ASSURED ACCESS TO THE GLOBAL COMMONS
Maritime | Air | Space | Cyber
FINDINGS AND RECOMMENDATIONS

APRIL 2011
“In peace and prosperity states and individuals have better sentiments, because they do not find themselves suddenly confronted with imperious necessities; but war takes away the easy supply of daily wants and so proves a rough master that brings most men’s characters to a level with their fortunes.”

Thucydides, History of the Peloponnesian War, Book III
I. INTRODUCTION

NATO NATIONS AND the world at large derive great benefit from open access to the Maritime, Air, Space and Cyberspace domains. Indeed, the security and prosperity of our nations and of the Alliance as a whole are linked inextricably with these domains, which are the backdrop of today’s international security and globalized economy.

From a military perspective, the Alliance relies and increasingly depends on assured access to all four domains – often simultaneously. Assured access is vital for the indivisibility of NATO’s security and a prerequisite for the Alliance to fulfil its essential core tasks: collective defence, crisis management, and cooperative security. Yet, the multiple ways in which the Alliance is enabled by and dependent on the four domains are often not realized or are taken for granted.

The four domains are closely interwoven and interdependent. The loss of access to any of them would affect the ability of the Alliance to operate effectively in the others. By exploiting vulnerabilities in these domains, adversaries increasingly will take the initiative to disrupt or deny NATO’s access. This will put at risk NATO’s populations, territories, and forces and challenge the Alliance as a unique community of values, committed to the principles of individual liberty, democracy, human rights, and the rule of law.

Although the four domains share many similarities, the differences between them are substantial. While the Maritime domain has been used for millennia and is the oldest and best understood, access to the other three is a much more recent phenomenon, ranging from a century for Air to fewer than thirty years for Cyberspace. They also differ as to the scale, nature and level of existing regulation.

Opinions vary on the analytical validity of considering all four domains as a unity. While acknowledging these differences, this report argues that important commonalities between the four domains make the notion of the global commons a valuable tool for both analysis and recommendations.

Using the insights of NATO’s new Strategic Concept and the 2010 Lisbon Declaration, this report is intended to inform and support a strategic dialogue within the Alliance on the global commons as an appropriate and critical area of attention. To
this end, this report examines the relevance and the security implications of a notion of the global commons for the Alliance, particularly through the lens of NATO’s agreed tasks, roles and missions. It then provides a set of policy, training and capability recommendations for consideration, taking into account the different post-Lisbon strands of work. Finally, this report will set out broader conclusions and perspectives aimed at stimulating further reflection and debate on the global commons.

The full importance of the commons for the globalized economy and their implications for management of natural resources, although acknowledged in principle, are beyond the scope of this report.

As a companion for this food-for-thought paper, Allied Command Transformation has recorded a detailed account on assured access to the global commons, based on the findings of a series of workshops and discussions with Alliance members, partner nations, international organisations and subject matter experts from Europe, the Americas and Asia. This report is available on request.

2. The Global Commons

The global commons can be defined as those areas that are not under any national jurisdiction or sovereignty and that are potentially accessible to any and all actors, be they states, non-state, or individuals. The classic analysis of the commons applied this definition to the high seas, and the definition was later extended to other domains as they became accessible to mankind.

In academic literature there is broad agreement that parts of the Maritime (open ocean), Air (outside of what is considered national airspace), and Space domains comprise the global commons. Cyberspace has been identified by some as a new addition to the global commons, because it shares a number of similarities. Cyberspace is not owned or controlled by any single entity or sovereign state and it is potentially accessible to any and all actors with the requisite technological capabilities.

The Cyberspace domain, however, is also very different from the traditional global commons. The established domains are physical, whereas Cyberspace is also virtual. By definition the global commons are not owned, whereas the man-made components that comprise in their totality the infrastructure that generates Cyberspace are owned, albeit by a very disparate and large group.

Nevertheless, this report argues that since the Cyberspace domain is of increasing importance to our security and there is a growing need for mechanisms to regulate the domain, there is logic and utility for including it under the umbrella of the global commons. Cyberspace will therefore be considered as an enabling domain that has an increasing influence on the way the other domains are accessed.

Currently, no unified body of international law exists that regulates or assures the right to access the global commons. The character and extent of existing regulation for each of the domains is very different. For the Maritime domain, there is a body of codified international agreements derived initially from common law and refined over hundreds of years. Regulations and international law covering Air and Space are more recent and were developed in response to specific concerns that galvanised international action. Agreements developed in the wake of World War II further defined international airspace, while concurrently confirming nations’ exclusive sovereignty over the airspace above their territory. Treaties covering Space were largely a response to the space race conducted between the United States and the former Soviet Union. Cyberspace stands apart because it is incompletely governed by both national legislation and private regulation.

Among the main difficulties with the notion of the global commons has been the duality between the domains as a resource and as communal spaces. Analysts have tended to consider the commons from two different perspectives. While academia has been primarily concerned with resource conservation and husbandry and with the flow of commerce and ideas, others have studied the security and military aspects of the commons.

This diversity of perspectives has resulted in a certain degree of doubt as to the relevance for NATO of conjoining the commons. While the preoccupation with the importance of individual domains in security studies has an established history, only contemporary studies have considered the global commons as a whole. This latter work has posited the hypothesis that only a single, dominant power could unify international efforts to protect and regulate the global commons and is therefore not applicable to the Alliance.
The key conclusion of Allied Command Transformation’s study on assured access to the global commons is that the construct is a useful lens through which to assess the main security challenges the Alliance faces today. It encompasses and highlights the shared interest that all responsible nations have in ensuring access in ways consistent with international norms, practice or law. The use of the construct could help the Alliance to communicate that NATO, as an actor in the preservation of assured and responsible access to the commons, is contributing to a greater and universal good.

Finally, it brings home the paramount importance of the four domains, their interconnection and the multiplicity of challenges they represent collectively. By helping to build an understanding of shared interests, both within the Alliance and beyond, NATO could leverage this construct to encourage a range of nations to cooperatively work with the Alliance.

As the use of the commons continues to grow, securing assured access to them will become a more difficult and pressing security task. From a military perspective, however, the complexity and pervasiveness of the interrelationships between the domains is a fundamental challenge for security analysis and defence planning. Assured access to the global commons necessitates coordinated and concurrent actions – political, legal and military – in every domain. This point has not yet been well internalized by the Alliance.

3. Relevance of the Global Commons for the Alliance

Strengthening the understanding of the threat to the domains amongst Alliance populations and governments will be crucial. Particularly in times of fiscal austerity, the Alliance will have to build support for the policies and investments required for assured access to the commons.

The new Strategic Concept directs the Alliance to turn its attention not only to current operations and immediate threats, but also to longer-term risks and challenges. Among these is the potential for denial of access to the global commons.

NATO relies on the global commons to carry out operations, to maintain communications, to generate intelligence, and to meet its mandate of ensuring security for its members. For the foreseeable future, the primary means by which the Alliance will project power, maintain credible deterrence, and respond to crises, either natural or man-made, will be via modern sea and air power in support of ground operations, enabled through Space and Cyberspace. The loss of access to one of these domains would affect detrimentally NATO’s ability to operate effectively in any of the others. Maybe the most compelling example would be NATO’s integrated air and missile defence system that depends on concurrent access to all four domains. A missile targeting NATO territory would be detected and tracked by a combination of cyber- and space-enabled systems and finally intercepted by a ground or sea-based missile.

With dependency comes vulnerability. As the use of the commons has evolved and increased over time, the cost of disrupting and interdicting access to the domains has declined. The necessary technology has become more readily available, more affordable and easier to use. This enables adversaries to target NATO’s populations, centres of commerce, and the vital flow of information and resources.

One of the vulnerabilities of NATO’s assured access to the global commons is the existence of multiple chokepoints that an adversary can target easily: straits used for international navigation, key airfields, satellite launch sites, and servers and other infrastructure for Cyberspace. An adversary can leverage these chokepoints to elaborate anti-access strategies that could potentially disrupt Alliance command and control and force projection capabilities.

Adversaries are likely to confront the Alliance by combining available irregular or conventional modes of attack, using a blend of traditional and modern weaponry and tactics. They will extend their lethality and increase their capabilities in non-traditional areas of conflict. Seeking a psychological advantage, adversaries will, for example, attempt to use the instantaneous connectivity of the globalized world as a force multiplier to maximise the impact of their actions and weaken the unity of the Alliance.

An example of this phenomenon relevant to the global commons is piracy. Globalisation, inadequate governance and limited security regimes have allowed modern-day pirates to exploit the Maritime, Space and Cyberspace domains simultaneously. Pirates use technologies, such as satellite phones and navigation enabled by global positioning systems, in
combination with conventional means, such as small boats, to plan and execute their attacks.

As identified in the Strategic Concept, the Alliance will ensure that it has the full range of capabilities necessary to deter and defend against any threat to the safety and security of Alliance populations. Piracy is but one example of a range of conventional and emerging security challenges associated with the global commons: proliferation of WMDs, terrorism, trafficking in arms, narcotics and people, cyber-attacks, and impeded access to space.

The nature of these continuously evolving risks and threats will pose new demands for instruments of prevention and response, when assuring access to the global commons. NATO’s partnerships and its comprehensive political and military approach are crucial instruments for successfully addressing evolving risks and threats to the commons. Decisions regarding NATO’s cooperation with other international actors could therefore consider their potential contributions to the task of assuring access to the global commons.

NATO’s effectiveness and credibility to deter threats is also based on its ability to respond to acts of disruption or denial to the commons. Deterrence therefore depends on reliable means to attribute violating activities in a timely manner and with unequivocal precision.

In the Maritime, Air, and Space domains, NATO has capabilities to attribute hostile actions to their source, although significant gaps remain, especially in the Space domain. In Cyberspace, the Alliance currently lacks a comparable capability to attribute, which leaves the Alliance with no credible ability to deter attacks. In Space and Cyberspace, the effects of hostile actions may not be immediate, further complicating retaliation under the doctrine of a right to self-defence. Effective attribution, deterrence, and retribution will be increasingly difficult to achieve for the Alliance or its member nations, due to the diversity of actors and interests at play.

To prevail in this complex security environment, the Alliance will require comprehensive policies, training and education, and capabilities to both respond and defend against threats to assured access to any of the commons. The implementation of NATO’s new Strategic Concept through the Political Guidance and the Military Committee Guidance for the Military Implementation of Alliance Strategy (MC 400/3) provides a framework and political direction for Alliance’s assured access to the global commons.
4. RECOMMENDATIONS FOR THE ALLIANCE

The Alliance should focus on protecting its assured access to the Maritime, Air, Space and Cyberspace domains where adversaries can deny access in ways that impact the strategic interests of the Alliance. Failing this, the Alliance needs the resilience, means and capabilities, supported by training and doctrine, to be able to operate in a degraded access environment. To this end, Allies should consider the continuing utility of systems that are less dependent on cyber and space for operating in a future conflict in which access to one or more domains is impeded.

Consideration should be given to establishing appropriate policies and strategies, including the use of NATO’s defence planning process for effective development of capabilities that enable the Alliance to ensure access to the commons. Based on the foregoing analysis the following recommendations have been identified.

A: POLICY AND PLANNING

POLICY
The Alliance has been developing policies and concepts on the individual domains (e.g. Maritime Security Strategy, Air Defence Committee’s work on Space, and Cyber Defence concept) but not on the global commons. This report acknowledges this body of work and supports its implementation. The Alliance therefore should consider:

- Establishing operational concepts for the development of effective attribution in the commons, which is a foundation for credible deterrence.
- Developing a comprehensive space policy based on a thorough understanding of NATO’s needs for access to space and the consequences of the denial of that access, the capabilities of its members, and a realistic picture of the future space environment.
- Developing appropriate plans, coordinated procedures, and capabilities for the protection of critical physical and cyber infrastructure and lines of communication.
• Initiating a strategic discussion between Allies and industrial partners to determine Alliance requirements in the commons. In particular, an analysis is needed to assess whether NATO should set up mechanisms to access national and private space and cyber assets in response to emerging capability needs.

PARTNERSHIPS AND OUTREACH
Common interests and the tenets of a comprehensive approach suggest a need for strong cooperation with partner nations and organisations, especially with the United Nations, European Union, Organization for Security and Cooperation in Europe and African Union, in support of assured access to the global commons. The Alliance therefore should consider:

• Strengthening its role as a forum for consultations among NATO nations and partners, in order to discuss emerging security issues and share best practices concerning access to the global commons.
• Cooperating with relevant actors to find solutions in areas of shared interest including cyber security, information sharing, piracy, proliferation of WMD, trafficking and the security of choke points.
• Encouraging the continuing development of regional organizations that uphold principles of assured access and work with them toward peaceful resolution of regional maritime disputes and strengthening international law and practice.

DEFENCE PLANNING
The NATO defence planning process is the appropriate place to determine the implications of the global commons for Alliance requirements and the scale of any capability gaps. The Alliance therefore should consider:

• Using the NATO defence planning process to establish the Alliance’s state of preparedness and to determine implications for the ability of the Alliance to conduct its core tasks if access to the commons were denied.
• Undertaking sensitivity analyses in order to identify the robustness of NATO force configurations under different levels of loss of access to the commons. This analysis would inform areas for priority action, and identify potential counter measures or alternative actions to alleviate the loss.

• How best to represent and address the interconnected nature of the commons given that the commons require a holistic assessment and therefore pose particular challenges for defence analysis.

B: CAPABILITY DEVELOPMENT

DOMAIN AWARENESS
Domain awareness in the commons will become increasingly important as the commons become ever more crowded and our dependence on them becomes more fundamental. The Alliance therefore should consider how to:

• Improve information-sharing among Allies, partners and with other international actors in order to increase NATO’s situational awareness capability so that the Alliance can identify, respond or deter threats in the commons (e.g. unmanned aerial vehicles).
• Close gaps in its ability to attribute hostile actions to their source in the commons; priority areas to address are in the Space and Cyberspace domains.
• Address the requirements for archiving, storing, and retrieving situational awareness information so actions may be attributed a posteriori in order to justify lawful countermeasures.
• Develop space situational awareness capabilities and ensure that these are shared with NATO partners.

TRAINING & EDUCATION
Superior training standards and the professionalism of its personnel will remain the strategic edge of the Alliance. Education and training are thus of paramount importance and NATO’s best means to successfully address risks and challenges that will arise from disruption or denial of access to the commons. The Alliance therefore should consider how to:

• Educate and train NATO forces in alternative processes and procedures for operations in a degraded environment. In individual and collective training, NATO should emphasize greater awareness of the risks and challenges to the four domains.
• Establish a series of exercises to train across the continuum of operational environments, ranging from protection, via degradation, to denial of access.
to the commons. Training that includes anti-access and denial of access scenarios should be added at the senior leadership level to the existing Pinnacle and Pyramid training program.

• Continue to improve Alliance computer network defence capabilities through equipment, software, and training of personnel. Conduct frequent cyber defence exercises. It is in the Alliance’s interest that all members have the resources needed to meet common standards, and to follow agreed rules, practices, and protocols.

**Organisation and Standards**
The Alliance should preserve and strengthen common standards and structures that bind its members in assuring access to the global commons. The Alliance therefore should consider:

• Establishing a dedicated NATO mechanism to address critical space mission areas with the ability to share information and assessments with Alliance partners, as required.
• How best to continue the establishment of organisations and mechanisms to foster closer relations with national cyber security organizations. This should include discussions on the development of active cyber defence, agreement on common cyber security standards and the establishment of an alliance-wide watch and warning network.
• Supporting the development of international regulations and quality standards for the manufacturing of IT hardware in order to strengthen cyber security.
• Cooperating with infrastructure and service providers to put in place effective information assurance safeguards. Allies will continue to work with the companies that host their essential services to incorporate strong, reliable security measures.
• Setting rules and standards for civil-military cooperation and information sharing in response to disruptive behaviour and in support of crisis management in the global commons.
• Assessing, identifying, and locating those cyber- and space-enabled services which are critical to the command and control of operations and logistics, including hosted services. Incident Response Teams would be important assets to reconstitute these critical services if attacked.

“*This is a time to concentrate upon essentials. It does not at all follow that this means a vast augmentation of expenditure. It is necessary to concentrate upon essentials and beware, of all things, of frittering strength away on remedies against dangers which have passed away in time.*”

**Sir Winston Churchill, UK House of Commons, 16 March 1950**
5. **Additional Perspectives for the Alliance**

In a world that is characterized by an ever more integrated international political system and an increasingly globalized economy, NATO nations and the Alliance as a whole are amongst the main beneficiaries of free and stable access to the commons. Due to its still unsurpassed technological, economic and military potential, the Alliance currently enjoys an unparalleled command of the commons that enables access to them in support of its goals and in the conduct of its operations without major hindrance. NATO nations owe a good deal of their power, wealth, and security to the open access to the global commons and therefore have a vested interest in its preservation.

Those dissatisfied with the current international political system and the related distribution of wealth and power around the globe acknowledge NATO’s predominance, but they also recognize the growing dependency of the Alliance on the global commons. By challenging NATO’s access, they see opportunities to devolve and reorder the status quo in their favour.

It is therefore likely that, in a process often characterized as the “rise of the rest”, emerging powers will attempt to redefine the current “terms of access” to the global commons. One example of this is territorial claims on parts of the maritime commons that are enshrined in the 1982 United Nations Convention on Law of the Sea. Another is the increasingly crowded geo-stationary orbit, to which future space-faring nations will demand access.

Efforts by the Alliance to protect and further regulate access to the commons could run the risk of being discredited as further attempts to protect the perceived political, economic and military supremacy of the Western industrialized world.

This does not mean, however, that NATO should not advocate strengthened governance of the global commons. As pointed out earlier, domain-specific regulations have been established in the past in a patchwork manner that does not recognize sufficiently the interconnectedness of all domains. It is likely that such an approach will soon find its limits and that there must be a discussion on how to improve governance framework of the commons. There is a case for the Alliance to be involved in such discussions.

Finally, the Alliance must convey carefully its message that assured access to the commons is of universal interest and benefits all. NATO’s partnership and outreach policies, in this regard, will be crucial and need to be informed by a clear view of what the Alliance has to offer that can be in the interests of both NATO and its partners. This is why, in the long run, the Alliance and its member nations will have to define what they expect from the global commons in a volatile and dynamic environment.
“I believe it is probably true that fortune is the arbiter of half the things we do, leaving the other half or so to be controlled by ourselves.”

Niccolò Machiavelli

The Prince