GRU specialists had been analysing the US cloudlet system in detail and have developed programs to hack it. On the morning of the fourth day, the Russian unit finally succeeds and inserts into the system a polymorphic attack package (or 'worm') – a type of malware that repeatedly changes its identifiable features to evade detection in the cloudlet by subverting the cryptographic security of the wireless networking protocol that supports the cloudlet operations. From the cloudlet, it is transferred to the cloud. The malware, disguised as a datapoint on a 9K720 Iskander mobile short-range ballistic missile system, would (or so the Russian hackers hoped) make it all the way to NATO's Joint Force Training Centre in Poland, where the exercise was coordinated, given the likely high priority classification it would receive from the ML algorithm. In reality, the Russian malware goes well beyond that. As a result of the rapid fusion and redistribution of data under ABMS and NJWCC, the malware makes it all the way to US Strategic Command and its NC3 artificial intelligence (AI)-enabled intelligence gathering system, which is connected to the ABMS. Within four days of the successful breach, ABMS and multiple NC3 displays at Strategic Command go dark.

# NATO Joint All-Domain Operations and Cyberspace

Joint All-Domain Operations (JADO) is an evolution of the US Army's concept of multi-domain operations (MDO).[2] A tentative definition by NATO's Joint Air Power Competence Centre characterises JADO as 'actions taken by the joint forces of two or more NATO nations, comprised of all available domains, integrated in planning and synchronized in execution, at a pace sufficient

2 For an official US Army summary of developing MDO doctrine, see U.S. Army Training and Doctrine Command [TRADOC], *The U.S. Army in Multi-Domain Operations 2028*, Pamphlet 535-3-1 (Newport News, VA: TRADOC, 1 December 2018), https://api.army.mil/e2/c/downloads/2021/02/26/b45372c1/20181206-tp525-3-1-the-us-army-in-mdo-2028-final.pdf.

to effectively accomplish the mission'.[3] In short, JADO mandates the effective integration of capabilities, and the synchronisation of operations and fires, across all the warfighting domains, including air, sea, land, space, and cyberspace, as well as across military branches. JADO is underpinned by the US concept of Joint All-Domain Command and Control (JADC2), which aims to link sensors from weapon systems and other platforms across service branches – and in the case of NATO, across the armed forces of the member states – into a single IoMT network in order to provide NATO commanders with a common operating picture.[4] From a technical perspective, JADO and JADC2, and their broad NATO equivalents of Integrated Multi-Domain Defence and Cross-Domain Command, require a mesh cloud and network architecture integrated within a battle management system.[5] NATO's Federated Mission Networking, a 'capability aiming to support command and control and decision-making in future operations through improved information-sharing', could potentially serve as the basis to achieve the interoperability required for JADO and JADC2.[6] It is unclear to what degree the two interlinked concepts would impact or be entangled with NATO NC3 systems.

At present, JADO remains in conceptual development at NATO. The NATO Warfighting Capstone Concept (NWCC), produced by Allied Command Transformation (ACT), was released at the end of December 2020 and endorsed in 2021 by NATO leaders.[7] In January 2021, the NATO Military Committee formally tasked ACT with expanding on JADO within NWCC in a 'Multi-Domain Operations Roadmap'. ACT has worked on this response throughout 2021 as part of the 'Initial Warfare Development Agenda' which will guide NATO capability development efforts for the next 20 years.8 Although the details remain classified, the roadmap also lays out steps for the synchronisation of kinetic and non-kinetic fires and the integration of multi-domain effects. In a previous report, Alexander Stronell and I laid out a preliminary and non-comprehensive list of technical, structural, and organisational requirements for the effective integration of cyber and conventional operations or fires.[9] One of our conclusions was that effective JADO integration would require the revision of the Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA) mechanism for the conduct of offensive cyberspace operations and an update of the existing AJP-3.20 Allied Joint Doctrine for Cyberspace Operations.[10] At the NATO level, it would also require further work on the concept of joint fires and effects, which includes establishing processes such as Fires and Effects Synchronisation Boards under the ongoing NATO Command Structure Adaptation (NCS-A) effort.[11] Given that JADO is to be introduced into official doctrine in Allied Joint Publication (AJP)-01(E) – the capstone NATO

3 '"NATO JADO": A Comprehensive Approach to Joint All-Domain Operations in a Combined Environment', *Joint Air Power Competence Centre*, March 2021, https://www.japcc.org/portfolio/nato-joint-all-domain-operations.

4 Nishawn S. Smagh, *Joint All-Domain Command and Control (JACC2)*, CRS 'In Focus' IF11493 (Washington, DC: Congressional Research Service, 1 July 2021), 1–2, https://fas.org/sgp/crs/natsec/IF11493.pdf.

5 'NWCC: NATO Warfighting Capstone Concept', fact sheet, NATO Allied Command Transformation [undated], https://www.act.nato.int/nwcc.

6 'Federated Mission Working', fact sheet, NATO Allied Command Transformation [undated], https://www.act.nato.int/activities/fmn.

7 'NWCC: NATO Warfighting Capstone Concept', fact sheet, NATO Allied Command Transformation [undated], https://www.act.nato.int/nwcc.

8 Interview with senior NATO official Franz-Stefan Gady, January 2021.

9 Franz-Stefan Gady and Alexander Stronell, 'Cyber Capabilities and Multi-Domain Operations in Future High-Intensity Warfare in 2030', in *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*, edited by Amy Ertan et al. (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence [CCDCOE] Publications, 2020), 151–176, https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf.

10 Gady and Stronell, 'Cyber Capabilities and Multi-Domain Operations', 166.

11 Marcus A. Jones and Jose Diaz de Leon, 'Multi-Domain Operations: Awareness Continues to Spread about the Importance of Operating in Multiple Domains', *Three Swords Magazine*, no. 36 (November 2020), 40–41, https://jwc.nato.int/application/files/5616/0523/5418/issue36_08lr.pdf.

doctrine for Allied joint operations – only later this year, it is understandable that JADO remains in the experimental stage.

# NATO Joint All-Domain Operations and NC3

NC3 systems are information systems 'supporting the exercise of command and control, as well as the communications between units of command in military operations involving the planning and use of nuclear weapons'.[12] Within the NATO Alliance, only three major powers – the United States, France, and Great Britain – possess independent NC3 architectures.[13] Because the US is the only member state that allots a select number of nuclear weapons for sharing within NATO, thereby making it 'inevitable that that the NC3 system in place within NATO is inextricably linked to the US's own NC3 system', the focus of this paper will be on US NC3.[14] According to the US Nuclear Posture Review (NPR), the American 'NC3 system performs five crucial functions: detection, warning, and attack characterization; adaptive nuclear planning; decision-making conferencing; receiving Presidential orders; and enabling the management and direction of forces'.[15] The NC3 system encompasses around 160 individual systems, including early warning radars, early warning and detection satellites, and communication satellites, as well as airborne operations centres.[16] The current NC3 system is reportedly disconnected from the internet, and all of its mission-critical networks are air-gapped, although the precise network connectivity of an architecture that includes 160 individual systems, including air and space sensors, is difficult to ascertain. Air-gapped systems are traditionally thought to provide an additional layer of cybersecurity, although cybersecurity providers have noticed that the perception of an air-gap often reduces investment in cyber capabilities due to a sense of island safety.

However, the US is currently seeking to develop replacements for various NC3 systems that leverage developments in the JADC2 concept. According to 2020 US Senate testimony by the head of US Strategic Command, Admiral Charles A. Richard, '[w]hile we develop the next generation NC3 to conduct nuclear command and control (NC2) over assured communication paths, we must consider how NC2 infrastructure will align and interoperate with the future Joint All-Domain Command and Control (JADC2) structure. Future NC3 architecture will retain elements specific to NC2 while leveraging JADC2 to maintain resilient and redundant C2 and facilitate quick decision cycles.'[17] Admiral Richard's statement is in line with comments made in 2020 by the vice-chairman

12 Yasmina Afina, Calum Inverarity, and Beyza Unal, 'Ensuring Cyber Resilience in NATO's Command, Control and Communication Systems' (Research Paper, Chatham House, July 2019), 14, https://www.chathamhouse.org/2020/07/ensuring-cyber-resilience-natos-command-control-and-communication-systems-0/3-nuclear.

13 Those countries hosting US nuclear weapons, including Belgium, Germany, Italy, the Netherlands, and Turkey, are also members of the Nuclear Planning Group (NPG), which coordinates and sets the nuclear policy of the alliance. 'Nuclear Planning Group (NPG)', fact sheet, NATO, 27 May 2020, https://www.nato.int/cps/en/natolive/topics_50069.htm.

14 Afina, Inverarity, and Unal, 'Ensuring Cyber Resilience in NATO', 14, 36–44.

15 Office of the Secretary of Defense, *Nuclear Posture Review 2018* (Washington, DC: Office of the Secretary of Defense, 2018), xiii, https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF.

16 John R. Hoehn, *Nuclear Command, Control, and Communications (NC3) Modernization*, CRS 'In Focus' IF11697 (Washington, DC: Congressional Research Service, 8 December 2020), https://fas.org/sgp/crs/nuke/IF11697.pdf.

17 U.S. Strategic Command, U.S. Congress, Senate, Committee on Armed Services, *Statement of Charles A. Richard, Commander United States Strategic Command, before the Senate Committee on Armed Services*, 116th Cong., 2nd sess., 13 February 2020, 16–17, https://www.stratcom.mil/Portals/8/Documents/2020_USSTRATCOM_Posture_Statement_SASC_Final.pdf.

of the Joint Chiefs of Staff, General John E. Hyten, who noted that 'it's important to realize that JADC2 and NC3 are intertwined because, well, NC3 will operate in elements of JADC2.... NC3 has to inform JADC2 and JADC2 has to inform NC3. You have to have that interface back and forth, and that's been recognized.'[18] Similarly, according to Werner J. A. Dahm, the chair of the Air Force Scientific Advisory Board, nuclear weapons will have 'some level of connectivity to the rest of the warfighting system'.[19]

The precise mechanism by which NC3 will interface with JADC2 remains unclear. One possibility is that JADC2 will feed NC3 systems with data on conventional military operations[20] processed by AI-enabled battle management systems such as the US Air Force's still-in-development Advanced Battle Management System.[21] Among other things, this information could then be used to assess the risk of possible shifts in an adversary's nuclear posture based on recent conventional developments. Another NC3-JADC2 technical interlinkage could be dual-use systems such as communication satellites. For example, the current Advanced Extremely High Frequency (AEHF) constellation provides both tactical and strategic communication for conventional and nuclear forces, respectively.[22] The follow-on Evolved Strategic Satcom Program (ESS), which will replace the AEHF starting at the end of the decade, will split the tactical and strategic roles into two separate programmes to avoid single-point-of-failure vulnerabilities (although during the transition phase, JADC2 and NC3 will continue to rely on AEHF).[23] It remains unclear to what degree strategic communication systems can really stay entirely separate from other communications systems under the JADC2 philosophy 'of connecting any sensor to any shooter in any domain at any time'.[24] A larger point of consideration is the degree to which the JADC2 and JADO concepts make the deeper entanglement of conventional and NC3 all but inevitable, regardless of whether this occurs by deliberate design.

# NC3 Cyber Risks

If JADO and JADC2 are adopted across NATO and the US armed forces, it is likely to lead to the deeper entanglement of conventional and NC3 systems. This system entanglement will increase the digital attack surface such that cyber effects may influence leadership decisions in times of crisis. A recent Carnegie Endowment report contains a general overview of the existing literature

18 Colin Clark, 'Nuclear C3 Goes All Domain: Gen. Hyten', *Breaking Defense*, 20 February 2020, https://breakingdefense.com/2020/02/nuclear-c3-goes-all-domain-gen-hyten/.

19 Patrick Tucker et al., 'Will America's Nuclear Weapons Always Be Safe from Hackers?' *Atlantic*, 20 December 2016, https://amp.theatlantic.com/amp/article/511904/.

20 Michael T. Clare, '"Skynet" Revisited: The Dangerous Allure of Nuclear Command Automation', *Arms Control Association*, April 2020, https://www.armscontrol.org/act/2020-04/features/skynet-revisited-dangerous-allure-nuclear-command-automation.

21 David Allvin, 'Why We Need the Advanced Battle Management System', *Defense One*, 6 May 2021, https://www.defenseone.com/ideas/2021/05/why-we-need-advanced-battle-management-system/173861/.

22 'Advanced Extremely High Frequency (AEHF) Satellite System', *Airforce Technology* [undated], https://www.airforce-technology.com/projects/advanced-extremely-high-frequency-aehf/.

23 U.S. Air Force Space and Missile Systems Center, 'The Future of DoD SATCOM: Delivering Fighting SATCOM', *Milsat Magazine*, April 2019, http://www.milsatmagazine.com/story.php?number=733539744.

24 Elaine McCusker, Ron Boxall, and David L. Norquist, 'Department of Defense Press Briefing on the President's Fiscal Year 2021 Defense Budget' (press conference transcript, Washington, DC: U.S. Department of Defense, 10 February 2020), https://www.defense.gov/Newsroom/Transcripts/Transcript/Article/2080378/department-of-defense-press-briefing-on-the-presidents-fiscal-year-2021-defense/.

on cyber nuclear risks, which range from the false detection of a nuclear attack to disruption of communication in times of crisis and the accidental launch of nuclear weapons.[25] Likewise, in a paper on the subject, Jon R. Lindsay lists 21 different ways in which offensive cyber operations might increase the prospects of nuclear escalation.[26] He notes the potential impact of offensive cyberspace operations against networks used for both conventional C2 and NC3 and how it can trigger nuclear escalation. Specifically, he outlines the risks of probing NC3 systems for intelligence which, if discovered, could be mistaken for preparation for a nuclear first strike. Additionally, cyber vulnerabilities of NC3 systems may, with various degrees of plausibility, lead to:

→ False positives: hackers spoof early warning satellites and radar systems, leading to the (wrong) assessment that a nuclear first strike is taking place.

→ False negatives: hackers blind early warning satellites and radar systems, preventing an actual nuclear first strike from being detected.

→ Unauthorised launch: hackers launch nuclear weapons by using false credentials.

→ Accidental launch: hackers trigger an automatic launch of nuclear weapons by accident.

→ Launch failure: hackers disconnect NC3 systems from nuclear missile launch sites.

→ Targeting error: hackers manipulate a launch order, and the nuclear weapon diverts from its pre-assigned target.[27]

The plausibility of each of these scenarios depends on a host of factors, including the status and exact architecture of network defences, the ability of individual hackers, the exploitation of potential human error, and – perhaps most importantly – luck. In each case, multiple elements would need to align, including a cascading failure of safeguards. An additional factor is time. This includes attacker time spent reconnoitring within the target environment; attacker time exfiltrating information from the 160 interconnected systems to piece together the interoperability; and attacker time in establishing hardware as well as software testbeds. Finally, there is attacker time in probing for defensive responses and deconflicting from any denial and deception effects.

No public assessment of the status of cybersecurity of NSC3 exists. However, a 2018 US Government Accountability Office reports 'mission-critical cyber vulnerabilities' in major weapon systems the US Department of Defense is currently developing. It also notes that the department is only beginning to appreciate the scale of, and mount an effective response to, such vulnerabilities.[28] Thus the ongoing upgrade of NC3 systems, paired with new operating concepts, may indeed increase cyber vulnerabilities. Furthermore, as suggested in the above scenario, offensive cyberspace operations need not trigger an actual launch of nuclear weapons or the simulation of an attack in order to

25 George Perkovich et al., 'China-U.S. Cyber-Nuclear C3 Stability' (Research Paper, Carnegie Endowment for International Peace, 8 April 2021), https://carnegieendowment.org/2021/04/08/china-u.s.-cyber-nuclear-c3-stability-pub-84182.

26 Jon R. Lindsay, 'Cyber Operations and Nuclear Weapons', NAPSNet Special Report (Research Paper, Nautilus Institute, 20 June 2019), https://nautilus.org/napsnet/napsnet-special-reports/cyber-operations-and-nuclear-weapons/.

27 See appendix in Lindsay, 'Cyber Operations'.

28 Government Accountability Office [GAO], *Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities*, GAO-19-128 (Washington, DC: GAO, October 2018), 11–37, https://www.gao.gov/products/gao-19-128.

escalate tensions in the nuclear realm. Indeed, a temporary loss of situational awareness would likely suffice.

# Discussion

The above-mentioned exercise, Spring Storm 2031, describes a fictionalised but plausible scenario in which a cyber intrusion against a conventional target unintentionally leads to nuclear crisis simply by turning the screens off at US Strategic Command headquarters during a peacetime military exercise. It outlines a hypothetical future cyber vulnerability emerging through edge cloud architecture underpinning JADO and JADC2 in the 2030s. Obviously, it is difficult to assess how realistic the scenario is, given the difficulty of predicting either exact advances in cyber defensive and offensive capabilities over the next decade or the precise JADC2 network architecture in the future. However, as attacker and defender tactics and techniques evolve, they will influence the probability that these types of attacks will be conducted and whether the desired cyber effect is eventually delivered. The probability of any attack is predicated on a dynamic set of attributes that include security-informed architectures, defensive capabilities, incident response experience, and human ingenuity, underpinned by novel operating concepts and technological advances.

Future NC3 and JADC2 network architecture will also be, to some degree, heterogeneous, with some components featuring stronger cyber protection than others. NC3 systems will most likely remain largely air-gapped, save for some strongly protected interlinkages to JADC2. Nevertheless, as Herbert Lin has pointed out, the historical record of cybersecurity issues in system acquisitions suggests that system functionality is rarely sacrificed for improved protection from attacks from cyberspace.[29] The historical record also shows that air-gapped systems can still be targeted, and the human factor – whereby carelessness and negligence on the part of personnel is exploited by hackers to gain access to otherwise well-defended systems – remains even for the best-defended systems.[30]

This raises another important question: at what point does the complexity of a system create cybersecurity vulnerabilities at such a scale that they risk undermining the system in the future battlespace?

JADC2 is a complex system that will require vulnerability management and incident response capabilities to operate resiliently. If JADC2 becomes a reality, its supposed all-domain functionality could in theory create such complexity in the system's design that many vulnerabilities would likely not be immediately spotted.[31] Narrow AI/ML classifiers feeding into a probabilistic assessment against an event model could help mitigate this risk. At the same time, such AI-enabled battle management systems might be able to use AI and ML to automate cyber defence to such a degree that the complexity is managed and vulnerabilities are detected in real time. The larger point of the scenario is a basic one: the cyber vulnerabilities of conventional and nuclear forces are bound to

29 Herbert Lin, 'Cyber Risk across the U.S. Nuclear Enterprise', *Texas National Security Review* 4, no. 3 (summer 2021), https://tnsr.org/2021/06/cyber-risk-across-the-u-s-nuclear-enterprise/.

30 Robin Harris, 'Four Methods Hackers Use to Steal Data from Air-Gapped Computers', *ZDNet*, 20 November 2017, https://www.zdnet.com/article/stealing-data-from-air-gapped-computers/.

31 According to Herbert Lin, 'at a given level of technological sophistication, more functionality means more complexity'. See Lin, 'Cyber Risk'.

increase as a consequence of the deeper network integration that underpins JADC2. This in turn is likely to lead to further entanglement of NC3 and conventional C2. Thus it could be argued that NATO's JADO concept can create additional cyber vulnerabilities for the NC3 system. In particular, NATO's new operating concept could make unintentional nuclear escalation as a result of a deeper entanglement of conventional and NC3 systems *more* likely, given the interconnective nature of JADC2 and its inherent tendency to open various new attack vectors for adversaries.

# Conclusion

This brief discussion paper has attempted to highlight some of the potential cyber vulnerabilities within NATO NC3 systems likely to emerge as a result of new JADO and JADC2 operating concepts. These are likely to emerge primarily due to the technical characteristics of these new warfighting concepts, which aim to connect distributed sensors and shooters in an IoMT and which reportedly also include some interlinkage with NC3.

If JADO and JADC2 do indeed become the new *modus operandi* of NATO forces in the 2030s, it will have a number of implications for the application of offensive cyberspace operations by nuclear-armed states. Firstly, given that JADC2 will lead to the increasing entanglement of conventional C2 and NC3, creating the possibility that a cyberattack on the former will impact the latter, NATO policymakers and military commanders may be reluctant to order attacks against conventional C2 targets of adversaries in times of crisis in order to avoid vertical escalation. (This point presupposes that a potential nuclear escalation is a sufficient deterrent for one or both actors in the crisis.) Such reluctance by NATO policy-makers and military commanders to order cyberattacks could effectively cancel NATO's Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA) against adversaries' conventional C2 if they are intermingled with NC3.[32] (Whether such an entanglement would also deter future NATO adversaries from conducting similar attacks via cyberspace is unclear.) Secondly, however, even if offensive cyberspace operations under the NATO SCEPVA framework are confined to the civilian critical-information infrastructure of nuclear states, they still could be perceived to be highly escalatory by the opponent, given that such attacks directly or indirectly support military operations. Thirdly, if attacks on civilian critical information infrastructure by NATO policy-makers and military commanders are deemed too escalatory, in a future crisis between nuclear-armed states, operations in cyberspace could be confined to different mission sets, including cyber intelligence, surveillance and reconnaissance, cyber preparation of the environment, electromagnetic interference (jamming and spoofing), tailored cyberattacks against specific weapon systems, and information operations. Given the conventional and nuclear intermingling of C2 and NC3, even cyber preparation of the environment may be deemed too risky. This might lead the responsible military actor to limit its offensive cyberspace operations to tailored battlespace effects against weapon systems and carefully targeted information operations.

Nevertheless, it must be noted that the prosecution of successful offensive cyberspace operations against NC3 systems will not *automatically* trigger nuclear escalation. The escalation of a crisis is a deliberate choice made by policymakers and military commanders. However, JADO and JADC2 may contribute to the new crisis dynamics originating from cyberspace in the 2030s.

32 Wiesław Goździewicz, 'Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA)', *Cyber Defense Magazine*, 11 November 2019, https://www.cyberdefensemagazine.com/sovereign-cyber/.

Chapter 4

# NATO's Role in Responding to China's 'Cyber Superpower' Ambitions

**Laura G. Brent**[1]

1 At the time of writing, Laura G. Brent was a Senior Fellow at the Center for a New American Security.

## Abstract

As the Alliance works to address, in the words of the London Declaration, 'both the opportunities and challenges' that China poses, it must focus on responding to China's conception of, objectives for, and activities in cyberspace. China's efforts to become a 'cyber superpower' test the foundational principles of the Alliance and its commitment, established in the Washington Treaty, to 'promote stability and well-being in the North Atlantic area'. NATO must act. First, NATO must treat China as a strategic challenge that is of immediate and long-term concern. Second, NATO should require more of Allies to ensure that they are sufficiently resilient – and it should also provide more assistance to Allies on resilience issues. Third, as NATO does not have sole responsibility or authority to address China matters, it must strengthen cooperation with the European Union. Finally, NATO should work to act collectively as much as possible – and serve as a forum for multilateral coordination even when not seeking to achieve full consensus. Even as the Alliance addresses China specifically, however, it must also understand China as only one aspect of the changed security environment. While military power is still fundamental to national power, competition stretches far beyond conventional military capabilities and strength. Collective defence should remain the bedrock of the Alliance, but collective security – that is, coordinated and consensus approaches to the broad spectrum of security challenges below the threshold of armed conflict – should become an enhanced focus of its day-to-day business.

**Keywords:** *NATO, China, cyberspace, technology, standards, resilience*

# Introduction

Allied heads of state and government first expressed mild concern about China after their December 2019 meeting in London, finding that 'China's growing influence and international policies present both opportunities and challenges that [they] need to address together as an Alliance'.[2]

Their words following the June 2021 summit in Brussels were far blunter. While stressing NATO's desire to continue to engage with China, the Allies declared unequivocally: 'China's stated ambitions and assertive behaviour present systemic challenges to the rules-based international order and to areas relevant to Alliance security.'[3] They acknowledged that China has adopted some 'coercive policies which stand in contrast to the fundamental values enshrined in the Washington Treaty'.[4] And they 'call[ed] on China to uphold its international commitments and to act responsibly in the international system, including in the space, cyber, and maritime domains'.[5]

NATO secretary general Jens Stoltenberg has also described China as 'coming closer' to NATO through, for example, its investments in Euro-Atlantic critical infrastructure, the range of its weapons systems, and its activities in cyberspace.[6]

This paper is concerned with this final issue: as NATO grapples generally with China's increasing power, what must it do specifically to respond to China's conception of, objectives for, and activities in cyberspace? Given the global, ubiquitous, interconnected nature of cyberspace – as well as China's demonstrated capabilities in everything from cyber-enabled espionage[7] to network technology development[8] – this dimension of China's rise is acutely relevant to NATO.

This paper will briefly lay out China's views on the relationship between cyberspace and national power. It will then highlight a few of China's cyberspace activities that may present the most issues for and relevance to NATO. Finally, it will discuss how NATO can and should take action to meet these challenges.

2 'London Declaration', NATO, 4 December 2019, https://www.nato.int/cps/en/natohq/official_texts_171584.htm.

3 'Brussels Summit Communiqué (2021)', NATO, 14 June 2021, https://www.nato.int/cps/en/natohq/news_185000.htm.

4 Ibid.

5 Ibid.

6 Roula Khalaf and Henry Foy, 'Transcript: "China Is Coming Closer to Us" – Jens Stoltenberg, Nato's Secretary-General', Financial Times, 18 October 2021, https://www.ft.com/content/cf8c6d06-ff81-42d5-a81e-c56f2b3533c2.

7 'Chinese Cyber Threat Overview and Actions for Leaders', U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, 19 July 2021, https://www.cisa.gov/publication/chinese-cyber-threat-overview-and-actions-leaders.

8 John McCormick, Meghan Bobrowsky, and Dan Strumpf, 'Huawei, Ericsson or Nokia? Apple or Samsung? U.S. or China? Who's Winning the 5G Races', Wall Street Journal, 12 October 2021, https://www.wsj.com/articles/huawei-ericsson-nokia-apple-samsung-u-s-china-winning-5g-race-11634000044.

# China's Conception of Cyber Power as National Power

Chinese president Xi Jinping[9] has laid out a vision of cyberspace as critical to national power – and of China as committed to achieving 'cyber superpower' status.[10]

In 2014, Xi established the Central Leading Group on Cybersecurity and Informatisation.[11] In his speech announcing this decision, Xi put forward a number of key concepts that continue to define the importance of cyberspace to China's international ambitions. Xi highlighted the impact of the information technology revolution on 'developments in international political, economic, cultural, social, [and] military' matters.[12] He declared an indelible link between cybersecurity and national security, as well as between informatisation[13] and modernisation.[14] He further advanced the idea that 'cybersecurity and informatization are two wings of one body, and two wheels of one engine'.[15] And finally, he indicated it was necessary to build China into a 'cyber superpower'.[16]

In other words, information technology will 'profoundly influence' all human affairs.[17] The security of this technology is integral to national security; technological maturation and integration are required for modern economic development; and security and development must go hand in hand. And, critically, China should build a position of 'comparative power internationally in the online world' in

---

9 For a discussion on English-language titles for Xi, see Jessie Yeung, 'US Lawmakers Want to Stop Calling Xi Jinping a President. But Will He Care?' CNN, 9 September 2020, https://www.cnn.com/2020/09/08/asia/xi-jinping-title-us-bill-intl-dst-hnk/index.html.

10 New America (www.newamerica.org), cited throughout this paper, has done extensive work to both explain and translate key Chinese speeches and documents on cyberspace. On the concept of 'cyber superpower' in particular, their experts note that 'it can be read as both a goal (to become a "cyber superpower" or a "strong power in cyberspace") and a process ("building China into a national power in cyberspace")'; in any case, it certainly concerns the relative strength of China. Elsa Kania, Samm Sacks, Paul Triolo, and Graham Webster, 'China's Strategic Thinking on Building Power in Cyberspace', New America, 25 September 2017, https://www.newamerica.org/cybersecurity-initiative/blog/chinas-strategic-thinking-building-power-cyberspace/.

11 This Central Leading Group – 'responsible for ensuring security and promoting Chinese government interests in cyberspace and the digital economy' – was transformed into the Central Commission for Cybersecurity and Informatisation in 2018. It is worth noting that this body's name is officially translated into English as the 'Central Commission for Cyberspace Affairs'. As Creemers et al. note, 'cyberspace' in English does not necessarily denote the full remit of the Central Commission; this paper, when discussing the Chinese conception of cyberspace, will take it to mean these concepts that range from cybersecurity to technological development to governance (i.e. closer to the more literal translation of 'cybersecurity and informatisation'). Rogier Creemers, Paul Triolo, Samm Sacks, Xiaomeng Lu, and Graham Webster, 'China's Cyberspace Authorities Set to Gain Clout in Reorganization', New America, 26 March 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cyberspace-authorities-set-gain-clout-reorganization/.

12 Xi Jinping, 'Speech upon the Establishment of the Central Leading Group for Internet Security and Informatization', trans. Rogier Creemers, 1 March 2014, https://chinacopyrightandmedia.wordpress.com/2014/03/01/central-leading-group-for-internet-security-and-informatization-established/.

13 As Kania and Costello note, 'the notion of "informatization" is infamously amorphous'. This paper will take it to mean the ability of the People's Liberation Army to fully leverage information and information technology. Elsa Kania and John Costello, 'China's Quest for Informatization Drives PLA Reforms', *The Diplomat*, 4 March 2017, https://thediplomat.com/2017/03/chinas-quest-for-informatization-drives-pla-reforms/.

14 Xi, 'Central Leading Group for Internet Security and Informatization'.

15 Ibid.

16 Paul Triolo, Lorand Laskai, Graham Webster, and Katharin Tai, 'Xi Jinping Puts "Indigenous Innovation" and "Core Technologies" at the Center of Development Priorities', New America, 1 May 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/xi-jinping-puts-indigenous-innovation-and-core-technologies-center-development-priorities/.

17 Xi, 'Central Leading Group for Internet Security and Informatization'.

order to realise these ideas of security, prosperity, and power.[18]

These topics have carried into Xi's subsequent speeches. At the first Cybersecurity and Informatisation Work Conference in 2016, he again highlighted the impact of the ongoing information revolution.[19] He also associated China's continued development in 'cybersecurity and informatization' with its ability to achieve the 'great rejuvenation of the Chinese nation', which can roughly be understood as the return of China to a position of international power and prestige.[20]

At this time, Xi further discussed the imperative for a domestic production capability, stating: 'Internet core technology is the greatest "vital gate", and the fact that core technology[21] is controlled by others is our greatest hidden danger.'[22] He placed core technology in three categories: 'basic' or 'commonly used' technology; 'trump card' technology; and 'advanced' or 'disruptive' technology.[23] Significantly, he stated that 'advanced' technology represented a competitive opportunity for China to '[run] abreast or even ahead' of other nations.[24]

In 2017, in the official party journal *Qiushi*, the Cyberspace Administration of China further described Xi's plan for China to achieve 'cyber superpower' status. In addition to reiterating the points described above, this article also lays out the need for China to control online content and drive it towards 'positive energy', as well as become more seriously involved in internet governance fora.[25] It also assessed the internet as critical to domestic power: if the 'Party cannot traverse the hurdle represented by the Internet, it cannot traverse the hurdle of remaining in power for the long term'.[26]

In 2018, at the second Cybersecurity and Informatisation Work Conference, Xi again noted the inseparability of cybersecurity from national security, as well as from economic and social stability.[27] This may be the first significant speech to highlight 'civil-military integration' as regards cyberspace.[28] He also advanced the concept of 'core technologies' as 'important instruments of the state'.[29] Here, '"important instruments" has the sense of both a tool and a weapon'.[30] That is, core technologies are

18 Kania et al., 'China's Strategic Thinking'.

19 Xi Jinping, 'Speech at the Work Conference for Cybersecurity and Informatization', trans. Rogier Creemers, 26 April 2016, https://chinacopyrightandmedia.wordpress.com/2016/04/19/speech-at-the-work-conference-for-cybersecurity-and-informatization/.

20 Xi, 'Work Conference for Cybersecurity and Informatization'. For a discussion of 'rejuvenation', see Ken Moritsugu, 'Analysis: Communist Party Seeking China's "Rejuvenation"', AP News, 9 March 2021, https://apnews.com/article/technology-legislature-coronavirus-pandemic-china-asia-pacific-562b40c73740d97f8ddd3099f08fa0a4.

21 As Triolo et al. describe, there is no singular, authoritative accounting of all 'core technologies'. Core technologies would 'almost certainly' include, among others, cryptography, some advanced semiconductors, servers, and 'a growing list of software'. Triolo et al., 'Indigenous Innovation'.

22 Xi, 'Work Conference for Cybersecurity and Informatization'.

23 Ibid.

24 Xi, 'Work Conference for Cybersecurity and Informatization'. Doshi et al. also offer their analysis, as well as a slightly different translation of this speech, in their report for Brookings; this report also offers useful analysis of the sharp divergence between how China communicates domestically and internationally. Rush Doshi, Emily de La Bruyère, Nathan Picarsic, and John Ferguson, 'China as a "Cyber Great Power": Beijing's Two Voices in Telecommunications', Brookings, April 2021, 7–8, https://www.brookings.edu/wp-content/uploads/2021/04/FP_20210405_china_cyber_power.pdf.

25 For a full translation of the *Qiushi* article, as well as relevant analysis, see Kania et al., 'China's Strategic Thinking'.

26 Ibid.

27 Xi Jinping, 'April 20 Speech at the National Cybersecurity and Informatization Work Conference', trans. Rogier Creemers, Paul Triolo, and Graham Webster, New America, 30 April 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-xi-jinpings-april-20-speech-national-cybersecurity-and-informatization-work-conference/.

28 Triolo et al., 'Indigenous Innovation'.

29 Xi, 'April 20 Speech at the National Cybersecurity and Informatization Work Conference'.

30 Triolo et al., 'Indigenous Innovation'.

not simply 'commercial products… [but] actually constitute instruments of national power – whether employed for domestic stability, international security, or economic leadership'.[31]

China thus has a conception of cyberspace as fundamental to everything from domestic economic growth to international governance. Cyberspace is at the heart of the information revolution, which will continue to define modern societal progress. Its security is inseparable from national security. Its technologies are central to economic development, military capability, and the stability and operation of society. And ultimately, China's ability to become a 'cyber superpower' will help define its role in the international system.

# China as a 'Cyber Superpower'

China has undertaken a broad range of activity to achieve this 'cyber superpower' status. Four lines of effort are most strategically relevant to NATO: technology development, standards work, military modernisation, and cyber capabilities.

*Technology development:* China has invested heavily in advanced technology development. In 2015, China announced 'Made in China 2025' (MIC 2025),[32] an industrial plan aimed at 'transforming China into a leading manufacturing power' across 10 sectors, to include information technology and new materials.[33] China has also produced a 'New Generation Artificial Intelligence Plan',[34] which identifies artificial intelligence (AI) as 'a strategic technology that will lead in the future' and will be critical to both competition and security.[35]

While a precise assessment of China's implementation of these plans is challenging, China's overall progress is clear. China has focused on increasing its science, technology, engineering, and mathematics (STEM) prowess. From 2012 to 2021, the Chinese government 'roughly doubled its spending on higher education', and China has produced more STEM PhDs than the United States every year since 2007.[36] It is now a 'manufacturing powerhouse' as well as 'a serious competitor in the foundational technologies of the 21st century', which include AI, quantum technologies, and semiconductors.[37] Even as US sanctions have negatively impacted Huawei's operations, Huawei remains the largest supplier of telecommunications equipment in the world and has an annual

31 Ibid.

32 While the specific name 'MIC 2025' is no longer used by China, the basic policy continues. Lingling Wei, 'Beijing Drops Contentious "Made in China 2025" Slogan, but Policy Remains', *Wall Street Journal*, 5 March 2019, https://www.wsj.com/articles/china-drops-a-policy-the-u-s-dislikes-at-least-in-name-11551795370.

33 '"Made in China 2025" Plan Issued', State Council, People's Republic of China, 19 May 2015, http://english.www.gov.cn/policies/latest_releases/2015/05/19/content_281475110703534.htm.

34 'New Generation Artificial Intelligence Development Plan', China State Council, trans. Graham Webster, Rogier Creemers, Paul Triolo, and Elsa Kania, New America, 1 August 2017, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/.

35 'New Generation Artificial Intelligence Development Plan'.

36 Remco Zwetsloot, Jack Corrigan, Emily Weinstein, Dahlia Peterson, Diana Gehlhaus, and Ryan Fedasiuk, 'China is Fast Outpacing U.S. STEM PhD Growth', Center for Security and Emerging Technology, August 2021, 2–3, https://cset.georgetown.edu/wp-content/uploads/China-is-Fast-Outpacing-U.S.-STEM-PhD-Growth.pdf.

37 Graham Allison, Kevin Klyman, Karina Barbesino, and Hugo Yen, 'The Great Tech Rivalry: China vs the U.S.', Harvard Kennedy School Belfer Center for Science and International Affairs, December 2021, 2, https://www.belfercenter.org/sites/default/files/GreatTechRivalry_ChinavsUS_211207.pdf.

research and development budget of US $22 billion.[38] Furthermore, in some critical technologies, China is now the world leader and, 'in others, on current trajectories, [China] will overtake the [United States] within the next decade'.[39] In short, China is investing holistically in its technology sector – from education, to research and development, to production – and is seeing tangible results.

China is also working to promote its technology – and standards and approach to governance – through the Digital Silk Road (DSR), a component of its Belt and Road Initiative (BRI). The DSR enables China's technology companies to export their products and provides support to recipient countries for technology development, including areas such as 'telecommunications networks, artificial intelligence capabilities, cloud computing, e-commerce and mobile payment systems, surveillance technology, [and] smart cities'.[40] As many as one-third of the nations involved in the BRI may similarly participate in DSR engagements.[41] There are concerns that nations who participate in the DSR will ultimately use Chinese technology to repress their citizens (for example, through pervasive surveillance or internet content control) or will be vulnerable themselves to spying or coercion from China.[42]

There are complicating factors for China's technology development, however. US sanctions are having an impact: Huawei, for example, saw its revenue decrease in the first three quarters of 2021, has moved from first to ninth in smartphone market share, and has experienced a decrease in telecommunications equipment market share for the first time since at least 2014.[43] Large Chinese government investment in the private sector can have distorting effects on both domestic and international markets.[44] Furthermore, a recent spate of Chinese government regulatory action aimed at the technology sector has raised questions about the continued trajectory of these companies' growth and operations.[45]

*Standards setting*: China is also working to improve its ability to set both domestic and international technical standards through its China Standards 2035 project.[46] Launched in 2018, China Standards 2035 has been described by some China observers as a project that is 'more important, that is deeper, that is more ambitious' than MIC 2025.[47] Particularly in areas of emerging technology where standards have not yet been fully defined, China's ability to set standards is viewed by the ruling Chinese Communist Party (CCP) as the ability to 'realize the transcendence of China's industry and

38 As the journalist notes, this research and development spending is larger than Apple's. Dan Strumpf, 'U.S. Set Out to Hobble China's Huawei, and So It Has', *Wall Street Journal*, 7 October 2021, https://www.wsj.com/articles/u-s-set-out-to-hobble-chinas-huawei-and-so-it-has-11633617478.

39 Allison et al., 'Great Tech Rivalry', 2.

40 'Assessing China's Digital Silk Road Initiative: A Transformative Approach to Technology Financing or a Danger to Freedoms?' Council on Foreign Relations, accessed 18 October 2021, https://www.cfr.org/china-digital-silk-road/.

41 Ibid.

42 Ibid.

43 Strumpf, 'U.S. Set Out to Hobble China's Huawei'.

44 James McBride and Andrew Chatzky, 'Is "Made in China 2025" a Threat to Global Trade?' Council on Foreign Relations, 13 May 2019, https://www.cfr.org/backgrounder/made-china-2025-threat-global-trade.

45 Jing Yang, Keith Zhai, and Quentin Webb, 'China's Corporate Crackdown Is Just Getting Started. Signs Point to More Tumult Ahead'. *Wall Street Journal*, 5 August 2021, https://www.wsj.com/articles/china-corporate-crackdown-tech-markets-investors-11628182971.

46 The Chinese domestic standards regime is deeply complex, not always nationally driven, and can be out of line with international standards. Jack Kamensky, 'Standards Setting in China: Best Practices', U.S.-China Business Council, February 2020, https://www.uschina.org/sites/default/files/standards_setting_in_china_challenges_and_best_practices.pdf.

47 Emily de La Bruyère and Nathan Picarsic, 'China Standards 2035: Beijing's Platform Geopolitics and "Standardization Work in 2020"', Horizon Advisory, April 2020, 4, https://www.horizonadvisory.org/china-standards-2035-first-report.

standards'.[48] It is the ability to determine the rules for commerce, for technology, for 'discourse' – and the associated 'power to lead the future order'.[49]

Some of China's standards activity has already generated concern. In 2019, China put forth a proposal to the International Telecommunication Union (ITU) on a new internet architecture called 'New IP'. The proposal, developed by Huawei, is premised on the idea that the current internet is not secure or robust enough to deal with the forthcoming volume and variety of emerging technologies;[50] New IP instead seeks to establish a new global network with a 'top-to-bottom design'[51] and 'intrinsic security'.[52] Western experts, however, fear that New IP introduces centralised and authoritarian-enabling control to the internet – and seeks to solve many technical issues that have already been or are currently being tackled.[53] It should be noted that China made the proposal to the ITU, which is a forum of governments. This sort of technical consideration more traditionally would have been brought, additionally if not exclusively, to the Internet Engineering Task Force (IETF), which is a multi-stakeholder (i.e. government, business, and civil society) forum.[54] It is possible to thus characterise China's actions as, at least in part, politically, rather than purely technically, driven.

While China is certainly focusing more on standards-setting, the impact of these efforts is still developing. New IP has not been adopted – and has sparked a response in democratic countries. Other efforts to perpetuate technological standards have seen progress if not full success. Huawei, for example, may have the largest number of 5G patents,[55] but it is likely not the leader in standard essential patents,[56] or patents that denote 'core, pioneering innovation' and 'are unavoidable for the implementation of a standardized technology'.[57]

*Military Modernisation:* In 2020, the NATO Reflection Group judged that China was 'not, at present, a direct military threat to the Euro-Atlantic area'.[58] Two cyberspace-related aspects of Chinese military modernisation bear close watching by NATO, however: its military-civil fusion (MCF) policy and its advanced technological capabilities.[59]

---

48 Ibid., 6.

49 Doshi et al., 'China as a "Cyber Great Power"', 6.

50 Madhumita Murgia and Anna Gross, 'Inside China's Controversial Mission to Reinvent the Internet', *Financial Times*, 27 March 2020, https://www.ft.com/content/ba94c2bc-6e27-11ea-9bca-bf503995cd6f.

51 Ibid.

52 Hascall Sharp (author) and Olaf Kolkman (Internet Society editor), 'Discussion Paper: An Analysis of the "New IP" Proposal to the ITU-T', Internet Society, 29 April 2020, https://www.internetsociety.org/wp-content/uploads/2020/04/ISOC-Discussion-Paper-NewIP-analysis-29April2020.pdf.

53 Murgia and Gross, 'Reinvent the Internet'; Sharp and Kolkman, 'An Analysis of the "New IP" Proposal'.

54 Mark Montgomery and Theo Lebryk, 'China's Dystopian "New IP" Plan Shows Need for Renewed US Commitment to Internet Governance', Just Security, 13 April 2021, https://www.justsecurity.org/75741/chinas-dystopian-new-ip-plan-shows-need-for-renewed-us-commitment-to-internet-governance/.

55 'Huawei to Start Demanding 5G Royalties from Apple, Samsung', Bloomberg News, 16 March 2021, https://www.bloomberg.com/news/articles/2021-03-16/huawei-to-start-demanding-5g-royalties-from-smartphone-giants.

56 Robert Stoll, '5G SEP Leadership in 2021', Managing IP, 4 October 2021, https://www.managingip.com/article/b1twtv75vtknvq/5g-sep-leadership-in-2021.

57 Gene Quinn, 'Standard Essential Patents: The Myths and Realities of Standard Implementation', IP Watchdog, 4 February 2019, https://www.ipwatchdog.com/2019/02/04/standard-essential-patents-myth-realities-standard-implementation/id=105940/.

58 'NATO 2030: United for a New Era; Analysis and Recommendations of the Reflection Group Appointed by the NATO Secretary General', 25 November 2020, 17, https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf.

59 'NATO 2030', 17 and 19.

MCF is a 'program and plan to leverage all levers of state and commercial power to strengthen and support' the People's Liberation Army (PLA).[60] The 'fusion' of the defence and commercial sectors on technology and innovation issues is a core aspect of MCF strategy.[61] While the outcome of MCF – a technologically advanced PLA – clearly holds risks for Allies, the process of MCF does as well. First, if the PLA makes greater use of civilian technology, technology transfer from Allies to any part of the Chinese economy could be riskier.[62] Second, the Chinese government may be further incentivised to engage in intellectual property theft, particularly around advanced technology, to meet the goals of MCF.[63]

The CCP is also committed to technologically advanced warfighting. In 2017, Xi made intelligentisation a priority for PLA modernisation and success.[64] Whereas informatised warfare – the approach of the CCP since the 1990s – can be roughly defined as warfare characterised by information and information technology, intelligentised warfare is warfare characterised, more or less, by decision-making and decision-enabling technology, such as AI.[65] The CCP has already demonstrated some of its military technology advances. In 2021, for example, China tested a hypersonic weapon system.[66]

Despite significant progress, the PLA's ability to take full advantage of the private sector and modernise effectively is still in question. MCF is a policy because the close relationship between the public and private sectors has not been achieved, 'even though China has been pursuing MCF in some form since at least the early 1980s'.[67] Even with Xi's focus on MCF, the willingness and ability of the private sector to participate more closely with defence organisations remains unclear.[68] Furthermore, while the PLA has engaged in 'historic restructuring' to prepare for advanced technological warfare and has shown itself to have cutting-edge military capabilities, its ability to truly integrate advanced doctrine and capability is uncertain.[69] The PLA is a 'highly hierarchical' institution that has trouble attracting and retaining technical talent, and it may be unable to adequately adapt and train to its goals of intelligentised warfare.[70]

*Cyber Capabilities:* Finally, China has developed considerable cyber capabilities. The US government

60 Alex Stone and Peter Wood, 'China's Military-Civil Fusion Strategy', China Aerospace Studies Institute, 2, https://static1.squarespace.com/static/5e356cfae72e4563b10cd310/t/5ee37fc2fcb96f58706a52e1/1591967685829/CASI+China%27s+Military+Civil+Fusion+Strategy+Full+final.pdf.

61 Ibid., 7.

62 Elsa B. Kania and Lorand Laskai, 'Myths and Realities of China's Military-Civil Fusion Strategy', Center for a New American Security, 28 January 2021, https://www.cnas.org/publications/reports/myths-and-realities-of-chinas-military-civil-fusion-strategy.

63 'Military-Civil Fusion and the People's Republic of China', U.S. Department of State, May 2020, https://www.state.gov/wp-content/uploads/2020/05/What-is-MCF-One-Pager.pdf.

64 Elsa B. Kania, 'Chinese Military Innovation in Artificial Intelligence, Testimony before the U.S.-China Economic and Security Review Commission', 7 June 2019, 3, https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/June-7-Hearing_Panel-1_Elsa-Kania_Chinese-Military-Innovation-in-Artificial-Intelligence.pdf?mtime=20190617115242&focal=none.

65 Informatised and intelligentised warfare are complex concepts that are difficult to summarise. For more precise and detailed descriptions, see Kania, 'Chinese Military Innovation', and Edmund J. Burke, Kristen Gunness, Cortez A. Cooper III, and Mark Cozad, 'People's Liberation Army Concepts', RAND Corporation, 2020, https://www.rand.org/content/dam/rand/pubs/research_reports/RRA300/RRA394-1/RAND_RRA394-1.pdf.

66 Phil Stewart, 'Top U.S. General Confirms "Very Concerning" Chinese Hypersonic Weapons Test', Reuters, 27 October 2021, https://www.reuters.com/business/aerospace-defense/top-us-general-confirms-very-concerning-chinese-hypersonic-weapons-test-2021-10-27/.

67 Kania and Laskai, 'Myths and Realities of China's Military-Civil Fusion Strategy'.

68 Ibid.

69 Kania, 'Chinese Military Innovation in Artificial Intelligence', 2 and 26.

70 Ibid., 26–30.

has assessed that China poses a 'prolific and effective cyber-espionage threat' and also 'possesses substantial cyber-attack' capabilities.[71] The United Kingdom has similarly found that China is engaging in 'systematic cyber sabotage',[72] and the United States has described China as targeting organisations in industries ranging from healthcare to manufacturing, telecommunications, and financial services.[73]

In its review of leading cyber powers, the International Institute for Strategic Studies placed China second only to the United States in cyber capability.[74] China has openly undertaken change to make itself more capable, such as the military reorganisation that centralised cyber operations under the Strategic Support Force.[75] It also appears to have signalled its capabilities in other ways – through, for example, the Tianfu Cup, where Chinese hackers compete to find new cyber vulnerabilities. This competition has demonstrated the notable technical talent of participating Chinese individuals; it has also shown that China has significant tools at its disposal and can 'hold key Western systems and networks at risk'.[76]

# What China as a 'Cyber Superpower' Means for NATO

In the preamble of the Washington Treaty, the Allies affirm that they 'founded [NATO] on the principles of democracy, individual liberty and the rule of law' and that 'they seek to promote stability and well-being in the North Atlantic area'.[77] China's efforts to become a 'cyber superpower' are deeply relevant to this understanding of NATO's purpose.

Take China's technology ambitions and actions. A range of security and stability concerns arises if the Alliance becomes reliant on key technology developed by China. If specific technology, such as 5G infrastructure, is designed to allow access for the Chinese government, Allies could be spied upon – and then blackmailed or coerced.[78] If the technology is poorly designed and can be compromised, critical communications or infrastructure could be disrupted in peacetime or in a crisis, whether by China or other capable actors.[79] The spread of Chinese technology, such as surveillance capabilities

71 'Annual Threat Assessment of the US Intelligence Community', Office of the Director of National Intelligence, 9 April 2021, 8, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf.

72 'UK and Allies Hold Chinese State Responsible for a Pervasive Pattern of Hacking', Foreign, Commonwealth and Development Office, National Cyber Security Centre, and the Rt Hon Dominic Raab MP, 19 July 2021, https://www.gov.uk/government/news/uk-and-allies-hold-chinese-state-responsible-for-a-pervasive-pattern-of-hacking.

73 'China Cyber Threat Overview and Advisories', U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, accessed 17 December 2021, https://www.cisa.gov/uscert/china.

74 The International Institute for Strategic Studies further stated that 'China has conducted large-scale cyber operations abroad, aiming to acquire intellectual property, achieve political influence, carry out state-on-state espionage and position capabilities for disruptive effect in case of future conflict'. 'Cyber Capabilities and National Power: A Net Assessment', International Institute for Strategic Studies, 29 June 2021, https://www.iiss.org/blogs/research-paper/2021/06/cyber-power---tier-two.

75 Kania, 'Chinese Military Innovation in Artificial Intelligence', 2.

76 J. D. Work, 'China Flaunts Its Offensive Cyber Power', War on the Rocks, 22 October 2021, https://warontherocks.com/2021/10/china-flaunts-its-offensive-cyber-power/.

77 'The North Atlantic Treaty'.

78 Bojan Pancevski, 'U.S. Officials Say Huawei Can Covertly Access Telecom Networks', *Wall Street Journal*, 12 February 2020, https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256.

79 Michael Kan, 'UK Blames "Defects" in Huawei Tech on Bad Design, Not Spies', *PC Magazine*, 28 March 2019, https://www.pcmag.com/news/uk-blames-defects-in-huawei-tech-on-bad-design-not-spies.

or internet monitoring technologies, also presents risks to Allied and international freedoms. Even if these technologies are not deployed in Allied territory, their widespread adoption could lead to a more technologically bifurcated world, with one group of nations more free than the other.[80] Both China and the United States have portrayed technological competition as central to geopolitical competition;[81] technology is the backbone of modern societies and militaries, and overdependence on Chinese-developed technology presents the risks of subversion, repression, and disruption.

China's work on standards similarly holds implications for democratic governance and individual liberty. If New IP, or a similar proposal, were adopted, Allied governments and citizens would be faced with an internet more prone to control and surveillance.[82] If the Chinese government and its industry defines standards across the emerging technologies that will underpin modern economies and societies, Allies may face a less open and less free world.[83]

China's military development is also of concern. MCF presents economic and security risks if Allies do business with China – and it also incentivises cyber espionage and intellectual-property theft. China has now also tested technology that can reach the Euro-Atlantic area, and it is cooperating more with Russia.[84]

The impacts of China's cyber capabilities have already been felt and hold future risk. The US government has judged that China is capable of causing 'at minimum, localized, temporary disruptions to critical infrastructure within the United States'.[85] China has compromised organisations – such as 'telecommunications firms' and 'providers of managed services and broadly used software' – that offer value for 'intelligence collection, attack, or influence operations'.[86] And when NATO released a statement on the Microsoft Exchange Server compromise – which it noted that many Allies had attributed to China – NATO described such activities as 'designed to destabilize and harm Euro-Atlantic security and disrupt the daily lives of [its] citizens'.[87]

NATO thus has a clear imperative to address China as a 'cyber superpower', and it should undertake four lines of effort.

First, NATO must treat China as a strategic challenge that is of both immediate and long-term concern. Secretary General Stoltenberg has noted that China has affected Allied security and will continue to do so;[88] the recognition of this fact must prompt further action. NATO is a complex, consensus-based organisation: while decision-making takes time, there must be a bias towards action on China. When the Allies present their new strategic concept at the Madrid Summit in

80 'Assessing China's Digital Silk Road Initiative'.

81 Bill Burns, director of the Central Intelligence Agency, has identified technology as 'the main arena for competition and rivalry with China'. 'Transcript: NPR's Full Conversation with CIA Director William Burns', NPR, 22 July 2021, https://www.npr.org/2021/07/22/1017900583/transcript-nprs-full-conversation-with-cia-director-william-burns. Xi has also declared: 'Technological innovation has become the main battleground of the global playing field, and competition for tech dominance will grow unprecedentedly fierce'. Allison et al., 'Great Tech Rivalry', 3.

82 Murgia and Gross, 'Inside China's Controversial Mission to Reinvent the Internet'.

83 De La Bruyère and Picarsic, 'China Standards 2035', 4.

84 Stewart, 'Chinese Hypersonic Weapons Test'; Khalaf and Foy, 'China Is Coming Closer to Us'.

85 'Annual Threat Assessment of the US Intelligence Community', 8.

86 Ibid.

87 'Statement by the North Atlantic Council in Solidarity with Those Affected by Recent Malicious Cyber Activities Including the Microsoft Exchange Server Compromise', NATO, 19 July 2021, https://www.nato.int/cps/en/natohq/news_185863.htm.

88 Khalaf and Foy, 'China Is Coming Closer to Us'.

2022, they should have specific, clear plans to address the challenges China poses in and through cyberspace. Allies should require NATO civilian and military bodies to make regular reports on progress and ensure that NATO has the appropriate resources to accomplish its assigned tasks.

Second, NATO should revisit how it approaches resilience as an alliance. Article 3 of the Washington Treaty helps define NATO and Allied responsibilities outside of Article 5's collective defence commitments. Article 3 states that Allies, 'separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack'.[89] This justifies NATO involvement in resilience, which Allies recognise as 'an essential basis for credible deterrence and defence... and vital in [their] efforts to safeguard [their] societies, [their] populations and [their] shared values'.[90]

In 2021, the Allies committed to bolster their 'national and collective resilience'.[91] The Allies stated that they 'will develop a proposal to establish, assess, review and monitor resilience objectives to guide nationally-developed resilience goals and implementation plans'.[92] They also recognised that 'it will be up to each individual Ally to determine how to establish and meet national resilience goals and implementation plans'.[93] NATO is dependent upon Allied resilience in both peacetime and crisis, and it should take a more active role in reviewing not just overall objectives, but actual Allied implementation. While NATO should not set specific resilience targets or methods, NATO can and should routinely meet with Allies to assess and advise on their resilience, particularly in areas that will impact all Allies, such as core network technology.

Even as NATO should require more of Allies on resilience, it can also provide more assistance. Resilience is 'first and foremost a national responsibility', but modern resilience challenges – from pandemics to supply chains to cyberspace – are inherently more interconnected.[94] NATO established Counter Hybrid Support teams in 2018[95] and has deployed them twice, once each to Montenegro[96] and Lithuania.[97] Teams can deploy in the face of any hybrid challenge, upon request of an Ally, and Allies should consider how they can be more creatively utilised for advice and assistance in the face of the broad range of security challenges that exist below the threshold of armed conflict.

Third, NATO should strengthen cooperation with the European Union (EU). NATO is not alone in facing a challenge from China, and NATO is greatly impacted by Allied decisions outside its traditional purview. NATO will have concerns, for example, if it must rely upon untrusted telecommunications networks or other insecure critical infrastructure that enables Allied military deployment. It is the EU and national governments, however, that have the primary role in setting standards and rules for acquiring and operating this civilian infrastructure. While NATO has conducted political

89 'The North Atlantic Treaty'.

90 'Strengthened Resilience Commitment', NATO, 15 June 2021, https://www.nato.int/cps/en/natohq/official_texts_185340.htm.

91 Ibid.

92 Ibid.

93 Ibid.

94 'Resilience and Article 3', NATO, 11 June 2021, https://www.nato.int/cps/en/natohq/topics_132722.htm.

95 'NATO's Response to Hybrid Threats', NATO, 16 March 2021, https://www.nato.int/cps/en/natohq/topics_156338.htm.

96 Pierluigi Paganini, 'NATO Will Send a Counter-Hybrid Team to Montenegro to Face Russia's Threat', *Security Affairs*, 20 January 2020, https://securityaffairs.co/wordpress/96627/cyber-warfare-2/montenegro-nato-hybrid-attacks.html.

97 'NATO Counter Hybrid Support Team Arrives in Lithuania', *Baltic Times*, 7 September 2021, https://www.baltictimes.com/nato_counter_hybrid_support_team_arrives_in_lithuania.

consultations with the EU on China,[98] the most recent report on the 74 common proposals for NATO-EU collaboration includes no specific mention of China.[99] NATO and the EU must consult more specifically and explicitly on China as a 'full-spectrum systemic rival' that involves the roles, responsibilities, and equities of both organisations.[100]

Fourth, particularly on issues related to China, NATO should act collectively as much as possible, as well as serve as a forum for multilateral coordination even when not seeking consensus. NATO has begun to do this by, for example, discussing the attribution of malicious cyber activity. After the Microsoft Exchange Server compromise, NATO declared its 'solidarity' with Allies who had been impacted, 'condemned' such malicious activity, and 'acknowledge[d]' the attribution of the activity to China by the United States, United Kingdom, and Canada.[101] NATO should make definitive, collective attribution routine and follow such attribution with a clear response. At the Brussels summits in 2018 and 2021, Allies said, in the context of malicious cyber activity, that they would seek to 'impose costs on those who harm' them.[102] NATO can and should impose costs in response to malicious cyber activity. After the United Kingdom plausibly attributed the nerve agent attack on its soil to Russia, for example, NATO expelled seven Russian staff from Brussels, citing that specific action as well as Russia's general 'pattern of unacceptable and illegal behaviour'.[103] NATO must treat malicious activity in cyberspace with similar resolve.

Allies should also use NATO as a forum to discuss how coordination, outside of agreed consensus action, can make individual nations' efforts stronger and more coherent. Even if NATO does not always attribute malicious cyberspace activity, for example, discussion of such issues can help harmonise Allied approaches and responses. Even if NATO does not mandate exactly what network gear can be purchased for domestic civilian networks, Allies can understand the range of concerns better through consultation. And even if NATO does not get a vote in other international organisations, it can help its Allies work more effectively together. The United States and Russia both currently have candidates to be the next secretary general of the ITU; NATO should discuss what all Allies should do concerning that election – or in the ITU in general.[104]

---

98 'Relations with the European Union', NATO, 21 June 2021, https://www.nato.int/cps/en/natohq/topics_49217.htm.

99 'Sixth Progress Report on the Implementation of the Common Set of Proposals Endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017', NATO and the EU, 3 June 2021, https://www.nato.int/nato_static_fl2014/assets/pdf/2021/6/pdf/210603-progress-report-nr6-EU-NATO-eng.pdf. This set of proposals was agreed upon in 2016 and 2017, so it does precede the increase in NATO's focus on China. The report, however, does include a forward-looking program for discussion in 2022, which could have presented an opportunity to put China on the agenda.

100 'NATO 2030', 27.

101 'Statement by the North Atlantic Council in Solidarity with Those Affected by Recent Malicious Cyber Activities Including the Microsoft Exchange Server Compromise'.

102 'Brussels Summit Declaration (2018)', NATO, 11 July 2018, https://www.nato.int/cps/en/natohq/official_texts_156624.htm; 'Brussels Summit Communiqué (2021)'.

103 Patrick Wintour and Julian Borger, 'Nato Expels Seven Staff from Russian Mission over Skripal Poisoning', *Guardian*, 27 March 2018, https://www.theguardian.com/uk-news/2018/mar/27/russia-to-respond-harshly-to-us-expulsion-of-diplomats.

104 David Ignatius, 'Russia's Plot to Control the Internet Is No Longer a Secret', *Washington Post*, 4 May 2021, https://www.washingtonpost.com/opinions/2021/05/04/russias-plot-control-internet-is-no-longer-secret/.

# Conclusion

China – and particularly China as a 'cyber superpower' – presents an immediate and long-term challenge for NATO. Even as the Alliance addresses China specifically, however, it must also understand China as only one aspect of the changed security environment.

In the 20th century, nations sought global power through large-scale conflict. In the opening decades of the 21st century, however, nations have challenged the international order using all instruments of national power. While military power is still fundamental to national power, competition stretches far beyond conventional military capabilities and strength. Collective defence should remain the bedrock of the Alliance, but collective security – that is, coordinated and consensus approaches to the broad spectrum of security challenges below the threshold of armed conflict – should become an enhanced focus of its day-to-day business.[105]

Modern security threats cross multiple boundaries: civil and military, cyber and physical, economic and security, public and private, and domestic and international. The challenges posed by China typify this interconnectedness, but China is not the only multifaceted issue that NATO faces. Everything from resilience to malicious cyber activity to civilian and military technology development pose grave risks below (and hold profound relevance above) the threshold of armed conflict.

NATO has proven enduring and powerful because it can adapt, and it must continue to do so to meet these threats that resist easy definitions and solutions. NATO must systematically take on more of these challenges that fall below the threshold of armed conflict, as they define much of the current security environment.

Fundamentally, NATO must maintain its high-end military capabilities while expanding its political, cooperative tool set to address today's global, interconnected, and complicated security matters.[106] NATO was established 'for the preservation of peace and security', and that purpose now demands more effectively and collectively addressing threats below, as well as those above, the threshold of armed conflict.[107]

---

105 The author thanks the relevant NATO experts for their inspiration and advice on these points.

106 Secretary General Stoltenberg laid out a vision for NATO in 2030 in which it 'remains strong militarily, becomes even stronger politically, and takes a more global approach'. 'NATO 2022 Strategic Concept', NATO, accessed 16 December 2021, https://www.nato.int/strategic-concept/.

107 'The North Atlantic Treaty'.

Chapter 5

# Drivers of Change Impacting Cyberspace in 2030

**Piret Pernik**
Researcher
CCDCOE

## Abstract

This paper describes global drivers of change relevant to cyberspace that NATO should consider when preparing for continuous competition (shaping, contesting, and fighting) in 2030 in cyberspace. First, it describes the cyber domain in the multi-domain operational environment. Second, it discusses key emerging and disruptive technologies relevant to cyberspace, and anticipates the future use of them by authoritarian opponents and non-state actors. Third, the paper identifies other drivers of change and areas impacting interactions in the cyber domain (such as the legal framework, influence and information operations, and intelligence collection). The conclusions propose considerations for future research.

**Keywords:** *cyber threats, cyber domain, multi-domain, strategic thinking, future thinking, horizon scanning and foresight methods*

# Introduction

In 2012, Leon Panetta, then the United States secretary of defence, cautioned that cyberattacks can become as destructive as Pearl Harbour or 9/11. He has been proven wrong – cyberattacks have not caused large scale physical destruction or causalities comparable to these events. This has been acknowledged by Jim Lewis, a leading cybersecurity scholar, who said that 'a lot of predictions people made 10 and 20 years ago [about cyberattacks], including me, have been proven wrong'.[1] Many future paths are possible, and forecasters might get them wrong. Similar to the warnings about cyberattacks, technological progress is often slower than people have thought. For decades visionaries and technologists have issued alerts about the development of general artificial intelligence (AI) or popularly dubbed 'superintelligent computers', which would quickly become an existential threat to humankind with catastrophic consequences.[2] Today, there is consensus among computer scientists and technologists that general AI is at least 50 years away and the likelihood of malicious machine consciousness harming humankind is fictional.[3] Another example of a tendency to overrate the pace of technological development is predictions about quantum technologies/information science (quantum computing, quantum sensing, quantum communications, etc.) and distributed ledger technology (in particular, blockchain technology as a type of it). These technologies are existent but there are many challenges in implementing them in the real-world and their potential applications are limited to some functional areas or fields. According to the National Security Agency, it is uncertain if (and when) a quantum computer will be able to break public key encryption.[4]

In addition to the failure to forecast future cybersecurity and technology related trends, the so-called unknown unknowns (things that we do not know that we do not know) further increase uncertainty related to cyberspace.[5] There are popular semi-scientific theories of a black swan and grey rhino, which policymakers often like to refer to. These hypotheses describe a surprise disruption to the continuation (or acceleration) of current trends, which is impossible to predict, in contrast to known unknowns (things we know that we do not know).

It is hard – if not impossible – to predict 'strategic surprises'. If we could anticipate them, they would not be surprises. A case in hand is the COVID-19 pandemic. For many years, international organisations and national governments have warned about global pandemics caused by human

---

1 Joseph Marks, 'The Cybersecurity 202: Cybersecurity Pros Want to Stop Talking about a "Cyber 9/11"', *Washington Post*, 10 September 2021.

2 In a book entitled *Superintelligence: Paths, Dangers, Strategies* (2014), Nick Bostrom explores the risks AI and related technologies may pose to human civilisation, arguing that the development of superintelligent machines will, if not properly managed, create catastrophic risks to humanity. See Miles Brundage, 'Taking Superintelligence Seriously: *Superintelligence: Paths, Dangers, Strategies* by Nick Bostrom (Oxford University Press, 2014)' [book review], *Futures* 72 (2015), 32–35, https://doi.org/10.1016/j.futures.2015.07.009.

3 Some general AI pilot projects aim to build 'common-sense' AI technology, but they have not yet met their goal. See 'IBM, MIT and Harvard Release "Common Sense AI" Dataset at ICML 2021', IBM blog, 19 July 2021, https://www.research.ibm.com/blog/icml-darpa-agent.

4 'Quantum Computing and Post-Quantum Cryptography', National Security Agency, August 2021, https://media.defense.gov/2021/Aug/04/2002821837/-1/-1/1/Quantum_FAQs_20210804.PDF.

5 In February 2002, Donald Rumsfeld, the then US secretary of defence, stated at a Defense Department briefing: 'There are known knowns. There are things we know that we know. There are known unknowns. That is to say, there are things that we now know we don't know. But there are also unknown unknowns. There are things we do not know we don't know.' https://eu.usatoday.com/story/news/politics/2021/06/30/donald-rumsfelds-most-famous-and-infamous-quotes/7811766002/.

respiratory viruses, for example, a recent report by the UK government.[6] At the same time, few if any organisations or individuals were able to adequately predict its impacts to all areas of human activities, including cyberspace. As such, COVID-19 is an example of a black swan event, and an example of a known unknown. It is a highly unlikely high-impact event, but most national governments failed to prevent or mitigate its negative effects in 2020.[7]

In recent years, one type of cybercrime, ransomware, has turned into a national security issue for many countries and can be considered a systemic risk. Systemic cyber risks impact many horizontal business vectors and cause second- and third-order effects.[8] It is forecasted that by 2025, economic losses from all types of cybercrime will amount to US $10.5 trillion annually.[9] Cybercrime can be considered a known unknown in the sense that it is difficult to predict what types of tools will be used to target businesses and organisations, but it can be safely predicted that the scale and impact of global cybercrime is likely to grow, despite multilateral and unilateral efforts by national governments to curb criminal groups and support targets.

It is worth mentioning the conceptual underpinnings of this paper. There are two main methodologies to envision the uncertain future. The first methodology is horizon scanning, which asks unasked questions, explores the unknown unknowns, and draws implications of global trends not seen to date.[10] Horizon scanning is 'a technique for detecting early signs of potentially important developments through a systematic examination of potential threats and opportunities, with emphasis on new technology and its effects on the issue at hand'.[11]

Second, future thinking is a method of social science for informed reflection on the major changes. 'While the future cannot be reliably predicted, one can foresee a range of possible futures and ask which are the most desirable for particular groups or societies.'[12] Both of the methodologies are qualitative.

Additionally, there exists other common methodologies for strategic assessment of the future security environment, to name a few: desk research (systematic or non-systematic previous literature review), expert interviews, structured workshops, etc. These techniques must enable the

---

6 For example, a 2006 UK government report anticipated that a future pandemic would end within a few months due to universal vaccination. This did not happen in the case of COVID-19. See I. Barker et al., 'Foresight. Infectious Diseases: Preparing for the Future. A Vision of Future Detection, Identification and Monitoring Systems', Office of Science and Innovation, 2006, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/294243/06-760-infectious-diseases-report.pdf.

7 Michele Wucker, 'Was the Pandemic a Grey Rhino or a Black Swan?' *Economist*, 17 November 2021, https://www.economist.com/the-world-ahead/2020/11/17/was-the-pandemic-a-grey-rhino-or-a-black-swan.

8 An example of such systemic cyber risk is a recent ransomware attack against Colonial Pipeline, attributed to the Russian cybercrime group DarkSide, which led to long queues at US gas stations. See Aarian Marshall, 'In the Colonial Pipeline Mess, Tanker Trucks Come to the Rescue', *Wired*, 13 May 2021, https://www.wired.com/story/colonial-pipeline-mess-tanker-trucks-come-to-rescue/; Michael Schwirtz and Nicole Perlroth, 'DarkSide, Blamed for Gas Pipeline Attack, Says It Is Shutting Down', *New York Times*, 8 June 2021, https://www.nytimes.com/2021/05/14/business/darkside-pipeline-hack.html.

9 'Cyber Strategic Outlook', United States Coast Guard, August 2021, https://www.uscg.mil/Portals/0/Images/cyber/2021-Cyber-Strategic-Outlook.pdf.

10 In 2017, the UK government published *The Futures Toolkit*, which describes tools relevant for gathering intelligence about the future, such as horizon scanning, Seven Questions, the issues paper, the Delphi method, and SWOT analysis. *The Futures Toolkit: Tools for Futures Thinking and Foresight across UK Government*, 1.0 ed. (Government Office for Science, November 2017), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/674209/futures-toolkit-edition-1.pdf.

11 'Horizon Scanning and Foresight Methods', *Safeguarding the Bioeconomy* (National Academies Press, 14 January 2020), https://www.ncbi.nlm.nih.gov/books/NBK556423/.

12 Ibid.

identification of key future trends and alternative future paths, and reflect on their implications for societies, groups, and organisations.[13]

In the context of this uncertainty about future trends and key drivers relevant to cyberspace, this paper describes relevant findings from previous literature (strategic documents of national government and armed forces, and academic papers) about future trends relevant to NATO in 2030. First, it describes the cyber domain in the multi-domain operational environment. Second, it discusses key emerging and disruptive technologies (EDTs) relevant to cyberspace, and anticipates the likely future use of them by authoritarian opponents and non-state actors. Third, the paper identifies other cyberspace-relevant drivers of change and areas of activity. The last section of the paper offers initial conclusions and policy recommendations, as well as outlining considerations for future research.

# Cyber Domain and the Operational Environment

## Scenarios of the Future Operational Environment

A strategic outlook towards the cyber domain and cyber threat landscape should be informed with an understanding of the characteristics of future cyberspace and cyber threats, and interactions with and interdependencies from other domains (land, maritime, air, space, electromagnetic spectrum, and information/cognitive). Future warfighting in a continuum from cooperation to armed conflict will take place in a joint, multi-domain (all-domain) operational environment. Of note, even though distinct concepts, in this paper multi-domain, cross-domain, and all-domain will be used interchangeably. By 2030, AI and machine learning (ML), automation, autonomy, internet of military things (IoMT) and next generation (5G, 6G) networks will become more integrated into the operational theatre than today. The more technology is integrated as part of warfighting, the more vulnerable military communications and data links will be. Risks such as cyberattacks, electromagnetic interferences (navigation and positioning systems shutdown, jamming and spoofing) will grow in scale and impact; due to greater interconnections and interdependencies, vulnerabilities, threats and risks from civilian networks will migrate more easily to classified and national security related computer and information systems (CIS) and telecommunication networks.

As illustrated in the introduction, alternative future paths pertaining to the cyber domain are likely and it is impossible to predict with considerable certainty which ones will prevail in 2030. Four possible future scenarios of the operational environment until 2030 are described in strategic documents of the US Army Training and Doctrine Command (TRADOC) and US Army Futures Command. The most likely scenario in 2030 is largely a continuation of today's global power dynamics but compared to the authoritarian opponents China and Russia, the West could be less able to handle stress from the COVID-19 pandemic. China's and Russia's military modernisation efforts could outpace those of the US in 2030.[14]

---

13 There is a wide array of more structured future thinking, forecasting, and horizon-scanning methodologies and tools (including the development of scenarios, war games and serious games, net assessment, and the Delphi process). Foresight tools are qualitative, quantitative, and semiquantitative. Qualitative tools include brainstorming, expert panels, workshops, literature reviews, and SWOT analysis. See a full list in 'Horizon Scanning and Foresight Methods', Table 6-2.

14 'The Operational Environment (2021–2030): Great Power Competition, Crisis, and Conflict', U.S. Army Training and Doctrine Command (TRADOC), 4 October 2021, https://oe.tradoc.army.mil/2021/10/04/the-operational-environment-2021-2030-great-power-competition-crisis-and-conflict-2/.

Before 2035, the US domination in technology could be challenged by a nation-state who has the ability to operate in the multi-domain and deny domains.[15] Adversaries (authoritarian opponents) will take advantage of acquisition of EDTs and advances in doctrine and strategic concepts. After 2035, no single country will have an overwhelming strategic or technological advantage. In that era, 2035–2050, revolutionary technologies will be available for the armed forces on a large scale. The vast majority of cyberspace communications will consist of autonomous machine-to-machine communications; and human-computer teaming enables new military capabilities (such as augmented reality (AR) systems painted directly on a retina, and neural implants), according to TRADOC's forecast.[16] The global world order can evolve into four different scenarios, respectively: under-governed, unipolar, multipolar, and bipolar world order. In the following paragraphs, the last three scenarios will be briefly described.

In the unipolar world, technological development will be revolutionary. China's People's Liberation Army is continuing to exploit cyberspace and launch attacks against US space assets and surveillance and navigation capabilities. China will also attack vital financial assets via AI-enabled malware and ransomware, and it will use cyberspace to disrupt civilian and military logistics, and target autonomous (self-driving) traffic. It is expected that China will use quantum sensing to capture adversary information and quantum key distribution (QKD) to secure its communications. China will use AI-generated deep fakes and execute electronic warfare (EW) and anti-satellite attacks.[17]

In a multipolar world characterised by rapid EDT development, the likelihood of cyber conflict and escalation between, on the one hand, democratic and like-minded alliances and coalitions, and on the other, authoritarian countries, could be increased.[18] In this context, past empirical evidence indicates that the status of a nuclear power is associated with significantly higher odds of cyber conflict.[19] Israel and Iran have engaged in mutual cyberattacks since spring 2020, which some scholars consider escalatory 'with each side showing its unwillingness to absorb a blow without responding and displaying its unwavering resolve'.[20] In the future, nuclear powers such as China, Russia, and arguably Iran or even North Korea could, under certain circumstances, come into direct cyber conflict with NATO. The rationale for cyber conflict is that direct military confrontation between nuclear powers is considered too risky, so nation states may choose less escalatory and damaging attacks such as cyberattacks and information operations. Economic or military asymmetry between rival states as well as cultural differences may also increase the likelihood of a cyber conflict because imbalances of power tend to contribute to international insecurity and make conflict more likely.[21]

---

15 'The Operational Environment and the Changing Character of Future Warfare', U.S. Army TRADCOC, October 2019, https://adminpubs.tradoc.army.mil/pamphlets/TP525-92.pdf.

16 Ibid., 4–6.

17 Some of these capabilities are developed and used today on a smaller scale by authoritarian opponents, but they will be enhanced in the next 10 years. 'The Future Operational Environment 2035–2050', AFC Pamphlet 525–2, U.S. Army Futures Command, https://community.apan.org/wg/tradoc-g2/mad-scientist/b/weblog/posts/check-out-the-army-futures-command-s-new-afc-pamphlet-525-2-future-operational-environment-forging-the-future-in-an-uncertain-world-2035-2050.

18 Ibid.

19 'Cyber Capabilities and National Power: A Net Assessment', International Institute for Strategic Studies, 28 June 2021, https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power, 10–11.

20 Farnaz Fassihi and Ronen Bergman, 'Israel and Iran Broaden Cyberwar to Attack Civilian Targets', *New York Times*, 27 November 2021, https://www.nytimes.com/2021/11/27/world/middleeast/iran-israel-cyber-hack.html; Yael Ram, Isaac Israel, and Gil Baram, 'Cyberwar Between Iran and Israel Out in the Open', 2020, https://www.researchgate.net/publication/348417218_Cyberwar_Between_Iran_and_Israel_Out_in_the_Open.

21 However, on the positive side, political and economic interdependence may deter cyber conflict, as interdependent states may share an interest in mutual peace and prosperity. 'Cyber Capabilities and National Power: A Net Assessment', 10–11.

In a bipolar world, where technological development is evolutionary, slower technological development will favour defence against offence, as far as peer-to-peer competition is concerned. China invests heavily in EDTs, cyberspace, and EW capabilities, as well as launches cyberattacks against vital US targets, but in this scenario, the pace of technological change is slower, and targets have enough time to develop countermeasures; thus, cyber effects are less pronounced.[22]

## Cyber Domain Characteristics and NATO's Approach to Warfighting

At the latest summit in Brussels in June 2021, NATO leaders announced that 'we are increasingly confronted by cyber, hybrid, and other asymmetric threats, including disinformation campaigns, and by the malicious use of ever-more sophisticated emerging and disruptive technologies'.[23] The summit communiqué mentioned for the first time in history that low-end cyber activities (those below the threshold of armed attack, also dubbed grey-zone or hybrid threats), if cumulative, can cause serious enough effects to invoke article 5 of the North Atlantic Treaty.[24] Although examples of such low-end cyber activities were not given, presumably they could include strategic cyber espionage, election interference, and large scale high-impact ransomware attacks against vital services and critical targets.

In 2021, NATO issued a 20-year forward-looking NATO Warfighting Capstone Concept (NWCC), which outlines five imperatives for the Alliance's warfare development.[25] NWCC recognises that multi-domain defence and cross-domain command and control (C2) must be developed, stating that 'the threats the Alliance faces are no longer in any one domain and a joint and flexible approach to a fluid environment is needed to protect the Alliance's integrity against all threats, regardless of their origin or nature'. Inevitably, all C2 is connected to cyberspace, which renders the domain critically important to warfighting in other domains.

One of those warfighting imperatives associated with cyberspace is cognitive superiority, which entails shared 'political-military understanding of the threats, adversaries and environment NATO operates in, from tech, doctrine, to Joint Intelligence, Surveillance and Reconnaissance, and big data'.[26] Today, the national cyber capabilities and forces of NATO members have different maturity levels, and therefore their perceptions of cyber threats and the sources of those threats differ. Whether cognitive superiority over cyberspace will be achieved by 2030 depends first and foremost on improving information and intelligence sharing among nations.

Another imperative for NATO warfighting is layered resilience, which refers to the ability 'to withstand immediate shocks to supply lines or communications, as well as attacks in the cognitive domain'.[27] Cyber resilience and cognitive resilience have been a strategic objective of NATO for many years; more recently NATO has put greater focus on developing a common policy and guidelines for the CIS supply chain and 5G security.

---

22 'The Future Operational Environment 2035–2050'.

23 Brussels Summit Communiqué. Issued by the heads of state and government participating in the meeting of the North Atlantic Council in Brussels, NATO, 14 June 2021, https://www.nato.int/cps/en/natohq/news_185000.htm.

24 Ibid.

25 'The NATO Warfighting Capstone Concept', Allied Command Transformation, https://www.act.nato.int/nwcc, accessed 29 August 2021.

26 Ibid.

27 Ibid.

Due to similarities to other domains, the cyber domain is considered an operational domain, but at the same time, it is recognised that it differs in important respects from other domains.[28] Some characteristics that make cyberspace operations more complex than conventional ones are anonymity, secrecy, and stealth, the difficulty to attribute cyberattacks to actors, global reach and the high speed of operations, and uncertain or unexpected cyber effects. NATO's cyberspace operations standard, Allied Joint Publication 3.20, describes the fundamental characteristics of cyberspace operations as follows: (global) reach, asymmetric effect, time and speed, versatility and anonymity.[29]

In cyberspace, compared to traditional operational domains, private sector and non-state actors have a greater role in a conflict. The cyber domain is constantly changing and being modified (e.g. zero-day vulnerabilities can be disclosed and patched quickly). Lastly, no single country currently has superiority or dominance in the cyber domain which they can keep perpetually.

Although the characteristics of the cyber domain depend on the speed of technological development, most are not likely to simply disappear. For example, in the case of anonymity, attribution has become easier over the years and nations have attributed more attacks but technical challenges in attribution remain and can delay the process. By 2030, some of the mentioned characteristics of cyberspace may grow in significance – for example, greater automation and autonomy of offensive cyberspace operations will increase their speed, reach and unforeseen effects – and the greater role of non-state actors and their increase in number may undermine stability in cyberspace. Overall, cyberspace in 2030 might be even more complex (when new technologies are introduced), and more integrated and interdependent with other operational domains. The attack surface will be larger. Understanding precise interactions between the cyber domain and other domains will remain a challenge.

## Shaping, Contesting and Fighting All-Domain

Today, the security environment is characterised by a lack of clear lines between peacetime, crisis and conflict, and a continuum of (strategic) competition from cooperation to armed conflict in all domains.[30] NATO has adopted new terminology to describe the lack of clear lines between the 20th-century warfighting phases, referred to as shaping, contesting, and fighting.[31] It is anticipated that future armed conflict will be fought by a joint and combined force across all domains. Researchers at the Atlantic Council suggest that the US and its allies need to develop new warfighting concepts that include all-domain sensing to 'rapidly aggregate, correlate, fuse, and analyse vast amounts of data', all-domain C2, and all-domain fires, including cyber effects and information operations.[32] As the future battlefield will be data-centric, networked, and fast-paced, the Allies must 'harness available data across all domains and deny the adversary the ability to do the same'.[33] Cognitive

28 For description of cyberspace as an operational environment, see *Joint Doctrine for Military Cyberspace Operations*, 1st edition A (Royal Danish Defence College, September 2019).

29 *Allied Joint Publication (AJP)-3.20, Allied Joint Doctrine for Cyberspace Operations*, Edition A Version 1 (UK Ministry of Defence Crown, January 2020), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf.

30 Clementine G. Starling, Tyson Wetzel, and Christian Trotti, 'Seizing the Advantage: A Vision for the Next US National Defense Strategy', 22 December 2021, Report, Atlantic Council, https://www.atlanticcouncil.org/content-series/atlantic-council-strategy-paper-series/seizing-the-advantage-a-vision-for-the-next-us-national-defense-strategy/, 21.

31 'The NATO Warfighting Capstone Concept'.

32 Starling, Wetzel, and Trotti, 'Seizing the Advantage', 48–49.

33 Ibid.

superiority could be attained only if the Allies' ability to use data for an improved understanding of threats will be greater than that of their authoritarian opponents.

Since a vast majority of cyberattacks take place below the threshold of the use of force (or armed attack) NATO should develop cyberattack response options for strategic cyberattacks that cumulatively require a joint response. It is anticipated that in 2030, NATO's focus should remain on the grey zone, hybrid campaign and below-the-threshold cyber activities.

In shaping and contesting phases during peacetime, deterrence and defence must be proactive. According to the Brussels Summit Communiqué, NATO considers 'possible collective responses to cyberattacks' and will impose costs in response to an attack.[34] These collective response options should include, in addition to diplomatic, political, and economic measures, also proportional counter-cyberattacks that will be run in accordance with international law and cyber norms.[35] Offensive and defensive cyberspace operations can be identical from a technical perspective (in the same way that software and tactics, techniques and procedures (TTP) can be dual use for defence and offence); what distinguishes defensive and offensive cyberspace operations are different targets and networks, cyber effects, executers, mandates, etc. Therefore, NATO nations should improve collective attribution capability (both classified and public attribution) by developing attribution procedures and sanctions regimes. Information and intelligence sharing must be improved for quick and confident attribution even though in some exceptional cases attribution is not necessary for a response.

Further, robust and comprehensive cyber capabilities are necessary for the armed forces to achieve strategic goals and perform military missions.[36] In 2030, the defensive and offensive cyberspace operations of NATO nations are likely to be run as joint multi-domain/all-domain operations through AI-enabled cross-domain C2.[37] Before the kinetic conflict begins, in a contesting phase, the NATO Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance, and Reconnaissance (C5ISR) and space assets will be the primary targets of adversaries. The cyber domain underpins and enables operations in other domains; C5ISR is intrinsic to cyberspace, and thus vulnerabilities, risks and threats from cyberspace migrate to C2. Open-source intelligence (OSINT), signal intelligence (SIGINT) and geospatial intelligence (GEOINT) rely largely on the cyber and space domains. Therefore, advances in cyber capabilities and TTPs are often driven by the intelligence community.

Cyber and EW threats (such as a shutdown of positioning, navigation, timing (PNT) systems, jamming, spoofing) could increase in the next ten years. This is predicated by the introduction of new technology and the larger cyberattack surface. The cyberattack surface is enlarging because armed forces use more and more commercial-off-the-shelf (COTS) software and hardware (rather than proprietary alternatives) and that can bring new risks compared to using custom code. COTS

34 Brussels Summit Communiqué.

35 NATO's measures to counter cyber threats include the full spectrum of tools – military and non-military. Traditional military and non-military instruments of state power can be used to deter cyberattacks, including diplomatic/political, military/intelligence, information, economic, financial, legal, and cyber. See Brussels Summit Communiqué.

36 'Cyber Strategic Outlook', United States Coast Guard.

37 Offensive cyberspace operations aim to create effects to achieve military objectives. *Cyber Commanders' Handbook* (Tallinn: NATO CCDCOE, 2020). These are distinguished from intelligence operations, whose goal is to collect information, although technically, these two types of operations may use the same intrusion methods.

software is generic, well-known and widely available, which makes it attractive for the attacker.[38] In addition, the number of cyber-physical systems integrated to the battlefield – for example, battlefield IoMT (sensors, robotics, etc.) and AI-enabled C5ISR – will be augmented.[39] The growing reliance of the armed forces on cyber-physical systems will render critical assessing and discovering cyber threats through hunting forward cyberspace operations.[40]

Given that cyberspace operations are fused with information operations, EW, SIGINT and space operations, and interact with operational activities in other domains, future research should consider how activities across domains interact with each other and what new vulnerabilities and risks are introduced in all-domain.

In summary, NATO needs to consider responses to the cyberattacks and cyber activities of its opponents, and develop its own comprehensive cyber capabilities in the context of shaping and contesting, as well as fighting, across all domains. It needs to identify and mitigate new vulnerabilities and risks emerging from interactions between increasingly integrated domains.

# EDTs Relevant to Cyberspace

In March 2020, NATO designated eight emerging and disruptive technologies (EDTs), which are currently in nascent stages of development or undergoing rapid development as major strategic disruptors over the next 20 years. These technologies include: data, AI, autonomy, space, hypersonics, quantum, biotechnology, and materials.[41] The EDTs most relevant to the cyber domain are autonomy, automation, AI, ML, deep neural networks, human-machine interaction (also known as human-computer interfacing or teaming), data analytics/data science, and quantum technologies (in particular, quantum computing, sensing, communications and quantum key distribution).[42] The complex interaction and combination of these technologies will have the greatest impact on the

38 'Security Considerations in Managing COTS Software', CISA, 14 December 2006, https://us-cert.cisa.gov/bsi/articles/best-practices/legacy-systems/security-considerations-in-managing-cots-software.

39 The electromagnetic spectrum (EMS) is not a part of cyberspace, but data and code can reside in or be transmitted through the EMS (e.g. wireless connections, radio waves). EW can be used to jam a wireless connection or very high frequency radio band. *Joint Doctrine for Military Cyberspace Operations*, Royal Danish Defence College.

40 'Cyber Strategic Outlook', United States Coast Guard.

41 'Science & Technology Trends 2020–2040. Exploring the S&T Edge', NATO Science & Technology Organization, March 2020, https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf. In addition to the abovementioned EDTs relevant to cyberspace, another study includes the following technologies that will impact cyber threats: computing power, data storage, sensors, 5G and next Gs, satellites, and space assets. Jacopo Bellasio and Erik Silfversten, 'The Impact of New and Emerging Technologies and the Cyber Threat Landscape and Their Implications for NATO', in *Cyber Threats and NATO 2030: Horizon Scanning and Analysis,* eds. Amy Ertan et al. (CCDCOE, 2020), 88–108.

42 Autonomy is a 'capacity of systems to decide by themselves on their course of action in uncertain and challenging environments without the help of human operators'. By contrast, automation is 'the aptitude of systems to perform set tasks according to set rules in environments where uncertainty is low and characterized'. Mauno Pihelgas, 'Automating Defences against Cyberspace Operations in Computer Networks', TalTech, 11 August 2021, https://digikogu.taltech.ee/et/Item/beb3e841-9c6e-4496-a73a-17148bc941ef, 189.

cyber threat landscape.[43] A recent study notes that EDTs 'are most disruptive at the boundaries of the physical, information and human domains', and the synergies and interdependencies (e.g. combination of autonomy, data analytics and AI, or combination of data and quantum technologies) are important in the development of future capabilities.[44]

EDTs are expected to facilitate the so-called revolution in military affairs and revolution in intelligence affairs – both are contested concepts in academic literature. Even without diving into conceptual discussions, a popular view is that EDTs will in the future affect the doctrinal thinking, and operational and organisational concepts of militaries. EDTs simultaneously create new opportunities and new vulnerabilities, risks and threats for the armed forces and defence sector. Some scholars even hold that in the future 'machines will become intelligence consumers, decision-makers, and even targets of other machine intelligence operations'.[45] This is not likely to happen in the next ten years, but human-machine interactions will become more widespread across diverse business sectors. Some experts hold that EDTs will have such a profound effect that they will change the characteristics or even nature of future warfare.[46]

According to some assessments, cyber threats have by today outpaced threats from the physical domain for the armed forces.[47] The future battlefield will be shaped by the interaction of technology with political, social, economic, environmental and other trends.[48] A NATO expert group recognised in a recent report that 'in the coming decade, EDTs will play an increasing role in the security environment'.[49] The authors of the report assert that the 2030 security environment will be characterised by the re-emergence of geostrategic and strategic completion, 'systemic rivalry and growing transboundary threats and risks'.[50] Great power competition, and geopolitical shaping and competition extends to the cyberspace, which is one area of human and nation-state activity and has been contested for decades. In 2030, military cyber organisations, forces and capabilities will be more mature than today and have broader authorities. Military cyber forces are currently gaining greater authority to run (jointly with the law enforcement and intelligence community) counter-cyberspace operations to curb cybercrime (e.g. ransomware attacks).[51] Military cyber forces are likely to employ AI-enabled defensive and offensive cyberspace operations and target the AI-systems of adversaries. The prospects of subverting AI-driven battlefield functions (e.g. by launching AI-poisoning attacks) will likely provide an incentive for attackers 'for operation in

43 For an in-depth overview of how these EDTs impact cyberspace, see Bellasio and Silfversten, 'The Impact of New and Emerging Technologies'. A full technology longlist is in 'Annex E: Horizon Scanning Technology Longlist', in Jacopo Bellasio et al., 'Innovative Technologies Shaping the 2040 Battlefield', Panel for the Future of Science and Technology EPRS, European Parliamentary Research Service, Scientific Foresight Unit (STOA), August 2021, https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690038/EPRS_STU(2021)690038_EN.pdf, 108–29.

44 'Science & Technology Trends 2020–2040'.

45 Anthony Vinci, 'The Coming Revolution in Intelligence Affairs', *Foreign Affairs*, 31 August 2020, https://www.foreignaffairs.com/articles/north-america/2020-08-31/coming-revolution-intelligence-affairs.

46 'NATO 2030: United for the New Era', NATO, 25 November 2020, https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf, 16–19.

47 'Cyber Strategic Outlook', United States Coast Guard, 5.

48 Bellasio et al., 'Innovative Technologies Shaping the 2040 Battlefield'.

49 'NATO 2030: United for the New Era', 16–19.

50 Ibid.

51 Erica Borghard and Lauren Zabierek, 'What is Cyber Command's Role in Combating Ransomware?' Lawfare, 18 August 2021, https://www.lawfareblog.com/what-cyber-commands-role-combating-ransomware.

cyberspace beyond in-domain effects and outcomes'.[52]

The NATO 2030 report also alerts that if adversaries gain a competitive advantage in EDTs, it 'would impede NATO's ability to win on the battlefield, challenge strategic stability and change the fundamentals of deterrence, but also offer state and even non-state actors, including eventually terrorists, the potential to threaten our societies from within'.[53] EDTs 'could undermine NATO's political cohesion by raising questions about technology sharing within the Alliance, impairing interoperability, and potentially fuelling dependencies on rival states'.[54] Therefore, to pre-empt these future challenges, NATO should develop a joint vision and strategies not only in regards to data and AI (NATO adopted policies in both of these areas in 2021) but also in other EDT fields, and for next generation telecommunications (5G and beyond). By 2030 non-standalone 5G networks will enable machine-to-machine communications, low latency, high speed, and reliability. This will facilitate the acquisition of IoMT, military robotics and autonomous systems. On the one hand, 5G networks are more secure and resilient than previous generations of telecommunication networks, but on the other, the attack surface will expand and the 5G architecture and the implementation of standards does not mitigate all risks.[55] By 2030, several NATO nations might deploy private and hybrid 5G networks for maintenance, logistics and training but possibly also to support kinetic operations in expeditionary operations.

## Autonomy and Human-Machine Teaming

In future warfighting, fast operational tempo, complexity and diversity of networks, quantity of friendly targets, intelligent autonomous agents of adversaries, and a scarcity of human defenders, among other factors, will make intelligent autonomous cyber defence agents necessary for NATO.[56] In 2019, NATO Research Task Group (RTG) IST-152 'Intelligent Autonomous Agents for Cyber Defence and Resilience' released a report that describes 'a reference architecture for intelligent software agents performing active, largely autonomous cyber defence actions on military networks of computing and communicating devices'.[57] An agent is defined as of software or hardware 'capable of deciding on its own about its course of action in uncertain, possibly adverse, environments'.[58] It is plausible that the authoritarian opponents of NATO will be able to employ autonomous agents for offensive cyberspace operations in 2030–2040. Therefore, NATO should increase support to scientific research in this area. It has previously been recommended that NATO should ensure innovation in the cyber domain, identify its requirements for technology development in cooperation with industry, and strengthen trust and interoperability across the Alliance.[59]

---

52 For a discussion of AI-augmented cyberattacks and cyber conflict as it relates to the military, see Christopher Whyte, 'Problems of Poison: New Paradigms and "Agreed" Competition in the Era of AI-Enabled Cyberspace Operations', in *12th International Conference on Cyber Conflict: 20/20 Vision: The Next Decade*, eds. T. Jančárková et al. (NATO CCDCOE, 2020), 226.

53 'NATO 2030: United for the New Era', 29.

54 Ibid.

55 For an overview of civilian 5G risks to military 5G, see Piret Pernik et al., 'Research Report Supply Chain and Network Security for Military 5G Networks', CCDCOE, October 2021, https://ccdcoe.org/library/publications/research-report-supply-chain-and-network-security-for-military-5g-networks/.

56 Alexander Kott et al., 'Initial Reference Architecture of an Intelligent Autonomous Agent for Cyber Defense Autonomous Intelligent Cyber-Defense Agent (AICA) Reference Architecture. Release 2.0', Army Research Laboratory, September 2019, https://uniss.org/news-events22/final-report-of-the-nato-ist-152-research-group-on-autonomous-agents-for-cyber-defense/.

57 Ibid.

58 Pihelgas, 'Automating Defences against Cyberspace Operations in Computer Networks', 199.

59 Bellasio and Silfversten, 'The Impact of New and Emerging Technologies'.

Autonomy might become one of the key drivers of change concerning cyberspace. This is illustrated by the fact that the US Army prioritises supporting scientific research in the area of autonomy (autonomous network defence and AI-based offensive cyberspace capabilities) and AI-enabled IoT networks, among other priority research areas.[60] Research in alternative technologies to replace the Global Positioning System (GPS), which is vulnerable to EW, simulation and modelling (displaying data from multiple sources to improve human decision-making) and AI for sensing the physical battlefield based on cyber signatures are also areas of novel research to the US Army.[61] Hence, in the short term, research into autonomy, AI-enabled sensing and IoT deserve more support from NATO nations and the NATO Science and Technology Organisation.

In the domain of ISR, 'autonomous sensors equipped with AI will be capable of generating on the ground aggregated, high-level information that can be more easily transmitted to command posts as they require much less bandwidth than raw data, also lowering the human workload needed to process high volumes of complex multi-source raw data'.[62] These technological advances would benefit NATO and authoritarian opponents alike.

Human-machine teaming could become a game changer for intelligence collection and information operations in the next decade. On the counter-intelligence side, advanced cyber threat intelligence (CTI) capacities could fuse data from many sources and human-machine interfaces could make that data better understandable to humans. Autonomous collection, aggregation and synthesis of data from sensors placed in cyberspace would free humans for other tasks that require cognition, such as gaming an adversary's strategy.[63] Combined with AI-enabled analytics, data sciences could create robust situational awareness.[64]

Previous literature suggests two implications for NATO strategic planners and policymakers regarding future EDTs. First, when the battlefield becomes AI-enabled, situational awareness could be untrustworthy because AI-systems used for data fusion are not robust enough, are not explainable to decision-makers, have a human bias or are based on poor data or deficient learning models. If situational awareness cannot be trusted, how valid will NATO strategic thinking and early warning be?

Second, NATO cyber domain strategic thinkers and planners should 'move beyond simple logic-of-the-domain characterizations of cyberspace affairs'.[65] This means they must have a comprehensive cross-domain understanding of interactions between different domains, and of the strategic motivations of key geopolitical nation-state adversaries. Friendly and adversary actions taken in the cyber domain will affect the processes and assets in other domains.

---

60 Andrew Eversden, 'Army Futures Command Outlines Next Five Years of AI Needs', C4ISRNET, 12 August 2021, https://www.c4isrnet.com/artificial-intelligence/2021/08/12/army-futures-command-outlines-next-five-years-of-ai-needs/.

61 Ibid.

62 Pihelgas, 'Automating Defences against Cyberspace Operations in Computer Networks', 190.

63 Chris Inglis, 'Illuminating the New Domain: The Role and Nature of Military Intelligence, Surveillance, and Reconnaissance in Cyberspace', in *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyberspace Operations*, eds. Herbert Lin and Amy Zegart (Brookings Institution Press, 2019).

64 Inglis, 'Illuminating the New Domain'.

65 Whyte, 'Problems of Poison', 232.

# Key Cyberspace Adversaries

In the next ten years, current trends concerning today's key cyberspace actors, main threat vectors, and EDTs are expected to continue or accelerate. Some threat vectors may unexpectedly gain greater prominence. Examples of such threat vectors are foreign election interference and ransomware that are today national security issues.

## Authoritarian Opponents and Violent Extremism

When it comes to the use of cyberspace in projecting national power, the basic assumptions of the US intelligence community assessment from 2021 are likely to apply for the next ten years. Per this assessment, nation states will continue to use cyberspace operations as a tool of national power. Nation states will run cyberspace operations to 'steal information, influence populations, and damage industry, including physical and digital critical infrastructure' and cooperate with non-state actors in cyber espionage, sabotage and pre-positioning for warfighting.[66] The authoritarian control of the internet and the surveillance of domestic populations and individuals located abroad will increase.[67] Moreover, China has recently expanded domestic surveillance programmes into multinational social media companies (Facebook and Twitter) targeting foreign journalists and academics.[68]

Prior research has established that in the last decade, nation-state cyberattacks have not been severe enough to reach the threshold of an armed attack. Some empirical data indicates that opponents prefer soft targets to hard ones. In 2020, only 2% and 13% respectively of Russia's and China's state cyberspace operations targets were in critical infrastructure sectors.[69] The strategic goals of the nation-state opponents of NATO are intelligence collection (cyber espionage) and theft of trade secrets, IP and data. Therefore, the effect of cyberattacks is annoyance and disruption rather than severe physical damage or disabling of another nation state.[70]

Of course, there are exceptions to this general rule – some cyberattacks attributed to nation states or their proxies have caused damage to physical infrastructure (e.g. Stuxnet) and disrupted critical services (e.g. WannaCry, NotPetya and a retaliatory cyberattack by Israel on infrastructure facilities in an Iranian port in May 2021).[71]

Major authoritarian opponents to democratic countries are China, Russia, North Korea, and Iran,

66 'Annual Threat Assessment of the US Intelligence Community', Office of the Director of National Intelligence, 9 April 2021, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf.

67 'Annual Threat Assessment of the US Intelligence Community'.

68 Adam Segal, 'Cyber Week in Review: January 7, 2022', Council on Foreign Relations, 7 January 2022, https://www.cfr.org/blog/cyber-week-review-january-7-2022?utm_source=blognotification&utm_medium=email&utm_campaign=Blog%20Post%20Notification%20Net%20Politics&utm_term=NetPolitics.

69 'Microsoft Digital Defense Report', Microsoft, October 2021, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi, 54.

70 Allison Pytlak and George E. Mitchell, 'Power, Rivalry and Cyber Conflict: An Empirical Analysis', in *Conflict in Cyber Space: Theoretical, Strategic and Legal Perspectives*, eds. J. Ringsmose and K. Friis, 1st ed. (Routledge, 2016), https://doi.org/10.4324/9781315669878.

71 Joby Warrick and Ellen Nakashima, 'Officials: Israel Linked to a Disruptive Cyberattack on Iranian Port Facility', *Washington Post*, 18 May 2021, https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html.

and violent extremism – often referred to as the four-plus-one.[72] In addition, cybercrime groups increasingly threaten the economies and societies of NATO nations, as mentioned earlier. More than 30 countries as well as the EU recently recognised 'that ransomware is an escalating global security threat with serious economic and security consequences' that 'poses a significant risk to critical infrastructure, essential services, public safety, consumer protection and privacy, and economic prosperity'.[73] It is difficult to predict what additional threat vectors will become national security issues in 2030. However, the cyber domain and information domain will become even more important theatres of digital battles. Some scholars believe that 'the capability to successfully undertake cyberspace operations may become as important a signifier of national power as nuclear weapons were during the Cold War'.[74] If that is true, Russia as a regional power is likely to prioritise investments in cyber and information operations capabilities.

Cooperation between authoritarian opponents is likely to increase. Should NATO engage in kinetic conflict with Russia, China could provide Russia disruptive cyberspace operations, or leverage its investments in infrastructure in Europe to aid Russia in times of crisis by shuttering down transportation or telecommunications.[75]

The role of non-state actors in state-orchestrated cyberattacks might also increase. Relying on proxies saves resources and creates confusion on who is responsible for cyberattacks. Currently, China and Russia leverage non-state actors (domestic and foreign research institutes and think tanks, domestic IT companies, cybercriminals and hacktivists) in cyber shaping, competition and fighting. Iran likewise supports various proxies (e.g. the Iranian Cyber Army).[76] Russian intelligence services will 'maintain an established and systematic relationship with criminal threat actors, either through association or recruitment'.[77]

## China and Russia: Innovating Strategic and Doctrinal Thinking, and Tactics

Advances in the doctrinal thinking of authoritarian opponents could strengthen their cyber power and cyber operational capabilities, and their intent to use cyber capabilities more frequently or against high-end targets may increase. This may cause competition in cyberspace to become fiercer and might decrease the stability of cyberspace, which would have a bearing on NATO cybersecurity and

72 The US Department of Defense adopted the '2+3' framework for great-power competition, which ranks China and Russia as primary threats while framing North Korea, Iran, and terrorism as secondary threats. See Arun Iyer, 'Recalculating the Math of Great-Power Competition', Atlantic Council, 2 April 2021, https://www.atlanticcouncil.org/blogs/new-atlanticist/recalculating-the-math-of-great-power-competition/.

73 'Joint Statement of the Ministers and Representatives from the Counter Ransomware Initiative Meeting October 2021', White House, 14 October 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021/.

74 Pytlak and Mitchell, 'Power, Rivalry and Cyber Conflict: An Empirical Analysis', 77.

75 'The China Plan: A Transatlantic Blueprint for Strategic Competition', Atlantic Council Scowcroft Center, March 2021, https://www.atlanticcouncil.org/in-depth-research-reports/report/china-plan-transatlantic-blueprint/, 79.

76 'Cyber Power—Tier Three: Cyber Capabilities and National Power; A Net Assessment', International Institute for Strategic Studies, 28 June 2021, https://www.iiss.org/blogs/research-paper/2021/06/cyber-power---tier-three; 'GEC Special Report: Pillars of Russia's Disinformation and Propaganda Ecosystem', U.S. Department of State, August 2021, https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf.

77 'Dark Covenant: Connections Between the Russian State and Criminal Actors', Recorder Future, Inskit Group, 9 September 2021, https://go.recordedfuture.com/hubfs/reports/cta-2021-0909.pdf.

cyber resiliency policies.

At the present, in addition to the US, the most advanced policies and doctrinal thinking concerning the cyberspace and information environment are exhibited by China and Russia.[78] If other NATO nations will not be able to innovate their strategic thinking to a similar degree, the balance of power in cyberspace could shift to authoritarian countries. It is possible that near-peer adversaries in cyberspace, namely China and Russia, might become in some areas of strategy and doctrine more advanced than the majority of NATO nations. For example, their influence operations, mass information control and mass surveillance strategies can be considered more sophisticated than those of democratic countries, and they are teaming up with criminal actors and other cyberspace proxies who help to attain the government's geopolitical objectives. China and Russia have the largest operational experience in using offensive cyber capabilities (perhaps larger than that of the US and Israel), which contributes to developing innovative strategies.

Some NATO countries consider that China is a 'systemic competitor' in cyberspace.[79] Similarly, in June 2021, NATO leaders noted that China's 'ambitions and assertive behaviour present systemic challenges to the rules-based international order and to areas relevant to Alliance security'.[80] The NATO 2030 expert group noted in the same vein that 'grave risks are posed by China in some critical sectors such as telecommunications, space, cyberspace, and new technologies, as well as disinformation campaigns'.[81] More worryingly, some studies indicate that China will join the US in the tier one of cyber powers in the near future.[82] At the same time, Western think tanks, universities and research institutions supporting NATO policies, including CCDCOE, do not amass a large body of knowledge on authoritarian opponents' cyber polices and operational capabilities. Clearly, studying the strategies and operational capabilities of China and Russia should be a focus area of their research agenda.

During the last decade, 2010–2020, China and Russia have pushed for greater control of cyberspace and technical isolation from the global internet, dubbed as cyberspace sovereignty. China and Russia lag behind the largest NATO nations in cybersecurity maturity levels but are considered world leaders in the control of national cyberspace. This relative autonomy could increase the cyber resiliency of their networks and protect against Western counter-cyberspace operations.[83] It has been argued that implementing domestic DNS will expose Russia to new risks and vulnerabilities, but in the overall balance of power, the greater cyberspace autonomy of Russia will favour her greater resilience.[84] Russia may use offensive cyber capabilities to disrupt the information on the internet by disabling global DNS and at the same time, ensuring continuity of domestic internet traffic through RuNet and domestic DNS. Undersea cables can also be destructed, which can halt the

78 'Cyber Capabilities and National Power: A Net Assessment', 10–11.

79 The UK government's national cyber strategy depicts China as the biggest driver impacting the UK's cybersecurity, but the same can be said about Russia and the NATO alliance as a whole. 'Policy Paper National Cyber Strategy 2022', Cabinet Office, 15 December 2021, https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022.

80 Brussels Summit Communiqué.

81 'NATO 2030: United for the New Era'.

82 'Cyber Capabilities and National Power: A Net Assessment', 10–11.

83 For Russia's isolation from the global internet and how it increases the country's resilience, see Juha Kukkola, 'The Russian National Segment of the Internet as a Source of Structural Cyber Asymmetry', in *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*, eds. Amy Ertan et al. (CCDCOE, 2020), 9–30.

84 Justin Sherman, 'Reassessing RuNet: Russian Internet Isolation and Implications for Russian Cyber Behaviour', Atlantic Council, 12 July 2021, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/reassessing-runet-russian-internet-isolation-and-implications-for-russian-cyber-behavior/.

bulk of internet traffic and cause societal chaos and economic loss outside Russia. Through greater domestic isolation and control, Russia's RuNet and domestic DNS initiatives, and the Chinese New IP proposal – which is believed to fragment the internet and render it 'less interoperable, less stable, and even less secure' – could decrease NATO nations' cybersecurity and the stability of cyberspace.[85]

If global telecom and other technology standards (including their security specifications) will be based on the Chinese technology model (which is China's strategic policy goal), equipment manufacturers and service providers in the West using those standards may be exposed to new risks, such as mass surveillance. For example, software produced by Chinese manufacturers (or maintained by non-Western service providers) and controlled by the Chinese state may be built in a way that enables installing backdoors for nation-state surveillance during software updates. Given that China is designated an authoritarian opponent, even when technical evidence about software backdoors is missing, adopting Chinese global standards may legitimise mass surveillance and government information control, and impair global internet freedom. If Chinese 5G technology (which many EU and NATO nations consider high risk and untrusted)[86] is used in the European commercial 5G network's core networks and critical functions, which support associated business verticals (such as smart harbours and warehouses, intelligent transportation systems (ITS), railroads), this technology could be used by malicious actors to interdict sensitive government and corporate information, and disrupt public services in societies.

Russia and China have expanded bilateral cooperation in AI-related research and investment, but the output so far remains relatively low.[87] In the future, Sino-Russian technological and scientific cooperation could accelerate the authoritarian control of global cyberspace (especially because less expensive Chinese surveillance technology is attractive to non-democratic countries) and dilute the effect of Western sanctions and export restrictions on Chinese technology.

## Targets of Nation-State Cyberspace Operations

The most common aim of the cyberspace operations of nation-state actors is cyber espionage (intelligence collection) and only in exceptional cases has there been the disruption or destruction of a target (e.g. some of Iran's cyberattacks against Israel) or monetary gain (e.g. North Korea).[88] The main targets of nation-state cyberspace operations have been foreign governments, non-governmental organisations, and think tanks, and more recently in 2021 also IT-service providers

85 Mark Montgomery and Theo Lebryk, 'China's Dystopian "New IP" Plan Shows Need for Renewed US Commitment to Internet Governance', Just Security, 13 April 2021, https://www.justsecurity.org/75741/chinas-dystopian-new-ip-plan-shows-need-for-renewed-us-commitment-to-internet-governance/.

86 Many NATO countries have already banned the use of non-EU or high-risk equipment in their 5G networks, and others are phasing out such products within a few years. The presence of Huawei equipment in telecommunication networks of NATO nations hosting US troops could, in the event of a crisis or conflict, undermine US capabilities for command and control and power projection, as well as create new security risks. Elsa B. Kania, 'Securing Our 5G Future: The Competitive Challenge and Considerations for U.S. Policy', 7 November 2019, Center for a New American Security, https://www.cnas.org/publications/reports/securing-our-5g-future. For risks associated with the Chinese technology, see, for example, Rush Doshi et al., 'China as a "Cyber Great Power". Beijing's Two Voices in Telecommunication', Brookings Institution, April 2021, https://www.brookings.edu/wp-content/uploads/2021/04/FP_20210405_china_cyber_power.pdf; 'National Security Implications of Fifth Generation (5G) Mobile Technologies', Congressional Research Service, 23 April 2021, https://fas.org/sgp/crs/natsec/IF11251.pdf.

87 Margarita Konaev et al., *Headline or Trend Line? Evaluating Chinese-Russian Collaboration in AI* (Issue Brief, Center for Security and Emerging Technology, August 2021), https://cset.georgetown.edu/publication/headline-or-trend-line/.

88 'Microsoft Digital Defense Report', October 2021, 52–53.

(e.g. supply chain attack SolarWinds/Solarigate and Microsoft Exchange Server vulnerability).[89] Common TTP in nation-state cyberspace operations are reconnaissance, credential harvesting, malware, and virtual private network (VPN) exploits.[90] According to a current assessment of US federal agencies, Chinese state-sponsored actors tend to exploit public vulnerabilities by consistently scanning their targets' networks, while using open-source and commercial penetration tools and virtual private servers (VPS) to hide their identity and evade detection.[91] It is likely that both Chinese and Russian state-sponsored actors might in the future incorporate AI-enhanced and automated TTP into their toolkits. According to a recent academic assessment, Russia possesses credible offensive cyber capabilities and has used them extensively but so far 'appears not to have given priority to developing the top-end surgical cyber capabilities needed for high-intensity warfare'.[92]

Besides cyberattacks, confidentiality, integrity, and availability of data and computer systems can be compromised through electromagnetic interference, notably through the shutdown of PNT, and jamming and spoofing, and identification of geolocation. Militaries consider the electromagnetic domain separate from the cyber domain, and the latter is often perceived as part of the broader information environment.[93] During peacetime, when transitioning operational headquarters and staff to a remote working mode due to COVID-19, NATO should not ignore threats from electromagnetic spectrum and operational security. In the initial period of war, EW will be used to supress broadcast (radio and TV) and online media (including social media) in order to delay information delivery to decision-makers.[94] A key task of Russian EW troops is to 'counter the enemy's advances in the information and telecommunications space'.[95] Before overt hostilities begin, both EW and cyberattacks can target satellites and their ground stations to prevent them from communicating and to deliver corrupted information or malware.[96] Notably, Russia's capability to interfere in the operation of the Global Positioning System (GPS) has been demonstrated repeatedly – for example, during NATO's Trident Juncture exercise – and the shutdown of navigation systems would achieve the adversaries' objectives.[97]

Russia considers space an operational domain, and military operations are likely to be run there in

89 Ibid.

90 Ibid.

91 The joint advisory lists procedures and TTPs of Chinese actors across the MITRE ATT&CK framework. See 'Chinese State-Sponsored Cyberspace Operations: Observed TTPs', National Security Agency, Cybersecurity and Infrastructure Security Agency (CISA), and Federal Bureau of Investigation (FBI), July 2021, https://media.defense.gov/2021/Jul/19/2002805003/-1/-1/1/CSA_CHINESE_STATE-SPONSORED_CYBER_TTPS.PDF.

92 'Cyber Power—Tier Two: Cyber Capabilities and National Power; A Net Assessment', International Institute for Strategic Studies, 28 June 2021, https://www.iiss.org/blogs/research-paper/2021/06/cyber-power---tier-two.

93 *Joint Doctrine for Military Cyberspace Operations*, Royal Danish Defence College. Other sources use concepts such as 'human domain', 'cognitive domain', and 'information domain'. In this paper, 'cyber domain' is used in the context of NATO missions and operations for the purposes of shaping, contesting, and fighting, that is, in continuum from peacetime to an armed conflict. 'Cyberspace', by contrast, refers to the uses of cyber domain outside military operational planning. 'Domain' is defined as 'the sphere of interest and influence in which activities, functions, and operations are undertaken to accomplish missions and exercise control over an opponent in order to achieve desired effects.' Patrick D. Allen, and Dennis P. Gilbert, 'Qualifying the Information Sphere as a Domain', *Journal of Information Warfare* 9, no. 3 (2010): 39–50, https://www.jstor.org/stable/26487457.

94 Keir Giles and Kim Hartmann, 'Adversary Targeting of Civilian Telecommunications Infrastructure', *13th International Conference on Cyber Conflict: Going Viral*, eds. T. Jančárková et al. (NATO CCDCOE, 2021).

95 Ibid.

96 Keir Giles, 'Missiles Are Not the Only Threat', in *Beyond Bursting Bubbles: Understanding the Full Spectrum of the Russian A2/AD Threat and Identifying Strategies for Counteraction*, FOI (Swedish Defence Research Agency), June 2020, https://www.foi.se/rest-api/report/FOI-R--4991--SE, 173–174.

97 Ibid.

the future.[98] Russia claims it has the ability to disrupt the provision of GPS in Northern Europe.[99] As mentioned earlier, Russian military thinkers discuss the goal of disrupting their adversary's military communication, PNT, ISR (which depend on GPS) prior to and in early phases of a kinetic conflict. Therefore, Russia is likely to develop operational concepts that will provide them the capability for disrupting space assets, on which NATO relies. In addition, the disruption of GPS could disrupt the provision of essential public services, such as transportation.[100] Future military logistics (transportation of military vehicles, vessels and other equipment) will likely rely on commercially provided services: smart railroads, smart harbours, ITS, which depend on GPS. For example, the US Coast Guard's military transportation system's operations today involve increased use of autonomous shipping, autonomous offshore platforms, and autonomous cargo facilities, and in the future, autonomous vessels will also be used.[101] The integration of autonomous systems will enlarge the cyberattack surface.

## Role of Non-state Actors

The role and influence of non-state actors in cyberspace, including multi-national corporations, is likely to increase when EDTs become easily accessed by a range of non-state actors.[102] NATO strategic thinkers should consider whether non-state actors could threaten the realisation of NATO's core tasks. Some assessments propose that nation states may lose their monopoly over EDTs to multinational corporations or cybercrime groups, and the proliferation of EDTs to a greater number of actors could alter interactions between nation states and non-state actors.[103]

Non-state actors are likely to continue stealing zero-day vulnerabilities from intelligence agencies and leak them publicly (e.g. the Shadow Brokers).[104] Software vulnerabilities that have been publicly disclosed will continue to be used by criminal groups. Ransomware attacks launched by various cybercrime groups are currently considered a national security issue, and have in some cases impaired public services and caused societal chaos (e.g. Colonial Pipeline).[105] The annual cost of intellectual property (IP) and trade theft in the US is $225–600 billion.[106] To counter this severe new threat, the US Cyber Command has taken on the role of protecting nations against ransomware

98 Giles and Hartmann, 'Adversary Targeting of Civilian Telecommunications Infrastructure'.

99 Ibid.

100 See ibid. for further discussion on the degradation of space-based systems.

101 'Cyber Strategic Outlook', United States Coast Guard.

102 Bellasio et al., 'Innovative Technologies Shaping the 2040 Battlefield', 10.

103 Ibid., 48.

104 'The Shadow Brokers Publishing the NSA Vulnerabilities (2016)', CCDCOE, 2016, https://cyberlaw.ccdcoe.org/wiki/The_Shadow_Brokers_publishing_the_NSA_vulnerabilities_(2016).

105 After a recent wave of ransomware attacks against US targets, US president Joe Biden declared that cybersecurity was a core national security challenge. Biden raised the issue a few times with Russian president Vladimir Putin, indicating 16 critical national infrastructure sectors that should not be attacked. Since then, there have been fewer high-profile attacks against the US, and there are also some signs of reduced activity on Russian-language cybercriminal online forums. US officials say that Russian authorities have not cooperated with them. Dustin Volz and David Uberti, 'Biden Says Cybersecurity Is the "Core National Security Challenge" at CEO Summit', *Wall Street Journal*, 25 August 2021, https://www.wsj.com/articles/biden-to-hold-cybersecurity-summit-with-tech-giants-top-banks-energy-firms-11629882002; Joseph S. Nye, 'US-Russian Cyber Stability Needs "Drunken Party" Approach: Limits, Deterrence and Communication', Russia Matters, 6 October 2021, https://russiamatters.org/analysis/us-russian-cyber-stability-needs-drunken-party-approach-limits-deterrence-and.

106 Marks, 'The Cybersecurity 202: Cybersecurity Pros Want to Stop Talking about a "Cyber 9/11"'.

attacks.[107] Likewise, the US Coast Guard will 'execute operations through the law enforcement and military spectrums to impose costs on criminal actors or nation-state adversaries'.[108] NATO nations have created joint task forces and working groups to tackle ransomware attacks. As mentioned, NATO recognised in 2021 that cumulative significant cyber activities could cause severe enough effects to trigger article 5 of the North Atlantic Treaty.[109] These reactions indicate that in the future non-state actors could pose even more significant national security threats (e.g. when they employ automated and AI-enabled tools). It is possible that in addition to criminal groups, violent extremists may gain access through digital black markets to advanced AI-enabled cyberattack tools, which could be used for extortion. It is also possible that lone individuals affiliated with violent extremist ideologies (e.g. individuals with Western STEM education who were born in Europe and support ISIL/ISIS and Al-Qaida's ideology) will target the civilians and governments of NATO countries for extortion purposes. Malicious insiders controlled by foreign governments could in certain cases also cause severe damage, especially through manipulating CIS and telecommunications supply chains. However, individuals (lone hackers) are not likely to have enough skills and resources to gravely endanger NATO through cyberspace.

As mentioned, China and Russia cooperate with a wide array of diverse proxies (e.g. cybercrime groups, research institutions, think tanks, private IT companies) in order to gain access to foreign computer networks for the purposes of intelligence collection, and they outsource government-sponsored surveillance, influence and information operations. In China and Russia, the roles and operational activities of intelligence and non-state actors are intermingled. The actors tend to use the same cyber infrastructure and TTP for legitimate and malicious purposes, which complicates the attribution of attacks. Even today, intelligence and influence operations are being sold as a service on digital black markets. Commercial surveillance and intrusion software may also be used by criminal groups for cyberattack purposes, which will complicate attributing attacks to perpetrators (today mostly governments use them). The role of private sector IT companies in supporting authoritarian surveillance efforts has increased. In the future, this trend may accelerate.

# Other Drivers of Change in Cyberspace

## Information Operations

In order to address foreign disinformation operations and hybrid threats, the NATO 2030 expert group advises the Alliance to develop capabilities 'to detect disinformation and provide support in preventing or limiting its impact, including by better understanding people, networks, online information, and related narratives' and 'establish the legal and ethical framework to be able to effectively and legitimately operate in these dimensions'.[110] In the future, influence and information

107 Joseph Marks, 'The Cybersecurity 202: Analysis. Still No Signs of Russian Cooperation on Ransomware', *Washington Post*, 14 September 2021, https://www.washingtonpost.com/politics/2021/09/15/still-no-signs-russian-cooperation-ransomware/; 'Dark Covenant: Connections Between the Russian State and Criminal Actors'; Erica Borghard and Lauren Zabierek, 'What Is Cyber Command's Role in Combating Ransomware?' Lawfare, 18 August 2021, https://www.lawfareblog.com/what-cyber-commands-role-combating-ransomware. 'Cyber Strategic Outlook', United States Coast Guard, 7.

108 Ibid.

109 Brussels Summit Communiqué.

110 'NATO 2030: United for the New Era', 46.

operations are likely to become enhanced by data analytics, automation and ML applications, which will complicate defence. Automated social media bots and deep fakes (synthetic audio, video, and images) have become a reality but have not had the devastating impact on societies that some experts in the past warned about. It is possible that a major feature of information warfare in the new decade will be AI-enabled automation, which could be used to generate instant responses to events.[111] Accordingly, 'an intelligent information warfare campaign should be able to identify rising interest in a relevant topic (such as the popularity of a specific individual or action) and generate a coordinated automatic response to leverage the interest. Response patterns could include producing counter-arguments, fake news, "trolling" or cheap propaganda'.[112] At the same time, crowdsourcing OSINT to more non-state actors (such as Bellincat) would increase detection of malicious actors and harness resiliency of the cognitive domain.

## International Law and Norms

The cyberspace operations of NATO nations are naturally predicated by obligations under international law applicable to cyberspace, voluntary cyber norms and confidence-building measures. Therefore, NATO strategic planners must factor in how national and international legal frameworks would limit or enable offensive cyberspace operations. In the ten-year outlook, a larger set of voluntary cyber norms than exist today are likely to be agreed upon and their implementation is also likely to remain poor. In 2019, CCDCOE legal experts identified key issues for international law in cyberspace, predicting that by 2024, nation states will not agree on whether a new cyber treaty instrument is needed.[113] Similarly, Joseph Nye believes that the conclusion of a treaty is unlikely but nation states might agree on limits regarding the extent and type of cyber espionage and interventions in other's domestic political processes.[114] It is possible that new legal arrangements will be concluded regarding cybercrime and cyber espionage; however, at the moment binding treaties do not seem likely. It is more likely that great cyber powers will continue to exhibit self-restraint to avoid escalation and, as a rule, not target critical high-end targets (such as nuclear command and control). Like-minded nations are likely to publicly attribute more and more cyberattacks to foreign governments, individuals, and organisations. However, measures like naming and shaming, travel bans, economic sanctions, and indictments will continue to fall short in stopping or decreasing the number and severity of low-end cyberattacks.

In a worst-case scenario, authoritarian opponents could instigate in their sphere of influence a regionally binding treaty. A treaty proposal submitted by Russia in July 2021 to the UN's ad hoc committee tasked with drafting a new cybercrime convention proposes to criminalise what it calls 'acts of terrorism and extremism in cyberspace', which may be used by authoritarian countries against domestic political opposition, journalists, human rights activist, etc.[115] Legal instruments designed by authoritarian opponents could legitimise government control over information and

111 Kim Hartmann and Keir Giles, 'The Next Generation of Cyber-Enabled Information Warfare', in *12th International Conference on Cyber Conflict: 20/20 Vision; The Next Decade*, eds. T. Jančárková et al. (NATO CCDCOE, 2020), 226.

112 Hartmann and Giles, 'The Next Generation of Cyber-Enabled Information Warfare'.

113 For future trends in developments of international law, see *Trends in International Law for Cyberspace*, ed. Kadri Kaska (CCDCOE, May 2019), https://ccdcoe.org/library/publications/trends-in-international-law-for-cyberspace/.

114 Joseph S. Nye, 'US-Russian Cyber Stability Needs "Drunken Party" Approach: Limits, Deterrence and Communication', Russia Matters, 6 October 2021, https://russiamatters.org/analysis/us-russian-cyber-stability-needs-drunken-party-approach-limits-deterrence-and.

115 'United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes', 29 July 2021, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_E.pdf.

internet infrastructure regionally. Some sources forecast the emergence of a distinct Chinese model of multilateral (versus multistakeholder) internet governance, in which 'stakeholders may choose a combination of views across different sub-topics'.[116] Instead of the European Union's general data protection directive (GDPR), China's privacy law could become a regional model in some African countries.[117] It is possible that unlimited access to online information could become severely limited in Africa and ASEAN countries as well.

## NATO's Cohesion and Interoperability

At present, NATO nations diverge in regard to their cyber policy goals and the ways and means to achieve these goals, which according to some scholars can cause tension between the Allies, in particular regarding the necessity and legitimacy of operating on each other's national computer systems and networks.[118] There are different opinions among the Allies on how the international law applies to cyberspace. The Netherlands and France consider that state sovereignty is a rule, but the UK 'has taken the position that a remote cyber operation by one state into another's cyber systems or network does not violate the latter's sovereignty'.[119]

If NATO nations interpret the rules and principles of international law (e.g. the law of state neutrality) differently, this can indeed also cause tension between the Allies. For example, when the Allies use the Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA) mechanism (in the context of a North Atlantic Council approved NATO mission or operation), and cause cyber effects (such as physical destruction of an adversary's C2 server) under the jurisdiction of another Allied nation, should that nation be warned before the operation is executed? Such a warning could jeopardise achieving the mission goals and disclose sensitive information. In regard to cyber threat hunting operations outside national networks, which support NATO operations and are coordinated by Cyberspace Operations Centre, more clarity is needed under what conditions threat hunting operations can be run under the SCEPVA mechanism.

When NATO nations have conflicting understandings on how international law applies to cyberspace, the implementation of NATO's comprehensive cyber defence policy might be challenging. Given that some nations are at present on a different cyber policy path, if that trend accelerates, NATO's cohesion, and collaterally, deterrence and defence could suffer. At the same time, the authoritarian block (China, Russia, Iran, North Korea, etc.) may successfully improve their cyber resilience through ever greater state sovereignty and control over the information and infrastructure of the internet. This may shift the global balance of power in the area of internet governance, in particular when developing countries become more dependent on China's technology and standards.

Future developments concerning international law applicable to cyberspace, voluntary cyber norms and confidence building measures (CBMs) are likely to impact the current constellation of nation-state power cyberspace. NATO's next Strategic Concept, which is expected to be approved in summer 2022, should set a level playing field for NATO cyberspace operations, and underscore

116 *Trends in International Law for Cyberspace*, ed. Kaska.

117 Josh Horwitz, 'China Passes New Personal Data Privacy Law, to Take Effect Nov. 1', Reuters, 20 August 2021, https://www.reuters.com/world/china/china-passes-new-personal-data-privacy-law-take-effect-nov-1-2021-08-20/.

118 Max Smeets, 'NATO Allies' Offensive Cyber Policy: A Growing Divide?' The Hague Centre for Strategic Studies, 6 August 2021, https://hcss.nl/report/nato-allies-offensive-cyber-policy-a-growing-divide/.

119 Ibid.

the criticality of the cyber domain for realising NATO's core tasks – deterrence and defence. The Strategic Concept needs to address how NATO will operate in cyber and cognitive domains, and encounters hybrid and grey zone threats. The concept should address opportunities and challenges emerging from EDTs and their synergies, interdependencies and interactions across domains, and implications for shaping, contesting and fighting in the cyber domain.

# Conclusions and Future Research

## Positive and Negative Scenarios

In a negative future scenario, geopolitical competition and systemic rivalry is likely to intensify until 2030. Achieving superiority in cyberspace for a single country may not be a realistic goal. Russia and China may become more autonomous of the global internet infrastructure, which may decrease the stability of cyberspace. In this world, foreign intelligence agencies and military cyber forces could run technologically more advanced cyberspace operations against higher-end targets. Cyberspace operations against NATO are expected to intensify in the new decade. Authoritarian nation states will most definitely innovate their strategies, policy and TTP. The scale and impact of autonomous operations is almost certainly likely to increase (some warn that autonomous operations may become primary cyber actors in a future cyber conflict).[120]

In a positive future scenario, nation states will be able to agree to protect the public core of the internet, including the global DNS.[121] In case democratic and authoritarian countries are able to agree on the basic 'rules of the road', the cyber diplomacy and capacity building efforts of NATO nations will improve the global stability of cyberspace, and joint Allied efforts will keep cybercrime actors at bay, the future of cyberspace could be more stable and secure.

In any case, NATO should prepare to defend and protect in and through cyberspace in the era when Western countries could lose their technological edge to authoritarian opponents, and internet governance may become more multilateral than multistakeholder. Given the threat of the cyberspace operations of autonomous adversaries, NATO should increase R&D and investments in the development of their own autonomous cyber defence agents who 'stealthily patrol the networks, detect enemy agents while remaining concealed, and then destroy or degrade the enemy malware'.[122]

Implementing the recommendations of the NATO 2030 expert group regarding EDTs, and countering hybrid and cyber threats would support NATO's deterrence and defence. In addition, NATO should commission more social science research into operational concepts, and strategy, policy and doctrinal innovations of key adversaries. It is difficult to predict whether the advances in EDTs and cyberspace capabilities reviewed in this paper would increase the authoritarian opponents' cyber power so that Western countries lose their dominant positions globally.

---

120 Mauno Pihelgas, 'Automating Defences against Cyberspace Operations in Computer Networks', TalTech, 11 August 2021, https://digikogu.taltech.ee/et/Item/beb3e841-9c6e-4496-a73a-17148bc941ef, 184.

121 In November 2017, the Global Commission on the Stability of Cyberspace (GCSC) issued a 'Call to Protect the Public Core of the Internet'. 'Call to Protect the Public Core of the Internet', Global Commission on the Stability of Cyberspace, 21 November 2017, https://cyberstability.org/research/call-to-protect/.

122 Stanislav Abaimov and Maurizio Martellini, *Cyber Arms: Security in Cyberspace*, 1st ed. (Boca Raton: CRC Press, 2020), https://doi.org/10.1201/9780367853860.

Further research is needed to understand the interaction between all domains, and their strategic and policy implications for NATO. Future research should identify how technological advances will impact cyber power, and would that increase or decrease stability. For instance, should authoritarian opponents acquire a leading position in AI, quantum information sciences, space operations, and other key technologies and operational domains, how would these developments affect the current global cyber power balance between the democratic and authoritarian blocks? There are many known unknowns that require further elaboration and analysis.

Future research should employ both qualitative and semiquantitative methods, future thinking, foresight and horizon scanning tools, and construct several alternative paths. NATO should discuss on a regular basis the nature and implications of EDTs, adversaries' innovations in strategic and doctrinal thinking, and developments in other domains (especially EW and intelligence, information operations, as well as law and ethical issues). The opportunities for innovation and transformation should be better scrutinised and challenges to them better understood and addressed. To that end, NATO nations should continue supporting future thinking and cyberspace horizon scanning research and events, including those conducted by academia and think tanks.

This paper illustrated that the strategic outlook for 2030 cyberspace should consider not only the characteristics of cyberspace and the threat landscape, but the broader geopolitical, technological, socio-political and socio-economic developments and trends, as well as identify key drivers of change. Global trends in other domains of human interaction are likely to profoundly affect the cyber domain. NATO needs to broaden its understanding of interactions and interdependencies between the domains, and how the growing complexity of all-domain may lead to greater systemic security risks.

## Future Research Avenues

Future research should identify game changers and key drivers in cyberspace in 2030. It should focus on the implications for NATO across the following main categories:

→ **The (All-Domain) Operational Environment**
- How will AI-enabled multi-domain warfighting concepts and doctrines impact the cyber domain and cyber capabilities?
- What are the interactions and dependencies between domains and how do they affect shaping, competing and fighting in all-domain and the cyber domain?

→ **EDTs**
- How will innovations in adversaries' EDTs and strategic and doctrinal thinking (e.g. the Chinese concept of military-civil fusion) impact global cyber power?[123]
- How will innovations in intelligence collection and information operations change shaping, contesting and fighting in all-domain and the cyber domain?
- How will EDTs impact NATO's deterrence and defence?

→ **International Law and Norms**
- How will the development of international law, cyber norms, CBMs, technology standards (including 5G and 6G, IoT, AI, etc.) impact the cyber power of countries and the stability of cyberspace?

123 'Cyber Power—Tier Two'.

Chapter 6

# NATO Cyber Policies in Relation to the International Stability Framework

**Lieutenant Colonel Berend Valk**
Researcher
CCDCOE

## Abstract

This paper describes the additional layer of understanding that the 2021 United Nations Group of Governmental Experts (GGE) report offers on how international law applies to the use of information and telecommunication technologies (ICTs) by states. It outlines the elements of the international framework for security and stability and examines the normative environment for NATO and Allies. It also describes NATO's possible role in the process of setting international norms. The paper further describes how NATO policies evolved as the result of a dynamic cyber threat landscape. It closes by considering NATO's possible actions when confronted with cyberspace operations that fall below the threshold of an armed attack and with those that reach that threshold. It considers the use of Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA) in supporting NATO's collective defence and its operations and missions.

**Keywords:** *Sovereign Cyber Effects Provided Voluntarily by Allies, United Nations Group of Governmental Experts, United Nations Open-Ended Working Group, confidence-building measures, NATO policies*

# Introduction

In the 2021 Brussels Summit Communiqué, the heads of state and government stated that NATO members are increasingly being confronted by cyber, hybrid, and other asymmetric threats, including disinformation campaigns, and by the malicious use of ever-more-sophisticated emerging and disruptive technologies.[1] Cyber threats to the security of the Alliance are complex, destructive, coercive, and increasingly frequent.[2] The United Nations (UN) General Assembly (GA) noted that states are increasingly concerned about the implications of the malicious use of information and telecommunication technologies (ICTs) for the maintenance of international peace and security and subsequently for human rights and development.[3] Global cyber threats seem to threaten the international framework for security and stability, the core of which has been recognised by the UN GA in endorsing the consensus reports of the UN Group of Governmental Experts (GGE) in 2010,[4] 2013,[5] and 2015.[6] The latest report noted that a common understanding on how international law applies to state use of ICTs is important for an open, secure, stable, and accessible ICT environment.

Based on the 2021 UN GGE report,[7] this paper describes the additional layer of understanding that the 2021 GGE offers on how international law applies to the use of ICTs by states. It outlines the elements of the international framework for security and stability and examines the normative environment for NATO and Allies. It also describes NATO's possible role in the process of setting international norms. The paper further describes how NATO policies evolved as the result of an ever-evolving cyber threat landscape. It closes by considering NATO's possible actions when confronted with cyber operations that are under the threshold of an armed attack or those that reach the threshold, including the use of Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA), in collective defence and Alliance operations and missions. Finally, it provides some conclusions on NATO's policies in an ever-evolving cyber threat landscape.

# International Stability Framework

In the consensus reports of the GGE in 2013 and 2015, the elements of the 'international framework for security and stability' are described. These reports, which are cumulative in nature,[8] examined

1 Brussels Summit Communiqué Issued by the Heads of State and Government Participating in the 2021 Summit in Brussels, paragraph 3, issued 14 June 2021, https://www.nato.int/cps/en/natohq/news_185000.htm.

2 Ibid., paragraph 32.

3 Conference Room Paper A/AC.290/2021/CRP.2, 1 March 2021, https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

4 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/65/20, 30 July 2010, https://undocs.org/A/65/201.

5 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98, 24 June 2013, https://undocs.org/A/68/98.

6 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/17, 22 July 2015, https://undocs.org/A/70/174.

7 Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, A/76/135, 14 July 2021, section 4, https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf.

8 Conference Room Paper A/AC.290/2021/CRP.2, 1 March 2021, paragraph 7, https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

existing and potential threats arising from the use of ICTs by states. The reports also considered actions to address those threats, including the applicability of existing international law, voluntary and non-binding norms of responsible state behaviour, confidence-building, and capacity-building between states. This chapter will first describe the 2021 GGE assessment on the applicability of international law and the additional layer of understanding that the 2021 GGE offers on how international law applies to the use of ICTs by states. It describes the elements of the international framework for security and stability and the implications for NATO as a political military alliance. It will also describe the role of NATO in the process of creating international norms.

## Applicability of Existing International Law

The world of ICTs is a dynamic one. New technologies develop quickly, creating new possibilities but also new threats. It is internationally recognised that international law[9] is applicable in cyberspace, but there are still many unanswered questions concerning precisely how to apply it.[10]

The recently concluded UN cyber norms processes shed further light on that. The GGE, established pursuant to UN GA resolution 73/266,[11] adopted its report by consensus on 28 May 2021; its sister format, the Open-Ended Working Group (OEWG), concluded its work in March 2021.[12] In its 2021 report, the GGE reaffirms the previous assessments and recommendations of the GGE and OEWG on international law and offers an additional layer of understanding to the 2015 GGE report's assessments and recommendations of how international law applies to the use of ICTs by states (hereafter the '2021 report').[13] The 2021 report notes that in accordance with Article 2(3) and Chapter 6 of the UN Charter, any dispute between states, including those involving ICTs, should be solved in a peaceful way.[14] It furthermore reaffirms that state sovereignty and international norms and principles that flow from sovereignty apply to the conduct by states of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory.[15] The 2021 report further reaffirms that states, in accordance with the principle of non-intervention, must not intervene directly or indirectly

9 International law arises from international treaties and international custom (customary international law) and is supplemented by state practice and *opinio juris*. The political norms known as 'soft law' are not binding on states, but they have political relevance, and states subscribing to them will generally respect them.

10 The letter from the minister of foreign affairs to the president of the House of Representatives on the international legal order in cyberspace of 5 July 2019 describes this very well: 'As the government has indicated on multiple occasions and consistently argues, international law is applicable in cyberspace. This is also recognised internationally. Nevertheless, there are still many unanswered questions concerning the precise manner in which international law should be applied in cyberspace. This is due to the unique characteristics of the digital world in comparison with the physical world. Digital data generally moves rapidly and is therefore often difficult to localise. It can be transferred to another country in a matter of seconds, and can be stored across a range of different countries. What is more, undesirable activity in cyberspace does not necessarily always have an immediate physical impact, even though its effects may nonetheless be serious. It is not yet entirely clear how these and other unique characteristics should be dealt with in the application of international law. The government is encouraging international debate on ways to clarify the application of international law in cyberspace. Clarity and consensus on these points are essential to the international legal order.' https://www.government.nl/binaries/government/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace/International+Law+in+the+Cyberdomain+-+Netherlands.pdf.

11 UN GA Resolution 73/266, 2 January 2019, https://undocs.org/A/RES/73/266.

12 Conference room paper A/AC.290/2021/CRP.2, 1 March 2021, https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

13 Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, A/76/135, 14 July 2021, section 4, https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf.

14 Ibid., paragraph 71 (a).

15 Ibid., paragraph 71 (b).

in the internal affairs of another state, including by means of ICTs.[16] As for the threat of the use of force, the 2021 report mentions that states should refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state or in any other manner inconsistent with the purposes of the UN.[17] The principle of the peaceful use of ICTs is underscored, but the 2021 report notes the inherent right of states to take measures consistent with international law and as recognised in the UN Charter and the need for continued study on this matter.[18] As for international humanitarian law, the 2021 report notes that it applies only in situations of armed conflict and recalls the principles of humanity, necessity, proportionality, and distinction. However, it also recognises the need for further study on how and when these principles apply to the use of ICTs by states.[19] Finally, the 2021 report reaffirms that states must meet their international obligations regarding internationally wrongful acts attributable to them under international law. States should not use proxies to commit internationally wrongful acts and should ensure that their territory is not used by non-state actors to commit such acts. It recalls the importance of attribution and that accusations should be substantiated. The mere fact that an ICT activity was launched or otherwise originated from the territory or infrastructure of a state may be insufficient in itself to attribute the activity to that state.[20]

As stated in the Brussels Summit Communiqué, international organisations like NATO 'recognise that the impact of significant malicious cumulative cyber activities might, in certain circumstances, be considered as amounting to an armed attack[21] and 'remain committed to act in accordance with international law, including the UN Charter, international humanitarian law, and international human rights law as applicable'.[22]The European Commission states, 'The EU continues to work with international partners to advance and promote a global, open, stable and secure cyberspace where international law, in particular the United Nations (UN) Charter, is respected, and the voluntary non-binding norms, rules and principles of responsible state behaviour are adhered to.'[23] The above statements acknowledge that international law applies in cyberspace. NATO adopted an enhanced cyber defence policy and action plan that was endorsed by the Allies at the Wales Summit in September 2014. The policy recognised that international law, including international humanitarian law and the UN Charter, applies in cyberspace and that the North Atlantic Council would decide on a case-by-case basis as to when a cyberattack would lead to the invocation of Article 5.[24] In 2016, NATO recognised cyberspace as a domain of operations[25] and adopted the Cyber Defence Pledge.[26] In 2018, NATO nations agreed on how to integrate Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA) into Alliance operations and missions.[27] In the 2021 comprehensive cyber defence policy, NATO states that 'it is determined to employ the full range of capabilities at

16 Ibid., paragraph 71 (c).

17 Ibid., paragraph 71 (d).

18 Ibid., paragraph 71 (e).

19 Ibid., paragraph 71 (f).

20 Ibid., paragraph 71 (g).

21 Brussels Summit Communiqué, paragraph 32, issued 14 June 2021.

22 Ibid.

23 'The EU's Cybersecurity Strategy for the Digital Decade', 16 December 2020, p. 20, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020JC0018&from=EN.

24 Wales Summit Declaration Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Wales, 5 September 2014, http://www.nato.int/cps/en/natohq/official_texts_112964.htm#cyber.

25 Warsaw Summit Communiqué Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Warsaw, 9 July 2016, http://www.nato.int/cps/en/natohq/official_texts_133169.htm#cyber.

26 Cyber Defence Pledge, 8 July 2016, https://www.nato.int/cps/en/natohq/official_texts_133177.htm.

27 Brussels Summit Declaration, 11 July 2018, https://www.nato.int/cps/en/natohq/official_texts_156624.htm#20.

all times to actively deter, defend against, and counter the full spectrum of cyber threats, including those conducted as part of hybrid campaigns'.[28] In all of these statements, as well as in doctrines like Allied Joint Publication-3.20,[29] this point of view is reiterated.

How would states apply international law if it is applicable? In accordance with the GGE's mandate, an official compendium of voluntary national contributions on the subject of how international law applies to the use of ICTs by states was published.[30] While the compendium only presents the views of states who participated, such views give a good insight into the positions of states and how they view their rights, duties, and responsibilities. Furthermore, the view of a state on international law can be found in individual documents or statements. As an example, states generally recognise state sovereignty in cyberspace, but different states may attach different meanings to the notion. France stated that 'any cyberattack against French digital systems or any effects produced on French territory by digital means by a state organ, a person or an entity exercising elements of governmental authority or by a person or persons acting on the instructions of or under the direction or control of a state constitutes a breach of sovereignty'.[31]

The position of the United Kingdom in this is that,

> Sovereignty, as a general principle, is a fundamental concept in international law. The United Kingdom recalls that any prohibition on the activities of States[,] whether in relation to cyberspace or other matters, must be clearly established either in customary international law or in a treaty binding upon the States concerned. The United Kingdom does not consider that the general concept of sovereignty by itself provides a sufficient or clear basis for extrapolating a specific rule or additional prohibition for cyber conduct going beyond that of non-intervention referred to above. At the same time, the United Kingdom notes that differing viewpoints on such issues should not prevent States from assessing whether particular situations amount to internationally wrongful acts and arriving at common conclusions on such matters.[32]

In a letter to the UN secretary-general, the permanent representatives of China, the Russian Federation, Tajikistan, and Uzbekistan[33] presented a draft international code of conduct for information security. A state adapting the code would voluntarily subscribe to the code pledges, one of them being as follows:

> To comply with the Charter of the United Nations and universally recognized norms governing international relations that enshrine, inter alia, respect for the sovereignty, territorial integrity and

28 Brussels Summit Communiqué, paragraph 32, issued 14 June 2021.

29 Allied Joint Publication-3.20, Allied Joint Doctrine for Cyberspace Operations, Edition A, Version, 1 January 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf.

30 Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States Submitted by Participating Governmental Experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security Established Pursuant to General Assembly Resolution 73/266, A/76/136, 13 July 2021, https://front.un-arm.org/wp-content/uploads/2021/08/A-76-136-EN.pdf.

31 Ministry of Defence of France, International Law Applied to Operations in Cyberspace, 9 September 2019, https://cyberlaw.ccdcoe.org/wiki/Sovereignty#cite_note-42.

32 United Kingdom Foreign Commonwealth & Development Office, Application of International Law to States' Conduct in Cyberspace: UK Statement, 3 June 2021, https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement.

33 Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations addressed to the Secretary-General, A/66/359, https://undocs.org/A/66/359.

> political independence of all states, respect for human rights and fundamental freedoms and respect for the diversity of history, culture and social systems of all countries.[34]

States would further 'reaffirm all the rights and responsibilities of states to protect, in accordance with relevant laws and regulations, their information space and critical information infrastructure from threats, disturbance, attack and sabotage'.[35] The view of Russia on information security 'goes beyond concerns regarding the security of information and communication technologies systems and also includes the regulation of information or content flows'.[36]

In a 2011 Russian proposal for a draft convention on international information security, information security is defined as 'a state in which personal interests, society, and the government are protected against the threat of destructive actions and other negative actions in the information space'.[37] Russia's reply to the invitation of the UN General Assembly to states to give their view on information security[38] said, 'States shall strive to restrict threats in the field of international information security.'[39] The same reply defined threats as 'the use of information to undermine the political, economic and social system of other states, or to engage in the psychological manipulation of a population in order to destabilize society',[40] 'the transboundary dissemination of information in contravention of the principles and norms of international law and of the domestic legislation of specific countries',[41] and 'the manipulation of information flows, disinformation and the concealment of information in order to corrupt the psychological and spiritual environment of society, and erode traditional cultural, moral, ethical and aesthetic values'.[42]

This view of Russia on information security shows that it goes beyond concerns regarding the security of ICT systems and also includes the regulation of information or content flows. In the 2011 draft international code of conduct, Russia mentions the 'rights and freedom to search for, acquire and disseminate information on the premise of complying with relevant national laws and regulations'.[43] Together with its views on sovereignty[44] and non-intervention,[45] Russia uses this to regulate the use of information and content flows, for example, by blocking certain websites on the internet; all this is based on the premise of complying with relevant national laws and regulations.

NATO's position is that it 'will promote a free, open, peaceful, and secure cyberspace, and further pursue efforts to enhance stability and reduce the risk of conflict by supporting international law and voluntary norms of responsible state behaviour in cyberspace'.[46] It is therefore in NATO's and

---

34 Ibid., p. 4 (a).

35 Ibid., p. 4 (c).

36 Elaine Korzak, 'Russia's Cyber Policy Efforts in the United Nations', Tallinn Paper no. 11, 2021, https://ccdcoe.org/uploads/2021/06/Elaine_Korzak_Russia_UN.docx.pdf.

37 'Convention on International Information Security', 2011, https://carnegieendowment.org/files/RUSSIAN-DRAFT-CONVENTION-ON-INTERNATIONAL-INFORMATION-SECURITY.pdf.

38 United Nations General Assembly, 'Developments in the Field of Information and Telecommunications in the Context of International Security: Report of the Secretary-General', A/55/140, 10 July 2000, https://undocs.org/A/55/140.

39 Ibid., p. 5.

40 Ibid., (c), p. 5.

41 Ibid., (i), p. 5.

42 Ibid., (k), p. 5.

43 Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations addressed to the Secretary-General, A/66/359, https://undocs.org/A/66/359.

44 Ibid., p. 4.

45 See, for example, the Russian submission in Report of the Secretary-General, A/55/140, p. 4.

46 Brussels Summit Communiqué, paragraph 32, issued 14 June 2021.

Allies' interest to be proactive in this process rather than merely observe it. Not acting could result in Russia taking the initiative, such as by passing resolutions on a binding universal convention on international information security that could win over the undecided countries. NATO's and Allies' efforts should be focused on implementing and further developing clarity on the existing rules – sovereignty, non-intervention, and the prohibition of the use of force; state responsibility and the right to countermeasures and self-defence; human rights and international humanitarian law – rather than be distracted by vague promises of new instruments.

That said, it could be assumed that proposals for a new agreement will continue in the future.[47] It cannot be ruled out that there will be pressure to regulate specific issues concerning cyberspace (for example, specific uses of artificial intelligence),[48] but given that states have different views on the matter, there are no short-term prospects for the conclusion of a new treaty.

## Non-Binding Norms of Responsible State Behaviour

The 2015 GGE report presents 11 non-binding norms, rules, and principles for responsible state behaviour aimed at promoting an open, secure, stable, accessible, and peaceful ICT environment.[49] The 2019–2021 GGE added an 'additional layer of understanding to these norms, underscoring their value with regard to the expected behaviour of states in their use of ICTs in the context of international peace and security and providing examples of the kinds of institutional arrangements that states can put in place at the national and regional levels to support their implementation.'[50] One should note that these voluntary cyber norms help substantiate and implement established norms and rules of international law. They do not replace or dilute existing binding norms in the field of ICTs with non-binding ones.[51] Although the norms are addressed to states, this paragraph describes the 11 norms and their possible relevance for NATO as follows:[52]

'(1) Consistent with the purposes of the UN, which include the maintenance of international peace and security, states should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security.'

In the preamble of the North Atlantic Treaty (NAT), NATO nations 'reaffirm their faith in the purposes

47 For example, see Russia's point of view in Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States Submitted by Participating Governmental Experts in the GGE on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security Established Pursuant to General Assembly Resolution 73/266, A/76/136, 14 July 2021, https://front.un-arm.org/wp-content/uploads/2021/08/A-76-136-EN.pdf.

48 See 'ICRC Position Paper: Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centred Approach', March 2021, https://international-review.icrc.org/articles/ai-and-machine-learning-in-armed-conflict-a-human-centred-approach-913.

49 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/17, 22 July 2015, https://undocs.org/A/70/174.

50 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/76/135, 14 July 2021, Chapter 3, https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf.

51 As an example, existing norms are set down in the International Telecommunication Union (ITU) constitution or the UN Convention on the Law of the Sea. Both contain parts relevant for ICTs and are binding for member states.

52 Unless otherwise defined, paragraphs (1) to (11) are quoted from the Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/76/135, 14 July 2021, Chapter 3.

and principles of the Charter of the United Nations and their desire to live in peace with all peoples and all governments. They are determined to safeguard the freedom, common heritage and civilisation of their peoples, founded on the principles of democracy, individual liberty and the rule of law and promote stability and well-being in the North Atlantic area.'[53] Furthermore, in Article 1, NATO nations 'undertake to settle any international dispute in which they may be involved by peaceful means in such a manner that international peace and security and justice are not endangered'.[54] In the latest summit communiqué,[55] the cooperation as mentioned in Article 3 of the NAT is reaffirmed, as 'Allies will further seek to develop mutually beneficial and effective partnerships as appropriate, including with partner countries, international organisations, industry, and academia, furthering our efforts to enhance international stability in cyberspace'.[56]

'(2) In case of ICT incidents, states should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment, and the nature and extent of the consequences.'

The Brussels Communiqué mentions attribution in cases of hybrid warfare, recognising that attribution is a sovereign national prerogative.[57] It also states that 'individual Allies may consider, when appropriate, attributing hybrid activities and responding in a coordinated manner'. The AJP 3.20 also recognises that 'attribution of activities in or through cyberspace is essential, but does not solely depend on digital information. A combination of multi-source intelligence, regular forensics and other methods all contribute to reveal an actor's identity.'[58] It is the responsibility of the state that is the object of the armed attack, as well as that of those states coming to its collective defence, to perform an independent assessment. Any collective defence response by NATO will be subject to the political decisions of the North Atlantic Council (NAC).[59] That political decision could be based on Article 4 consultations[60] or the invocation of Article 5.[61]

'(3) States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs.'

As NATO is a political military alliance and has no territory, this norm is not relevant for NATO as an organisation. It would be up to the individual NATO nations to take reasonable steps within their capacity to end ongoing malicious activity on their territory.

'(4) States should consider how best to cooperate to exchange information, assist each other, prosecute the terrorist and criminal use of ICTs, and implement other cooperative measures to

53 North Atlantic Treaty, 4 April 1949.

54 Ibid., Article 1.

55 Brussels Summit Communiqué, paragraph 32, issued 14 June 2021.

56 Ibid., paragraph 32.

57 Ibid., paragraph 31.

58 Allied Joint Doctrine for Cyberspace Operations Edition A Version, 1 January 2020, paragraph 2.4.

59 North Atlantic Council, 10 October 2017, https://www.nato.int/cps/en/natolive/topics_49763.htm.

60 NAT, Article 4: 'The Parties will consult together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened.'

61 NAT, Article 5: 'The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.'

address such threats. States may need to consider whether new measures need to be developed in this respect.'

Law enforcement is not one of NATO's tasks. However, the Cyber Defence Pledge states that 'Allies will improve their understanding of cyber threats, including the sharing of information and assessments'.[62] Also worth noting is the technical arrangement that was signed between NATO and the EU that 'provides a framework for exchanging information and sharing best practices between emergency response teams' from both organisations.[63] Furthermore, according to its website, the 'NATO Industry Cyber Partnership, endorsed by Alliance leaders at the 2014 Wales Summit, fosters timely information sharing on cyber threats, allowing participants to enhance their situational awareness'.[64] The aforementioned exchange could also include information on the terrorist and criminal use of ICTs.

'(5) States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection, and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression.'

In summit declarations and communiqués, NATO heads of state and government state that NATO 'remains committed to acting in accordance with international law, including the UN Charter, international humanitarian law, and international human rights law as applicable'.[65]

'(6) A state should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public.'

NATO has stated in summit declarations and communiqués[66] that it acts in accordance with international law. Within NATO's defensive mandate, it cannot conduct or support ICT activity contrary to its obligations under international law.

'(7) States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199.'

Although NATO has no critical infrastructure as described in the resolution,[67] it goes without saying that national and NATO military systems will be considered critical and that NATO cybersecurity is aimed at its appropriate protection. The Cyber Defence Pledge also states that 'Allies will develop

62 Cyber Defence Pledge, paragraph 5, subparagraph IV, 8 July 2016, https://www.nato.int/cps/su/natohq/official_texts_133177.htm.

63 Technical Arrangement on Cyber Defence between the NATO Computer Incident Response Capability (NCIRC) and the Computer Emergency Response Team of the European Union (CERT-EU), 10 February 2016, https://www.nato.int/cps/en/natohq/news_127836.htm.

64 NATO Industry Cyber Partnership, https://www.ncia.nato.int/business/partnerships/nato-industry-cyber-partnership.html. See also the website of NATO Industry Cyber Partnership, https://nicp.nato.int/.

65 Brussels Summit Communiqué, paragraph 32, issued 14 June 2021; 2018 Brussels Summit Declaration, paragraph 20; 2016 Warsaw Summit Communiqué, paragraph 70; 2014 Wales Summit Declaration, paragraph 72.

66 Ibid.

67 General Assembly Resolution 58/199 mentions critical infrastructure used for, inter alia, the generation, transmission, and distribution of energy; air and maritime transport; banking and financial services; e-commerce; water supply; food distribution; and public health: https://undocs.org/en/A/RES/58/199.

the fullest range of capabilities to defend their national infrastructures and networks.'[68]

'(8) States should respond to appropriate requests for assistance by another state whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another state emanating from their territory, taking into account due regard for sovereignty.'

NATO nations will, based on Article 3 of the North Atlantic Treaty,[69] cooperate and respond to malicious ICT acts. This is practised in exercises like Locked Shields, organised by the CCDCOE, where teams of several nations 'take on the role of national cyber Rapid Reaction Teams that are deployed to assist a fictional country in handling a large-scale cyber incident with all its implications. ... The teams must be effective in reporting incidents, executing strategic decisions and solving forensic, legal and media challenges.'[70]

'(9) States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions.'

Although this norm is specifically aimed at actions that states can take to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products, the integrity of supply chains is also essential to NATO as end user. NATO customarily uses ICT systems off the shelf and so must have complete confidence that these systems are safe. This is recognised by NATO in the Strengthened Resilience Commitment, which states that NATO and Allies 'will step up efforts to secure and diversify our supply chains, as well as to ensure the resilience of our critical infrastructure (on land, at sea, in space and in cyberspace) and key industries, including by protecting them from harmful economic activities'.[71] The Not-For-Profit Framework (NFPF) by the NATO Communications and Information (NCI) Agency is another example; the aim is 'to diversify the NATO supply chain to make NATO more resilient and maintain the Alliance's technological edge'.[72] Thus NATO nations should inform each other on specific steps taken.

'(10) States should encourage responsible reporting to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure.'

It is for the individual NATO nations to decide to report on ICT vulnerabilities and share associated information on available remedies with other nations. On 12 February 2019, the NCI Agency took the first step in launching a network for sharing such information.[73] The sharing of such information with

---

68 Cyber Defence Pledge, paragraph 5, subparagraph I, 8 July 2016, https://www.nato.int/cps/su/natohq/official_texts_133177.htm.

69 NAT Article 3: 'In order more effectively to achieve the objectives of this Treaty, the Parties, separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack.'

70 Locked Shields is the unique international cyber defence exercise offering the most complex technical live-fire challenge in the world, organised by the CCDCOE. See https://ccdcoe.org/exercises/locked-shields/.

71 'Strengthened Resilience Commitment', 14 June 2021, https://www.nato.int/cps/en/natohq/official_texts_185340.htm.

72 Statement by NCI Agency Director of Acquisition Jennifer Upton, 4 November 2020, https://www.ncia.nato.int/about-us/newsroom/nato-agency-to-roll-out-cooperation-framework-with-notforprofit-organizations.html.

73 'The Agency took the first step to launch the network on 12 February 2019. Allied Computer Emergency Response Teams from 20 Nations can access NATO's protected business network, which provides an encrypted workspace with secure video, voice, chat and information gathering': 'NATO's Cyber Security Centre', NCI Agency, https://www.ncia.nato.int/what-we-do/cyber-security.html.

non-NATO nations or entities would require a NAC decision. The signing of the joint declaration[74] by the president of the European Council, the president of the European Commission, and the secretary general of NATO, which includes a common set of proposals, including the sharing of time-critical information between the EU Hybrid Fusion Cell and the relevant NATO counterpart, is one example of such a decision. The technical arrangement on cyber defence between the NATO Computer Incident Response Capability and the Computer Emergency Response Team of the European Union is a practical implementation of this declaration.[75] During the aforementioned Locked Shields exercise, but also during the NATO Cyber Coalition exercise, procedures are practised for the sharing of information between Allies and non-NATO participants.

'(11) States should not conduct or knowingly support activity to harm the information systems of the authorised emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another state. A state should not use authorised emergency response teams to engage in malicious international activity.'

NATO has Cyber Rapid Reaction teams on standby to assist Allies 24 hours a day.[76] In keeping with NATO's defensive mandate, these teams are not authorised to support activity to harm the information systems of authorised emergency response teams. Nor are they authorised to engage in malicious international activity.

Some of the 11 norms are very clear, like the norm that states should not conduct or knowingly support ICT activity that intentionally damages or otherwise impairs the use and operation of critical infrastructure, or the norm that states should not knowingly allow their territory to be used for internationally wrongful acts using ICTs. Recent cyber events make it clear that several cyber-capable states regularly ignore these norms, even if some of them voiced support for them at the UN GGE table.[77] NATO[78] and the EU[79] stated that China was behind the compromise of the Microsoft Exchange Server. Hackers suspected to be from North Korea (which is not a member of the UN GGE) infiltrated South Korea's nuclear research institute, the Korea Atomic Energy Research Institute (KAERI), and defence company Korea Aerospace Industries (KAI).[80] Until now, responses to malicious cyber activity have been limited to retorsions, meaning legally non-controversial

74 Statement on the Implementation of the Joint Declaration Signed by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization, NATO, 6 December 2016, https://www.nato.int/cps/en/natohq/official_texts_138829.htm.

75 'Technical Arrangement on Cyber Defence between the NATO Computer Incident Response Capability (NCIRC) and the Computer Emergency Response Team of the European Union (CERT-EU)', 10 February 2016, https://www.nato.int/cps/en/natohq/news_127836.htm.

76 'Cyber Defence', NATO, last updated 2 July 2021, https://www.nato.int/cps/en/natohq/topics_78170.htm.

77 Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, A/76/135, 14 July 2021, Annex, lists the 25 participants. These include Russia and China.

78 'Statement by the North Atlantic Council in Solidarity with Those Affected by Recent Malicious Cyber Activities Including the Microsoft Exchange Server Compromise', NATO, 19 July 2021, https://www.nato.int/cps/en/natohq/news_185863.htm?selectedLocale=en.

79 'China: Declaration by the High Representative on Behalf of the European Union Urging Chinese Authorities to Take Action against Malicious Cyber Activities Undertaken from Its Territory', Council of the EU, Press Release 615/21, 19 July 2021, https://www.consilium.europa.eu/en/press/press-releases/2021/07/19/declaration-by-the-high-representative-on-behalf-of-the-eu-urging-china-to-take-action-against-malicious-cyber-activities-undertaken-from-its-territory/pdf.

80 Cho Mu-Hyun, 'North Korean Hacking Group Allegedly behind Breach of South Korean Nuclear Institute', ZDNet, 21 June 2021, https://www.zdnet.com/article/north-korean-hacking-group-allegedly-behind-breach-of-south-korean-nuclear-institute/; Park Si-soo, 'North Korea-Linked Hackers Accessed South's Rocket Developer: Spy Agency', Space News, 9 July 2021, https://spacenews.com/north-korea-linked-hackers-accessed-souths-rocket-developer-spy-agency/.

measures such as sanctions,[81] indictments,[82] or publicity.[83] However, there is no guarantee that this will remain the case for future responses. President Biden, responding to the growing threats posed by Russia and China in cyberspace, stated that if the United States ended up in a 'real shooting war' with a 'major power', it could be the result of a significant cyberattack.[84]

As for other norms, commercial or even military interests could stand in the way of implementing them. The advice that states should encourage the responsible reporting of ICT vulnerabilities could not be of interest to a commercial company. Reporting vulnerabilities in one's own products still runs the risk of reputational and economic damage, even if the parties involved follow all the principles of responsible disclosure. Responsible disclosure refers to the practice of not disclosing the vulnerability until the organisation responsible for the hardware or software deals fixes the vulnerability.[85] The NATO Industry Cyber Partnership has as its objective to 'improve sharing of expertise, information and experience of operating under the constant threat of cyberattack, including information on threats and vulnerabilities, e.g. malware information sharing' with industry.[86] Governmental institutions might want to use a vulnerability for purposes such as intruding in an adversary's system. Thus they may not want to report it, which may create significant risks if such information is revealed.[87]

Looking at the relevance of the above-mentioned norms for NATO, formally the norms are addressed to states. NATO member states should take these norms into account when drafting their own legislation or policies. As the process of adapting norms in the GGE and OEWG takes time, due to the necessary consensus mechanism, NATO as an alliance has an interest in the discussions on how international law evolves and how it could apply in future. Therefore, NATO should find a way to be involved in these discussions on new politically binding norms, or those concerning an overarching treaty on cyberspace. As participation in a GGE or OEWG is only for states, the NAC could decide to have one member state representing NATO's position on this topic. However, a consensus-based position of 30 states runs the risk of being too general to have added value for the discussions. Therefore, the NAC could rely on NATO members participating in the GGE or OEWG to represent their national opinion, which at least should be in line with the NATO principles as described in the summit declarations.

---

81 'EU Imposes the First Ever Sanctions against Cyber-Attacks', Council of the EU, press release, 30 July 2020, https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/; Franck Dumortier, Vagelis Papakonstantinou, and Paul De Hert, 'EU Sanctions against Cyber-Attacks and Defense Rights: Wanna Cry?' European Law Blog, 28 September 2020, https://europeanlawblog.eu/2020/09/28/eu-sanctions-against-cyber-attacks-imposed-and-defense-rights-wanna-cry/.

82 'U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations', Office of Public Affairs, Department of Justice, October 2018, https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and.

83 'Statement by the North Atlantic Council in Solidarity with Those Affected by Recent Malicious Cyber Activities Including the Microsoft Exchange Server Compromise', NATO, 19 July 2021, https://www.nato.int/cps/en/natohq/news_185863.htm?selectedLocale=en.

84 Nandita Bose, 'Biden: If U.S. Has "Real Shooting War" It Could Be Result of Cyber Attacks', Reuters, 27 July 2021, https://www.reuters.com/world/biden-warns-cyber-attacks-could-lead-a-real-shooting-war-2021-07-27/.

85 Jonathan Trull, 'Responsible Disclosure: Cyber Security Ethics', CSO, 26 February 2015. https://www.csoonline.com/article/2889357/responsible-disclosure-cyber-security-ethics.html.

86 NATO Industry Cyber Partnership, https://www.ncia.nato.int/business/partnerships/nato-industry-cyber-partnership.html.

87 'The Shadow Brokers, a hacker group, published several leaks containing hacking tools, including several zero-day exploits, from the Equation Group, who are widely suspected to be a branch of the National Security Agency (NSA) of the United States.' 'The Shadow Brokers', Wikipedia, last edited on 19 September 2021, https://en.wikipedia.org/wiki/The_Shadow_Brokers. These exploits and vulnerabilities were later used for the major global malware campaigns WannaCry and NotPetya, resulting in huge economic damage and threats to human life and health. 'EternalBlue', Wikipedia, last edited on 23 October 2021, https://en.wikipedia.org/wiki/EternalBlue.

## Confidence-Building Measures

One part of the 2015 GGE report is focused on confidence-building measures (CBMs). They focus on the increase of interstate cooperation, transparency, predictability, and stability and include identification of points of contact (POCs) at the policy and technical levels,[88] cross-border cooperation,[89] and information-sharing. The aforementioned voluntary norms could be seen as part of a structure of CBMs. Building confidence is a long-term and progressive commitment requiring the sustained engagement of states. The support of the UN, regional and sub-regional bodies, and other stakeholders can contribute to the effective operationalisation and reinforcement of CBMs. An example of a directory with POCs is the computer security incident response team (CSIRT) list by countries of the European Union Agency for Cybersecurity (ENISA),[90] while the Memorandum of Understanding between Lithuania, Estonia, Croatia, Poland, the Netherlands, and Romania, which enables the operation of the Cyber Rapid Response Team (CRRT),[91] shows cross-border cooperation. Furthermore, the PESCO Cyber Threats and Incident Response Information Sharing Platform (CTIRISP) project aims to help mitigate these risks by focusing on sharing cyber threat intelligence through a networked member-state platform, with the aim of strengthening nations' cyber defence capabilities.[92]

It can be concluded that there are initiatives for CBMs. However, the pace is slow, especially given that the GGE recommends 'regular institutional dialogue with broad participation under the auspices of the UN, as well as regular dialogue through bilateral, regional, and multilateral forums and other international organisations'.[93] NATO, as an international organisation, should work on a policy to encourage the development of CBMs and safeguard the Alliance's interests in order to promote stability and help reduce the risk of misunderstanding, escalation, and conflict. The NATO-EU Joint Declaration[94] is an example of two international organisations working on establishing CBMs. NATO should, however, also develop CBM initiatives with states outside the EU like Russia and China. As for CBMs with Russia, the NATO-Russia Council would be the forum to discuss this topic. As for China, after NATO has established its agreed official standpoint, it needs to find a way to start discussions on CBM. This could first be done at working level before starting official consultations.

## Capacity-Building Measures

The 2019 GGE underscores the importance of cooperation and assistance in the area of ICT security and capacity-building. Increased cooperation, alongside more effective assistance and capacity-building in the area of ICT security, involving other stakeholders such as the private sector, academia, civil society, and the technical community, can help states apply the framework for the responsible behaviour of states in their use of ICTs. They are critical to bridging existing divides

88 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/17, 22 July 2015, https://undocs.org/A/70/174.

89 Ibid.

90 'CSIRTs by Country: Interactive Map', ENISA (European Union Agency for Cybersecurity), https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map.

91 'Cyber Rapid Response Team Established by Six EU Countries', *Lithuania Tribune*, 5 March 2020, https://lithuaniatribune.com/cyber-rapid-response-team/.

92 'Cyber Threats and Incident Response Information Sharing Platform (CTIRISP)', Permanent Structured Cooperation (PESCO), https://pesco.europa.eu/project/cyber-threats-and-incident-response-information-sharing-platform/.

93 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/17, 22 July 2015, paragraph 18.

94 NATO-EU Joint Declaration, signed 10 July 2018, https://www.consilium.europa.eu/media/36096/nato_eu_final_eng.pdf.

within and between states on policy, legal, and technical issues relevant to ICT security.[95] Providing such assistance through capacity-building measures helps prevent situations in which states with vulnerable ICTs have to fear for their critical infrastructure or become a haven for malicious actors. Capacity-building measures are therefore essential for international security.

The GGE recommends eight voluntary measures that not only focus on the technical aspects of ICTs, like improving the security, resilience, and protection of critical infrastructure, but also include developing and implementing national ICT policies, strategies, and programmes. Furthermore, support should be given for building or enhancing the technical, legal, and policy capacities of states to detect, investigate, and resolve ICT incidents, including through investment in the development of human resources, institutions, resilient technology, and educational programmes. The creation of a computer response team and/or cybersecurity incident response teams will enhance ICT resilience, and arrangements for international cooperation will strengthen these teams.[96]

NATO has its Defence and Related Security Capacity Building Initiative,[97] which offers training or advice and assistance in specialised areas such as logistics or cyber defence. The programme is demand-driven and tailored to the needs of the recipient nations. However, based on the above-mentioned recommendations of the 2019–2021 GGE, NATO should determine whether the cyber defence part of such a training advice or assistance programme should be extended in order to strengthen the cyber capabilities of current or new partners.

## NATO's Role in Cyber Norms Discussions

As the Brussels Summit Communiqué declared, NATO 'continues to pursue efforts to enhance stability and reduce the risk of conflict by supporting international law and voluntary norms of responsible state behaviour in cyberspace'.[98] That raises the question of whether NATO is involved in the process of writing new norms. The participants in the OEWG are all UN member states invited by the UN GA to participate; they have the chance to take part and to discuss what kind of issues should be addressed. The GGE consists of 25 representatives of states.[99] According to the website Digwatch, it 'is composed "on the basis of equitable geographical distribution". Traditionally, the five permanent members of the Security Council have a seat on all GGEs, and the remaining seats are allocated by grouping.'[100] NATO, as an international organisation, has no seat in these. Would the participation of NATO in such working groups be beneficial? For this, we have to look at NATO's decision mechanism. 'All NATO decisions are made by consensus, after discussion and consultation among member countries',[101] states the NATO website, adding: 'Consultations take place until a decision is reached that is acceptable to all. Sometimes member countries agree to disagree on an issue. In general, this negotiation process is rapid, since members consult each other on a regular

95 Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, A/76/135, 14 July 2021, paragraph 87.

96 Ibid., paragraph 89.

97 'Defence and Related Security Capacity Building Initiative', NATO, last updated 9 June 2021, https://www.nato.int/cps/en/natohq/topics_132756.htm.

98 Brussels Summit Communiqué, 14 June 2021.

99 Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, A/76/135, 14 July 2021, Annex, lists the 25 participants.

100 Geneva Internet Platform Digwatch, UN Group of Governmental Experts (GGE), https://dig.watch/processes/un-gge/#GGE-vs-OEWG-vs-PoA.

101 'Consensus Decision-Making at NATO', last updated 2 October 2020, https://www.nato.int/cps/en/natolive/topics_49178.htm.

basis and therefore often know and understand each other's positions in advance.'[102]

For cyber norms, this means that a NATO position will be based on the consensus of 30 nations and will probably be very general. Examples are the texts of the summit declarations reiterating that NATO remains committed to acting in accordance with international law.[103] For voluntary norms like the aforementioned non-binding norms of responsible state behaviour, it is questionable whether NATO's consensus position would be of great added value.

# NATO Policies in an Ever-Evolving Cyber Threat Landscape

Based on the above, it is interesting to see how the policies of NATO developed over time and how NATO addresses the challenges in cyberspace. This chapter will give a short overview of how NATO policies evolved and what NATO's view is on cyberspace. It will address NATO's possible responses to cyberattacks below and above the threshold of an armed attack. Finally, the challenges for integrating SCEPVA will be described.

## Evolution of NATO's View on Cyberspace

NATO first suffered significant cyberattacks in 1999, during Operation Allied Force against Serbia, when a number of 'patriotic hackers' using various names conducted denial-of-service attacks and web page defacements.[104] The 2002 Prague Summit was the first summit to place cyber defence on the Alliance's political agenda. In the summit declaration, Allies stated that they decided to 'strengthen our capabilities to defend against cyber attacks'.[105] One of their actions was the creation of the NATO Cyber Incident Response Team (NCIRC).[106] In 2008, NATO adopted its first 'policy on cyber defence that placed emphasis on the need for NATO and nations to protect key information systems in accordance with their respective responsibilities; share best practices; and provide a capability to assist Allied nations, upon request, to counter a cyberattack'.[107] In the same year, at the initiative of Estonia (which faced the first politically motivated cyberattacks), Estonia and six

102 Ibid.

103 Examples are the texts of the summit declarations reiterating that NATO remains committed to acting in accordance with international law.

104 Jason Healey and Klara Tothova Jordan, 'NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow', Atlantic Council, September 2014, http://www.jstor.org/stable/resrep03426.

105 Prague Summit Declaration, press release, NATO, 12 November 2002, https://www.nato.int/cps/en/natohq/official_texts_19552.htm.

106 'Based at Supreme Headquarters Allied Powers Europe (SHAPE), the NCIRC protects NATO's own networks through round-the-clock cyber defence support. Its experts handle incidents and provide NATO and Allies with up-to-date analysis of the cyber challenges. The NCIRC is part of the NATO Communications and Information Agency, which supports NATO operations, connects NATO's information and communication systems, and defends NATO's networks.' Factsheet NATO Cyber Defence, April 2021, https://www.nato.int/nato_static_fl2014/assets/pdf/2021/4/pdf/2104-factsheet-cyber-defence-en.pdf.

107 Bucharest Summit Declaration, issued by the heads of state and government participating in the meeting of the North Atlantic Council in Bucharest, paragraph 47, 3 April 2008, https://www.nato.int/cps/en/natohq/official_texts_8443.htm?selectedLocale=en.

other NATO nations created the Cooperative Cyber Defence Centre of Excellence.[108] The strategic concept in 2010 stated that Allies would ensure that NATO had 'the full range of capabilities necessary to deter and defend against any threat to the safety and security of the Allies' population'.[109] To realise this, the ability 'to prevent, detect, defend against, and recover from cyberattacks needed to be developed'.[110] NATO realised that this was part of its normal activities, as it uses the NATO planning process to enhance and coordinate national cyber-defence capabilities. In the 2014 declaration, Allies agreed that cyber defence was part of NATO's core task of collective defence. For the first time, NATO officially stated that the impact of a cyberattack could be as harmful to modern societies as a conventional attack and could led to the invocation of Article 5. A decision as to when a cyberattack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis.[111] In 2018 at the summit in Warsaw, NATO recognised cyberspace as a domain of operations.[112] Although this is not stated in the communiqué text, it implies that cyber is a domain equal to land, sea, and air and that NATO has to prepare to defend itself in cyberspace by creating the necessary capabilities. With the adaptation of the Cyber Defence Pledge at the same summit,[113] the Allies committed themselves to enhancing the cyber defences of national networks and infrastructures as a priority. At the Brussels Summit in 2018, Allied leaders agreed to set up a new Cyberspace Operations Centre as part of NATO's strengthened command structure. The Centre provides situational awareness and coordinates NATO's operational activity in and through cyberspace.[114] Allies also agreed on 'enhanc[ing] the effective integration of sovereign cyber effects, provided voluntarily by Allies, into collective defence and Alliance operations and missions, in the framework of strong political oversight'.[115] The communiqué added: '[T]he Alliance is determined to employ the full range of capabilities at all times to actively deter, defend against, and counter the full spectrum of cyber threats, including those conducted as part of hybrid campaigns, in accordance with international law.'[116] After acknowledging the importance of cyberspace in 2002, NATO policies changed. From recognising that a cyberattack could lead to the invocation of Article 5,[117] NATO's position evolved to recognising that the impact of significant malicious cumulative cyber activities might, in certain circumstances, be considered as amounting to an armed attack.[118]

---

108 The CCDCOE was established at the initiative of Estonia together with six other nations – Germany, Italy, Latvia, Lithuania, Slovakia, and Spain – on 14 May 2008. The North Atlantic Council decided to award full accreditation and international military organisation status to the Centre in October of the same year. See also 'About Us', CCDCOE, https://ccdcoe.org/about-us/.

109 'Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization', adopted by heads of state and government at the NATO Summit in Lisbon, paragraph 19, 19–20 November 2010, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf.

110 Ibid.

111 Wales Summit Declaration, paragraph 72, http://www.nato.int/cps/en/natohq/official_texts_112964.htm#cyber.

112 Warsaw Summit Communiqué, paragraphs 70 and 71, 9 July 2016, https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

113 Cyber Defence Pledge, 8 July 2016, https://www.nato.int/cps/su/natohq/official_texts_133177.htm.

114 Brussels Summit Declaration issued by the heads of state and government participating in the meeting of the North Atlantic Council in Brussels, 11 July 2018, paragraph 29, https://www.nato.int/cps/en/natohq/official_texts_156624.htm.

115 Brussels Summit Communiqué, paragraph 32, 14 June 2021.

116 Ibid.

117 Wales Summit Declaration Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Wales, 5 September 2014, paragraph 72.

118 Brussels Summit Communiqué, paragraph 32, 14 June 2021.

## Defence in Cyberspace

If NATO is determined to employ the full range of capabilities,[119] the question arises of how this would be done. As a political and military alliance of 30 member states, each with its own view on how international law applies, how would NATO react to cyberattacks above and below the threshold of an armed attack?

There is no question that, under international law, a state that faces an armed attack has the inherent right to individual or collective self-defence.[120] However, there are controversies on what constitutes an armed attack. Without delving into this doctrinal debate, the question is important when a NATO member is faced with a large-scale cyberattack. The International Group of Experts in the Tallinn Manual 2.0 unanimously concluded that some cyber operations could be sufficiently grave to warrant classifying them as an 'armed attack' within the meaning of the Charter.[121] In order to classify a cyber operation as an armed attack, the scale and effect[122] of such an operation should be considered. A cyber operation resulting in the death of persons or extensive damage, comparable to that of a conventional kinetic attack, could be considered an armed attack. The International Group of Experts in the Tallinn Manual 2.0 noted that the law was unclear as to the precise point at which the effects of a cyber operation qualified that operation as an armed attack.[123] This raises the question of what NATO's position is on this. In the Brussels Summit Communiqué, the Allies reaffirm that the North Atlantic Council would decide on a case-by-case basis when a cyberattack would lead to the invocation of Article 5.[124] This is in line with the secretary general's earlier statements that Allies had decided that a cyberattack could trigger Article 5 but that refrained from elaborating on when the threshold for an armed attack would be reached: 'I am often asked, "Under what circumstances would NATO trigger Article 5 in the case of a cyber-attack?" My answer is: we will see.'[125] There is no reason to expect that this will change in the future. Clearly stating when a cyberattack would reach the threshold of an armed attack could be seen by a potential adversary as a green light to act just below that threshold. Another reason why a clear threshold will not be mentioned is that decisions are made by the NAC by consensus after discussion and consultation among member countries.[126] It is highly unlikely that the 30 member states would reach consensus on a threshold, instead of deciding on a case-by-case basis.

The Brussels Summit Communiqué also states that Allies recognise that the impact of significant malicious cumulative cyber activities might, in certain circumstances, be considered as amounting to an armed attack.[127] As previous declarations, starting with the Wales Summit Declaration of 2014, state that 'a decision as to when a cyberattack would lead to the invocation of Article 5 would be

119 Ibid., paragraph 32, 14 June 2021, https://www.nato.int/cps/en/natohq/news_185000.htm.

120 The dual basis of the right to self-defence is generally recognised and acknowledged as being Article 51 of the United Nations Charter and customary international law, which is indirectly referred to in that provision by the use of the term 'inherent' in its relation to the nature of self-defence. Terry Gill and Dieter Fleck, *The Handbook of International Law of Military Operations* (Oxford University Press, 2012), 189.

121 Tallinn Manual 2.0, Rule 71 – Self-defence against armed attack, paragraph 4.

122 Case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America) (merits) (1986), ICJ paragraph 195, https://www.icj-cij.org/public/files/case-related/70/070-19860627-JUD-01-00-EN.pdf.

123 Tallinn Manual 2.0, rule 71, paragraph 9.

124 Brussels Summit Communiqué, paragraph 32, 14 June 2021.

125 Speech by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference, Ecole Militaire, Paris, 15 May 2018, https://www.nato.int/cps/en/natohq/opinions_154462.htm.

126 'Consensus Decision-Making at NATO', last updated 2 October 2020, https://www.nato.int/cps/en/natolive/topics_49178.htm.

127 Brussels Summit Communiqué, paragraph 32, 14 June 2021.

taken by the NAC on a case-by-case basis',[128] this approach is new. This raises the question of at what point such a series of malicious cumulative cyber activities would be treated as an armed attack. 'The International Group of Experts in the Tallinn Manual 2.0 agreed that the determinative factor is whether the same originator (or originators acting in concert) has carried out smaller-scale incidents that are related and that, taken together, meet the requisite scale and effects. If there is convincing evidence that this is the case, there are grounds for treating the incidents as a composite armed attack.'[129] As Monica Hakimi and Jacob Katz Cogan explain, 'Under the so-called "pinprick" or "accumulation of events" theory of an armed attack, multiple small-scale attacks can together satisfy the threshold even if none of the attacks on its own would satisfy the threshold.'[130] Attribution in this case may pose a difficult factual and legal question. For the NAC to decide on whether significant malicious cumulative cyber activities should be considered to amount to an armed attack, a member state that was the target of malicious cumulative cyber activities would need to present its evidence on attribution for each of the attacks, as attribution is a national prerogative.[131] The latest summit declaration is clear on this. It states that 'Allies would make use of NATO as a platform for political consultation among themselves, sharing concerns about malicious cyber activities and exchanging national approaches and responses, as well as considering possible collective responses.'[132] Based on the presented evidence, the NAC would have to reach consensus on further actions, including the possibility of invoking Article 5. It goes without saying that for cumulative malicious cyberattacks, a clear threshold cannot be defined; decisions will have to be made on a case-by-case basis.[133]

If the NAC decided that a malicious cyber operation or series of malicious cyber operations did not meet the threshold of an armed attack, it would be interesting to know what the options are. If the malicious cyber operation or series of malicious cyber operations did constitute an internationally wrongful act of a state, responses such as retorsions and countermeasures could be considered. As for retorsions, NATO, as a political military alliance, does not have many options. It cannot fall back on economic sanctions, and its diplomatic sanctions are limited.[134] As for countermeasures,[135] the discussion would raise the question of whether an international organisation or a state can take countermeasures on behalf of another state.[136] Even within the Alliance, the national positions on this are not the same. Estonian president Kersti Kaljulaid announced, 'Estonia is furthering the position that states which are not directly injured may apply countermeasures to support the state directly affected by the malicious cyber operation.'[137] France's position is that 'Collective countermeasures are not authorised, which rules out the possibility of France taking such measures in

128 Wales Summit Declaration Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Wales, 5 September 2014, paragraph 72

129 Tallinn Manual 2.0, rule 71, paragraph 11.

130 Monica Hakimi and Jacob Katz Cogan, 'The Two Codes on the Use of Force', *European Journal of International Law* 27, no. 2 (2016), 257–291, https://academic.oup.com/ejil/article/27/2/257/1748396.

131 This would be what is known as an Article 4 consultation.

132 Brussels Summit Communiqué, paragraph 32, 14 June 2021.

133 See the statements of Secretary General Jens Stoltenberg in his speech at the Cyber Defence Pledge Conference, 15 May 2018, https://www.nato.int/cps/en/natohq/opinions_154462.htm.

134 There are some options. In October 2021, NATO expelled eight Russians for spying. 'Nato Expels Eight Russians from Its Mission for Spying', BBC, 7 October 2021, https://www.bbc.com/news/world-europe-58826980.

135 Responsibility of States for Internationally Wrongful Acts, 2001, Chapter 2 and Article 22, https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf.

136 Michael Schmitt and Sean Watts, 'Collective Countermeasures?' *Harvard National Security Journal* 12 (2021), 373–411, https://harvardnsj.org/wp-content/uploads/sites/13/2021/07/HNSJ-Vol-12-Schmitt-and-Watts-Collective-Cyber-Countermeasures.pdf.

137 Kersti Kaljulaid, president of Estonia, opening at CyCon 2019 (29 May 2019), https://news.err.ee/946827/president-kaljulaid-at-cycon-2019-cyber-attacks-should-not-be-easy-weapon.

response to an infringement of another state's rights.'[138] Other member states are not clear on their position on collective countermeasures.[139] Another factor to consider is that there is a difference between NATO[140] and the NATO member states. NATO as an organisation is responsible for the protection of its own computer information systems and networks. The NATO Computer Incident Response Capability (NCIRC), as part of the NATO Communications and Information Agency, protects NATO's own networks,[141] both those of static HQs and of HQs deployed for operations or exercises. It provides specialist services to prevent, detect, respond to and recover from cybersecurity incidents.[142] As countermeasures would result in operations outside the NATO network, these actions would lead to consultations in the NAC in order to reach consensus.[143] The 2021 Brussels Communiqué also states that NATO will, if necessary, impose costs on those who harm its member states and that its response will not necessarily be restricted to the cyber domain.[144] Given the recognition that a cyberattack can reach the threshold of an armed attack, the option already exists to respond outside the cyber domain, such as a kinetic response, but other options are also possible. Concerning cyberattacks that remain under the threshold of an armed attack, it is not clear how such costs would be imposed, but it is certain that such a decision will be made on a case-by-case basis after NAC consultations.

## Sovereign Cyber Effects Provided Voluntarily by Allies

The reports of the GGE and the OEWG do not mention the military use of cyberspace. Cyberspace will undoubtedly play a role in military operations. As an example, according to Wikipedia, 'during the Russo-Georgian War, a series of cyberattacks swamped and disabled websites of numerous South Ossetian, Georgian, Russian, and Azerbaijani organisations. The attacks were initiated three weeks before the shooting war began.'[145] This is regarded, according to David Hollis, as 'the first case in history of a coordinated cyberspace domain attack synchronized with major combat actions in the other warfighting domains (consisting of Land, Air, Sea, and Space)'.[146]

The fact that NATO recognised cyber as a new domain of operations in 2016 and established a Cyberspace Operations Centre that achieved initial operational capability in 2021[147] shows that NATO recognises that cyber operations will be a part of future military operations. It was also stated in the Warsaw Summit Declaration that 'cyber defence will continue to be integrated into operational

138 'International Law Applied to Operations in Cyberspace', Ministère des Armées (Ministry of Armed Forces), France, 9 September 2019, https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf.

139 See national positions at 'Countermeasures', International Cyber Law: Interactive Toolkit, last edited on 16 November 2021, https://cyberlaw.ccdcoe.org/wiki/Countermeasures#France_(2019).

140 NATO as an organisation means the North Atlantic Council, its subsidiary bodies as described in Article 9 of the North Atlantic Treaty, and the NATO Command Structure, composed of Allied Command Operations and Allied Command Transformation.

141 Factsheet, NATO Cyber Defence, April 2021, https://www.nato.int/nato_static_fl2014/assets/pdf/2021/4/pdf/2104-factsheet-cyber-defence-en.pdf.

142 NCIA (NATO Communications and Information Agency), 'NATO's Cyber Security Centre', https://www.ncia.nato.int/what-we-do/cyber-security.html.

143 'Consensus Decision-Making at NATO', last updated 2 October 2020, https://www.nato.int/cps/en/natolive/topics_49178.htm.

144 Brussels Summit Communiqué, paragraph 32, 14 June 2021.

145 'Cyberattacks during the Russo-Georgian War', Wikipedia, https://en.wikipedia.org/wiki/Cyberattacks_during_the_Russo-Georgian_War.

146 David Hollis, 'Cyberwar Case Study: Georgia 2008', Small Wars Journal, 6 January 2011, https://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf.

147 2021 Brussels Summit Communiqué, paragraph 32, https://www.nato.int/cps/en/natohq/news_185000.htm.

planning and Alliance operations and missions'.[148] As for cyber defence, the question arises how these operations would be conducted. Just as with conventional weapon systems, where Allies, with the exception of the Alliance Ground Surveillance System and Airborne Warning and Control System, possess tanks, ships, and aircraft for NATO missions, NATO also has to rely on Allies for cyber capabilities. In the 2021 Brussels Communiqué NATO introduced SCEPVA.[149] The NAC can decide that SCEPVA can be used in NATO operations irrespective of whether the intent is defensive or offensive. While the combat power of tanks, planes, and ships can be precisely estimated, for SCEPVA this might be more difficult. As an example, if a SCEPVA is based on a zero-day vulnerability, it might become useless if this zero-day vulnerability is fixed. Furthermore, the effect of an offensive cyber tool, or estimating the collateral damage, might be more challenging than that of a kinetic operation. Even if the desired effect of SCEPVA is clear, integrating this quickly at the right time and location in an operation might prove difficult. As strict political oversight means that a NAC decision is needed, a mechanism should be developed to allow quick decision-making.

# Conclusion

NATO's position that it will 'promote a free, open, peaceful, and secure cyberspace and continue to pursue efforts to enhance stability and reduce the risk of conflict by supporting international law and voluntary norms of responsible state behaviour in cyberspace'[150] is in line with the 2021 GGE position on international law: '[T]he Group reaffirms the assessments and recommendations on international law of the reports of previous Groups of Governmental Experts, notably that international law, and in particular the Charter of the United Nations is applicable and essential to maintaining peace and stability and for promoting an open, secure, stable, accessible and peaceful ICT environment.'[151] The 11 non-binding norms,[152] rules, and principles for responsible state behaviour aimed at promoting an open, secure, stable, accessible and peaceful ICT environment do not necessitate the adaptation of existing NATO policies.

Looking at the role of NATO in the normative process, we might conclude that, although NATO has an interest, its role might be limited. First of all, NATO is not an official participant in UN fora; the participants in the OEWG and GGE are all UN member states invited by the UN GA to participate. Furthermore, it is questionable whether NATO's consensus position would be of great added value. NATO member states, however, could try to find a way to be involved in discussions on voluntary or new politically binding norms, or those on an overarching treaty on cyberspace. As some NATO member states already participated in the last GGE,[153] they could together agree to represent the NATO position. Another option could be for the NAC to decide to have one member state representing NATO's position on this topic.

148 Warsaw Summit Communiqué, paragraph 70, 9 July 2016, https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

149 NATO 'will enhance the effective integration of sovereign cyber effects, provided voluntarily by Allies [SCEPVA], into collective defence and Alliance operations and missions, in the framework of strong political oversight'

150 Brussels Summit Communiqué, paragraph 32, 14 June 2021.

151 Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, A/76/135, 14 July 2021, section 4.

152 Ibid., section 3.

153 Estonia, France, Germany, the Netherlands, Norway, Romania, the United Kingdom, and the United States.

NATO as an international organisation should continue to work on a policy that encourages the development of CBMs and safeguards the Alliance's interests in order to promote stability and help reduce the risk of misunderstanding, escalation, and conflict. As for capacity-building, NATO has its Defence and Related Security Capacity Building Initiative, which offers training or advice and assistance in specialised areas such as logistics or cyber defence. The programme is demand-driven and tailored to the needs of the recipient nations, but NATO could, based on the recommendations of the 2019–2021 GGE on CBMs, consider whether the cyber defence part of such a training advice or assistance programme should be extended in order to strengthen the cyber capabilities of current or new partners.

Although NATO has policies on cyberspace operations, future work on policies will be needed, including finalisation of the effective integration of SCEPVA into collective defence and Alliance operations and missions, as well as creating the framework of strong political oversight. Responses to a cyberattack that do not rise to the threshold of an armed attack, and malicious cumulative cyber activities will need further discussion. That said, decisions on when a cyberattack would reach the threshold of an armed attack will always be taken by consensus on case-by-case basis.

# Contributors

**Laura G. Brent** is a former senior fellow in the Technology and National Security Program at the Center for a New American Security (CNAS). Before joining CNAS, Brent served on the NATO International Staff, where she developed and implemented cyber defence policy, focusing on NATO's ability to operate in cyberspace. Previously, at Ernst & Young, she led and supported cybercrime investigations and cybersecurity assessments, assisting clients in responding to incidents and improving their cybersecurity posture. Brent has served at the US Department of Homeland Security in the Immediate Office of the Secretary and what is now the Cybersecurity & Infrastructure Security Agency (CISA), and she also completed a rotation to the Joint Staff in the Office of the Vice Chairman.

**Franz-Stefan Gady** is a research fellow for cyber, space, and future conflict at the International Institute for Strategic Studies (IISS). Gady has advised militaries in Europe and the United States on structural reform and the future of armed conflict. Before joining the IISS, he held various positions at the EastWest Institute, the Project on National Security Reform, and the National Defense University. He conducted field research in Afghanistan and Iraq, where, among other things, he embedded with the Afghan National Army, NATO forces, and Kurdish militias. Gady has also reported from a wide range of countries and conflict zones as a journalist.

**Jason Healey** is a senior research scholar at Columbia University's School for International and Public Affairs specializing in cyber conflict, competition, and cooperation. Before this, he was the founding director of the Cyber Statecraft Initiative of the Atlantic Council, where he remains a senior fellow. Healey is also president of the Cyber Conflict Studies Association and previously was adjunct faculty at the National Cryptologic School, Georgetown University, and the Johns Hopkins School of Advanced International Studies. He is an affiliate at Stanford University's Center for International Security and Arms Control.

**James A. Lewis** is a senior vice president and director for the Strategic Technologies Program at the Center for Strategic and International Studies (CSIS). Before joining the CSIS, he was a diplomat and a member of the Senior Executive Service with extensive negotiating, politico-military, and regulatory experience. Lewis was rapporteur and senior adviser for four UN Groups of Governmental Experts on Information Security, and his work on norms and confidence-building measures to build stability in cyberspace is foundational. He leads a long-running Track II dialogue with the China Institutes of Contemporary International Relations. Lewis is the recipient of several awards and received his PhD from the University of Chicago.

**Piret Pernik** is a researcher of the Strategy Branch of the CCDCOE. She is a co-editor of a volume of edited papers, Cyber Threats and NATO 2030: Horizon Scanning and Analysis, published by the CCDCOE in 2020. Previously, Pernik was a research fellow at the International Centre for Security and Defence and a researcher at the Estonian Academy of Social Sciences. Her career includes several positions at the Estonian Ministry of Defence, and she has served as adviser of the National Defence Committee at the Parliament of Estonia.

**Virpratap Vikram Singh** is a research and program coordinator for the Saving Cyberspace Initiative at Columbia University's School for International and Public Affairs. He previously worked as a consultant at the Atlantic Council's Cyber Statecraft Initiative on issues relevant to maritime cybersecurity and their global Cyber 9/12 Strategy Challenge.

Lieutenant Colonel **Berend Valk** is a researcher of the Law Branch of the CCDCOE. Before joining the CCDCOE he has held several positions in the Royal Netherlands Air Force and served as a deputy legal adviser of the International Military Staff of NATO Headquarters in Brussels. He has been deployed in international missions in Iraq and South Sudan, serving as senior legal adviser.

**David van Weel** is NATO's assistant secretary general for emerging security challenges. He is the secretary general's primary adviser on emerging security challenges and their implications for the security of the Alliance and a member of the secretary general's senior management team. Before joining NATO, van Weel was the foreign policy and defence adviser for the prime minister of the Netherlands (2016–2020). This position followed a long career in the Netherlands Ministry of Defence, where he ended as director for international affairs and operations/policy director (2014–2016) after serving as the chief of cabinet for the minister of defence and the permanent secretary (2012–2014) and as the senior policy officer for, among others, operations in Afghanistan and Libya, NATO, nuclear policy and disarmament, special operations, and the preparation of the defence budget.