Air & Space Power Conference | 2022

ENHANCING NATO AIR AND SPACE POWER IN AN AGE OF GLOBAL COMPETITION
JAPCC JOINT AIR AND SPACE POWER CONFERENCE 2022

Enhancing **NATO Air and Space Power** in an Age of **Global Competition**

11–13 October 2022

READ**AHEAD**

Joint Air Power Competence Centre

Enhancing **NATO Air and Space Power** in an Age of **Global Competition**

ENHANCING NATO AIR AND SPACE POWER IN AN AGE OF GLOBAL COMPETITION
JAPCC JOINT AIR AND SPACE POWER CONFERENCE 2022

READ ***AHEAD***

Enhancing **NATO Air and Space Power** in an Age of **Global Competition**

Joint Air and Space Power Conference 2022

© This work is copyrighted. All inquiries should be made to: The Editor, Joint Air Power Competence Centre (JAPCC), contact@japcc.org.

Acknowledgements
This read ahead is a JAPCC product realized in collaboration with the authors of the essays contained herein. The JAPCC would like to thank the numerous authors who took the time to contribute to this product in an effort to advance this topic for discussion within NATO.

Editorial Team
Air Commodore Paul Herber
Col Matthew Willis
Col Thomas Schroll
Lt Col Rafael Ichaso Franco
Maj Massimo Di Milia
Maj Andreas Wurster
Maj Fotios Kanellos
Mr Simon J. Ingram
MSgt Björn Aarts
Ms Britta Klein

Disclaimer
The views expressed in this work are those of the authors. It does not represent the opinions or policies of the North Atlantic Treaty Organization (NATO), and is designed to provide an independent overview, analysis and food for thought regarding possible ways ahead on this subject.

Release
This document is releasable to the public. Portions of the document may be quoted without permission, provided a standard source credit is included.

Published and distributed by
The Joint Air Power Competence Centre
von-Seydlitz-Kaserne
Römerstraße 140
47546 Kalkar
Germany

M Denotes images digitally manipulated

Moderator’s Foreword

Esteemed Colleagues,

There is little doubt today that we live in a time of renewed global competition between major state powers. This also means that we live in what is, potentially, an extremely hazardous age. In recent times, we have little to be thankful for from some of the so-called ‘Great Powers’. China (albeit most likely by accident) has brought us pestilence in the form of the Covid-19 virus. Russia (most definitely, by design) has brought us war in Ukraine. Not even one-quarter of the way into the 21st Century, and already we seem to have endured (and may continue to endure) two of the Biblical ‘four horsemen of the Apocalypse’. It is against this forbidding backdrop that the 2022 JAPCC Conference will take place.

On the first day of last year’s JAPCC Conference, we heard that in the more than seventy years since the end of WWII and more than thirty since the end of the Cold War, NATO needed to find a ‘forcing function’ to make national governments realise that threats to our democratic way of life had not gone away. One of the main speakers expressed his (and everyone else’s) sincere hope that it would not be another war that provided this ‘forcing function’. Sadly, war on the European continent once more proves to be a powerful motivator for governments to take robust action in deterrence and defence.

Individual NATO nations, along with the EU and the UN, have to a greater or lesser degree, begun to give the Ukrainians the help they so desperately need. However, in our dealings with and perceptions of Russia prior to the invasion of Ukraine, many of us, including many of our political leaders, have been exposed as – at best – naive. At worst, some might even say complicit.

It is exceptionally timely that the JAPCC Conference plans to bring some of our greatest minds and senior decision-makers together to consider how NATO might enhance its air and space power in this age of global competition. Along with our keynote speakers, the four conference panels will consider the broader geopolitical situation and the implications this has for our security. The speakers and panel members will analyse the consequences this new environment brings for deterrence and defence and what it means for defence and operational planning, and for agile, cross-domain command, from both defence and industry perspectives.

The traditional DIME model – diplomatic, informational, military and economic – reminds us that military power does not sit apart from the other instruments of power. We have only to think of Europe's reliance on Russian oil and gas supplies to realise the complexity of miscalculations that may have emboldened Putin's decision to invade Ukraine. The comprehensive requirements for defence and security must not be ignored. If deterrence fails, the effective defence of NATO territory will depend on our military forces, their effective command and control, along with comprehensive resiliency in the domains of Space and Cyber. Additionally, NATO is well aware that a comprehensive resiliency must also include the ensured availability of vital state and economic functions and continued use of the EMS. Warfare in collective defence will need to include other instruments of power alongside the military.

The articles you are about to read are the result of a 'call for papers' that was put out shortly after last year's conference. Not all of them refer directly to Joint Air and Space Power. However, they are all relevant to a discussion about the future security environment and its consequences for NATO's posture, operational preparedness and the role of Air and Space Power in this environment.

The two introductory articles explain the term 'global competition' chosen for this conference and explore the principles of Great Power competition. Subsequent articles analyse the links and interdependencies between the space and cyberspace domains, refer to some interesting similarities between thresholds in these domains, and propose how deterrence might be ensured in space through a responsive space architecture.

Artificial Intelligence (AI) and the dangers of seeing it as a panacea to overcome information and data overload was already touched on at the 2021 Conference. One of our articles will therefore provide a perspective on 'humanly enhanced' AI to enable understanding and achieve decision advantage. Another author makes us aware that we have to expect Adversarial Machine Learning and delivers a very well-argued note of caution. Managing operational data in a 'combat cloud' can offer effective support in scenarios where forces and capabilities operate across domains. Finding principles for the safe sharing of cyber weapons and capabilities needs urgent consideration in response to the particular challenges we find in and through this domain. The JAPCC thanks all the authors that have contributed articles – what you will read in the following pages is a carefully curated subset of those contributions.

The success of the 2021 JAPCC Conference was, in no small part, due to the perseverance of all those who attended in some challenging circumstances. We live in difficult times, but the efforts of everyone in coming together to discuss, analyse and formulate courses of action for the future will ensure that the 2022 Conference is just as rewarding.

I look forward to meeting you all in October!

Bruce Hargrave BSc MBA
Independent Air and Space Power Advisor

Table of Contents

Table of Contents

© 2021 Black Salmon/Shutterstock.com

Global Competition

1

The Origin of the Term and its Use in Policy Statements

By Col (GS) Thomas Schroll, GE Air Force
Joint Air Power Competence Centre

Introduction

In general, we tend to have a rather positive relationship with the idea of competition, which is broadly accepted in sports, school, professional life and society. Liberal democracies also distinctly favour the contest between individuals and political parties to achieve the best policy outcome for society and the state.

Competition between states, however, rarely comes with such positive associations. Even though relations between states today are governed more than ever by a comprehensive set of legally binding rules that demand nations 'settle […] international disputes by peaceful means […]' and to 'refrain from the threat of use of force against […] any state'[1], ample examples demonstrate that this obligation is often disregarded. There seems to be an inherent potential for escalation, and, therefore, a particular need to 'manage' competition between states to prevent escalation into violence and armed conflict.

This article will help frame the term global competition and outline how it was used or referred to in recent national governments' and NATO policy documents.

It's About the Relative Status of Power in the World

In the context of the international system of states, global competition is a term used by political analysts to understand the interaction between state powers. The term provides a framework for analysing interstate relations and an analytical tool to support global security assessments. Competition between states can be understood as part of a continuum that sees cooperation and collaboration at one end and confrontation/conflict as well as violent clash/armed warfare at the other.[2] This competition may escalate, but it 'is not [per se] synonymous with conflict'.[3]

Particular relevance is given to the competition between states characterised as 'Major' or 'Great' Powers. They can be defined as those states that a) possess a range and quality of capabilities they can use to shape the world, b) have the apparent intent and will to use them, and c) are considered by others to have this special status. The National Defence University (NDU) Strategic Assessment 2020 calls them the 'three substantive features': 'unusual capabilities', 'behaviour' and 'status attribution by others'.[4]

Entities like the European Union, but also some non-state actors, and 'super-empowered individuals' may decisively shape the international system's development.[5] However, focusing only on nation-states, most analysts will agree that in the contemporary era, particularly the United States, Russia, and China hold the attributes of a global Great Power.[6] During the last decade, it became increasingly apparent that these states compete for influence in broader regional areas of the world and the rules and norms that govern international relations.

Global Competition is Nothing New

An analysis of interstate competition includes identifying and understanding the relevant dimensions of power available to states and its use in maintaining or enhancing their status. In 1987, British historian Paul Kennedy published his famous book 'The Rise and Fall of the Great Powers'. He explored the period from 1500 to 1980 and the struggle between major powers to maintain or enhance their position relative to other states.[7] His intellectual approach to looking at categories that are the basis for the power and the potential of states to gain or lose power relative to other states[8] provided grounds for further academic analysis.

From a historical perspective, the world has seen many eras where states endeavoured to develop and increase the status of their power compared to other states and their competing ambitions. Most periods of history were characterized by distinct competition between countries, and most of them happened in a world of several major state powers. Therefore, today's interstate competition is 'unique but not unprecedented'.[9]

A survey of significant studies of interstate power competition, as done by Thomas F. Lynch III and Frank Hoffman, can help us understand interstate power competition's categories and dynamics. This study also allows us to explore in which cases competition escalated into a violent clash and an enforced transition and under which conditions transitions happened without resorting to war.[10]

The bad news is: Historical case studies reveal that 75 % or more of the analysed competition resulted in major military clashes.[11] On the other hand, the competition often involved simultaneous elements of collaboration and (non-violent) conflict.[12] And evidence shows that a relative decline of the dominant state and a violent clash is 'not predestined in any way'.[13]

Global Competition in Recent Policy Documents

The re-emergence of global interstate competition has already been articulated in several major policy documents and policy statements. To provide a short overview, this section will focus on those issued by the United States of America, the United Kingdom and NATO.

United States of America – the National Security Strategy 2017 and following documents

The **United States National Security Strategy (NSS) 2017**, published in December 2017, was the first national policy document released to the public that clearly characterized the current global system of states as 'a competitive world'.[14] In general, competition between states is regarded as the norm and, to be noted, 'healthy when nations share values and build fair and reciprocal relationships'.[15]

China and Russia are classified as 'revisionist powers'[16] that 'challenge American power, influence, and interests, attempting to erode American security and prosperity'. Both states are assessed to be 'determined to [...] expand their influence'[17] as they 'try to change the international order in their favour'.[18] Notably, the NSS distinctly emphasizes that competition does not automatically mean hostility, nor [ ] inevitably lead[s] to conflict'.[19]

The **United States National Defense Strategy (NDS) 2018**, as a follow-on document issued by the US Department of Defense, firmly assessed that 'China and Russia want to shape a world consistent with their authoritarian model – gaining veto authority over other nations' [...] decisions'[20]. Consequently, the NDS emphasized that 'inter-state strategic competition, not terrorism, is [...] the primary concern in US national security'[21]. 'Long-term strategic competitions with China and Russia' are outlined as the 'principal priorities for the [Defense] Department [...]'.[22]

Four years later, President Biden's **Interim National Security Strategic Guidance (INSSG)**, issued in March 2021, stated that […] alliances, institutions, agreements, and norms underwriting the international order […] are being tested'.[23] The guidance acknowledged that 'we face a world of rising nationalism, receding democracy, growing rivalry with China, Russia, and other authoritarian states'.[24]

China is regarded as 'the only competitor potentially capable of combining its economic, diplomatic, military, and technological power to mount a sustained challenge to a stable and open international system'.[25] Russia is assessed to remain 'determined to enhance its global influence and play a disruptive role on the world stage'.[26]

To the national and international audience, the INSSG promised that regarding its security policy, the United States 'will make smart and disciplined choices […] elevating diplomacy as […] a tool of first resort.[27]

United Kingdom – the 'Competitive Age' review and defence paper

In the same month as the Biden Administration's guidance, the UK government published its integrated security policy review **Global Britain in a Competitive Age**.

Similar to the INSSG, the review assessed that 'the nature and distribution of global power is changing as we move towards a more competitive and multipolar world'[28], and additionally offered a kind of definition for international 'systemic competition':

'the intensification of competition between states and with non-state actors, manifested in: a growing contest over international rules and norms; the formation of competing geopolitical and economic blocs of influence and values that cut across our security, economy and the institutions that underpin our way of life; the deliberate targeting of the vulnerabilities within democratic systems by authoritarian states and malign actors; and the testing of the boundary between war and peace, as states use a growing range of instruments to undermine and coerce others.'[29]

Systemic competition 'will determine the shape of the future international order'.[30] Both Russia and China are identified as 'systemic competitors',[31] but Russia is distinctly assessed to remain the 'most acute threat' to security in the Euro-Atlantic area.[32]

The UK's Ministry of Defence paper **Defence in a Competitive Age**, also published in March 2021, underlined that 'in an era of systemic competition, the distinctions between peace and war; home and away; state and non-state; and virtual and real become increasingly blurred',[33] and stated the need, due to 'constant competition', to 'compete with and campaign […] below the threshold of armed conflict, and to understand, shape and influence the global landscape […]'.[34]

The NATO 2030 Report and follow-on statements

At their summit meeting on 3 and 4 December 2019, NATO leaders asked the Secretary General of NATO to initiate a 'forward-looking reflection process […] to further strengthen NATO's political dimension including consultation'.[35] The so-called 'Reflection Group' issued its Report **NATO 2030 – United for a new era** on 25 November 2020. This report stated 'a changing international scene characterised by the return of geopolitical competition'.[36] This geopolitical competition is later defined as 'the profusion and escalation of state-based rivalries and disputes over territory, resources, and values'.[37] Notably, the report did not only assess Russia as 'the most profound geopolitical challenge' and 'a threat across NATO territory'.[38] It also outlines the 'acute challenges to open and democratic societies' arising from China 'because of that country's trajectory to greater authoritarianism and an expansion of its territorial ambitions'.[39]

Based on the NATO 2030 Reflection Group report and its recommendations, NATO Secretary General Stoltenberg offered his considerations on 4 June 2021, ten days ahead of the Brussels Summit 2021, at a public event on **NATO 2030: a transatlantic agenda for the future**. In his address, he used the expression **‘**growing global competition’ for Russia and China, who are, as he states, ‘leading an authoritarian pushback against the rules-based international order‘. He assesses Global Competition as beneath ‘sophisticated cyber-attacks, disruptive technologies, brutal terrorism, the proliferation of nuclear weapons, and the security impacts of climate change‘, a defining element of a security environment that is ‘more complex and contested than ever before‘.[40]

The **Brussels NATO Summit Communiqué of 14 June 2021** stated the ‘multifaceted threats, systemic competition from assertive and authoritarian powers’ faced by NATO and confirmed that ‘Russia’s aggressive actions constitute a threat to Euro-Atlantic security‘. Additionally, the communiqué emphasized that ‘state and non-state actors challenge the rules-based international order and seek to undermine democracy across the globe’ and, with respect to China, stressed the particular challenges emanating from its ‘growing influence and international policies’ that NATO nations ‘need to address together as an Alliance‘. China causes security concerns to NATO, therefore, NATO will engage China with a view to defending the security interests of the Alliance.‘[41]

Conclusion and Outlook

Global systemic competition is not a new term; it describes the behaviour between major state powers that aim to increase their relative status of power. Various policy documents and statements have referred to this term in various ways. Be it a ‘competitive world‘, ‘geopolitical competition’ or ‘systemic competition‘, they have been used to describe the challenge for NATO and its member states to deal with a world where two major state powers, Russia and China, have embarked to influence the course of political developments in the world and more broadly, some main characteristics of the 'world order'.

The attack on Ukraine, ordered by the Russian president, is a blatant attempt to enforce a change of the political order on the Eurasian continent. More than that, if successful, it may encourage other actors to use military force to achieve their objectives to shape political developments in their broader regional neighbourhood and divide the world into areas of national influence and power. These same actors often choose not to respect the decisions of states and peoples to pursue their own, self-chosen and peaceful path as independent actors in the international system of states.

An understanding of the characteristics, foundation and principles of global competition will be helpful to inform political and military leaders in preparing to make the right choices that will provide security for our nations.

Colonel (GS) Thomas Schroll (GE Air Force) started his military career in 1989 and was trained as a ground-based air defence officer. He went through general staff training at the German Armed Forces Command and Staff College and the UK's Joint Services Command and Staff College and has subsequently served in national and international positions at various levels of command, including in the German CHOD's office and for the SACEUR. Colonel Schroll earned Master-level degrees in Economics and Defence Studies. Currently, he is the Branch Head of Assessment, Coordination and Engagement in the JAPCC. He also serves as the Conference Director for the annual Joint Air & Space Power Conference.

Endnotes

1. UN Charter, Article 2 (3) and 2 (4).
2. National Defence University, Strategic Assessment 2020 – Into a New Era of Great Power Competition, Edited by Thomas F. Lynch III, NDU Press, Washington DC 2020, (NDU StratAss), p. 3, Figure 1.1 Continuum of Major State Interaction Postures.
3. Ibid, p. 2.
4. Ibid, p. 4.
5. Ibid, p. 2.
6. Ibid, p. 4.
7. Paul Kennedy, The Rise and Fall of the Great Powers, Random House, New York 1987.
8. Paul Kennedy referred to the production base, productivity and the strength of the military as the main dimension that enable states to succeed in competition against others. The 'NDU's Strategic Assessment 2020' offers five categories of competition: Political and Diplomatic, Ideological, Informational, Military, and Economic (which includes the 'technological breadth', 'resource base' and ability to foster 'innovation') p. 21 and page 24 (table 2.2).
9. Thomas F. Lynch III, The new Era of Great Power Competition and the Biden Administration, Joint Forces Quarterly, 4th Quarter 2021, p. 19.
10. NDU StratAss, p. 17 ff.
11. Ibid, p. 22 ff.
12. Ibid, p. 36.
13. Ibid, p. 38.
14. The White House, US National Security Strategy (NSS), December 2017, p. 2.
15. Ibid, p. 19.
16. Ibid, p. 25.
17. Ibid, p. 2.
18. Ibid, p. 27.
19. Ibid, p. 3.
20. US Department of Defence, US National Defense Strategy (NDS), January 2018, p. 2.
21. Ibid, p. 1.
22. Ibid, p. 4.
23. The White House, Interim National Security Strategic Guidance (INSSG), March 2021, p. 8.
24. Ibid, March 2021, p. 6.
25. Ibid, p. 8.
26. Ibid, p. 8.
27. Ibid, p. 14.
28. UK Government, Global Britain in a competitive age (GB), March 2021, p. 24.
29. Ibid, p. 24.
30. Ibid, p. 28.
31. Ibid, p. 49.
32. Ibid, p. 18 and p. 71. On p. 26, Russia is assessed to be 'the most acute direct threat'.
33. UK Ministry of Defence, Defence in a competitive age (DCA), p. 5.
34. Ibid, p. 15.
35. NATO Press Release (2019) 115, London Declaration, 4 December 2019, Nr. 7.
36. NATO 2030, p. 8.
37. NATO 2030, p. 16.
38. NATO 2030, p. 16.
39. NATO 2030, p. 27.
40. NATO 2030: a transatlantic agenda for the future, Speech by NATO Secretary General Jens Stoltenberg previewing the NATO Summit in Brussels at event organised by NATO, The German Council on Foreign Relations (DGAP) and The Brookings Institution, accessed on 11 April 2022 at https://www.nato.int/cps/en/natohq/opinions_184636.htm.
41. Brussels Summit Communiqué. Nr. 3, 14 June 2021.

© Moon Light PhotoStudio/Shutterstock.com

The New Era of Great Power Competition

11

Emerging Patterns and Principles

By Dr Thomas F. Lynch III
National Defense University

Note: This article is an abridged version of 'The New Era of Great Power Competition and the Biden Administration', published in Joint Force Quarterly, N° 103, 4th Quarter 2021.

Introduction

The administration of President Joseph Biden began in early 2021 amid daunting domestic challenges and an evolving era of Great Power Competition (GPC). This era, emerging since 2008, evident since 2014, and on full display since 2017 – features a three-state GPC where the United States, China, and Russia joust for international status and power, and where the trajectory of relative power from a long-dominant America to either rival remains incomplete and far from certain.[1] […]. This article […] offers a collection of observations about the evolving new era of GPC that extend and expand on the insights about past and contemporary GPC found in Strategic Assessment 2020: Into a New Era of Great Power Competition

(NDU Press, 2020)[2] […and] summarizes and applies four historic GPC principles critical to […] success in the competitive Great Power dyad with China:

- firmness with flexibility
- partnerships, alliances, and alternative geometries
- leaders vs. peoples and the poison of mass denigration
- playing for time.

[…]

Relevant History and Contemporary Dynamics

The contemporary era is […] characterized by heightened competition between more than two Great Powers. This makes it like most eras of GPC over the past 500 years, but distinct from the most recent period of Great Power competition: a bipolar Great Power rivalry between the United States and the Soviet Union that played out over a 45-year Cold War. In previous multi-polar Great Power competitions, rivalries dyads ebbed and flowed. These dyads normally involved a rising power and a dominant one, raising the strategic question about the inevitability of relative power decline by the dominant state and a power transition between them. Great Power transitions challenge rising states with the dilemma of how to assert their relative power gains without provoking an outright clash with the dominant state. Transition also confronts the dominant, but relatively declining state with the vexing question of whether its rising challenger can be accommodated in a manner that avoids destructive military clashes and an unacceptable change in the status quo. These transitions play out over decades and centuries, not years.[3]

Although three-quarters of Great Power transitions since 1500 have featured a destructive period of war between the contestants, this outcome is not foreordained.[4] Great Power competitors joined in a relative power transition can culminate their interactions with accommodation or acquiescence short of war. However, the deck is stacked against such a benign end state. Peaceful Great Power transition outcomes require hard work and astute leadership. When one or both sides in a relative power transition dyad recognize a shift in the relative alignment of economic and military power moving decisively against it, it is much more inclined to risk a pre-emptive conflict than when it perceives a stable power status quo. For the most part, the United States and Soviet Union perceived a relatively stable power balance during the Cold War, and that intense bipolar era of Great Power competition ended peacefully. […]

The US-China Competitive Dyad

The Sino-American competitive dyad is likely to be a dominant Great Power rivalry well into the future.[5] It is the modern competitive dyad most fraught with the dangerous dynamics of Great Power transition, although any misstep leading to accidental war with Russia would be enormously destructive and consequential, especially if Russia escalated to a nuclear weapons threat or use to end a conventional conflict. While some Western pundits stoke fears of an imminent and disastrous power shift in favour of China on the horizon, a net power comparison between the United States and China indicates that the power transition timeline is longer than some now fear.[6] Properly understood, this elongated timeline affords China and the United States time to better appreciate the risks of unbridled rivalry and seek a path of modulated competition with elements of confrontation and collaboration underpinning the search for mutually acceptable strategic outcomes. […]

An America that competes smartly with China in an era of multipolar Great Power competition must understand both the value of time and where it can leverage its major advantages. […] America [ha] s relative advantages in ideas, information dissemination, political and military alliances, and conventional military power when applied away from regions of local Chinese advantage inform where the United States can build on strength. […]

Four Competitive Principles

A study of historic Great Power dyadic rivals offers several principles that can enable effective American competition with China while minimizing the prospect of Great Power transition collapsing into Great Power war.[7] Four of these historical principles stand out: firmness with flexibility; partnerships, alliances, and alternative geometries; leaders vs peoples and the poison of mass denigration; and playing for time.

Firmness with Flexibility

Firstly, to be successful, the dominant Great Power must […] clearly signal the strategic aims it will defend at all costs and then offer the prospect of dialogue on those it may be willing to negotiate. While firm on its non-negotiable aims, it should be flexible in finding issues and venues where win-win outcomes are possible. For example, at the turn of the 19th century, the United Kingdom (UK) accepted American primacy in the western Atlantic as a better path to sustaining high seas primacy on vital routes for its Middle Eastern and Asian colonies – and preferable to naval confrontation in recognition of growing American power. At the same time, the rising United States came to accept the once-abhorrent British monarchy in recognition of growing political enfranchisement for a great number of UK citizens.[8] […]

Flexibility must be paired with firm resolve. Strong security arrangements, backed by formidable US military power, might harden feelings of antagonisms and suspicion, but they are indispensable to preserving the peace with China.[9] […] The United States also can firmly support democratic institutions, individual liberties, and human rights in its alliances and in its interactions with China while demonstrating flexibility in pursuing aspirations for Chinese political reform. […] During the Cold War, US efforts to strengthen non-communist elements within the Soviet bloc often met with frustration in the near term. […] But over the long term, and especially after the Helsinki Accords of 1975, these activities gave hope to those labouring for a freer future behind Moscow's Iron Curtain. American support for democracy and liberty in regions around the world during the 1970s and 1980s made the global ideological climate steadily less friendly to the Soviet Union's repressive regime.[10] This kind of Cold War competitive mind-set is applicable for competition with China today and must be melded with modern, collective approaches that portray Chinese political and ideological representations as inappropriate. Now, as then, a large amount of America's appeal is the power of an uncensored world.[11]

Partnerships, Alliances, and Alternative Geometries

History demonstrates that the dominant Great Power must look to build and maintain durable, reciprocal interstate alliances that provide would-be partners with alternatives to the either-or choices posed by a hard-charging rival.[12] Great Britain was right to seek strategic partnerships and allies in its rivalry with Napoleonic France, parlaying these alliances into first containment of the threat and later its defeat. Napoleon took a less collaborative and ultimately failed approach of largely relying on territorial conquest and installation of family members in positions of political power to expand French national power and aspects of the French Revolution.[13]

Today, the United States has a far greater base for building economic and military partnerships than any Great Power in modern history. It also confronts a rising Great Power in China with little experience or inclination in this area. The United States has invested in critical global alliances and partnerships over the years for precisely this kind of moment. […] Many of America's eager partners are today apprehensive about the recent unpredictability of US foreign policy conduct. […] They want a United States that views commitment to rules-based international order and institutions to be less like self-imposed shackles and more like a truly competitive advantage.[14] To be fully competitive with China, American policy must […] practice a competitive foreign policy that views alliances as assets to be invested in rather than costs to be cut.[15]

Leaders vs. Peoples and the Poison of Mass Denigration

Thirdly, successful Great Power competition, short of a direct military clash, is extremely unlikely if the rivals descend into a poisonous, open, and reciprocal denigration of each other's people. The choice to criticize the government of a rival state while distinguishing it from the people is not as risky, although a tightrope must be walked to maintain the difference. Once the British and Imperial German press went after the character of each other's societies, the march towards World War I accelerated.[16] So too, World War II in the Pacific loomed ominously once the United States and Tojo's Japan devolved into mutual societal recrimination played out in newspapers and journal articles.[17] In contrast, the American government's conscious Cold War effort to distinguish between the Soviet Union's communist party and the Russian people, reserving greatest criticism toward the party and offering outreach to its people, generated a far different result. […]

A responsible American program of communication should concentrate on countering Chinese Communist Party (CCP) driven disinformation.[18] […] At the same time, the United States should try to maximize positive interactions and experiences with the Chinese people. The United States and its free-and-open partner states should consider issuing more visas and providing paths to citizenship for more Chinese, with proper security safeguards in place. Chinese who engage with citizens of free countries are the ones who are most likely to question their government's policies, either from abroad or when they return home. With this approach, the United States would do what it did with expatriate Russian communities during the Cold War: view Chinese expatriate communities as valuable citizens while discriminating between Ministry of State security agents for expulsion.[19]

Play for Time

Finally, some argue that time works in favour of the rising Great Power in a competitive dyad, putting the dominant Great Power at dire risk if it does not take swift confrontational action while its relative power is high. However, this thesis rests on at least two dubious assumptions: that the rising power's ascent is likely to be rapid and that the rising power will continue to ascend in a mainly linear fashion and not confront problems or challenges along the way. In the present moment, the critical factors […] work in favour of the United States.[20] […] At the same time, a US conclusion that China is destined for global dominance, especially in the near term, is both unsupported by the facts and likely to generate strategic overreaction.[21] China's economic rise will make it a long-term challenge for the United States to manage rather than one to be conquered or converted.[22]

Policies That Fit into the Geopolitical Realities of GPC

The United States and China are destined for a lengthy, uneasy co-existence, not decoupling or appeasement.[23] Thus, as American resilience and regeneration to confront a great challenge emerges anew, a US strategy, featuring a competitive mind-set, that plays for time as China's contradictions grow, seems best suited for successful contemporary Great Power competition.[24] The Biden administration's March 2021 INSSG demonstrates an understanding of these geopolitical realities of contemporary GPC and has presented a new array of policies to meet them:

> The most effective way for America to out-compete a more assertive and authoritarian China over the long-term is to invest in our people, our economy, and our democracy. By restoring US credibility and reasserting forward-looking global leadership, we will ensure that America, not China, sets the international agenda, working alongside others to shape new global norms and agreements that advance our interests and reflect our values. By bolstering and defending our unparalleled network of allies and partners, and making smart defence investments, we will also deter Chinese aggression and counter threats to our collective security, prosperity, and democratic way of life.[25]

It remains to be seen how well the Biden administration can put these principles into practice in the face of domestic political headwinds and distracting international challenges.

Dr Thomas F. Lynch III, Colonel (ret.) joined the INSS after a 28-year career in the active duty U.S. Army, serving in a variety of command and staff positions as an armour/cavalry officer and as a senior level politico-military analyst. Dr Lynch is a member of the U.S. Council on Foreign Relations (CFR) and an adjunct professor in the Security Studies Program in the School of Foreign Service at Georgetown University. He holds a B.S. from the U.S. Military Academy at West Point, a Master's in Public Administration (MPA) and a Masters (MA) & PhD in International Relations from the Woodrow Wilson School at Princeton University.

Endnotes

1. For an operational definition of a Great Power and the criteria met by China, Russia, and the United States today that make them the three modern Great Powers, see Thomas F. Lynch III, 'Introduction', in Thomas F. Lynch III, ed., Strategic Assessment 2020: Into a New Era of Great Power Competition (Washington, DC: NDU Press, 2020), 1–15, available at https://ndupress.ndu. edu/Media/News/News-Article-View/ Article/2404286/1-introduction/.
2. For a detailed listing of these major insights, see 'Major Findings on Contemporary Great Power Competition', in Lynch, Strategic Assessment 2020, xv–xxvii, available at https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2404283/major-findings-on-contemporary-great-power-competition/.
3. Kurt M. Campbell and Jake Sullivan, 'Competition Without Catastrophe: How America Can Both Challenge and Coexist with China', Foreign Affairs (September/ October 2019), available at https://www.foreignaffairs.com/articles/china/competition- with-china-without-catastrophe.
4. Ibid.
5. China does not possess and is unlikely to attain sufficient power assets in the coming decade to enable a strategy of remaking the international order in its favour before domestic risk factors collapse Chinese Communist Party (CCP) rule even if that was its actual strategy. See Lynch and Saunders, 'Contemporary Great Power Geostrategic Dynamics: Competitive Elements and Tool Sets', in Lynch, Strategic Assessment 2020, 97–99. For an opposite view that asserts China possesses a global grand strategy aspiring for leadership of a new tributary system soon to be resourced through a massive effort organized under three overlapping policies, carrying the names 'Made in China 2025', 'Belt and Road Initiative', and 'Military-Civil Fusion', see H. R. McMaster, 'How China Sees the World: And How We Should See China', The Atlantic, May 2020, available at https://www.theatlantic. com/magazine/archive/2020/05/mcmaster- china-strategy/609088/.
6. Michael Beckley, 'The Power of Nations: Measuring What Matters', International Security 43, no. 2 (Fall 2018), 22–25; Lynch and Saunders, 'Contemporary Great Power Geostrategic Dynamics: Competitive Elements and Tool Sets', in Lynch, Strategic Assessment 2020, 96–97.
7. For an overview of these main principles based upon comparative historical case studies, see Lynch and Hoffman, 'Past Eras of Great Power Competition', in Lynch, Strategic Assessment 2020, 36–38.
8. Ibid.
9. Charles Edel and Hal Brands, 'The Real Origins of the U.S.-China Cold War', Foreign Policy, 2 June 2019, available at https:// foreignpolicy.com/2019/06/02/the-real- origins-of-the-u-s-china-cold-war-big-think- communism/.
10. Edel and Brands, 'The Real Origins of the U.S.-China Cold War'.
11. Osnos, 'The Future of America's Contest with China'.
12. Choosing proper allies also was a competitive mindset success for the United States during the Cold War. See Stephen M. Walt, 'Yesterday's Cold War Shows How to Beat China Today', Foreign Policy, 29 July 2019, available at https://foreignpolicy.com/2019/07/29/yesterdays-cold-war-shows-how-to-beat-china-today/.
13. Michael Broers, 'Pride and Prejudice: The Napoleonic Empire Through the Eyes of Its Rulers', in Napoleon's Empire: European Politics in Global Perspective, ed. Ute Planert (New York: Palgrave Macmillan, 2016), 307–317; Michael V. Leggiere, 'Enduring Strategic Rivalries: Great Britain vs. France During the French Wars (1792–1815)', in Great Strategic Rivalries: From the Classical World to the Cold War, ed. James Lacey (New York: Oxford University Press, 2016), 289–390.
14. 'Don't Be Fooled by the Trade Deal Between America and China', The Economist, 2 January 2020, available at https://www.economist.com/leaders/2020/01/02/dont- be-fooled-by-the-trade-deal-between-america- and-china.
15. Campbell and Sullivan, 'Competition Without Catastrophe', 110.
16. Lynch and Hoffman, 'Past Eras of Great Power Competition', in Lynch, Strategic Assessment 2020, 29.
17. Ibid. 34, 37.

18. For details on the organizations involved in international propaganda and influence activities, see appendix 1 in Larry Diamond and Orville Schell, eds., China's Influence & American Interests: Promoting Constructive Vigilance (Stanford: Hoover Institution Press, 2019), 133–141. Some former policymakers specifically focus on the Chinese Ministry of State Security, the United Front Work Department, and the Chinese Students and Scholars Association as ones for attention to counter CCP-driven propaganda. See H. R. McMaster, 'How China Sees the World'.
19. Proper 'safeguards' for Chinese student, teacher, and research visas should include tight limitations on Confucius Institutes in the United States to eliminate their revealed role in espionage, monitoring, and thought-policing on behalf of the CCP. The ideas for an American strategy valuing the Chinese people, while holding the CCP to account, include those found in McMaster, 'How China Sees the World'.
20. Strategic patience during the Cold War also was an American competitive mindset virtue. See Walt, 'Yesterday's Cold War Shows How to Beat China Today'.
21. For similar conclusions, see Joseph S. Nye, Jr., 'Power and Interdependence with China', The Washington Quarterly 43, no. 1 (2020), 13; Wyne, 'How to Think About Potentially Decoupling from China', 50–52.
22. Osnos, 'The Future of America's Contest with China'; Martin Wolf, 'The Looking 100-Year U.S.-China Conflict', Financial Times, 4 June 2019.
23. Osnos, 'The Future of America's Contest with China'.
24. For a detailed assessment of options for a U.S. strategic mindset for competition with China, see Frank G. Hoffman, 'U.S. Strategies for Competing Against China', in Lynch, Strategic Assessment 2020, 289–308, available at https://ndupress.ndu.edu/Media/News/ News-Article-View/Article/2404635/14-us-strategies-for-competing-against-china/. For an overview of some of the Biden administration planned initiatives to renew and improve American productivity and poise it for vigorous, successful technological and strategic competition with China into the future, see Fact Sheet: The American Jobs Plan (Washington, DC: The White House, 31 March 2021), available at https://www.whitehouse.gov/briefing-room/statements-releases/2021/03/31/fact-sheet-the-american-jobs-plan/.
25. Interim National Security Strategic Guidance, 20.

This Page Intentionally Left Blank.

© 2021 Zoomik/Shutterstock.com

The Cyber and Information Domain and the Space Domain: Links and Interdependencies

III

By Maj Gen Juergen Setzer, GE Army
Vice Chief Cyber- and Information Domain Service Bundeswehr

Introduction

For a long time in NATO's history, the three traditional operational domains – Land, Sea and Air – were the basis for deriving the necessary capabilities and providing the framework for both the strategic and operational approaches to warfare. More importantly, those three operational domains which are representing the physical environment were naturally the most appropriate order to deal with military operations. Technical as well as social developments led to accelerated interconnectivity between the three operational domains. Today, civil society and the military rely on Space as well as Cyberspace. Adversaries want to deny the use of Space-based capabilities and create operational and strategic effects in and through Cyberspace in order to deter and influence whilst remaining below the threshold of an armed conflict. Peer and near-peer opponents, who may not be capable of directly challenging NATO on a large scale and enduring conventional manoeuvre warfare, could achieve considerable effects through Cyberspace by denying the use of Space through kinetic and non-kinetic means. However, should a crisis escalate to armed conflict, where the will of an adversary to achieve its goals at any cost, then the availability of Space-based capabilities is vital for civil societies as well as for operations and combat in theatre.

New Operational Domains

Based primarily on technological developments and their social implications, – which all together make up 'the information age', NATO declared Cyberspace (2016) and Space (2019) as operational Domains, thus answering the developmental and technical challenges of warfighting in the 21st century. Closely linked to NATO's establishment of Cyberspace as a new operational Domain, Germany chose a complementary approach: the definition of the Cyber and Information Domain (CID). This was followed by the establishment of the German Cyber and Information Domain Service (CIDS) in 2017. The CID conceptually integrated the overlapping elements of Cyberspace, the Electromagnetic Environment and the cognitive layer of the information environment. The CIDS is a holistic approach to contributing to CID Operations in a Joint Operation and to provide CID capabilities as an enabler. CIDS ensures information security, provides IT-Services and ISR, as well as geospatial and environmental information. In accordance with a domain-centric perspective, the Bundeswehr located the space-based CID capabilities within the CIDS. Further, the distinction between the two domains does not depend on the physical location of the assets, but their primary military purposes from an operational point of view.

In broad outlines, this article investigates the developments that led to the revolutionary declaration of the two new operational domains, their common aspects and their relationship.

An Approach to Operational Domains

Nobody would deny the relevance of technical and social development in warfare or for use within military operations. For example, it was not just the invention of the aircraft and their military employment which turned Air into an operational domain and to bring reason to the foundation of specific Air Forces. Just the aspect of operational relevance made the difference. It is the insight that a specific approach towards a 'sphere of activity' is promising to bring about a decision of operational relevance and raise it to an operational domain. The operational effects, which can be created in such a domain, are the ends that require specific ways and means. Ways and means have to match the specific circumstances of an operational Domain and require specific leadership. These are the essential elements that all operational domains have in common.

Although the face of warfare is constantly changing, the principles and the conduct of operations are quite constant. However, how are the new operational Domains distinct? The main aspect of the shared understanding of operational art and tactics is the need to apply capabilities in time and space to compel an adversary to the point of culmination. The three traditional domains are well understood by their physical nature. The ways and means to create the physical presence of troops and capabilities at a particular place have always been dependent upon the physical nature of Land, Sea and Air. Additionally, war, conflict and constant competition create complex and dynamic environments, which make information a relevant factor for decision making, command and control, as well as a means to affect the dynamics of the operational environment, e.g. by deception. Technological developments have had a significant influence on the classical domains, primarily through constant adaption in the relevant scale of time and space. Firepower, mobility and information have always been the main influential elements which create speed, precision and effectiveness in physical domains. This enables commanders to determine the where and when of decisive actions; however, to a certain degree, the confidentiality, integrity and availability of information have always been preconditions for military efficiency and effectiveness.

Space and the Cyber and Information Domains are Information Centric

The employment of Space technology and the developments in the Cyber and Information Domains are cross-correlated from an early stage. For CID, this applies not only to Cyberspace (and computing), but also to the Electromagnetic Environment and the Cognitive Layer of the Information Environment. The human need to communicate and to gather information have always been drivers for the development of Space technology and conversely the employment of Space technology fuelled the development of technologies which constituted the CID. Both domains were catalysts for military operations in the second half of the 20th century. Space and CID changed the significance of time and space without neutralising their relevance. However, Space support to operations by satellite communications, imagery intelligence and geospatial information allow early warning, the collection and processing of vast amounts of information (big data), Command and Control, navigation and finally, quick actions, in many cases regardless of distances and in far less time than without these technologies. These aspects are of increasing relevance and often represent core elements of the centres of gravity of warfare in the information age at the strategic and operational levels, namely the confidentiality, integrity and availability of information. Space and CID are information-centric and with the introduction of the Multi-Domain Operations approach, aiming to overcome Anti Access/Area Denial, underpin the mission-critical and decisive relevance of Space support to operations also at a tactical level. These insights, connected with a growing number of capable adversarial actors, make Space and the CID a congested and contested environment. The military use of Space is well known through the Russian anti-satellite missile test on 15 November 2021. It highlighted the vulnerability of satellites to interference. Space-based capabilities can be affected by exploiting elements of the Cyber- and Information Domain. This is commonly linked to the buzzwords hacking, jamming and spoofing. In other words, attacks to, from and within Space and CID are possible. It is clear that, the impending denial of Space support to operations would, at the very least, hinder every important element of operations and mark a total loss of crucial capabilities. Therefore, the availability and resilience of Space support to operations is a persistent need for military functions and capabilities. Furthermore, they are of utmost importance for deterrence at the political level. Adversaries operating in the grey zone could create a situation in which a loss of space-based capabilities sets the conditions for decisive military action on the ground. Interference with satellites can lead to debris, creating problems on a large scale for a longer period of time,which would affect civil societies in the aftermath. That said, NATO must be vigilant as actors may take that approach and hope for a strategic window of opportunity.

Information Technology-Dependent Operational Domains

The space race of the 21st century has just begun. Today information-centric equals technology dependent. Until the turn of the millennium, nation-states and militaries have been pioneers in technological development. This has changed. Increasingly, civil companies have been shaping the progress of modern information and Space technologies. For example, Apple's invention of the iPhone was revolutionary and brought CID and Space-dependent technology into one's hand[1]. Companies like SpaceX pushed Space technology forward and changed the whole technological environment. The development cycle in Space and Cyber domains is much faster than in classical domains. Still, at the same time, it affects the need for ongoing development and of established systems. The B-52 Stratofortress has been in service for about 70 years and will most likely experience a lifespan of a full century. Just its hull will be of that age and will have seen numerous reconditioning developments due to advances in technology.

However, the life cycles of IT are much shorter and faster, and the developments labelled New Space will also shorten the life cycle of Space technology. This leads to Space and CID as constantly evolving operational environments, both characterised by growing numbers of nodes and constant development of the functionality of those nodes and their connections. It is important to note that these connections are very often cross-domain connections between Space and CID. Nodes and connections also sprawl physically and significantly into the classical domains, thus changing their nature as operational environments. In conjunction with the dynamics and complexity of both Space and CID, shorter life cycles constitute an enormous challenge for military procurement. This also sets the condition for opportunities to create synergies and enhance flexibility and resilience. The term 'constant competition' in international relations and security politics is perhaps the most concrete and tangible description of this development. Realistically the modern space race will not be about winning, but will be about a leading group of a few nations, and the number of competitors is growing.

Unexpected Actors Entering the Stage

Although potent Space and CID capabilities need cutting-edge technology, a growing number of actors are playing a relevant role. This is primarily due to the necessary technology being generally available. Considering the potential strategic and operational benefits, CID and even Space technology is relatively cheap, compared to keeping capable ground, maritime and air forces ready. Not only global powers, but also emerging powers can afford Space technology, specifically for military purposes. Additionally, terrorist groups could target space-capabilities. Attacks on ground-based infrastructure, jamming, cyberattacks and other means are readily available. This has the potential to affect positioning, navigation and timing and other critical systems. Moreover, the risk of proliferation of anti-satellite weapons is much more likely, compared to weapons of mass destruction like nuclear weapons. The number of potential hacking, disinformation and propaganda actors is literally unlimited as nation-states, companies, terrorists and criminals seek to employ Cyberspace in favour of their own goals.

Conclusion

From a CID perspective, the reliance on space-based capabilities is as multifaceted as the means to deal with the diverse challenges. Political and military decision-makers are well aware of the relevance of Space and the criticality and the vulnerabilities of space-based capabilities must be understood. Space aspects must be considered from a holistic perspective by policymakers as well as from a military point of view requiring a whole government approach. NATO and its partners need a coordinated approach towards any actions regarding Space to ensure the continuous availability of space-based capabilities for civil societies and military use in peacetime and war. States need to identify an appropriate architectural approach to finding synergies between different Space systems in order to reduce costs, maximise benefits and enhance resilience. Additionally, there is an obvious need to develop responsive space capabilities.[2] Ultimately, the world community should aim toward creating an agreed space order, aiming at the peaceful use of Space and reducing security risks.

Major General Juergen Setzer is currently assigned as Vice Chief Cyber- and Information Domain Service and Chief Information Security Officer Bundeswehr. He is in charge of Space related aspects for the Cyber and Information Domain Service Headquarters. Major General Setzer started his career as an Infantry Officer and absolved the German as well as the US Command and General Staff Course. He held several posts as a Commander, also during operational deployments in Afghanistan.

Endnotes

1. For example: GPS, Satellite Imagery, Weather Forecasts.
2. Responsive Space is understood to be the ability to launch small satellites (up to 500 kg) on demand and on call into Low Earth Orbit (LEO = ant doe start operating within day, in order to reconstitute lost capabilities, augment existing – capabilities, fill unanticipated gaps in capabilities, and enhance survivability and deterrence (www.japcc.org/responsive-space-for-nato-operations).

THREATS

© Comfreak/Pixabay

Thresholds in Cyber and in Space

IV

Lessons Learned from State Positions on the Application of International Law to Cyber for the Evolving Space Domain

By Mr Sebastian Cymutta, Law Researcher
NATO Cooperative Cyber Defence Centre of Excellence

Introduction

On January 17th of 2022, NATO published its 'Overarching Space Policy',[1] laying down the Alliance's understanding and posture with regard to space. This policy document is a direct follow up to the 2021 NATO summit in Brussels and integrated the statement of the summit's communiqué regarding Article 5 of the North Atlantic Treaty[2] with almost identical wording:

'(…) Allies agreed that attacks to, from, or within space present a clear challenge to the security of the Alliance, the impact of which could threaten national and Euro-Atlantic prosperity, security, and stability, and could be as harmful to modern societies as a conventional attack. Such attacks could lead to the invocation of Article 5.'[3]

This part of the communiqué came across as logical, seeing that NATO already declared space as an operational domain in December 2019.[4] Moreover, it mirrors the approach taken by NATO with respect to interference in cyberspace. With regard to cyberspace, the Alliance first clarified the applicability of Article 5 of the North Atlantic Treaty during the 2014 Wales summit[5] before assigning cyberspace the status of an operational domain two years later in Warsaw.[6]

Comparing the declarations of Wales (concerning cyber) and of Brussels (concerning space) with regard to when Article 5 of the North Atlantic Treaty would be activated, the wording is almost identical as well:

'A decision as to when such attacks would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis.'[7]

While law and policy are sometimes ambiguous, with the prevailing view that international law applies to cyber operations,[8] a robust understanding regarding the operationalization of the cyber domain has emerged.

Even though there is a legal framework for space in existence[9] (which is not the case for cyberspace), some of the most pressing legal issues regarding that domain are identical to those discussed regarding cyber. The most prominent question revolves around the threshold for an 'armed attack' in the sense of Article 51 of the UN-Charter.[10] Closely connected is the question, of when the threshold to a prohibited 'use of force' according to Article 2(4) of the UN-Charter has been crossed.

The Cyber Discourse Regarding 'Thresholds'

These thresholds play an essential part when nations try to fill the above-mentioned 'case-by-case'-paradigms with life.

In July 2021, the United Nations Group of Governmental Experts published an official compendium of voluntary national contributions on how international law applies to the use of information and communication technologies by states.[11] While the comprehensiveness of this compendium is gradually decreasing as more and more nations continue to publish their state positions, these policy documents continue to provide practical solutions for the thresholds of armed attacks and the prohibited use of force.

Use of Force

The concept of the prohibition of the use of force, as it is enshrined in Article 2(4) of the UN-Charter, was shaped by the so-called 'Nicaragua Judgement' of the International Court of Justice (ICJ) in 1986.[12] Here, the ICJ established what has come to be known as the 'scale and effects'-test for determining if a certain state action qualifies as an 'armed attack'[13] while addressing the duality of the concept of 'use of force' in Article 2(4) and 'armed attack' in Article 51.[14]

These considerations still provide guidance today and have been adopted by the Tallinn Manual 2.0[15] to clarify the application and purpose of the prohibition of the use of force regarding cyber operations.[16] Although nations do not endorse them, the rules formulated by the Tallinn Manual 2.0 have nevertheless proven to be very influential[17] in the drafting of state positions.

While the benefit of translating the principles of the 'Nicaragua Judgement' into 'Tallinn Manual rules' for discussing the application of international law to cyber-operations is undeniable, it still leaves room for interpretation. Here, state positions benefit the discourse by commenting on certain situations, clarifying ambiguous legal terms and showcasing scenarios.

For example, the Norwegian State Position published in late 2021 reiterates that Norway would consider inter alia 'cyber-operations leading to the destruction of stockpiles of Covid-19 vaccines, which could amount to the use of force in violation of Article 2(4)'.[18]

Furthermore, there appears to be a growing willingness of states to assume a violation of the prohibition of the use of force by cyber-operations that do not result in physical effects. France is the most outspoken proponent of this view when it 'does not rule out the possibility that a cyber-operation without physical effects may also be characterized as a use of force'.[19]

Armed Attack

While some states would consider the legal effects of the terms 'use of force' and 'armed attack' synonymous[20] most states that have commented on this topic distinguish between the two concepts.

When the Tallinn Manual 2.0 proposed that

'A State that is the target of a cyber-operation that rises to the level of an armed attack may exercise its inherent right to self-defence',[21]

many nations subscribed to this rule,[22] effectively integrating it into their state positions on how international law applies to cyber.

As with the 'use of force threshold', there is a growing tendency to open up the concept of incorporating scenarios which are void of physical effects. For example, when discussing which factors to consider when assessing the effects of a cyber-operation, Germany points out that also 'injury and death (including as an indirect effect)' [23] could be taken into account. France puts forward the idea that even 'considerable economic damage' could be a deciding factor when appraising the legal consequences of a cyber-attack.[24]

Though not a predetermining factor, many states pointed to the impairment of critical infrastructure as a factor to be considered when assessing the 'scale and effects' of a cyber-operation potentially being categorized as an armed attack.[25]

Implications for the Space Debate

Legal questions regarding the application of international law in space have been discussed quite vividly in the last years. In accordance with Article III Outer Space Treaty, this paper will presume that Article 2(4) and Article 51 of the UN-Charter are applicable in the space domain.[26]

The following paragraphs will explore the implications of the above-mentioned state positions for the legal operationalization of space.

Use of Force

Leaving aside kinetic measures against space infrastructure,[27] it is conceivable that a cyber-attack could affect space assets like satellites and render them inoperable without creating physical damage. As more states are willing to consider attacks void of physical consequences as a use of force,[28] the 'scale and effects'-test needs to be applied to such a scenario.

Space infrastructure provides for many services considered essential today (for example, navigation, communication and banking). Thinking about the reliance of not only the national governments but also of private businesses and citizens, widespread service denials caused by a cyber-operation adversely affecting the provision of satellite services could easily be considered as breaking the 'use of force threshold'.

Armed Attack

Staying with the picture of a 'threshold', there is a logical step to be taken to consider an attack in the space domain not only a 'use of force' but also as 'armed attack'. That means that the allegorical 'threshold' to an 'armed attack' is actually an instrument to distinguish the scope of application of Article 2(4) and 51 of the UN-Charter from each other while at the same time underlining the interconnectedness of these concepts.

If states are willing to consider non-physical results sufficient for the invocation of Article 5 of the North Atlantic Treaty, the simple fact that almost all western nations are reliant upon space-satellite services is making it more likely that an attack against space infrastructure – whether staged through cyberspace or not – could cross this threshold.

Conclusion

Space has become NATO's 5th distinguished operational domain of warfighting, yet every major mission or operation has to be conducted in a cross-domain setting'.[29]

Hence, it is important not only to think of these domains together but also not to reinvent the wheel with regard to legal issues that have already been addressed in the context of the other domains.

Therefore, the author proposes referring to the lessons learned in the cyber domain to facilitate the evolution of NATO's legal posture in outer space.

Mr Sebastian Cymutta studied law at the University of Münster (Germany) as well as the University of Tartu (Estonia). After passing the German Bar, he started his career as a Legal Counsel with the German Aerospace Centre in Cologne in 2014, before moving on to the German armed forces as a Litigator (2015) and later as a Senior Adviser (2017). As of 2019, he is seconded to the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn (Estonia) as a Law Researcher. There, he focusses on the application of international law to cyber operations as well as to emerging technologies.

Endnotes

1. https://www.nato.int/cps/en/natohq/official_texts_190862.htm; hereafter referred to as 'Overarching Space Policy'.
2. https://www.nato.int/cps/en/natohq/news_185000.htm, para 33.
3. Overarching Space Policy, para 12.
4. https://www.nato.int/cps/en/natohq/official_texts_171584.htm, para 6.
5. https://www.nato.int/cps/en/natohq/official_texts_112964.htm, para 72.
6. https://www.nato.int/cps/en/natohq/official_texts_133169.htm, para 70.
7. Overarching Space Policy, para 12 and for cyber https://www.nato.int/cps/en/natohq/official_texts_112964.htm, see para 72, referring to 'cyber attacks'.
8. This opinion has been emphasized by numerous state position reflecting this point, amongst them Germany, France and Norway, just to name a few.
9. Most notably, the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies ('Outer Space Treaty').
10. This Article is the key reference in Article 5 of the North Atlantic Treaty.
11. Accessible here: https://www.un.org/disarmament/group-of-governmental-experts/.
12. CASE CONCERNING MILITARY AND PARAMILITARY ACTIVITIES IN AND AGAINST NICARAGUA, Judgement of 27 June 1986, henceforth referred to as the 'Nicaragua Judgement'.
13. Nicaragua Judgement, para 195.
14. Implying, that only the gravest forms of the 'use of force' could be considered an armed attack, effectively putting the two concepts into an escalatory hierarchy, see Nicaragua Judgement, para 191.
15. The Tallinn Manual 2.0 on the International Law applicable to Cyber Operations, Cambridge University Press, 2017.
16. See Tallinn Manual 2.0 rule 69, para 1.
17. See On the Application of International Law in Cyberspace Position Paper – March 2021 (henceforth referred to as the German State Position), available here; https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf, which is repeatedly referencing the Tallinn Manual 2.0, e.g. II.a.; II.c.

[18] Norwegian positions on selected questions of International Law relating to Cyberspace (henceforth referred to as the Norwegian State Position), para 3.3, see: https://www.regjeringen.no/contentassets/a8911fc020c94eb386a1ec7917bf0d03/norwegian_positions.pdf.

[19] See International Law applied to Operations in Cyberspace (henceforth referred to as the French State Position), para 1.1.2; also, the Norwegian State Position is leaning into this direction see footnote 19, para 3.3.

[20] The United States of America being the most outspoken proponent of this idea.

[21] Tallinn Manual 2.0, rule 71.

[22] Expressis verbis German State Position, para IV.b.4; 'Germany concurs with the view expressed in rule 71 of the Tallinn Manual 2.0'.

[23] German State Position, para IV.b.4.

[24] French State Position, para 1.2.1.

[25] Ibid; Norwegian State Position, para 3.3.

[26] Häussler, NZWehrr 2020, 221(223).

[27] Froehlich, NATO Legal Gazette, 86(95), rightfully argues that these actions should be considered an armed attack.

[28] See supra note 19 and 23.

[29] For further analysis, see Maj Fotios Kanellos', Defending Space in and through Cyberspace, JAPCC Journal Edition 33, 2021, p. 36–41.

This Page Intentionally Left Blank.

© LuckyStep/Shutterstock.com

Deterrence in the Space Domain

V

Increasing Deterrence in Space by Gaining a Mindset for Agile Space Operations

By Maj Gen Michael Traut, GE Air Force
Commander German Space Command

Dr Dirk Zimper, Christoph Müller, Wolfgang Jung, Dr Andreas Ohndorf
German Aerospace Center

The Need for Understanding Deterrence in the Space Domain

At Brussel's NATO Summit in 2020, NATO Secretary General Jens Stoltenberg launched the #NATO 2030 effort remarking that **'resilience – be it infrastructure, telecommunications, 5G or healthcare, access to protective equipment – all of that matters for the civilian society, but it actually also matters for NATO as a military alliance and our military capabilities. […] making sure that we have credible deterrence and defence, because that's the best way to prevent a conflict, is to remove any room for doubt, any room for miscalculation about NATO's readiness, willingness to protect all Allies. And as long as we provide that deterrence, there will be no conflict, no attack.'**[1]

With that NATO's Secretary General was basically voicing the general trend, following a number of member states recognizing the importance of space for their economies and as a warfighting domain. Since the United States established a new Command responsible for the Space Domain, other NATO members such as the United Kingdom, France, and Germany acknowledged the importance of space by setting up their respective commands. Consequently, NATO nations and NATO itself decided to bolster their expertise and operational structure by establishing NATO's Space Centre at Allied Air Command and to set up a dedicated Centre of Excellence for Space.

In recognizing the importance of space, all national efforts are supposed to aim at ensuring the best support to the Alliance's operations, missions and broader security – as well as the prosperity of their economies. The Alliance as well as its member nations underline the alignment with international law and defensive nature of their policies and actions in space. In parallel, **NATO recognises that attacks to, from or within space present a clear challenge to the security of the Alliance and could lead to the invocation of Article 5 of the North Atlantic Treaty** anchoring space deeply in the heart of the Alliance. [2]

In recent decades, space has become a central element for our society. Protection of critical infrastructures in space and on Earth is a priority task for maintaining crucial functions. Likewise, military operations and missions critically depend on NATO Space Functional Areas such as Positioning, Navigation and Timing (PNT), Shared Early Warning (SEW); secure Satellite Communication (SATCOM); Intelligence, Surveillance and Reconnaissance (ISR); Space Situational Awareness (SSA) and Space Weather (Space Wx). Current and future developments across all domains will further accelerate the dependency of the Alliance on Space Support to Operations.[3]

Consequently, in order to fully recognize the opportunities and challenges of the Space Domain, NATO has to strive for robust and resilient policies, as well as an organisation and a technology base. Besides actively securing reliable services from Space, it has to be made clear to any potential adversary that any attempt to degrade, disrupt or deny NATO's or member states' Space capabilities would be unsuccessful and would potentially lead to harmful responses in turn. The military principle of deterrence will work in the Space Domain by creating redundant, robust and standardised structures as well as providing flexible and responsive capabilities.

To create resilience, the existing NATO Integrated Air and Missile Defence could serve as a role model. Interoperability by standardisation of procedures, connectivity for seamless information exchange, integrating national and NATO capabilities and contributions in a robust, meshed network have been cornerstones of NATO's successful defensive posture in the Air Domain for decades. Even now in the light of the ongoing crisis at NATO's eastern flank, NATO's air defence proves to be swift, present, flexible and deterrent.

Besides a robust and redundant standing structure, the capability to quickly reconstitute lost elements, augment existing capabilities, fill unanticipated gaps and enhance survivability in space, i.e. a Responsive Space Capability, is crucial. By generally applying the respective principles and adopting a corresponding mindset, NATO and its members will foster integration and standardization of their space capabilities in a way that finally will uphold their collective deterrence posture in the Space Domain.

The Space Domain in NATO's Deterrence Posture

Deterrence, either in space or in any other domain, can be understood as an **'action of discouraging an [adverse] action or event through**

instilling doubt or fear of the consequences'.[4] In space, such harmful interference can be conceived as the loss, disruption, or degradation of space-based services, activities, or capabilities either as a whole or as a function of each of the elements of a space architecture – launch, ground, link, space and mission segment.

Capability, communication and credibility are commonly understood as the key characteristics of sincere deterrence. It requires to have the capabilities to punish and/or deny hostile actions. The consequences need to be communicated to and anticipated by possible opponents. Additionally, measures have to be perceived as credible regarding their extent and the willingness of the actor to suffer counter-retaliation or escalation.[5]

In its 2020 analysis on the U.S. Space Forces, the Center for Space Policy and Strategy has concluded that, even under optimal circumstances, **Deterrence by Punishment** will be most demanding, not only due to the technological challenges but particularly due to uncertainties about the adversary's perception. **Deterrence by Denial**, i.e. the absorbing of an attack through a robust and resilient Space Domain design at any time and place, might in comparison be the most encouraging approach towards deterrence in the space domain.[6] Hence, **Deterrence by Punishment** will remain the **ultima ratio** that will most likely be feasible only for a few NATO members.

Deterrence in the Space Domain will need to follow a nuanced policy. Moreover, space policies must not be viewed in isolation and have to be holistically discussed to prevent adversaries from exploiting vulnerabilities. New hybrid space architectures in combination with an overarching Responsive Space mentality will pave the way for a more robust and resilient deterrence posture in the Space Domain.[7] More technical speaking, effective deterrence is based on three factors – technological superiority, resilient system architecture, and the operational capability to implement it faster than the adversary.

Responsive Space – A Viable Answer?

Responsive Space ensures unhindered access to information, products and services from space by enabling redundant, interoperable, heterogeneous systems to be networked together. Degraded capabilities can be replaced immediately by re-routing of tasks or rapid replacement of failed systems. Building the technology base, demonstrating innovative and disruptive technologies, and translating them into operational capabilities within NATO is paramount to maintaining superiority and resilience in space.

Resilience is generally understood as robustness and survivability, i.e., the ability of a system to continue to function to an acceptable level or recover quickly after a disruption of any kind and from any source. The resilience of a system can be increased through various techniques, either disaggregation, distribution, diversification, proliferation, or protection. Reconstitution differs slightly because additional satellites must be launched or additional ground stations activated to restore a damaged space-based service.[8]

To be able to replace lost capabilities or services on demand and on call within weeks, days or even hours, it is necessary to build a Responsive Space capability. In a holistic and integrated approach, the entire operational chain ranging from launch to ground, link and space segment must be able to implement this rapid deployment and entry into service. The capability shall be fail-safe, i.e., redundant and resilient in its operational availability. Mobile, deployable and systems capable of being integrated are of interest, as is the ability for interoperability and combined Command and Control (C2).

In order to exploit the full range of possibilities, connectivity and data exchange between heterogeneous C2 systems will be one of the challenging tasks in the future. Connectivity requires interoperability through compatibility, similarly to the implemented Link 16 standard in the air domain. Modular open system architectures instead of proprietary systems are necessary to allow future C2 concepts. Connectivity with low latencies among the systems will pave the way for future multi-domain operations.[9] By additional integration of available commercial services into hybrid space architectures, military and political decision makers are enabled to keep up with rapid changing operational requirements.[10]

In addition, technological challenges have to be addressed by research and industry following a Responsive Space mentality. Components, systems, architectures and operations need to address that approach.[11] Moving away from isolated operations and proprietary systems will be an imperative. Leveraging higher numbers of single sensor or single task systems will likewise require advances in supervised autonomous operations of formations in hybrid architectures. Furthermore, it would require robust access to space enabled by Single Orbit Launch and Early Orbit Phases (LEOP) as well as resilient on-demand launch capabilities.[12]

To keep pace with the dynamic technological evolution of potential adversaries, it will be essential that NATO member nations participate in the joint development, sustainment, and evolution of state-of-the-art space-based capabilities. General Raymond, U.S. Chief of Space Operations, underlined that **'the grand challenges cannot be met by individual nations'.**[13] A joint approach is essential for success. Multilateral efforts such as the Combined Space Operations Initiative (CSpO) strive to align operational processes between multinational partnerships. Importantly, CSpO includes collaboration on enhanced Space Situational Awareness, data sharing and multinational command and control amongst the United States, United Kingdom, Canada, Australia, New Zealand, Germany and France to support space activities.[14]

Augmenting NATO's Deterrence Posture in the Space Domain by Responsive Space mentality

NATO as an Alliance does not intent to have its own space-based assets nor any infrastructure in space. Hence, all space-related capabilities, developments or research have to be provided by member nations or have to be procured from commercial providers by NATO agencies.[15] As a consequence, all efforts have to aim towards highly integrated and networked space-based capabilities.

In January 2022, NATO published its **Overarching Space Policy** outlying its basic principles and tenets consistent with its overall posture. Most importantly, it states the further lines of effort on its approach to deterrence, defence, and resilience in the Space Domain. These efforts must be addressed by Responsive Space Capabilities and require further considerations to augment the Alliance's deterrence posture[16].

First, a coherent response to threats will need to consider a range of potential options across the conflict spectrum. Applying the Responsive Space mentality to its maximum extent possible, will allow the Alliance's deterrence posture in the Space Domain to absorb hostile actions quickly and without actively stressing NATO's or nations' decision-making processes.

Second, the Alliance and its member nations will have to develop a common understanding of concepts. Harmonizing their individual approaches to Responsive Space Capabilities will primarily require defining and imposing further standardization.[17]

Third, readiness is considered a cornerstone within all operational domains. Hence, striving for operational availability across all space related services will be key and is generally augmented by a Responsive Space mentality.

Fourth, by exploiting further international cooperation and collaboration, the Alliance will gain force-multiplying redundancies. The underlying imperative of networking in Responsive Space capabilities will further accelerate this required process.

Furthermore, the Alliance shall strive for guidelines on access to space data, products, services and capabilities. Leveraging NATO's Science & Technology Organization and multinational efforts such as CSpO to its maximum extent possible, advance on Responsive Space capabilities will holistically foster its deterrence posture.

In summary, fostering a viable Responsive Space mentality and translating it into applicable policies augmenting NATO's existing Overarching Space Policy will be essential to transfer NATO's collective deterrence posture to the Space Domain. Responsive Space capabilities will allow all member nations to contribute to the Alliance's collective defence effort and strengthen the principle of **deterrence by denial**.

Major General Michael Traut is serving as the first Commander of the newly established Bundeswehr Space Command and as the Director of National Air Operations in Uedem. After holding staff positions in numerous military organizations, he most recently served as the Commandant of the Air Force Officer School as well as the Chief of the Armed Forces Training Division in the Headquarters of the German Joint Support Service. As trained Interceptor Controller and Interceptor Controller Instructor, General Traut studied Computer Science at the Bundeswehr University Munich and accomplished his Master as a Member of the Royal College of Defence Studies in London.

Mr Christoph Müller Is serving as Head of Defence Research at the German Aerospace Centre's (DLR) overall Program Coordination for Defence & Security Research. He was previously seconded to NATO's Science & Technology Organisation as Executive Officer in Neuilly-sur-Seine, France, from 2017 to early 2020. He also served twelve years in the German Armed Forces commanding an Explosive Ordnance Disposal platoon specialized in CBRNe including one assignment to the International Security Assistant Force (ISAF) in Afghanistan.

Mr Wolfgang Jung started as Reserve Officer for Tactical Ballistic Missiles (MGM-52 Lance), followed by two Academic Degrees (Aerospace and Space Systems Engineering). In the last 25 years at DLR's Mobile Rocket Base (MORABA) he was responsible for Launch Services and designing new Hypersonic Flight Vehicles. In 2019 he was nominated as DLR's Coordinator for Responsive Space. Since 2021, he has been responsible as Head of Technology and Head of Department for Technology Demonstration in the newly established DLR Responsive Space Cluster Competence Center (RSC3). Besides this, he supports the Air Force Command in Berlin in a Reserve Officer capacity.

Dr Andreas Ohndorf joined the German Air Force in 1996 and holds a doctoral degree in Aerospace Engineering. Professionally trained as an aircraft technical officer, he served in a fighter wing maintenance group as well as in several air force material command positions. Since 2008 he works at DLR in the mission operations department of the German Space Operations Center (GSOC) and further leads the ground segment department of the Responsive Space Cluster Competence Centre at DLR since 2020.

Dr Dirk Zimper joined the German Air Force in 2004 and holds a doctoral degree in Aerospace Engineering. Professionally trained as an ammunition specialist, he commanded a specialized maintenance unit for aerial missile systems. From 2013 to 2016, he served as Executive Officer for the Applied Vehicle Technology Panel at the NATO Science and Technology Organization. In 2019, was appointed as Executive Board Representative Defence and Security Research and, in 2020, as Managing Director to the Responsive Space Cluster Competence Center at DLR. Furthermore, he is a Member of the Science and Technology Board and is an advisor to the FMoD and the Munich Security Conference.

Endnotes

1. NATO, Remarks by NATO Secretary General Jens Stoltenberg on launching #NATO 2030 – Strengthening the Alliance in an increasingly competitive world, 2020. Retrieved from https://www.nato.int/cps/en/natohq/opinions_176197.htm on 3 April 2022.
2. NATO, NATO's approach to space, 2 December 2021, retrieved from https://www.nato.int/cps/en/natohq/topics_175419.htm on 4 January 2022.
3. Vasen, T., Joint Air Power Competence Centre, Resiliency in Space as a Combined Challenge for NATO, August 2021.
4. Jah, M. K., The University of Texas at Austin, Deterence in the Space Domain, 2018.
5. Gleason, M. P., Hays, P. L., Center for Space Policy and Strategy, Getting the most Deterrent Value from U.S. Space Forces, 2020.
6. Gleason, M. P., Hays, P. L., Center for Space Policy and Strategy, Getting the most Deterrent Value from U.S. Space Forces, 2020.
7. Boyce, B, Air & Space Power Journal Vol. 33, Issue 1, Twenty-First Century Deterrence in the Space War-Fighting Domain, Spring 2019.
8. Vasen, T., Joint Air Power Competence Centre, Resiliency in Space as a Combined Challenge for NATO, August 2021.
9. Carlisle, H. J., Joint Air & Space Power Conference 2019, The Complexity of Multi-Domain Operations of the Future, 8–10 October 2019.
10. La Cruz Caravaca, F., Joint Air & Space Power Conference 2021, Dynamic C2 Synchronized Across Domains, 7–9 September 2021.
11. Jung, W., Vasen, T., Zimper, D., JAPCC Journal 32, Responsive Space for NATO Operations – Part 2, September 2021.
12. Jung, W., Vasen, T., Zimper, D., JAPCC Journal 33, Responsive Space for NATO Operations – Part 3, December 2021.
13. Raymond, J. W., 36th Space Symposium, August 2021.
14. Jung, W., Vasen, T., Zimper, D., JAPCC Journal 32, Responsive Space for NATO Operations – Part 2, September 2021.
15. NATO, Science and Technology Committee, Space and Security – NATO's Role. 2021.
16. NATO, NATO's Overarching Space Policy, 17 January 2022, retrieved from https://www.nato.int/cps/en/natohq/official_texts_190862.htm on 29 January 2022.
17. Jung, W., Vasen, T., JAPCC Journal 31, Responsive Space for NATO Operations, February 2021.

This Page Intentionally Left Blank.

© Tod Seelie

Developing an Operational Framework to Enable Interoperable Allied NATO Responsive Space Activities

VI

Space Capabilities that are Allied by Design

By Mr John Fuller and Mr Bret Perry
Virgin Orbit

Introduction

With NATO facing a contested space domain, members have begun exploring responsive space capabilities that enable rapid deployment of space assets providing critical Data, Products, and Services (DPS). As explained by US Army General James Dickinson of the US Space Command (USSPACECOM), 'During conflict, the ability to rapidly reconstitute degraded systems within hours forces adversaries to rethink the economic benefit of attacking on-orbit assets. This capability allows USSPACECOM to provide warfighters continuous access to space-based capabilities for multi-domain overmatch.'[1]

The opportunity now exists to develop a NATO-specific responsive space architecture.[2] While several allies are deploying their own satellites and developing sovereign spaceports, the procedures and mechanisms for jointly executing responsive space operations do not yet exist. As responsive space activities are complex, a common set of operational processes is critically needed to achieve NATO interoperability.

This paper describes a framework for NATO members to field an interoperable responsive space capability. Through a scenario depicting the deployment of a responsive launch system to an allied spaceport, it highlights acquisition and infrastructure considerations for conducting joint responsive operations. It provides readers insight into how to direct allied responsive space investments so that duplicative effort is prevented, maximizing resources for the benefit of the alliance.

Coordinating Responsive Space Investments & Program Management

While the advent of small satellite platforms are enabling NATO members to deploy sovereign space capabilities, the unique challenges associated with acquiring and deploying space capabilities remain. It is impractical for every NATO member to finance and develop their own end-to-end space capabilities; multilateral collaboration is needed.

However, the commoditization of microsatellite platforms and emergence of layered constellations provide a foundation for joint space missions. This includes horizontal responsive space systems – in which different components, such as the satellite, encapsulated payloads, launch vehicle, carrier aircraft, and mission operations, can be shared across different allies. The ability to segment a responsive space system enables allies to coordinate investments by which each country owns or funds a specific element (e.g., one country funds the ground support equipment and another country manages the carrier aircraft). Distributing a responsive space architecture across multiple allies is more cost-effective than having each member own and operate their own standalone systems.

To build this interoperable, disaggregated responsive space architecture, NATO members will require a common program management framework. The challenges associated with space acquisition reinforce the need for allies to coordinate their investment and program management activities. A central program management and acquisition mechanism is needed to coordinate allied investments in responsive space capabilities to minimize these risks.

In building out a multilateral responsive space capability, allies can leverage the NATO Support and Procurement Agency (NSPA) to centralize the program management. Unlike other multilateral responsive space initiatives that are limited to research and development activities (e.g., the Responsive Space Capabilities MOU), an NSPA Support Partnership can facilitate the acquisition, management, and sustainment of a responsive space system. The forthcoming NSPA Support Partnership agreement on commercial satellite communications (SATCOM) provides a precedent for how NSPA can support space projects; the NSPA Multinational Multi-Role Tanker and Transport Fleet provides a template for the procurement of shared complex systems.[3,4] An NSPA Responsive Space Support Partnership would allow allies to focus on space requirements development, mission design, and space operations, allowing NSPA to become an allied centre for expertise in space program and acquisition management.

Demonstrating Multilateral Responsive Space Interoperability with a Mission Scenario

While the previous section described a concept for how allies could coordinate the investment of an allied responsive space system, NATO's employment of an interoperable responsive space capability is best demonstrated through a case study describing member states' responses during a scenario. This case study is predicated on future NATO investments into a responsive space architecture and the following assumptions:

- A NATO responsive space framework, as described in 'Leveraging Responsive Space and Rapid Reconstitution' is established.[5]
- Responsive horizontal launch infrastructure, launch vehicles, and a shared carrier aircraft have been designated across compatible airports within example allied states of the US, the UK, Germany, Luxembourg, the Netherlands, Norway, Poland, Italy, Portugal, and Spain.
- A space cargo and mission logistics hub is established in the central European theatre, hosting the single carrier aircraft, mobile ground support equipment, and/or air-launched rocket vehicles.
- Pre-selected and spacecraft payload processing facilities are maintained in Italy, Germany, and/or the UK.
- A unified responsive space program management mechanism forms the foundation of a NATO-allied interoperable responsive launch framework.

A European network of airports compatible with horizontal launch already exists.[6] Establishing a grouping of facilities that can support an allied responsive launch network is a matter of technical and regulatory evaluation. Most allies possess one or more airports capable of handling such activities, which operate under shared Eurozone airspaces and control authority. The case study assumes at least one launch-compatible spaceport per member state mentioned above.

A cost-effective interoperable responsive launch framework can be maintained with a minimized quantity of mobile launch assets. Rather than utilizing several launchpads with separate at-the-ready launch vehicles and ground support equipment, a single or few sets of launch assets are shared across different compatible spaceports. Leveraging those mobile assets to reduce the barriers for launch execution across those spaceports is key.

Case Study

This case study begins with an exemplary definition of NATO's responsive horizontal launch architecture. Given its central geographic location and air freight activity, Luxembourg is notionally chosen as a cargo and mission logistics hub to host mobile launch assets, including a carrier aircraft and supporting mobile ground support equipment. Attached to the central hub are the spokes of the allied interoperability model. Each of the other allies hosting a compatible spaceport are these spokes.

Resilience of satellite constellations is enabled by the guarantee of readily replacing on-orbit assets that are disabled. NATO allies can achieve this by locally storing ground spares of their spacecraft, which are pre-encapsulated and adhere to a launch standard already established as part of the horizontal launch service. The spacecraft would be pre-configured for certain Intelligence, Surveillance and Reconnaissance (ISR), Space Domain Awareness, or SATCOM missions leveraging commercially developed payloads. Security needs can be assured given that the encapsulated modules remain in-country until launch. In-country payload processing infrastructure can be maintained to the scale required by the desiring member state for added flexibility. The infrastructure lifecycle management would be managed by NSPA via the terms of a Support Partnership involving the participating allies.

The need for responsive space arises when a critical on-orbit asset is disrupted or lost. In this scenario, a sun-synchronous (SSO) Earth observation ISR satellite used by allies to observe territory in Eastern Europe ceases responding with the asset feared lost. Heightened tensions alongside loss of the asset are cause for concern given adversarial military operations in the region. Replacement of the satellite becomes an urgent requirement with a radar satellite identified to penetrate cloud coverage and provide ground moving target indicator data over contested areas.

Mobilization of the responsive space architecture begins with the activation of horizontal launch assets – the carrier aircraft and its mobile ground support equipment – in Luxembourg. Pre-encapsulated satellites that are compatible to replace the missing asset are already stored near their payload processing facilities in the UK, as well as Germany and Italy. Of the compatible spaceports that are present, Germany is chosen to host the launch given its proximity to the ground support equipment and carrier aircraft positioned in Luxembourg. The carrier aircraft is flown to the German airbase to begin the launch campaign alongside an operations squadron of allied personnel trained in launch operations.

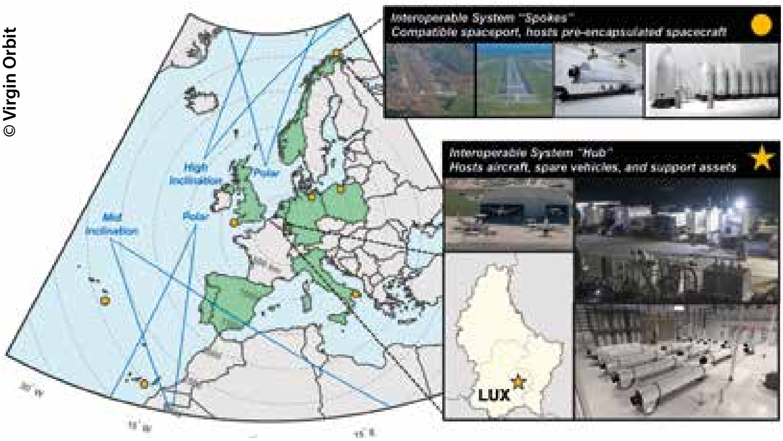
Pre-designed shipping logistics are employed, where support equipment and launch vehicle are air-shipped from Luxembourg to the waiting carrier aircraft and pre-encapsulated payload in Germany. Integration of the system on a pre-conceived but austere operations pad occurs within a 24-hour window, followed by a launch operation where the vehicle is fueled and readied for takeoff. Mission Control activities are managed by a remote central command centre, possibly facilitated by existing NATO Allied Air Command facilities.

Launch activities after takeoff follow a design scheme that is agnostic to the originating spaceport in Germany. Aside from the departure flight path of the aircraft, the launch vehicle release site and trajectory would be pre-designed as part of a Eurozone orbital access plan. This modularity in mission design continues the theme of interoperability, where shared azimuth corridors can permit a wide degree of inclination access to any NATO member state. Examples of these azimuth corridors are shown in Figure 1, indicating that a wide degree of access to orbits inclined between 45 degrees and SSO may be possible with a horizontal launch system.

In the case of this scenario, a mission racetrack and launch point in the North Sea is most appropriate for rapid launch into SSO with shared telemetry assets sourced from the UK and Norway. The carrier aircraft would reach this site within an hour of takeoff, where the launch vehicle would release and carry the spacecraft into a precise replacement orbit for the lost asset within approximately an hour thereafter. Mission operations could then seamlessly pass from the launch command centre to spacecraft operators. Once deployed, the spacecraft would leverage advanced automation and asynchronous system evaluations to be rapidly commissioned, making it available to tasking requests from allied Space Support Coordination Elements.

Despite having sourced the carrier aircraft, support equipment, rocket, and payload from separate locations, a responsive and interoperable architecture enabled integration and launch of the united system within 24 to 48 hours. The carrier aircraft, supporting ground assets, and operations team would return to their original stand-down locations across the member states, or to their roles as part of commercial European launch operations.

Similar operations could have also occurred in other member states with waiting pre-encapsulated payloads. While Germany was chosen due to proximity


Interoperable System "Spokes"
Compatible spaceport, hosts pre-encapsulated spacecraft
Interoperable System "Hub"
Hosts aircraft, spare vehicles, and support assets
High Inclination
Polar
Mid Inclination
Polar
LUX
30° W
15° W
15° E

© Virgin Orbit

Figure 1: *Illustrative European Disaggregated Horizontal Responsive Space Concept*

and convenience, other states such as those highlighted in Figure 1 could likewise host launch operations with access to the very same airspaces and orbital access corridors. This flexibility is of most value in scenarios when shared launch assets aren't necessarily headquartered in a single location. The hallmark of interoperability is that there is no limit to the variety and scale of NATO launch operations made possible with mobile horizontal launch infrastructure.

Conclusion: Leveraging Responsive Space Operations to Enable Resilient NATO Space Capabilities

This scenario exemplifies how NATO members can coordinate their investments and leverage the flexibility of horizontal launch systems to conduct joint responsive space missions. The prospect of joint NATO space missions is necessary to preserve space-based DPS for NATO members; as explained by General Raymond, Chief of Space Operations of the US Space Force, 'I really would like to get these partnership[s] to be more than just data sharing partnerships and really move towards mission sharing.'[7] In particular, a responsive space demonstration would create an opportunity for NATO allies to practice and exercise the multilateral CONOPs described in the aforementioned scenario.

Ultimately, a disaggregated allied responsive space capability will not only transform the way military space missions are performed, but also enable a new level of resilience for NATO space-based DPS in an era of near-peer space threats. With responsive space, allies can quickly replace degraded allied satellites as well as deploy new space assets in an unpredictable, unwarned manner. Private investment in dual-use satellites and horizontal launch systems creates favourable economic conditions for NATO members to fold this into an allied responsive space capability. By leveraging a disaggregated responsive launch architecture built upon shared allied contributions, NATO members will have tremendous flexibility in conducting joint space missions.

Mr Bret Perry is a Business Development Principal at Virgin Orbit, where he focuses on helping international governments and commercial operators fulfil their launch requirements. Previously, Bret worked at Avascent, where he provided critical support in strategy development for clients in the aerospace and defence sectors. Bret holds a Bachelor of Science in Foreign Service from Georgetown University.

Mr John Fuller is the Director of Advanced Concepts at Virgin Orbit. John has been with Virgin Orbit since 2016, and is responsible for the conceptual, financial, and competitive evaluation of developmental programs. Prior to joining Virgin, he worked at Orbital ATK. John holds Bachelor of Science and Master of Science degrees in Aerospace Engineering from North Carolina State University.

Endnotes

1. Cardillo, Robert, 'A responsive launch capability will deter enemies, boost national security', DefenseNews (published online 3 September 2021), https://www.defensenews.com/opinion/commentary/2021/09/03/a-responsive-launch-capability-will-deter-enemies-boost-national-security/, accessed on 27 December 2021.
2. B. Perry and J. Fuller, 'Leveraging Responsive Space and Rapid Reconstitution'. In JAPCC 2021 Conference Readahead [electronic journal]. Kalkar, Germany, 2021, cited 27 December 2021, available at: https://www.japcc.org/leveraging-responsive-space-and-rapid-reconstitution/.
3. Beaudot, G., 'Luxembourg Perspectives on MILSATCOM'. At Global MilSatCom 2021 Conference [presentation]. London, United Kingdom, 2021, cited 11 January 2022.
4. NATO Support and Procurement Agency, Multinational Multi-Role Tanker and Transport Fleet (MMF), [website], 2020, https://www.nspa.nato.int/about/life-cycle-management/MMF, accessed 7 January 2022.
5. Ibid. 2.
6. See Table 1. Ibid. 2.
7. Hitchens, Theresa, 'Raymond Urges NATO Space Ops; Europeans Fear Offensive Missions', Breaking Defense, published online 18 November 2019, https://breakingdefense.com/2019/11/raymond-urges-nato-space-ops-europeans-fear-offensive-missions/, accessed on 20 January 2022.

© 2019 Skorzewiak/Shutterstock.com

Terabytes of Unprocessed Data or Superior Pieces of Info

VII

Turning Airborne ISR into Multi-Domain Operations

By Col Gianmarco Di Loreto, IT Air Force
IT Air Force-Ministry of Defence

By Lt Col Roberto Diana, IT Air Force
Italian Air Force Staff

ISR: from Data to Comprehension

The info-operational environment in which we are immersed is characterized by conflicts that span the entire spectrum of the competition continuum,[1] including all possible combinations of conventional, asymmetric and hybrid operations.

Our military organizations have faced the changing intelligence and C2 environments by evolving a specific guideline: enhancing the information and decision-making processes and progressive decentralization. This approach was based upon a powerful assumption: information enables understanding, and understanding enables decision-making.

The Italian Air Force (ITAF), as with other Air & Space Components, follows this guideline, especially in the ISR field. As a pioneer in this evolution, it has discovered counter-intuitive evidence: the more both quality and quantity of information are improved and decentralized, the more evident it becomes that information doesn't necessarily enable understanding, and understanding doesn't enable decision advantage.

Hopping into the 'Rabbit Hole': a Theoretical Approach to ISR

One of the most interesting passages of J. Boyd's thinking is when he identifies the 'Synthesis-Analysis' or 'Induction-Deduction' interaction[2] which is the starting point of the understanding process we use 'to develop and manipulate concepts to represent observed reality'.[3] Orienting the following Decisions and Actions, this idea brings us to the so-called 'induction problem', long-debated before Boyd on how many observations are required to arrive at a synthesis capable of predicting how a scenario will develop (in order to orient decisions and actions)? One, ten, a hundred, a thousand?

K. Popper stated that 'the belief that we can start with pure observations alone [...] is absurd',[4] because 'Observation is always selective. [...] It needs a chosen object, a definite task, a point of view, a problem';[5] thus, it is impossible to understand reality inductively. In Popper's view, the creative, intuitive element is at the beginning of any attempt at understanding, so even if we are not directly aware of it, the OODA loop never really starts from an observation.

Proceeding with the thought process, we can hence identify a more realistic (i[6])(a[7])O(s[8])ODA loop: there is always an 'Ideate' phase before an observation, even if implicit or hidden. In his words, '[...] it is the [...] theory which leads to, and guides, our systematic observations [...]. *This is what I have called the "searchlight theory of science", the view that science itself*

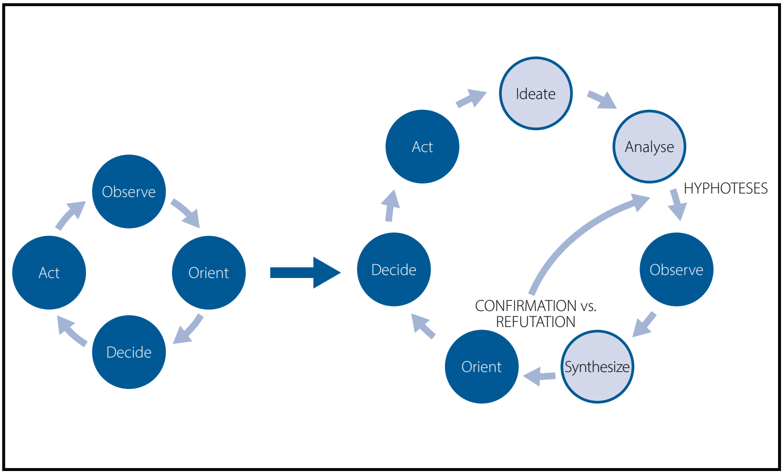


Figure 1: *(i)(a)O(s)ODA loop.*

throws new light on things; that […] it not only profits from observations but leads to new ones.'[9]

Before an Observation, another process also intervenes where we start from an idea, a postulate, or a general theory and then we draw conclusions on the phenomenon that should logically derive from the initial idea. K. Popper identified this process and we may refer to it as the 'deduct' or 'analyse' phase, yet bearing in mind there is an essential distinction from the term used by J. Boyd. For K. Popper, deduction precedes observation, as 'without waiting, passively, for repetitions to impress or impose regularities on us, we actively try to impose regularities upon the world. We try to […] interpret it in terms of laws invented by us.'[10]

Only then, can the observation phase start fulfilling its core role, namely disproving our assumptions. 'These may have to be discarded later, should observation show that they are wrong. This was a theory of trial and error, of conjectures and refutations'.[11] The most important information is the information that falsifies the hypotheses, inspiring the most correct decisions. The rest could be useless data at best, toxic details at worst. Finally, as anticipated at the beginning of the chapter, the 'Synthesize' phase comes into play to enable the Orient phase.

So, why is this **(i)(a)O(s)ODA** loop so difficult?

Process of Understanding Human Cognitive Bias Barriers

The last few decades of progress in cognitive psychology allowed us to identify the main biases hindering our process of understanding. From the most famous 'confirmation bias' to the 'WYSIATI[12] bias' to the inability to correctly frame statistical problems (i.e. regression to the mean[13] and law of small numbers[14]), ending with heuristics and other biases (i.e. substitution[15] cause and chance[16], affect[17]).

Furthermore, as humans, we cannot reliably convert information because:

- we tend to underestimate the chance and irrationality of occurrences;
- we often fall into the 'narrative fallacy' trap; [18]
- we are at the mercy of the 'ludic fallacy', which consists of comparing risks and opportunities derived from chances similar to those of gambling.[19]

Finally, among other powerful human biases, we should not forget Taleb's 'round-trip fallacy',[20] meaning the systemic logic confusion between statements made in similar terms but with totally different meanings.[21]

The analysis of cognitive biases helped us identify why the starting assumption[22] is now at stake. Before the digital revolution and the rise of high-density info-ops environments, human cognitive biases were thwarted by military-specific organizational workarounds: a centralized and pyramidal model with an interaction at the top between a Commander and their Headquarters. This model successfully stood the test of time. It was the filter of the different hierarchy levels and the dialectic between the two figures that mitigated, most of the time, the cognitive biases leading to potentially flawed decisions.

As we previously said, the advent of the digital revolution led us to think that the consequential huge information density could be managed by decentralizing and accelerating the decision-making process at 'the speed of relevance'.[23] Nonetheless, it is a partial solution that brings to the table an even greater issue, which in doing so; we lose an effective dam against cognitive biases.

Obstacles to Understanding: AI[24] is Not the Silver Bullet

Given the framework described in the previous paragraph, great expectations[25] are imposed upon the use of Artificial Intelligence (AI) in the ISR and decision-making processes. We must be aware of the risk that while trying to avoid human biases, we could fall boldly into those biases typical of AI. AI biases have the potential to be even more dangerous and subtle than human biases, which are categorized into two distinct areas:

- AI predictions[26, 27] always represent pre-existing data processing and thus are blind to novelty and exceptions (again…the induction problem)! They will always be a future version of…the past. This means that even the best AI algorithm, if not properly handled, could be of little use when we need it the most (i.e. to prevent a surprise on the battlefield).
- Human biases can be 'exported' in their entirety into the AI tool that we are counting on (i.e. coding) to rescue us from those very same biases.

This risk, theoretically identified by K. Popper almost a century ago[28] has materialized today with particularly harsh social consequences.

ISR: A New Paradigm to Orient Decisions and Actions

For information to lead to a decision advantage, airborne ISR must be enlightened by new awareness: current organizational and training models have noticeable limits.

The conceptual guideline behind our intelligence and C2 process is based upon the necessity to accelerate and decentralize decision-making: static Command and Control chains are outdated tools and need to be replaced by web chains capable of adapting rapidly and autonomously based on a single priority: mission understanding and operational environment comprehension. To realize such a change, it is necessary (both conceptually and technically) to transform the quantity of information into quality of understanding. Although easier said than done, 'technological capabilities depend on complementary institutions, skills and doctrines';[29] thus, new skills must be developed so that the contribution of AI reduces, rather than increases, the potential effects of toxic information. Furthermore, militaries must be informed and trained cognitive psychology to effectively be able to diagnose human intelligence biases and leverage AI to compensate for our weaknesses.

The human element could then fully exploit Big Data and AI, properly assisted by 'graceful degradation' systems,[30] becoming the main character in designing new theories, hypotheses, and scenarios to orient Analysis and Observation, detecting what is 'normal' (confirmation) and what is potentially an 'anomaly' (refutation).

These 'anomalies' will be our 'superior pieces of information', allowing us to predict events evolving along completely new and previously unknown scenarios (i.e., Machine Learning irrelevant). To identify them, we must train and utilize the human mind for its most peculiar and irreplaceable expertise: emotional intelligence, creativity, empathy, ability to consider elements of irrationality, randomness, and madness.[31] Characteristics are ultimately aimed at 'creating' and 'identifying' exceptions, and hence predictions.

To conclude, to find 'superior pieces of info' starting from terabytes of raw and unprocessed data, it is necessary to exit from the legacy dichotomy between human and artificial intelligence. We must bring the human back to the centre toward forms of 'humanly enhanced Artificial Intelligence', or the so-called human-machine teaming.[32] Machine augmentation will ultimately forge a more cognizant human being.[33]

Colonel Gianmarco Di Loreto joined the Air Force Academy in 1997, where he graduated as 1st of his class. On completion of NATO Flying Training in Canada (NFTC) School, he flew Electronic Warfare TORNADO fighter jet. In 2010 at Edwards AFB (US), he became an Experimental Test Pilot and accumulated 10 years of experience in the field of acquisition and aircraft experimentation on more than 80 different aeroplanes and helicopters. Among other duties, he completed the first transoceanic crossing of the F-35 and was a demo pilot of the C-27J Spartan transport aircraft. He attended the Senior Course at the NATO Defence College in 2019, graduated 'with honour' and won the Eisenhower Prize with his academic team. After being Section Chief of the General Planning and Transformation Office in the Aerospace Planning Department, he then became Vice Head of the Office, responsible for the coherent development of the AF Main Capability Areas. He is currently assigned to the Ministry of Defence Cabinet – Office for Military Policy.

Lieutenant Colonel Roberto Diana joined the Air Force in 1999 as an Intelligence Officer, graduated in Political Science and was awarded the 'Badge of Honour' at the end of the Officers Course. Assigned to the Italian Defence General Staff, he completed his Intelligence training and gained an extensive operational experience in key Intelligence positions in Italy, Iraq, Afghanistan, Kuwait and in the United States. He attended the Italian Air Force War College in 2015 and the 'Ecole de Guerre' (Paris) in 2019, where his dissertation 'The Black Swan Theory facing History: Garibaldi and Expedition of the Thousand' was awarded among the School's best research works.

Endnotes

1. 'A world of enduring competition conducted through a mixture of cooperation, competition below armed conflict, and armed conflict'. Joint Chiefs of Staff, Joint Doctrine Note 1-19 'Competition Continuum' (3 June 2019), p. V.
2. Frans P. B. Osinga, Science, Strategy and War – The Strategic theory of John Boyd, Routledge, Eburon Academic Publishers, Delft 2005, pp. 177–179.
3. Ibid., p. 177.
4. Popper Karl R., Conjectures And Refutations, Basic Books, Publishers New York London, 1962, p. 47.
5. Ibid.
6. Ideate.
7. Analyze.
8. Synthesize.
9. Ibid., p. 127–8.
10. Ibid., p. 47.
11. Ibid.
12. What You See Is All There Is: tendency to focus on available information rather than expanding the field of view to include unavailable information or data that doesn't support our thesis.

13. Daniel Kahneman, Thinking, Fast and Slow, Farrar, Straus and Giroux, New York, p. 201.
14. Ibid., p. 125.
15. Ibid., p. 112. Refers to the cognitive process of substituting complex judgements with more linear mental shortcuts (i.e., to access information stored in memory).
16. Ibid., p. 131. Refers to the cognitive process that always looks for a cause-effect relation between events without accepting the randomness of reality.
17. Ibid., p. 119. Refers to the dominance of conclusions over arguments that tends to occur when we let emotions determine our beliefs.
18. Nassim Nicholas Taleb, The Black Swan, Random House Trader Paperbacks, New York, p. 107.
19. Ibid., p. 181.
20. Ibid., p. 94.
21. In the Intelligence field, we perfectly know the difference between saying 'there is no evidence consistent with the hypothesis' and 'there is evidence that the hypothesis is not consistent', do we? Like for a doctor stating that 'there is no evidence of a tumor reappearance' is way different from stating 'there is evidence that the tumor has disappeared'. Still, we very often fall victim of this fallacy.
22. Information enables understanding and understanding enables decision-making.
23. US Department of Defense, National Defense Strategy, 2018.
24. For the scopes of this research, with the term 'AI' the authors intend 'narrow AI', or Machine Learning.
25. See, among others, A. Goldfarb and J. Lindsay, Prediction and Judgement – Why Artificial Intelligence Increases the Importance of Humans in War, International Security 46: 3, 2022.
26. On the topic of AI and decision-making, an interesting insight is given by A. Goldfarb and J. Lindsay, Ibid., pp. 8–9: 'Rapid advances in machine learning have improved statistical prediction, but prediction is only one aspect of decision-making. Two other important elements of decision-making – data and judgement – represent the complements to prediction. [. . .] When quality data are available and an organization can articulate clear judgements, then AI can improve decision-making.'
27. Another appealing insight on AI decision-making is given by S. Fortmann-Roe and Scharre: '[. . .] If the data behind the AI system are incomplete or biased, the quality of decision-making is degraded. Adversaries might be able to corrupt the data or hack into the AI system itself' in RAND, Military Trends and the Future if Warfare, Chapter Seven, Trend 6: AI as a Class of Potentially Disruptive Technologies, p. 63, ISBN: 978-1-9774-0297-4.
28. 'We may consider the idea of building an induction machine. Placed in a simplified "world" (for example, one of sequences of coloured counters) such a machine may through repetition "learn", or even "formulate", laws of succession which hold in its "world". [. . .] In constructing an induction machine, we, the architects of the machine, must decide a priori what constitutes its "world". In other words, we must build into the machine a framework determining what is relevant or interesting in its world: the machine will have its "inborn" selection principles. The problem of similarity will have been solved for it by its makers who thus have interpreted the "world" for the machine.' Popper Karl R., Ibid., p. 48.
29. Ibidem, p. 10.
30. The ability of a system to highlight to the human operator an error in the nominal parameters on which it is designed (potentially affecting the end result and/or the overall performance) and also capable of avoiding an exponential and non-manageable degradation.
31. 'The role of 'genius' in mission command becomes particularly important, and particularly challenging, in modern combined arms warfare and multi-domain operations'. Biddle, Military Power, in A. Goldfarb and J. Lindsay, Ibid., p. 24.
32. A. Goldfarb and J. Lindsay, Ibid., p. 12 '[. . .] For intelligence and operational tasks that have quality data but difficult judgements, teams of humans and machines can distribute the cognitive load of decision-making. We expect many if not most military AI tasks (including ISR, authors' note) to fall [. . .] into the category which we describe as human-machine teaming'.
33. Of note, to the same general conclusion came A. Goldfarb and J. Lindsay, Ibid., p. 9: 'Increasing reliance on AI [. . .] will make human beings even more vital for military power, not less.'

© local_doctor/Shutterstock.com

Adversarial Machine Learning

VIII

A Threat to NATO Missions

By Dr Elie Alhajjar
United States Military Academy at West Point

Introduction

The rapid progress in computer vision made possible by deep learning techniques has favoured the large diffusion of applications based on Artificial Intelligence (AI). The ability to analyse different kinds of images and data from heterogeneous sensors is making this technology particularly interesting for military and defence applications. However, these machine learning techniques were not designed to compete with intelligent opponents; therefore, the characteristics that make them so interesting also represent their greatest weakness in this class of applications. More precisely, a small perturbation of the input data is enough to compromise the accuracy of the machine learning algorithms and to render them vulnerable to the manipulation of adversaries – hence the term adversarial machine learning.

Adversarial attacks pose a tangible threat to the stability and safety of AI and robotic technologies. The exact conditions for such attacks are typically quite unintuitive for humans, so it is difficult to predict when and where the attacks could occur. In addition, even if we could estimate the likelihood of an adversary attack, the exact response of the AI system can be difficult to predict as well, leading to further surprises and less stable, less safe military engagements and interactions.[1] Despite this intrinsic weakness, the topic of adversarial machine learning in the military industry has remained underestimated for some time. The case to be made here is that machine learning needs to be intrinsically more robust to make good use of it in scenarios with intelligent and adaptive opponents.

AI Systems Are Vulnerable

For a long period of time, the sole focus of machine learning researchers was improving the performance of machine learning systems (true positive rate, accuracy, etc.). Nowadays, the lack of robustness of these systems can no longer be ignored; many of them have proven to be highly vulnerable to intentional adversarial attacks and/or manipulation. This fact renders them inadequate for real-world applications, especially mission-critical ones.

An adversarial example is an input to a machine learning model that an attacker has intentionally designed to cause the model to make a mistake. In general, the attacker may have no access to the architecture of the machine learning system being attacked, which is known as a black-box attack. Attackers can approximate a white-box attack using the notion of 'transferability', which means that an input designed to confuse a certain machine-learning model can trigger a similar behaviour within a different model. [2]

General concerns about the impacts of adversarial behaviour on stability, whether in isolation or through interaction, have been emphasized by recent demonstrations of adversarial attacks against these systems.[3]

Perhaps the most widely discussed attack cases involve image classification algorithms that are deceived into 'seeing' images in noise,[4] i.e., white noise randomly generated that does not correspond to any image is detected as one, or are easily tricked by pixel-level changes so they classify a school bus as an ostrich, for example. Similarly, game-playing systems that outperform any human (e.g., Chess or AlphaGo) can suddenly fail if the game structure or rules are slightly altered in ways that would not affect a human.[5] Autonomous vehicles that function reasonably well in ordinary conditions can, with the application of a few pieces of tape, be induced to swerve into the wrong lane or speed through a stop sign.[6] This list of adversarial attacks is by no means exhaustive and continues to grow over time.

AI in Military Applications

Many NATO countries utilize AI and machine learning to improve and streamline military operations and other national security initiatives. Regarding intelligence collection, AI technologies have already been incorporated into military operations in Iraq and Syria, where computer vision algorithms have been used to detect people and objects of interest. Military logistics is another area of focus in this realm. The US Air Force uses AI to keep track of when its planes need maintenance, and the US Army uses IBM's AI software 'Watson' for both predictive maintenance and analysis of shipping requests. Defence applications of AI also extend to semiautonomous and autonomous vehicles, including fighter jets, drones or unmanned aerial vehicles (UAVs), ground vehicles, and ships.

One might hope that adversarial attacks would be relatively rare in the everyday life since 'random noise' that targets image classification algorithms is actually far from random. Unfortunately, this confidence is almost certainly unwarranted for defence or security technologies. These systems will invariably be deployed in contexts where the other side has the time, energy, and ability to develop and construct precisely these types of adversarial attacks.[7] AI and robotic technologies are particularly appealing for deployment in enemy-controlled or enemy-contested areas since those environments are the riskiest ones for our human soldiers, in large part because the other side has the most control over the environment.

Having realized the importance of the technological lead of AI development and application, NATO launched the Military Uses of Artificial Intelligence, Automation, and Robotics (MUAAR) project under the Multinational Capability Development Campaign (MCDC) in 2020. The project's scope was to develop concepts and capabilities to address the challenges of conducting joint coalition operations and provide assessments on them.[8] The project's objective aimed to assess present and future military tasks and functions that could benefit from AI, automation and robotics. It also considering paybacks in efficiency and cost savings.

Examples of the dangers posed by adversarial manipulation of machine learning classifiers in defence applications are abundant, with different levels of severity. For example, a Lethal Autonomous Weapons System (LAWS) might misidentify friendly combat vehicles as enemy combat vehicles. Likewise, an explosive device or an enemy fighter jet might get misidentified as a rock or a bird. On the other hand, knowing that an AI spam filter tracks certain words, phrases, and word counts for exclusion, attackers can manipulate the algorithm by using acceptable words, phrases, and word counts and thus gain access to a recipient's inbox, further increasing the likelihood of email-based cyberattacks.[9]

Conclusion

In summary, AI-enabled systems can fail due to adversarial attacks intentionally designed to trick or fool algorithms into making a mistake. Such attacks can target the algorithms of the classifiers (white-box attacks) or target the output by just having access to the input (black-box attacks). These examples demonstrate that even simple systems can be fooled in unanticipated ways and sometimes with potentially severe consequences. With the widespread range of adversarial learning applications in the cyber security domain, from malware detection to speaker recognition to cyber-physical systems to many others such as deep fakes, generative networks, etc., it is time for this issue to take center stage as NATO is increasing its funding and deployment into the fields of automation, AI, and autonomous agents. There needs to be a high level of awareness regarding the robustness of such systems before deploying them in mission-critical instances.

Many recommendations have been offered to mitigate the dangerous effects of adversarial machine learning in military settings. Keeping humans in or on the loop is essential in such situations. When there is human-AI teaming, people can recognize an adversarial attack and guide the system to appropriate behaviours. Another technical suggestion is adversarial training, which involves feeding a machine learning algorithm a set of potential perturbations. In the case of computer vision algorithms, this would include images of the stop sign that displays those strategically placed stickers, or of school buses that include those slight image alterations. That way, the algorithm can still correctly identify phenomena in its environment despite an attacker's manipulations.

Given that machine learning in general and adversarial machine learning in particular, are still relatively new phenomena, the research on both is still emerging. As new attack techniques and defence countermeasures are being implemented, caution needs to be exercised by NATO military forces in employing new AI systems in mission-critical operations. As other nations, particularly China and Russia, are making significant investments in AI for military purposes, including in applications that raise questions regarding international norms and human rights, it remains of utmost importance for NATO to maintain its strategic position in order to prevail on future battlefields.

Dr Elie Alhajjar is a Senior Research scientist at the Army Cyber Institute and jointly an Associate Professor in the Department of Mathematical Sciences at the United States Military Academy at West Point, NY, where he teaches and mentors cadets from all academic disciplines. Before coming to West Point, Dr Alhajjar had a research appointment at the National Institute of Standards and Technology (NIST) in Gaithersburg, MD. His work is supported by grants from NSF, NIH, NSA, and ARL and he was recently named the Dean's Fellow for research. His research interests include mathematical modelling, machine learning and network analysis. He has presented his research work at international meetings in North America, Europe, and Asia. He is an avid science policy advocate, having received the Civilian Service Achievement Medal, the NSF Trusted CI Open Science Cybersecurity Fellowship, the Day One Technology Policy Fellowship, and the SIAM Science Policy Fellowship. He holds a Master of Science and a PhD in mathematics from George Mason University, Master's, and Bachelor's degrees from Notre Dame University.

Endnotes

1. Danks, D. (2020), 'How Adversarial Attacks Could Destabilize Military AI Systems.' IEEE Spectrum, available at https://spectrum.ieee.org/adversarial-attacks-and-ai-systems, accessed on 16 May 2022.
2. Alhajjar, E., Maxwell, P. and Bastian, N. (2021), 'Adversarial Machine Learning in Network Intrusion Detection Systems.' Expert Systems with Applications, 186 (115782), 1–13.
3. Biggio, B. and Roli, F. (2018), 'Wild patterns: Ten years after the rise of adversarial machine learning.' Pattern Recognition, 84, 317–331.
4. Nguyen, A., Yosinski, J. and Clune, J. (2015), 'Deep neural networks are easily fooled: High confidence predictions for unrecognizable images.' In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 427–436.
5. Raghu, M., Irpan, A., Andreas, J., Kleinberg, B., Le, Q. and Kleinberg, J. (2018), 'Can deep reinforcement learning solve Erdos-Selfridge-Spencer games?' In International Conference on Machine Learning, pp. 4238–4246.
6. Eykholt, K., Evtimov, I., Fernandes, E., Li, B., Rahmati, A., Xiao, C., Prakash, A., Kohno, T. and Song, D. (2018), 'Robust physical-world attacks on deep learning visual classification.' Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 1625–1634.
7. Danks, D. (2020), 'How Adversarial Attacks Could Destabilize Military AI Systems.' IEEE Spectrum, available at https://spectrum.ieee.org/adversarial-attacks-and-ai-systems, accessed on 16 May 2022.
8. NATO Allied Command Transformation Operational Experimentation (2020), 'Military Uses of Artificial Intelligence, Automation, and Robotics (MUAAR),' available at: https://www.act.nato.int/application/files/5515/8257/4725/2020_mcdc-muaar.pdf, accessed on 7 February 2022.
9. Biggio, B., Fumera, G. and Roli, F. (2010), 'Multiple classifier systems for robust classifier design in adversarial environments.' International Journal of Machine Learning and Cybernetics, 1(1), 27–41.

© 2019 Color4260/Shutterstock.com

IX

The Multi-Domain Combat Cloud in Light of Future Air Operations

An Enabler for Multi-Domain Operations

By Brig Gen (ret.) Jean Michel Verney, Col (ret.) Thomas Vinçotte
FR Air Force

Mr Laurent le Quement
Airbus Defence and Space

Introduction

Much has been published on new operational concepts to re-enhance Western air superiority when facing threats posed by peer or near-peer competitors with long-range and precise fires. Most experts advocate for a much more integrated force approach to impose multiple military dilemmas on opponents at a high tempo. Network-collaborated manned and unmanned assets will regain combat mass and the ability to manoeuvre. In doing so, opponents will be forced to make decisions based on uncertain, options thus jeopardizing the result of their actions. Such a new paradigm calls for Multi-Domain Operations (MDO).

MDO could be described as both the ability to produce military effects in one domain with sensors and effectors coming from all domains and the capability to delegate Command & Control (C2) to the lowest possible level. Advocating the integration of platforms and subsidiarity in the C2 chain constitutes a baseline for re-enforcing the flexibility, resilience and reactivity of a force. The Joint Force Commander (JFC) in theatre would act as an orchestrator of the MDO. They would have the ability to allocate sensors and effectors amongst tactical commanders for a dedicated task, synchronize the effects between all domains and delegate as needed the control of a task right down to the tactical edge.

This can be achieved through an inclusive Information Technology & Communications (IT & COM) ecosystem called the Multi-Domain Combat Cloud (MDCC), forming a combat network of actionable sensors, effectors and C2 nodes across domains. Using the NATO C3 Taxonomy, a MDCC would offer the means to enable and enhance interoperability within NATO nations and partners for increased operational effectiveness.

The following paper will illustrate the principles of integration and subsidiarity through a fictitious operational scenario on the horizon of 2040 and highlight their consequences in terms of operational perspectives and functional requirements for the MDCC.

The MDCC as an Inclusive Enabler in the Early Stage of an Operation

The fictitious operational scenario begins with an 'Air Force Protection' which shifts later on to an Air Advanced Base Operations (A2BO)[1] following an unacceptable raid from a red country against its ethnic minority. The United Nations (UN) mandates NATO to conduct a military campaign. NATO forces encompass a Next Generation Weapon System (NGWS)[2] squadron with New Generation Fighters (NGFs) and Remote Carriers (RCs), some Enhanced Legacy Fighters, a C2 Airborne Platform coupled with a constellation of Optical, Radar and Communications Satellites, Tankers, Cyber Assets and Special Forces on the ground. A Carrier Battle Group with Amphibious Forces also joins the area of operations.

Regarding Air Force protection, the objective is to prevent any air attack and counter red harassment on villages of the ethnic minority. At this stage, the JFC decides to designate the Air Force as the supported[3] component, the supporting[4] components being the Special Forces and the Navy. Thus, the Joint Force Air Component Commander (JFACC) is responsible for C2 of all air platforms at the tactical level.

To respond to the red attacks, the JFACC requires a fully recognized picture built from multi-domain sensor inputs (air, land, space and cyber). The detection of public agitation on specific social networks combined with real-time Intelligence Surveillance Reconnaissance (ISR) from Special Forces and space-based assets would allow for a rapid demonstration of force from NGWS over the troubled area. Furthermore, any social networks close to the red authorities and calling for violence against the ethnic minority would be countered by a cyberattack to render them inoperative.

At this stage of the operation, the MDCC is the inclusive enabler based on a shared open IT & COM architecture interconnecting all available sensors. It is providing a common recognized picture enriched by real-time ISR collection and past intelligence. In doing so, the MDCC offers a high level of awareness to properly develop and propose military options from the JFACC to the Future Combat Air System (FCAS[5]) Mission Commander's level in line with JFC directives.

Varying Demands during a Multi-Domain-Operation

The situation quickly deteriorates as red forces launch several surface-to-surface medium-range missiles against ethnic minority villages resulting in casualties. Furthermore, the reds activate all their Integrated Air Defence Systems (IADS), notably the long-range missiles. Following new UN resolutions, NATO immediately decides to change its military posture. The Alliance orders for the disruption of the red IADS whilst securing NATO's strategic initiative to conduct an amphibious assault later on, if needed.

The overall objective is to firmly respond to the aggression whilst keeping control of the level of escalation. The JFC receives directives from the strategic level to conduct Air Advanced Base Operations (A2BO)[6] in order to neutralise red airbases and to impede the red forces' 'fait accompli' strategy of seizing control of the ethnic minority's enclave. These A2BO aim at expanding air force employment options whilst mitigating the risk of having all air assets located on one vulnerable Main Operating Base. A2BO must also provide greater agility and the ability to outpace the red actions. Close to the fight, distributed Air Operating Locations (AOL) may contribute to the air strike but will also help saturate the red Anti Access Aerial Denial (A2/AD) efforts.

After allocating additional assets from the JFC, the JFACC is now responsible for the engagement against red airbases with ground and sea-based NGWS and cruise missiles from a Defence & Intervention Frigate (FDI). However, depending on the situation's hourly evolution and a possible pop-up threat against the Carrier Battle Group, the JFC maintains a reactive and dynamic reallocation of NGWS and FDI between the JFACC and the Joint Force Maritime Component Commander (JFMCC). Thus, the JFMCC will be able to ask for real-time Air Task Order (ATO), or Airspace Control Order (ACO) changes to the JFACC, after immediate synchronization with the JFC.

Because it is highly expected that several locations could lose connectivity with operational C2, the JFACC communicates beforehand his/her intent to the AOL Commanders by issuing 'Mission Type Orders' (MTO) in conjunction with delegated and conditions-based authorities.[7] Therefore, these persistent forward NATO-led air forces must be able to conduct Defensive and Offensive Counter Air operations using resilient, low-signature, low-maintenance, and significant quantity of manned and unmanned air assets. The aim is to generate effects against A2/AD red capabilities without the associated vulnerabilities of force concentration by creating more dispersed, resilient, and hard to target AOL. This force comprises NGFs, various RCs (both with sensors and effectors), Enhanced Legacy Fighters and Air Tactical Transports to serve as intra-theatre transport of weapons, unmanned platforms, fuel, and logistics support, all operating through dynamic Communities of Interest.[8] Depending on the state of communication between AOL and NGFs, specific 'Multi-Domain Tactical Functions'[9] will be delegated to the cockpit to allow the FCAS Mission Commanders to assume delegation of control for 'Dynamic Targeting' and 'Time Sensitive ISR'.[10] The Special Forces and dedicated satellites will contribute to the dynamic ISR collection. Due to the theatre's elongation, NGFs coupled with a constellation of satellites will benefit from an extended situational awareness and assume, if needed, broader control responsibilities alongside those already assumed by the 'Front Edge Controlling Team' on board the C2 Airborne Platform.

The Network Optional Systems within the MDCC in a Complex MDO

Coupling A2BO with JFACC and JFMCC's networks enables 'network optional systems' within the MDCC. Such 'network optional systems take advantage of 'centralized networks' when available and form 'opportunistic networks'[11] amongst available platforms at the tactical edge when cut off from higher authority. Here, the MDCC is the inclusive enabler for such complex MDO. On the one hand, the MDCC integrates all decision processes (from planning to assessment through execution), including force allocation and effects synchronization, from the JFC to tactical commanders, paving the way for a dynamic supported/supporting framework across domains. On the other hand, it provides subsidiarity between all commanders allowing delegation of C2 at the lowest possible level, such as AOL and NGF.

Following successful A2BO, NATO wants to take advantage of the situation and orders an amphibious operation to fully secure the ethnic minority in the enclave. During this operation, the JFMCC is designated as the supported command and the Air and Special Forces as the supporting ones. All platforms are potentially made available for the amphibious manoeuvre under Navy authorities. The MDCC will enable the JFMCC to integrate sensors and platforms from all domains into the large naval scheme manoeuvre fleet and to delegate C2, when needed, to the best navy platform commander.

Conclusion: A MDCC as a Networkable On-demand and Service Agnostic System

The fictional scenario illustrates the need for integration and subsidiarity through all decision-making processes. Doing so helps to shape a credible technical environment for generating global combat mass with a high operational tempo, integrating manoeuvres from all domains without the vulnerabilities of force concentration, and consequently posing multiple dilemmas to the opponent. This technical environment is provided by the MDCC, which can be described as a 'system of tailored networks' encompassing all available platforms from the rear to the edge. Therefore, the MDCC is the enabler for MDO with dynamic allocation of forces and distribution of C2 as previously described.

As a designer and provider of new technologies, industry stands ready to support the Armed Forces in shaping MDO as a new operational paradigm. Considering the ambition at stake, a strong partnership between both is crucial to ensure a thorough capture of the needs and to design the MDCC without selecting certain technical options too soon, which would hinder future MDO. This journey is still in its early days in terms of operational concepts and technological solutions. Only working hand in hand will allow the meeting of the challenges that lay ahead.

Brigadier General (ret.) Jean-Michel Verney (FR Air Force) graduated from the FAF Academy in 1987 and the US Air War College in 2003. He has 3,000 flying hours (Jaguar, Mirage 2000D) with 122 war missions and C2 expertise as a HQ officer. He joined Airbus in 2021 as a FCAS Senior Operational Advisor for Multi-Domain Operations.

Colonel (ret.) Thomas Vinçotte (FR Air Force) graduated as a French Air Force fighter pilot in 1987 and from the École de Guerre in 2003. He has over 3,300 flying hours (Jaguar, Mirage F1CR, Mirage 2000 RDI & Mirage 2000-5) with 83 war missions including one ejection and C2 expertise as a HQ officer. He joined Airbus in 2019 as a FCAS Senior Operational Advisor.

Mr Laurent le Quement graduated from Aston University in 1996. He worked in automotive and transformation consulting before joining Airbus' launcher division in 2010. He held numerous positions in business development and innovation before becoming FCAS Head of Marketing in 2018.

Endnotes

1. Air Advanced Base Operations (A2BO): This fictive doctrine is directly referring to the 'Agile Combat Employment' of the USAF, Air Force doctrine Note 1-21, Charles Q. Brown, JR, Chief of Staff of the Air Force. ACE is a future USAF doctrine, which meets the resiliency and forward presence requirements to face peer competitors employing long-range precision fires (A2/AD capabilities) directed at dislodging US forces dependent upon legacy bases, fixed infrastructure, and large targetable platforms. By enabling persistent presence and a more resilient force posture on some dispersed temporary contingency locations, ACE offers the opportunity to conduct air operations to defeat an adversary's strategy without the requirement to destroy all of its forces.
2. The NGWS, being developed by France, Germany and Spain, will include a New Generation Fighter teaming with various unmanned platforms called Remote Carriers.
3. Supported Component: The component having primary responsibility for all aspects of a task assigned by a Joint Commander and who receives forces or other support from one or more supporting components.
4. Supporting Component: A component providing a supported component with forces or other support and/or which develops a supporting plan.
5. Encompasses all Manned and Unmanned Air Combat Systems from JFAC to NGF through notably AEW, Tankers, Legacy Fighters and Remote Carriers.
6. These A2BO aim at expanding air force employment options, whilst mitigating the risk of having all air assets located on one vulnerable Main Operating Base.
7. 'Mission Command' and 'Mission Type Orders' are described in the 'Agile Combat Employment' doctrine of the USAF.
8. A Community of Interest (CoI) is here defined as a group of players from JFC to fighter level with shared mission or business processes at a specific time and location. An example of a business process could be the kill chain. Airbus considers this notion of CoI (referring to the NATO C3 Taxonomy) as a common tool for operational and engineering communities to describe all exchanges among combat systems.
9. 'Multi-Domain Tactical Functions': The principles of these MDTFs have been developed by Airbus and Dassault in the framework of the FCAS Joint Combat Study. They represent an extension of the already existing 'Tactical Battle Management Functions' exclusively dedicated to the Air Defense mission (Air Doctrine), to all missions and domains, allowing the delegation of multi-domain tactical functions down to the NGF level.
10. This notion of Time Sensitive ISR is part of the scope of MDTFs developed by Airbus with its industry partners.
11. These notions of 'system of network optional systems' and 'system of opportunistic networks' are addressed in the Expeditionary Advanced Base Operations (EABO) Handbook 'Considerations for Force Development and Employment' - 1 June 2018 – Arthur Corbett, Marine Corps Warfighting Lab, Concepts & Plans Division.

This Page Intentionally Left Blank.

© Sergey Nemirovskiy/Shutterstock.com

Sharing Cyber Capabilities within the Alliance

X

Interoperability Through Structured Pre-Authorization Cyber

By Dr Jan Kallberg, Research Scientist, Lieutenant Colonel Todd Arnold, Research Team Lead, and Colonel Stephen Hamilton, Technical Director

United States Army Cyber Institute at West Point

Introduction

Sharing cyber weapon/cyber capabilities requires trust between the member states, becoming a high-end policy decision due to the concerns of proliferation and the investment in designing a cyber-weapon that has a limited 'shelf-life'. The digital nature of cyber weapons creates a challenge. A cyber weapon can spread quickly, either self-propagating such as worms or via disclosure (and subsequent reuse) by malware researchers or malicious actors, raising proliferation concerns. Additionally, a cyber-weapon can be copied by the adversary or reverse engineered. Once the weapon is released, the adversary will eventually address the vulnerability, and the opportunity is gone. These factors raise the threshold between member states to share cyber weapons and cyber capabilities. Alliances, like NATO, prepare for a unified multinational, multi-domain fight; meanwhile, the national cyber forces are still operating as solitaires with limited interoperability and sharing. There is a need in the collective defence posture to integrate the multinational cyber force to achieve interoperability.

Time

The NATO framework such as the Sovereign Cyber Effects Provided Voluntarily by Allies SCEPVA[1] lays a foundation, but there are two obstacles – time and the concept of voluntarily enabling others. First, there is an expectation that future conflicts will unfold rapidly, as evidenced by the Russian invasion of Ukraine on 24 February 2022. It is doubtful that there will be the time[2] in conflict to communicate between member states seeking a voluntary release of cyber capabilities. Secondly, the voluntary provision for support to the mission requires that the provider be willing to provide the cyber capability, and there is a sharing of needs followed by a decision process. These hurdles will take days, or even weeks, to sort out. The narrowing time window to share cyber capabilities requires a framework for sharing between member states based on existing trust and relationships. There is also a risk that the adversary will repurpose and reuse the cyber weapon, leading to unintended consequences and lateral movements.

Solving Trust, Obligation, and Narrow Time Window

The concept of collective defence assumes an obligation to provide a cyber-capability. The Alliance multinational force seeks interoperability, but the national cyber forces are still tied to the member state's mission instead of the joint collective defence. The tenets of cyber capabilities hinder their rapid sharing because the weapons represent a significant time and resource investment for the provider. Effective tools require finding a vulnerability, weaponizing the opportunity, and once launched, the targeted adversary can nullify the weapon through patching and countermeasures. The provider has an understandable doubt about sharing these cyber weapons, especially under time pressure and without fully understanding how the cyber weapon will be handled by the receiving member state's cyber force.

In European and transatlantic politics, friendly nations mitigate distrust by arrangements that accept a variety of trust levels. Both the European Union and NATO have a history of cross-border dialogue, seeking common ground, and engaging in discussions of formalized relationships between friendly nations. There is a negotiation and hopefully an agreement. Even in computer security, there are negotiations between nation-states of mutual acceptance and agreements. The (ISO/IEC 15408) Common Criteria[3] framework is described by German certificate issuer TÛV Rheinland[4] as; 'It is a framework that provides criteria for independent, scalable and globally recognized security inspections for IT products.' In the Common Criteria framework, friendly nations negotiate the level of acceptance of another country's information security evaluations and enter binational agreements.

We propose that friendly nations, within a structured framework, negotiate cyber capability sharing pre-conflict. Our 'Framework for Pre-Authorized Joint Cyber Mobilization' is inspired by the success of the (ISO/IEC 15408) Common Criteria. Mutually accepted hardware security certifications as the Common Criteria face the same challenge as sharing cyber weapons of navigating trust, operational reality, and risk. The proposed framework for pre-authorized multinational cyber weapon sharing in a mixed trust environment utilizes the experience and structural concepts of the (ISO/IEC 15408) Common Criteria framework. The framework's prearranged acceptance of foreign information security certified evaluation. The Common Criteria, with defined levels of Evaluation Assurance Levels (EAL) ranging from 1 to 7, provides a framework that establishes trust levels between friendly nations. Critical to the proposed framework are transparency between partners, pre-conflict agreements and authorizations, specific limits to the extent of sharing cyber weapons, and responsibilities. Creating specific levels of cyber effects and the risks of collateral damages explains the cyber capability without comprising the actual utilization and functionality.

Our proposed cyber capabilities sharing framework will classify cyber capabilities by Expected Cyber Effect (ECE), Potential Lateral Uncontrolled Movement (PLUM), and Target Class (TC), which we will define in the subsequent sections.

Expected Cyber Effect and Potential Lateral Uncontrolled Movement

ECE and PLUM are vital components. ECE indicates what can be assumed to be achieved with the weapon. The classification for uncontrolled lateral movements assesses the chances for collateral damages, including potential hostile use of the tool once acquired/reverse engineered by the adversary. Each level's ECE level is described in Table A.

The second consideration – PLUM – is the ability of the cyber capability to act autonomously and potentially spread in an uncontrolled manner. The PLUM of a cyber-capability must be considered because, unlike collateral damage from kinetic weaponry, which has a limited physical range (not considering nuclear, biological, or chemical weapons which have a more extensive, but fundamentally limited effective range), cyber capabilities have the potential to spread rapidly and affect billions of devices connected to the Internet. Table B describes the PLUM for each level.

The ECE and PLUM levels are not 1:1; they must be considered independently. For example, a non-publicly known/released capability (Category 4 ECE) that affects low-priority targets can rapidly spread in an uncontrolled manner (PLUM 7). Despite the low ECE, the higher PLUM category will require guarantees in the negotiations that the receiving nation can safeguard and contain the cyber capability.

Category	Expected Cyber Effect
1	Known public tool, may be targeted with limited or medium effect
2	DoS, mass area of effect
3	Recently released or time sensitive usability (e.g. 1-day)
4	Non-publicly known/released capability (e.g., 0-day)
5	Targeted system capability, but requires (limited) physical access
6	Non-publicly known/released capability (e.g., 0-day) with high strategic importance
7	Highly targeted/specialized, non-publicly known/release capability (e.g., 0-day) with high strategic importance

Table A: *Allied Cyber Capability Sharing alignment of Expected Cyber Effect*

Category	Potential Lateral Uncontrolled Movement
1	Vulnerability is/should be patched, so will have limited spread and usability
2	Resources to make use of capability are required ahead of time, so limited uncontrolled movement
3	Requires wide distribution to make use of, due to imminent patching
4	Requires user interaction (e.g., phishing attack)
5	Requires little to no user interaction so minimal spread and highly targeted, but physical proximity limits usage
6	Requires little user interaction (e.g., watering-hole attack), so code must check for target system
7	Requires no user interaction (e.g., worm or remote), so spread must be checked in capability

Table B: *Allied Cyber Capability Sharing alignment of Potential Lateral Uncontrolled Movement*

Example Target Classes

The TCs – what can be affected by the capability – are defined within the framework to create uniformity in targeting definitions. As envisioned in the negotiations, the potentially receiving party puts forward a Targeting Request (TR), a well-defined request for a specific ECE against a specific TC. The providing party only presents TCs for a specific level of weapons. The presentation of the TC, and not capability, avoid spillage due to unnecessary information at the negotiating stage. For example, the receiving party puts forward a TR for the potential adversary's air defence system SAM-XXX and the providing party can reply with TC Air Defence. The provider knows in advance, what the receiver wants, and it becomes crucial to expedite the request in conflict and the execution of the agreement.

Examples of Member State's Pre-authorization Aligned with the Proposed Framework

Consider that pre-conflict, state X and Y agree to exchange cyber capabilities targeting Air Defence systems. State X agrees to share with state Y cyber capabilities up to ECE 5 and PLUM 3. State X's determining factors for acceptable levels are a concern regarding state Y's ability to safeguard the capabilities, primarily based on an assessment of cyber maturity, security controls, capabilities, and the impact on other systems if control of the capability is lost.

The acceptable levels between states may not be equivalent, and in this example, the risk appetite is different between states X and Y, which is reflected in the pre-authorization negotiation. Member state Y is only willing to share its high-level cyber capabilities by pre-authorizing up to ECE 3 targeting Air Defence to be shared with X. Member state Y considers itself to have a more secure cyber posture. Hence, a capability's potential lateral

Example preauthorization	Providing state	Receiving state	Expected Cyber Effect	Potential Lateral Uncontrolled Movement	Target Class
	X	Y	5	3	Air Defence
	Y	X	3	5	Air Defence

Table C: *Examples of sharing agreements between two member-states*

movement after use by X is of less concern to Y, so Y preauthorizes to X ECE 3 PLUM 5. These differences are reflected in Table C, which summarizes the pre-authorized sharing agreement between states X and Y.

While the states agree to pre-authorized levels, sharing or disclosing a capability's existence does not necessarily occur until one state requests a capability. In conflict, member state Y requests from member state X a cyber-capability targeting Air Defence at the highest level of the agreement: ECE 5 PLUM 3. State X delivers, without delay, a cyber-capability at ECE 5 PLUM 2, which is the highest-level capability targeting Air Defence available in X's arsenal and within the pre-coordinated levels.

Conclusion

The proposed framework is a model which naturally can be improved after further studies. The basis for the proposed framework is binational negotiations; NATO and EU states have experience and a history of numerous successful agreements. For example, NATO has established processes for defensive cyber operations whereby a member nation can request cooperation and assistance, but our concern is sharing mechanisms for offensive cyber operations. By agreeing to binational cyber capability sharing as a priority, response times can be reduced when a conflict arises, and a stronger response is possible within the Alliance. When rapid action is required, it is of the utmost importance that events cannot unfold faster than the Alliance's decision cycle. We consider preauthorization as a functional way to mitigate that risk.

Dr Jan Kallberg is a Research Scientist at the Army Cyber Institute at West Point. He earned a PhD in Public Affairs (Government) and MA in Political Science at the University of Texas at Dallas and holds a JD/LLM from Stockholm University. Dr Kallberg holds ISC2 CISSP and ISACA CISM professional certifications.

Lieutenant Colonel Todd Arnold is a 2001 graduate of the United States Military Academy, West Point. His first assignment was to the 22d Signal Brigade in Darmstadt, Germany, where he twice deployed in support of Operation Iraqi Freedom. He is currently a Cyber officer, has held various technical positions, and was the first Lead Developer for the Army's Cyber Solutions Development Detachment at Ft. Meade, MD. He completed his PhD in Electrical Engineering from Columbia University in 2020 and joined the Army Cyber Institute, West Point, shortly after that to serve as a Research Team Lead and Assistant Professor in the Dept. of Electrical Engineering and Computer Science.

Colonel Stephen Hamilton is an Associate Professor at the United States Military Academy, a Cyber officer in the US Army and an extra class licensed ham operator, KJ5HY. He has deployed to Iraq as a signal company commander, and to Louisiana in support of Hurricane Katrina relief efforts. He has held various staff positions in signal and cyber units. Stephen is currently the Chief of Staff and Technical Director of the Army Cyber Institute. He holds a Bachelor of Science degree in Computer Science from the United States Military Academy, a Master of Science in Software Engineering from Auburn University, and a PhD in Computer Science from Johns Hopkins University.

Endnotes

[1] Allied Joint Publication-3.20 Allied Joint Doctrine for Cyberspace Operations, Ministry of Defence (UK), p. 5. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf (accessed on 10 January 2022).

[2] J. Kallberg, and T. S. Cook, 'The unfitness of traditional military thinking in cyber,' IEEE Access 5 (2017): 8126–8130.

[3] Common Criteria Portal, About the Common Criteria, [website], https://www.commoncriteriaportal.org/ccra/index.cfm (accessed on 10 January 2022).

[4] TÜV Rheinland, Common Criteria Services – ISO 15408, [website], https://www.tuv.com/world/en/common-criteria-services---iso-15408.html (accessed on 10 January 2022).

© JAPCC

The Executive Director's Closing Remarks

Lt Gen Thorsten Poschwatta, GE Air Force
Executive Director, Joint Air Power Competence Centre

Global competition is not merely an academic concept; it is a reality that deserves our attention from various angles, including the security and defence perspectives. An increasing antagonism between major state powers is occurring and has to be acknowledged and managed to prevent violent clashes. For the team of the JAPCC, there was sufficient indication that this development needed further analysis when they started developing the theme of the 2022 conference in the autumn of last year. It will need well-considered activities in many areas of diplomacy and politics, as well as carefully balanced policy approaches to ensure security and defence in the Euro-Atlantic area and beyond.

Not all of us accurately assessed the probability that today, we would be confronted with a situation of comprehensive warfare on European soil. Indeed, aggressive foreign policy rhetoric and political assertiveness concerned both neighbouring countries and their partners. In hindsight, there were sufficient signals going back to 2007/08, demonstrating how Russia interprets its right to impose its will on others. On a global scale, we also recognize that some main actors have chosen in the last fifteen years to explicitly act against acknowledged rules of international behaviour and, at times, openly breach international law to promote their national interests.

What we see in Ukraine could be considered the first consequence of policies and politics that did not sufficiently address the antagonisms that developed in the global political arena. The choice of Russian state authorities to invade Ukraine in the last week of February will undeniably have consequences for our considerations to organise defence. Moreover, if we wish to uphold a rules-based international order and the benefits that globalization brought to many regions of our world, we will have to be very clear in how we answer this aggression against the sovereign state of Ukraine.

An impressive number of 141 votes in the UN's General Assembly condemned the breach of international law and demanded that Russia 'immediately, completely and unconditionally withdraw all of its military forces from the territory of Ukraine beyond its internationally recognized borders'. This vote provided a clear signal that a unilateral and unprovoked violation of recognized international borders will not be tolerated. Nevertheless, the states that supported this resolution, as well as those others that abstained or even voted against it, will attentively follow to what extent the support for Ukraine, the sanctions against Russia and the broader reaction of the North Atlantic Alliance will effectively achieve the objective and thereby discourage others from acting in similar ways.

So far, NATO and the EU, both as organisations and through coordinated activities of their member states, provided carefully chosen answers to the Russian military aggression in Ukraine. The package of diverse activities has been tailored to support Ukraine to stop the Russian war machine and – in the medium to long-term perspective – should enable a solution that will not allow Russia to profit from its attack. NATO clarified from the start that it would not become party to a military conflict with Russia, but in parallel, assured by the quick adaptation of its force posture and other measures that any spill over military activity against NATO territory would be deterred.

Moreover, NATO and its nations will ensure that any comprehensive military activity against NATO territory can be effectively countered. This will include adjustments to the readiness and posture of forces, as well as the force composition. Defence plans will be reviewed and adjusted as required to ensure maximum preparedness. Additionally, Finland and Sweden will contribute to the defence of NATO territory and be supported as necessary. Their application for NATO membership demonstrated to Russia and the broader world that Russia's invasion of Ukraine is not perceived as a bilateral conflict; instead, it is a challenge to the global order and a serious concern, particularly for the states in Russia's closer European neighbourhood.

I am confident that our overall set of answers will be comprehensive in nature and decisive regarding their signals to potential competitors. We will take balanced decisions and plan for effective, non-provocative activities that will steadily increase the costs of continued aggression and intimidation, but at the same time support political and diplomatic efforts that allow for de-escalation and a return to a lower level of crisis. In doing so, we should be aware that our management of this political crisis has to demonstrate to the broader world community that military aggression against a sovereign state – not to speak of the atrocities and proven breaches of the international laws of armed conflict – will not allow the aggressor to achieve undue gains.

As a senior military commander and defence practitioner, I am well aware that the warfighting we see and perceive today is unlikely to be a fitting template for any future armed conflicts. On the other hand, what we have seen in Ukraine so far reveals important aspects we should bear in mind. A thorough analysis of the current conflict can extract enduring lessons and some broader trends that make up a still incomplete but very relevant picture of the developments that may characterize future warfare.

The inability of Russian forces to achieve decisive effects or gains in the first phase of this war underlines the importance of a detailed assessment of the classical operational factors of time, space and forces. In a season where off-road movement of heavy vehicles offers particular challenges, the need to focus on particular roads prevented quick deployments of the force towards their objectives. Insufficient planning for logistical support and sustainment of troops further complicated this initial effort. Additionally, the absence of a previous shaping air effort and adequate force protection of the moving ground forces from the air contributed to the lack of success.

Concentration of effort is considered an indispensable component for effective warfare. However, this focus needs to be maintained, and the way to do so needs to be properly planned and supported. It seems fair to assess that the initial strategic approach to head towards Kiev via two axes was not bolstered by the right numbers and quality of forces – including a robust logistical backbone. The reconfiguration of Russian forces to concentrate on the Donbas region was a consequential decision and presents severe challenges to the Ukrainian defenders. In this situation, the number of forces and the availability of force capabilities count. Situational awareness and the anticipation of adversary moves will be decisive factors for a successful blunting of attacks.

Apart from these rather general perceptions on operational planning and conduct of war, three other observations deserve consideration. First, man-portable anti-tank guided missiles and air defence systems achieved considerable effects on the battlefield. They should not be underestimated and present a considerable threat that must be properly addressed. Second, unmanned aerial systems of various sizes with well-chosen loads that are smartly employed present comparably cheap tools to counter and destroy even heavily armoured vehicles. Third, advanced missiles reaching high speed to avoid air defences have once again been tested; their efficacy is still to be assessed.

Future warfare will take these observations and trends into account. Actors capable of exploiting technological advancements will strive to employ systems that can make a difference against classical warfare capabilities. Russia and others will learn from recent deficiencies and failures and further develop their warfighting capabilities. Unmanned Systems, in automated or semi-automated modes of operation, connected with Military Intelligence and Command and Control processes supported by Artificial Intelligence are becoming a military reality. Effectively operating in the Electromagnetic Environment will be paramount. A failure in one of these areas can have severe consequences for our common defence.

I look forward to our discussions at this year's Joint Air and Space Power Conference. Your thoughts, insights and perspectives are most welcome and encouraged. The collection of papers offered in this Read Ahead shall catalyse our debate. There is a need to look beyond the most recent events to get a comprehensive perspective on the future requirements for our security and defence and the role of joint air and space power in an age of global competition.

I sincerely hope to see you in October at Congress Centre Essen!

Thorsten Poschwatta
Lieutenant General, GE Air Force
Executive Director, JAPCC

Joint Air Power Competence Centre
von-Seydlitz-Kaserne | Römerstraße 140 | 47546 Kalkar (Germany)
Visit us in the web:

www.japcc.org