Assured Access to the Global Commons

by
Major General Mark Barrett
Dick Bedford
Elizabeth Skinner
Eva Vergles

Norfolk, Virginia USA
3 April 2011

A special thanks to Jeffrey Reynolds for his research, design and production expertise

Table of Contents

Title Page	**1**
Table of Contents	**2**
Foreword	**3**
Executive Summary	**5**
Introduction	**8**
Maritime	**11**
Air	**20**
Space	**26**
Cyberspace	**36**
Conclusion: NATO's Future in the Commons	**47**
End notes	**50**
Participants and Contributors	**60**

"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

Foreword

The domains of the high seas, international airspace, outer space, and cyber space are interlinked and critical to the prosperity and security of the Alliance nations. Access to these domains is both a military and economic necessity in today's world. In this inter-woven environment the loss of access would affect the ability of the Alliance to fulfill its essential core tasks of collective defence, crisis management, and cooperative security. A major assessment of this report is that in the coming decade the Alliance will face an adversary that will pose a range of threats to assured access and use by NATO across the four domains. From a military perspective, our response to these challenges will be based on a modern understanding of warfare that relies on deployable, sustainable, and interoperable forces, networked and dependent on maritime, air, space and cyberspace.

The idea of the Commons is not new. The chapters that follow describe the evolution of this idea, and illustrate its importance to NATO and the modern world. By no means, however, do we think this problem is NATO's alone to solve. Quite the contrary, "assured access to and use of the Commons" is a global concern, and while we believe the Alliance can play a role in advocating security and best practices, to name just two, it is not and never will be the sole contributor. In such an environment, as nations ponder their role and level of responsibility, they must be ready to respond, either individually or in alliance, to an aggressor that physically denies access to all or a portion of the four domains.

It is also important to note that the ideas presented here are not universally accepted. Clearly nations will need time to study and consider the implications of assured access to the Global Commons. We believe, however, that these ideas have utility for NATO for the following reasons. They highlight the shared interest that all responsible nations have in developing capabilities that ensure access to these domains in ways consistent with international norms, practice, and law. Further, this understanding of shared interests can be promoted by NATO to encourage countries that are not formal partners of NATO to cooperate with the Alliance. Finally, and most importantly, these ideas can be used to encourage nations to improve governance of these spaces, and to strengthen international norms of responsible behaviour.

Assured Access to the Global Commons is intended to inform and stimulate debate within NATO and the nations. Moreover, the implications and conclusions as presented provide a necessary starting point

for follow-on work and study. One opportunity to further this work will be through Multi-National Experiment 7 (MNE-7), which will, over the next eighteen months, evaluate the four domains, both individually and jointly. In the wake of the new Strategic Concept and the Political Guidance, we believe using this report, in conjunction with the output from MNE-7, is a prudent approach to thinking about the future. Doing so will help nations to better understand their potential roles and responsibilities in assuring access to and use of the four domains – actions that we believe are critical to the future security and prosperity of the Alliance.

Executive Summary

This report, *Assured Access to the Global Commons,* is the result of an open, transparent, and inclusive study built on the work of national and international organisations and consultations across the Alliance. Presenting the case for why assuring access to the four domains is an appropriate and important area of concern for NATO will help NATO adopt the appropriate approach to policy and planning in the immediate and near terms. The study has been conducted, and this report's conclusions are offered, in the distinct strategic, conceptual, and political context of the new Alliance Strategic Concept and NATO's Lisbon Summit.

The Global Commons comprise four domains: maritime, air, space and cyber. Maritime and air are the international oceans and skies that do not fall under the jurisdiction of any nation. Outer space begins at the point above the earth where objects remain in orbit, while cyberspace is defined in NATO's Cyber Defence Concept as "a digital world generated by computer networks in which people and computers co-exist, and which includes all aspects of online activity." The maritime domain has been used by humans for millennia, air for a century, and space for about six decades. Cyberspace, the newest domain, has been widely available for less than thirty years, yet more than a quarter of the world's population now use it every day, and that number continues rapidly to expand.

For 62 years, the enduring purpose of NATO has been to safeguard the freedom and security of the Alliance. In fact, the security and prosperity of our nations, individually and for the Alliance as a whole, rely on assured access to and use of the maritime, air, space and cyberspace domains that comprise the Commons. Both Alliance defence and the way of life of its nations depend on information, people, commodities, and goods that move across and through these areas, which are international and not under sovereign control. It is within, through, and from the Commons that trade, communications, transportation, and security operations take place.

A large part of NATO's strength and success comes from its ability to use the Global Commons in accordance with international law. Over time, access has become paramount to our ability to move troops into far-flung theatres of operation, to maintain command and control through the use of advanced information technologies in space and cyberspace, to control airspace in support of combat and rescue operations, and to support international disaster relief across the globe.

Because of the importance of these observations, in May 2010, General Stéphane Abrial, Supreme Allied Commander Transformation (SACT), directed a study of the Global Commons that would identify the challenges and vulnerabilities that affect assured access to and use of the Commons for NATO.

The four domains have many similarities and are closely interwoven, yet each has its own distinct properties, and thus they need to be addressed both individually and as a whole. Maritime, air, space, and cyber are crucial enablers of international security and prosperity. Most of the nations that are members of NATO, and many of its partners, have highly globalized economies that depend on assured access to all four domains. *Assured Access to the Global Commons* provides a useful and necessary lens through which to view the world as a complex, globalized whole that depends for its security and prosperity on access to the Commons. It articulates the importance of security in the Global Commons and its implications for the Alliance; highlights challenges the

Alliance will face with regard to assured access to the maritime, air, space, and cyberspace commons; and puts forward the implications for NATO in the future, including the development of capabilities.

Discussions about the Commons, what they encompass, who controls them, and the increasing complexity of each individually and how they interact, are not new. "Globalization in its present form speeds up the effects of actions all around the globe and magnifies their impact. The increasingly accelerated and interconnected nature of geopolitics and economic activity is generating new pressures and tensions."[1] The Global Commons are the most recent manifestation of these realities, and provide a crucial conceptual perspective for Alliance security in a globalized world. Thinking in the context of the then-solitary Maritime Commons:

> **Two prominent geo-strategists from the late 19th century, Halford Mackinder and Alfred Thayer Mahan, recognized the challenges posed by the increasing interconnectedness of their era...Mackinder characterized the growing economic interdependence of Europe as a closed political system of worldwide scope. He recognized that economic interdependence had made the world less resilient and more unstable as the "explosion of social forces" echoed sharply around the globe, and the weakest elements in the political and economic organisms of the world "shattered in consequence."**[2]

Access to and transit of the maritime, air, space, and cyber domains will continue to be threatened or disrupted by nations and non-state actors. In the future, we may be denied access to critical resources from the Global Commons, and the means to deliver them where they are needed. It is not difficult to imagine societies overwhelmed by large-scale disruptions of civil and military networks through increasingly sophisticated cyber-attacks. In many cases, international norms and laws, especially in space and cyber, are currently either insufficient or ineffective. It is particularly significant that, while globalization and the use of the Global Commons have increased dramatically, the cost of disruption has declined precipitously as disruptive dual-use technology has become more readily available, affordable, and easy to use. Building regulatory resilience and security capabilities against these threats will require improved capabilities and tools that build on both the technical and human elements of security.

To prevail in this complex security environment, the Alliance will require comprehensive maritime, air, space, and cyberspace strategies, policies, and capabilities to defend and respond to emerging threats. Is NATO ready to respond today to an aggressor who physically denies access to all or a portion of the four domains? Do we have contingency plans? Do we conduct sufficient planning scenarios and table-top war games with our Joint Force Commanders? Are defence planners evaluating the results and considering the capabilities required to conduct such operations in complex environments far from home? Do our maritime forces have the right Rules of Engagement and capabilities required to forcibly open a closed strait or canal? Are our forces properly integrated?

Assured Access to the Global Commons is also the point of departure for additional conceptual refinement and capability development with regard to these kinds of issues. We consider it a capstone document that can help nations prepare for Multi-National Experiment 7, which will study in detail access to the Global Commons. The report is based on in-depth research conducted in the course of the past ten months, as well as feedback solicited from nations, and is grounded in the

hard contemporary reality of uncertainty, rapid change, and budget constrictions. Equally important, however, is the message that the member nations of the Alliance can and must take positive steps now, if we are to protect our use of the Global Commons today, and continued access to them in the future.

Assuring access to the Global Commons will be the central challenge of the coming decade. In the wake of Lisbon, NATO is in a unique position to build partnerships in support of the goals presented here, reflecting this report's approach, which brings together innovators and practitioners from the public and private sectors, and from industry and the military. We will best do so by opening doors, and preserving common spaces on the high seas, in the air, in space, and in the cyber world. In this way, NATO will continue to demonstrate its enduring support for openness rather than exclusivity as vital Alliance interests and for the unconstrained use of the Global Commons in responsible ways that sustain and nurture our mutual security and prosperity.

Introduction

> The only way to cope effectively is to learn to cope with ambiguity, to coevolve with a constantly changing environment and adapt effectively with changing circumstances as best we can. Being able to do this should not be left to chance.[3]
>
> Grant Hammond

The Global Commons comprise four domains: maritime, air, space and cyber. Maritime and air, are the international oceans and skies that do not fall under the jurisdiction of any nation. Outer space begins at the point above the earth where objects remain in orbit, while cyberspace is the electromagnetic spectrum that enables digital processing and communications. The maritime domain has been used by humans for millennia, air for a century, and space for about six decades. Cyberspace, the newest domain, has only been widely available for some thirty years, yet more than a quarter of the world's population now use it every day, and that number continues to rapidly expand.

For 62 years, the enduring purpose of NATO has been to safeguard the freedom and security of the Alliance. In fact, the security and prosperity of our nations, individually and for the Alliance as a whole, rely on assured access to and use of the Maritime, Air, Space and Cyberspace domains that comprise the Commons. Both Alliance defence and the way of life of its Nations depend upon information, people, commodities, and goods that transit and move across and through these areas that are international and not under sovereign control. It is in, though, and from the Global Commons that trade, communications, transportation, and security operations take place.

The concept of the Global Commons provides a useful lens through which to view the world as a complex, globalized whole that depends for its security and prosperity on access to all four domains. *Commons* comes from Roman law, which categorized everything in the world according to the rights of ownership. Stray cats and whales, for instance, were *res nullius*, owned by no one, while air and sunlight were *res communes*, available to all but not subject to exclusive ownership.[4] Commons in feudal England were areas of land held by members of a group, typically local villagers or *commoners*, to be used according to legally explicit limits that prevented the land's division or over-exploitation. The thread that runs through these definitions is the idea of *use*.[5]

Maritime, air, space, and cyberspace have many similarities and are closely interwoven, yet each has its own distinct properties, and thus they need to be addressed both individually and as a whole. Most of the nations that are members of the North Atlantic Treaty Organization (NATO) have highly globalized economies that depend on assured access to all four domains, and the free flow of goods, services, people, and information.

The order in which the domains are presented (maritime, air, space, and cyber) reflects the historical development of access to the domains. Furthermore, it reflects the evolution of regulatory

regimes in the domains: use of the maritime domain from ancient times has allowed a substantial body of law and regulation, from English Common Law to Conventions on the Law of the Sea, to develop over the past 400 years. This precedent served as a foundation for the development of similar laws, regulations, and norms regarding use of the air domain.

The use of outer space and cyber space in contrast, is developing at a pace that often outstrips the ability of nations and other stakeholders to agree on best practices and procedures, let alone policy. As use has increased, both the cost of potentially disruptive technology and barriers to its acquisition, have rapidly declined. These are areas of increasing vulnerability for the Alliance, but also ones in which NATO, as a political and military alliance of like-minded nations, can provide invaluable expertise and leadership. It is important that we build on existing systems to develop best practices, norms, and regulations in these two domains, before circumstances, or our adversaries, overtake us.

A significant threat to the viability of the Commons is inadequate governance, insufficient norms and regulations, a lack of verification measures to ensure compliance, and more often than not ineffective mechanisms for enforcement. The development of technology that allows humans to exploit the resources of the Commons to their fullest is gradually exposing weaknesses in the regulatory regimes that seek to constrain exploitation. The potential opening of the Arctic due to climate change is an example of a change to the maritime domain that is placing pressure on the existing maritime regime. Legal regimes can be viewed as constraints on action or limits to sovereignty, but they are also a primary means to protect access to the Commons, and ensure their usefulness well into the future. If there is a "key" to the Commons, it lies in applying an approach that draws on the knowledge and abilities of all stakeholders to help solve the problems of access, use, and security across the four domains of the Global Commons.

In May 2010, General Stéphane Abrial, Supreme Allied Commander Transformation (SACT), directed a study of the Global Commons that would identify the challenges and vulnerabilities that affect assured access to and use of the Commons for NATO. The goal of the final report is to provide findings and recommendations for appropriate policy and planning in the immediate and near terms. To meet General Abrial's mandate, a series of seven workshops were held, both internal and external to the Alliance. These workshops built on the successful example of the Multiple Futures Project, and facilitated discussion among Alliance members, partners, and experts from nations across the globe. Each workshop was organized around a theme, for example, trans-Atlantic relations and views, perspectives from outside the Alliance, and each of the four domains: maritime, air and space, and cyber. Analysts from ACT presented each assembly with a tailored read-ahead outlining the aim of the workshop, along with questions of interest that were designed to elicit individual perceptions regarding the importance of the Commons in a globalized world. Lastly, the workshops asked participants whether they saw a role for of NATO, and if so, what that role might be.

To complement the discussions that took place, a survey for participants and subject matter experts was developed to elicit their concerns. These ranged from where further study might best focus, to the appropriate role for NATO in specific activities such as counter-piracy and non-proliferation. Over time, several common threads emerged which form the backbone of the analysis and the conclusions of this report. The goal is to present the study's findings in a clear, understandable way, so they can become the basis for a discussion among Alliance nations. The report describes each of the four domains in turn, according to four related topics: the importance of the domain to

NATO; NATO's activities in that domain; changes and emerging threats that can affect NATO's access; and possible future roles for NATO, as well as the potential constraints it faces, as it considers options for dealing with these problems.

The report presents a case for why the four domains that are presented as the Global Commons are an appropriate and important area of concern for NATO. It concludes with a set of general recommendations that NATO should consider as it implements the decisions taken at the 2010 Lisbon Summit. These recommendations, based on the feedback received from nations and research conducted in the course of the past ten months, are grounded in the hard contemporary reality of uncertainty, rapid change, and budget constrictions. Equally important, however, is the message that the member nations of the Alliance can and must take positive steps now, if we are to protect our use today and continued access in the future.

How well do members of the Alliance understand the effects of competition and constrained access on NATO's capabilities and readiness across the domains of the Commons? In a rapidly changing world, the answer to this question should not be based on assumptions or dismissed as irrelevant. It is important to keep in mind that the speed and complexity of the world we find ourselves in are phenomena of human activity. Thus, it is equally within our abilities to take steps now that will help us understand and plan for the future. But such steps can only be accomplished through a conscious decision to confer and collaborate with all sectors of society on finding solutions to common concerns.

Maritime

"The ocean is a mighty harmonist."
William Wordsworth

The maritime domain, the oldest and best understood of the four domains of the Global Commons, has been used by humans as a highway for trade and conquest ever since the first Phoenicians began to explore the Mediterranean Sea more than 4000 years ago. Today, many consider the maritime domain, the international waters of the world's oceans, to be globalization's circulatory system. Multi-national manufacturing has evolved over the last half century to make more goods available at lower cost, while simultaneously creating new markets world-wide. This trend has transformed the system from a global supply network into an integrated supply chain. A single product such as the iPhone4, engineered, designed, and patented in the United States, is made of parts manufactured in a number of different countries and shipped to a factory in China for assembly; the finished phones are then exported world-wide for sale.[6] The military supply chain that is the heart beat of deployed operations all over the world relies heavily on this integrated private sector model. Thus, threats to and vulnerabilities within both the civil and military supply networks should concern military defence planners, who have fashioned their own time-phased force deployment model on this integrated system.

Eighty-five per cent of all raw commodities and merchandise that move between nations are transported by sea, with a full three-quarters of that cargo transiting through international chokepoints such as a canal or strait at some point in that journey. Some 50,000 merchant ships, registered to 150 nations, and crewed by more than a million seafarers of every nationality, use the maritime domain annually. From 1968 to 2008, the volume of goods transported via the oceans of the world essentially quadrupled.[7] More than half of the world's oil travels across the world's oceans. Both China and Japan import 80% of their oil through the Strait of Malacca.[8] Thanks to maritime security, enhanced command and control via internet, and satellite-enabled global positioning, maritime commerce is a major aspect of the "just-in-time" inventory system. Containers and the ships that carry them have replaced warehouses. As in any system where timing is essential, the ocean-borne transportation system is vulnerable to disruptions, whether natural or man-made, which can create cascading effects throughout the supply chain.

In this complex, interconnected sphere of global commerce, no nation's economy can be entirely isolated. The recession of 2007-2010 demonstrated how quickly a downturn can spread among globalized economies. Governments regard their ports as strategic assets, because they are the gateways through which commerce – the life blood of trade and the global economy – must pass on its way to and from the maritime domain. Therefore, maintaining freedom of navigation, maritime trade routes, critical infrastructure, and the flow of energy are all in the best security interests of the Alliance and by extension, the global economy.[9]

The Dutch jurist Hugo Grotius (1583-1645) is widely recognized as having developed the first modern study of international law. His 1609 book, *Mare Liberum (The Freedom of the Seas),* which defends freedom of access for all nations to the maritime domain, is a cornerstone for modern treatment of the Commons.[10] From this beginning, European jurisprudence gradually constructed a body of law regarding national sovereignty and international relations that ushered in the epoch of the nation state. Even as states consolidated power, however, they recognized that no single nation could claim sovereignty over the oceans.[11] Centuries later, Admiral Alfred Thayer Mahan, in his authoritative work "The Influence of Sea Power Upon History," was the first to clearly articulate the importance of the maritime commons to national power, not primarily as a means to conduct war, but as a means to conduct commerce. Admiral Mahan described the primary reason a country maintains a Navy as being to ensure freedom of the sea lanes for the movement of commerce; otherwise, a nation's navy is merely an instrument of aggression.

The 1982 United Nations Convention on the Law of the Sea (UNCLOS), which first entered into force in 1994, is, like the UN Charter, an "umbrella" treaty in the sense that it is the basis for a number of follow-on treaties and laws that regulate conduct in both the maritime and air domains.

> **Because the Convention balances the rights and duties of flag, port, and coastal states, the entire architecture of oceans law represents a "package deal," in which states are required to accept all of its provisions, enjoying rights and fulfilling concomitant responsibilities. This careful balance between the rights and duties of flag and coastal states represents a grand bargain that unfolded during the negotiation of the Convention.[12]**

As this quote suggests, the UNCLOS treaties, which carefully delineate levels of sovereignty in the littoral, offshore, and international waters of the maritime domain, embody a series of critical compromises among its negotiators and signatories. As such, they reflect the understanding that in order for such systems to remain useful to all, there are limits to sovereignty. There will always be legal difficulties in establishing a single framework that clearly defines the rights and the obligations of all users under all circumstances. In an attempt to alleviate the concerns of those nations that found these codifications too limiting, subsequent agreements applied the concept of "functional sovereignty" to the continental shelf and archipelagic waters, and established exclusive economic zones (EEZs) as a means to apportion fishing and seabed resources, while protecting the right of "innocent passage" for foreign vessels to forestall economic warfare.[13] Paradoxically, this process amounts to a maritime version of the historical enclosure of the English village commons by large landowners. This illustrates the tension and shortfalls between the legal inclination to regulate the maritime domain as a common, and the political and geostrategic tendency of states to maximize their interests and protect their resources.

NATO Activities in the Maritime Domain

Only recently, with the end of the Cold War, has economic strength and regional supremacy been based on factors other than the ability of a nation to project military power beyond its region. China and Japan, for instance, have become the second and third largest economies in the world without having more than a regional naval presence.[14] This does not mean, however, that naval power – the ability to project power over the horizon, to control a region of the seas, and curtail the free movement of an adversary – is any less vital to global stability and prosperity. To the contrary, the integrated maritime portion of the global supply chain depends on long-standing tacit security

guarantees provided by strong blue-water navies, not only for their own nations' merchant fleets, but also for the foreign-flagged merchant ships that use their ports.

As the Alliance Maritime Strategy makes clear, it is highly unlikely that any future crisis response operation undertaken by the Alliance will be without a significant maritime dimension.[15] It is probable, given the tightly integrated and global nature of the world's economy, that challenges to security and economic interests in a distant maritime region (outside the Euro-Atlantic region) will have the potential to directly affect the strategic interests of the Alliance.

Naval forces also are an important means for NATO to fulfil its mandate to provide humanitarian assistance for disaster relief. Eighty per cent of the world's population live within 100 miles of a coastline, and allied navies have played a vital role in providing relief to littoral regions in the aftermath of devastating events such as Hurricane Katrina, the massive Indonesian and Japanese tsunamis of 2004 and 2011, and the 2010 Haitian earthquake. Aside from the moral imperative to mitigate suffering when and wherever possible, there is little to match the goodwill that the swift arrival of food, equipment, doctors, and trained personnel can foster in the affected community.

The new Alliance Maritime Strategy and the recent Strategic Concept emphasize the importance of a strategy of deterrence that goes beyond strategic nuclear forces. NATO has undertaken a number of missions in recent years to counter emerging threats in the maritime domain,

> **... which often involve forward engagement with non-NATO partners, such as Australia, Finland, Japan and Ukraine, the world over. At any one time, Allied vessels and supporting assets may be engaged in Operation Ocean Shield – NATO's contribution to determined international counter-piracy operations in the Indian Ocean – or participating in NATO's counter-terrorism maritime operation in the Mediterranean Sea – Operation Active Endeavour – or exercising with the navies of the nations currently participating in NATO's Istanbul Cooperative Initiative – Bahrain, Kuwait, Qatar and the United Arab Emirates – or with a Partnership for Peace country like Sweden in the context of the NATO Response Force.[16]**

An important aspect of the contemporary maritime domain is that its use depends on reliable access to space and cyberspace. The core mission of NATO's Operation Active Endeavour, for instance, is to deter, disrupt, and prevent efforts by terrorists to use the Mediterranean Sea, one of the world's strategic crossroads, for illegal activities such as the smuggling of personnel and weapons into Europe. It does this by using the capabilities of the Alliance to build strong maritime situational awareness, using an array of surveillance and intercept assets on land and sea, and in space and cyberspace. The new Alliance Maritime Strategy also calls for NATO's naval forces to deter aggression through the continued development of a ship-based theatre missile defence. The four-phase development of missile defence, which includes a significant maritime dimension, illustrates the requirement for secure access to all four domains of the Global Commons, and will be a hallmark of NATO's deterrent strength.[17]

The utility of the maritime domain depends on more than ships and harbours. The transmission of information such as orders, inventories, and the tracking of assets utilizes a vast network of both intercontinental undersea cables and space-based satellite links, and is a critical enabler of "just in

time" business models. The naval equivalent of supply chain efficiency has been smaller crew sizes, reduced armour and survivability, and greater dependence on commercial "off-the-shelf" (rather than custom-designed) equipment. Even more than commercial operators, navies are dependent on digital communications and satellite reconnaissance and navigation for deployed operations, maritime related flight data, and missile guidance.[18]

Although maritime situational awareness is still in the developmental stages, technological developments such as space-based systems, over-the-horizon radar, and near-shore and harbour acoustics are being incorporated into a layered approach to increase security. To identify and address weaknesses in the system, industry and academia continue to discuss ways in which technology, based on advanced modelling and simulation tools can be used to identify threats and determine potential impacts. NATO is expected to follow suit and place added emphasis on exercises and simulations to help decision-makers identify the best course of action.[19] The nations of the Alliance must therefore have a thorough understanding of the effects that on-going changes in force structure will have on access to the maritime domain. Future crises on the high seas that will have the largest impact in the near-term are less likely to take the shape of warfare between naval powers. Most probably, crises involving the maritime domain will involve major disruptions to the movement of cargo within the global supply chain. It is impossible to predict with certainty whether it will be a nation-state, a non-state actor, or even a hybrid of the two, that will choose to instigate anti-access activities. What is clear is that the destruction of, or long-term denial of access to, any portion of this dense web of trade and information would have deep and long-lasting effects.

Changing Conditions and Emerging Concerns

NATO relies on maritime assets for both rapid and long-term deployments, and overseas presence. By combining and leveraging a variety of capabilities and capacities among its members, NATO has the ability to project power across the maritime domain virtually uncontested, so for the time being loss of access must be seen in relative rather than absolute terms. However, challenges to maritime law, missile proliferation, advanced ships deploying high-technology mines, submarines capable of conducting anti-access operations, and increased competition among seafaring nations, if left unaddressed, will give opponents the potential to change this favourable picture in a relatively short span.[20]

In one example of denial and disruption at the state level, some nations are contending that, contrary to the provisions of UNCLOS, foreign warships must now obtain permission prior to transiting their exclusive economic zone.[21] Several states have also expanded their territorial claims to islands and waters in the South China Sea. Aside from the danger of regional conflict, such claims, if left uncontested, have the potential to enter into customary international law, and permanently interfere with the strategic sea lanes used to transport goods and information to and from the Pacific and Indian Oceans.[22] The region is also seeing an unprecedented naval build-up, primarily of green-water and littoral vessels. China's increasingly capable regional fleet, currently composed of frigates, destroyers, and submarines, will soon begin outfitting its first aircraft carrier.[23] In the highly sensitive Persian Gulf region, Iran has repeatedly experimented with anti-access tactics to interfere with the movement of both naval and commercial vessels through the Strait of Hormuz.[24]

As trade between the East and West expands, the Indian Ocean will play an ever-increasing role in global maritime operations. In light of this trend, India has determined that its national interests will be best protected by increasing its procurement and development of naval weapon systems, including a world-class submarine fleet to support an anti-access defence strategy.[25] One security expert has postulated "a NATO of the seas for the Indian Ocean comprising South Africa, Oman, India, Pakistan, Singapore and Australia," that could enhance regional security and cooperation.[26] While cooperation between some of these states seems highly unlikely at present, support from the international community for regional partnerships could help to stabilize what threatens to become an increasingly volatile maritime region. If, by contrast, seafaring nations choose to use their naval power to deny free transit of their EEZ as a means to curtail competition or assert new territorial rights, this would have a serious impact on global trade and the future of access to the maritime domain.

A combination of conventional weapons systems and irregular tactics can give state and/or non-state opponents the potential to disrupt the global system of commerce through ever cheaper anti-access capabilities. Several nations, for instance, have become global suppliers of anti-ship and surface-to-air cruise missiles as a means to raise state revenues. One commercial arms manufacturer is now marketing "missiles-in-a-box" – four surface-to-surface cruise missiles packaged in a modified CONEX shipping container, ready to launch by remote command. Such a system in the wrong hands can pose a significant threat to naval vessels, and thus potentially to NATO's access to the maritime domain.[27]

Commercial shipping containers, in 20-foot equivalent unit (TEU) and 40-foot equivalent unit (FEU) varieties, which carry approximately 85 per cent of the world's seaborne cargo, are the perfect means to conceal and smuggle a variety of contraband, ranging from weapons of mass destruction to currency to people. It is well-known that only a small percentage of shipping containers are inspected by port or customs authorities. In the United States, this amounts to only three per cent of all containers that land in U.S. ports. Criminal organizations regularly take advantage of the container shipping industry to smuggle contraband goods of all kinds, move illegal weapons into conflict zones, and traffic human beings all over the globe. Similarly, there are reports of terrorist groups using trans-oceanic commercial shipping to move personnel, explosives, and weapons into Europe and the Americas.[28] As noted in a 2004 report from the Organization for Economic Cooperation and Development, "the assessed threat of a Chemical, Biological, Radiological or Nuclear Weapon (CBRN) being delivered via an anonymous shipping container has risen above other terrorist-linked threats to become a principal concern of international transport security policy."[29] Given the access a range of adversaries, from states to individual groups, have to the maritime domain and the potential for disaster from CBRN devices, this is a potentiality that the nations of the Alliance have to take seriously. Above all, concerns about possible cost or inconvenience should not forestall NATO from working with the commercial sector to model and study the risks and consequences of such an event.

The economy of every country in the Alliance depends on a reliable supply of raw petroleum and petroleum by-products, which in most cases are transported by water over long distances. There is growing concern among experts that this represents a vulnerability adversaries will exploit, by either hijacking oil and liquefied gas tankers to steal their cargo, or by destroying them at sea in order to disrupt supplies. The destruction of passenger and commercial vessels at sea is another tactic terrorists might use to spread fear and gain publicity. While some consider this a remote risk,

the increasing availability of cheap conventional weapons, from speed boats packed with explosives to small cruise missiles and sophisticated underwater mines, make such scenarios a realistic danger.[30] The terrorist attack on the USS Cole in Yemen in 2000 is one example, startling in its simplicity and effectiveness; besides crippling a significant naval asset, the bombing also strained relations between the United States and the Yemeni government for some time.

The critical value of straits to international commerce and security, long recognized in common maritime law, is an important aspect of UNCLOS. Despite being well within the territorial waters of their adjacent nations, the more than 125 straits around the world are designated international waters, with the full rights of transit this term signifies. Some 30-40% of the world's trade passes through the Strait of Malacca every year – and the pirates of the modern era know it.[31] Protecting the right of passage is in the best interest of all maritime nations, and one way of doing so is by endorsing regional cooperative efforts that increase deterrence by raising the costs to pirates.[32] The Association of Southeast Asian Nations (ASEAN) is one forum in which these efforts have been coordinated.[33] The coastal nations of Southeast Asia, plus India and Australia, for instance, have entered into a number of bilateral agreements to delineate maritime national boundaries as a means to enhance cooperation. The littoral nations of Malacca, along with neighbouring Thailand, agreed to apportion responsibility for security in the Strait, and to coordinate their activities, such as regular sea patrols. They also created multinational institutions to study issues regarding the Strait. While these efforts have not provided a complete solution to regional piracy (many pirates have moved their operations east into the South China Sea), attacks in the Strait declined dramatically between 2004 and 2008. The effort to combat piracy also led to progress in regional governance, and helped establish cooperative mechanisms by which the littoral states can effectively manage their maritime interests.

Piracy off the eastern coast of Africa and in the Gulf of Aden, unlike in the Strait of Malacca, has burgeoned in the past decade, from a nuisance for commercial shippers to a significant threat to vital trade routes. The number of attacks worldwide has risen every year since 2006; 92% of the total occurs off the Somali coast. Nearly twelve hundred people were taken hostage at sea in 2010, more than in any other year on record, and an increase of close to tenfold in four years.[34] A combination of globalization, inadequate or non-existent governance, lack of international will, and weak security have allowed these modern pirates to exploit the maritime, space, and cyberspace domains by using a hybrid of newer technologies, such as satellite phones and GPS-enabled navigation, coupled with low-tech, small-boat swarming tactics, to plan and execute attacks, while simultaneously avoiding interdiction.[35]

Until effective governance returns to Somalia, pirates and terrorists will continue to flourish and nations will struggle to contain them. While naval vessels from a number of nations have joined regional states in patrolling the Gulf as a deterrent to piracy, the questions of where and how to try captured pirates in a court of law, along with who conducts and pays for trials and incarceration, persist. In the absence of a functioning government, returning convicted Somalis to their homeland for punishment is out of the question, while Kenyan courts, which until recently accepted jurisdiction along with financial assistance, are "overloaded with pirate cases from Somalia," and have stopped taking new referrals.[36] Several Somali pirates, captured after they fired on a U.S. navy vessel they mistook for a merchant ship, were brought to the United States and convicted in a U.S. court.[37] In another case, South Korean Special Forces rescued twenty-one hostages from the Samho Jewelry, a South Korea-operated ship that was being held by pirates in the Arabian Sea. Eight

Somali abductors died and five were captured in the operation.[38] It remains to be seen how and where South Korea will charge and try the five prisoners.

Piracy has been an international crime with universal jurisdiction for centuries, but the key to enforcement lies with national law. In April 2010, the UN Security Council called on nations to criminalize piracy,[39] but further proposals to establish an international tribunal to try pirates stalled in the face of objections from the U.S. State Department, among others, which argued that existing law was sufficient. The matter was recently raised again by Spain, with the backing of most NATO members, plus Russia, India, and China.[40]

Climate-induced change and enhanced deep-sea mining techniques are introducing instability in the maritime domain that will require legal and political foresight and cooperation to resolve. The world's oceans threaten to become a focal point for future conflict as increasing demand for resources minimizes the incentive to cooperate, while simultaneously intensifying both competition and the impulse to deny access to competitors. In the Far North, the melting of the Arctic ice pack is opening stretches of formerly inaccessible sea lanes and ocean floor to transit and deep-sea miming.[41] This topographical change, combined with advances in deep-seabed exploration and mining and the rising value of scarce mineral resources, is making the northern continental shelves of Asia, Europe, and North America more accessible and therefore more desirable. Arctic border nations are already staking competing claims under the provisions of UNCLOS.[42] NATO Secretary General Anders Fogh Rasmussen noted that "climate change had 'potentially huge security implications' for NATO in the Arctic Circle."[43] In 2009, when Russia sent a submarine to plant a symbolic flag on the Arctic seabed, the Alliance expressed its concern:

> **"I look at the high north and I think it could either be a zone of conflict – I hope not – a zone of competition, probably," said Admiral Stavridis, Supreme Allied Commander Europe. "There are certainly going to be areas of disagreement between the Alliance and Russia, but the issues are so big and so important that a cooperative approach, finding zones of cooperation, will be very important in the time ahead."[44]**

NATO's Future in the Maritime Domain

The new Alliance Maritime Strategy describes the four primary roles of naval forces in the maritime domain:

- deterrence and collective defence;
- crisis management;
- cooperative security through partnerships, dialogue, and cooperation; and,
- maritime security.[45]

These basic principles reflect NATO's roles and strengths across the Global Commons. Creating a picture of those key global maritime regions where large populations, vital resources, and maritime chokepoints (such as straits, canals, and narrow seas) overlap is one way to assess where Alliance interests lie throughout the maritime domain, and how best to protect them.

> **[The] emerging strategic context requires a substantial re-appraisal of the contribution of maritime forces in supporting NATO's objectives over the coming decades. Whether**

in support of Alliance joint operations, or when leading in a predominantly maritime mission, appropriately resourced and enabled maritime forces have critical roles to fulfil, defending and promoting the collective interests of the Alliance across a spectrum of defence and security challenges, as defined in the Strategic Concept. The maritime environment also lends itself well to strengthened engagement in cooperative security.[46]

As a political-military alliance with a strong naval history, bound by treaty and united by common goals, NATO has a key role to play in the maritime domain, at several levels and in several ways. Indirectly, working with partners and allies external to the Alliance, NATO can serve as a powerful advocate for and supporter of legal norms and acceptable behaviour. NATO must also be prepared to take action against threats to maritime security and assured access when Alliance interests are at stake.

The 1982 Law of the Sea Convention, founded on centuries of customary international law, is part of a broad, layered regime that defines international access to the maritime domain through a series of balanced compromises among nations. Despite weaknesses, it has proved both a resilient and an important stabilizing factor since its entry into force a quarter century ago. NATO, which includes some of the largest maritime nations in the world, should stand as a strong advocate for the observance and enforcement of UNCLOS as new concerns and challenges arise.

As in the other domains of the Commons, advocating responsible behaviour in the maritime domain is one of NATO's most important roles. Port visits as part of the routine activities of the Standing NATO Maritime Groups, for instance, can raise visibility and strengthen relations with nations across the globe. Another is to build consensus on shared interests, such as freedom of navigation in international waters, and preparing for the opening of the Arctic Circle to transit and exploration by sharing mapping and logistical information. Crisis management is another critical aspect of maritime security, and can include such missions as embargo and interdiction operations, precision strike in support of ground operations, flexible transport of personnel and equipment for rapid response, logistics and relief support, surveillance and reconnaissance, and even offshore basing.[47]

Anti-piracy operations off the Horn of Africa are a good example of a cooperative approach between NATO, the EU, the UN, local governments, commercial operators, and other regional powers to solve a problem with global implications. Maritime nations should be encouraged to adopt strong anti-piracy laws in line with UN Security Council resolutions, and to work within these organizations to find ways to mitigate the causes of piracy.

The emerging maritime issues in the Arctic Ocean present both a serious concern and an opportunity for the Alliance. In the same way that illegal limitations on the rights of passage through a nation's EEZ, if undisputed, can lead to those limitations' becoming an established part of international customary law, so can uncontested claims on the Arctic's resources. Once again, UNCLOS presents a viable basis on which to determine nations' rights in the far North over the coming years. The sea ice is not going to disappear all at once, and there is time to engage in a process that will forestall serious conflict or undermining of the existing maritime regime. Four of the five nations that are making territorial claims to portions of the Arctic (Canada, the United States, Norway, and Denmark) are NATO members. The fifth, Russia, has had special partnership status within NATO since 2002. This may be a further opportunity for NATO to support legal remedies by serving as a place for these nations to broach their interests and concerns about the

future of the Arctic. The more Alliance members can cooperate to solve mutual problems, the more NATO can exercise "leadership by attraction," demonstrating the value of supporting a regime like maritime law, and the benefits of cooperating with like-minded nations to accomplish goals.

The Alliance has an interest in protecting the global commerce that sustains modern societies, and in promoting security and stability well beyond its immediate borders. The combined navies of the Alliance, with their substantial operational capabilities, are well-prepared to protect the Alliance's combined security and economic interests across the maritime domain. NATO should, however, remain realistic in its expectations about the best ways to afford maritime engagement beyond the geographic scope of its current maritime partnership arrangements (these include the Euro-Atlantic Partnership Council, the Mediterranean Dialogue, and the Istanbul Cooperation Initiative areas).

If nations like India and organizations like ASEAN show a real interest in developing regional partnerships for cooperation and stability in the Commons, this may be an area where NATO can serve as both an advocate and a role model. It is in NATO's interests to understand why some regional nations are interested in improving their capability to project power at sea and, where possible, establish supportive relationships. The Alliance could offer to set mutual standards of interoperability and cooperation across a series of maritime missions, from anti-mine and submarine warfare, to maritime interdiction and anti-piracy measures.

Sea-based crime and global terrorism have specific, serious implications for maritime security, and for the Alliance. NATO should consider establishing standards for effective legal and military cooperation, and responsible behavior in the Maritime Commons. Credible deterrence of potentially disruptive activities requires capabilities for both prevention and, when conflict is unavoidable, retaliation. Determining what capabilities the Alliance requires, and how to achieve the needed force levels and capabilities in a rapidly changing political, economic, and strategic environment is the essential first step for Alliance maritime security. Building on that, force planners should evaluate the ability today and potential in the future for NATO's forces to deploy maritime-based theatre missile defences that can defeat the threat of ballistic missile attacks against Europe, North America, and elsewhere. Finally, enhanced maritime situational awareness is a key functional capability that will contribute to the effective security of the oceans and global trade. At present, this capability is in the development phase, which gives NATO leadership the opportunity to align supportive programs, doctrine, and capabilities to suit the requirements of the Alliance.

Air

"There is the sky, which is all men's together."
Euripides

Ever since the Montgolfier brothers began their pioneering experiments with hot air balloons in 1783, humans have invented ways to claim the skies as their own. While successors to the Montgolfiers' balloons played a small role in 19th and early 20th century warfare, primarily for weather and terrain observation, it was not until World War I and the development of fixed-wing, propeller-driven aircraft, that humans decisively gained access to the air domain.[48]

The demarcation between airspace and outer space is not clearly defined. One widely accepted definition puts the extent of the airspace domain at the highest point of aerodynamic lift, about eighty kilometres above the surface of the earth.[49] The precedent for setting an upper limit to national airspace was expressed in a conversation between Nikita Khrushchev and Charles de Gaulle at the time of early satellite over-flights. Uncontested U-2 and SR-71 flights further modified most working definitions of national airspace. Modifications of this type will undoubtedly continue as the growing availability of unmanned aerial vehicles for intelligence and surveillance reinforces limits on "national" airspace, and the expanding concept of an overlying common international airspace at very high altitudes.

Although access to the air domain is scarcely one hundred years old, international airspace, like its maritime counterpart, is a critical enabler of the globalized economy. Commercial air carriers transported more than two billion people on some 20 million flights in 2010. At the same time, a burgeoning air cargo industry now transports over 35 per cent by value of the world's manufactured exports. More than 30 million people worldwide are estimated to make their living directly or indirectly from the air transport industry.

The tiered delineation of coasts, seas, oceans, and straits as national or international waters, originally defined by Grotius and further codified in UNCLOS, provided a model for subsequent treaties regarding the use of airspace. As in the maritime domain, a nation has sovereignty over its national airspace (defined as that over national land, internal waters, archipelagic waters, and territorial seas), while international airspace as defined by treaty – the air domain of the Commons – is open to use by all.[50] Like territorial waters, national airspace is divided into zones, depending on proximity to land, altitudes, and designation of aircraft (military, civilian, or official). The maritime domain, however, is regulated largely by exception, while the regulation of commercial en-route and terminal traffic is virtually universal because of the physical nature of flight. Cross-border air traffic typically requires the "right of continuous transit" through sovereign airspace, and thus entails careful and detailed agreements that define, limit, and protect those rights.

There are fairly obvious reasons why flight, both national and international, is much more regulated and controlled than maritime activity. If a ship's port call is delayed or changed, the change rarely poses any danger for the captain and crew. By contrast, an airplane must land safely, one way or another, within a matter of hours from take-off. Passenger ships are a very small portion of ocean-

going vessels, while thousands of passenger airliners, often carrying hundreds of people, make up the vast majority of aircraft that fly every day. Ships travel across the different national and international maritime zones relatively slowly, and can sail in international waters for weeks, or even months, at a time. Airplanes move very quickly, and in the course of an intercontinental flight may enter and leave sovereign airspace several times. A flight from Munich to New York, for instance, will cross the national airspace of several nations before entering international airspace over the Atlantic for four or five hours; it then might enter Canadian airspace before finally crossing over into U.S. national airspace and landing in New York. Like ports in the maritime domain, international airports function as essential enabling nodes for the air domain, but are not of it: they are located on sovereign territory, and are often commercially owned and operated, but they also serve as vital supporting infrastructure for the use of airspace. Thus, security, right of use, common practices, and ready access to air routes and airports are matters of national and international interest, and require a close degree of cooperation, standardization, and normalization among nations.

Almost all nations of the world depend on safe, well-regulated access to airspace, both for national defence and to participate in the global economy. In doing so, they have found it in their interest to meet the global aviation standards for equipment and training that enable modern air commerce, and to cooperate with the global legal regimes and norms that give them access to international airport hubs. These modern norms and regulations were established by the 1944 Convention on International Civil Aviation (Chicago Convention), a major milestone in the regulation of airspace. Among other provisions, this convention sets requirements for aircraft to file flight plans and identify themselves when approaching national airspace.[51] Nations are allowed to set rules for the airspace adjacent to their national airspace, in what are called air defence identification zones (ADIZ). Thus, aircraft intending to enter sovereign airspace are required to identify themselves while still in adjacent international airspace as a condition of entry. Only in time of war or imminent hostilities, however, may nations demand identification from or attempt to deny passage to potentially threatening aircraft that remain in adjacent airspace.[52]

The rapid development of space and cyberspace capabilities is changing profoundly the way we use airspace and operate manned and unmanned aircraft. Today, virtually all civilian and military air operations depend on access to space-based, cyber-enabled communications and information transfer, to improve both safety and efficiency, and in the case of the military, the effectiveness of its operations. These include air traffic control, global positioning, precision timing, environmental monitoring of real-time conditions, collision and missile warning capabilities, weapons guidance, coordination, and constant surveillance and reconnaissance. Specialized aircraft function as critical mobile command, control, and vital communications links during operations.

NATO Activities in the Air Commons

The security of civil and military aviation is a concern to NATO, and by extension all nations that comprise the Alliance. Air commerce is a crucial element of the global economy, and its uninterrupted and safe operation is essential to prosperity and economic security. Many of the world's most important international airports are located on the territory of NATO members. They are the gateways to international airspace, and to the high-altitude airways that cover the globe. Like international shipping ports in the maritime domain, loss of access to one or more of these

major airports for more than a few days could have consequences for the Alliance, as the volcanic eruptions and severe winter weather of the past year have demonstrated.

Since the beginning of the Cold War era, NATO jointly and collectively has filled the crucial roles of air defence and security, to ensure the sovereignty of Alliance airspace against unwanted incursion. These basic but critical functions, with their component C2 systems, tracking and identification capabilities, and interceptors, place consistently high demands on the Alliance. As NATO struggles to balance capabilities with national and regional requirements, interoperability and burden-sharing will be important and on-going Alliance concerns.

In an Alliance as broad as NATO, some member states insist on keeping complete control of their own airspace and assets,[53] while others lack those critical capabilities required to meet Alliance standards. Regional systems such as the Baltic Joint Airspace Surveillance Network (BALTNET, 1998) are one means to address these problems. In other cases, individual states within these regional groups take on specific responsibilities, such as Finland's agreement to patrol the airspace of its region rather than only Finnish territory.[54] When properly balanced and planned for, these cooperative measures represent one of the chief assets of NATO: its ability to leverage the strengths and offset the weaknesses of its diverse members.

Unlike the maritime domain, where naval vessels routinely operate with and in close proximity to commercial vessels while simultaneously engaging in anti-piracy operations, show-of-force activities, and the patrol of commercial waterways, military air operating and training areas are usually kept well separate from commercial air routes. Nevertheless, air forces must always remain cognizant of their proximity to and potential effects on commercial airspace. Careful separation and vigilant command and control are essential to prevent the recurrence of incidents like the downing of an Iranian passenger plane by a U.S. ship-launched SAM during the Iran-Iraq war, and the Soviet destruction of South Korea's Flight KAL 007, which provoked harsh criticism and intense scrutiny around the world. In the ensuing quarter century, improved communications, data sharing agreements, better reconnaissance and tracking, and more exacting identification technologies have greatly improved our ability to search, track, and identify aircraft.

Changing Conditions and Emerging Concerns

The air domain is generally resilient, and as a whole can recover from disruptions quickly once the cause is remedied. Because of congestion and tight scheduling, however, the effects of a disruption in any one sector or at a major air terminal can quickly spread across the entire system. Deliberate denial-of-access attacks by state or non-state adversaries that caused a large-scale break-down of the commercial air industry would trigger consequences throughout the global supply system that could persist for weeks and months, with possibly serious effects for the interests of the Alliance.

Volcanic activity and severe weather played intermittent havoc with European and trans-Atlantic aviation in the spring and winter of 2010, causing large-scale disruptions at major international hubs. Thousands of people were stranded on both sides of the Atlantic, hundreds of planes were grounded or diverted, and the effects were felt for weeks. When Iceland's Eyjafjallajokul volcano erupted, an event that was both predictable and unstoppable, its persistent ash clouds disrupted traffic across the vital trans-Atlantic corridor for two months.[55] The International Air Transport Association estimated industry-wide losses as high as £130 million (€148 million) per day.[56]

Volcanic ash is a well-known hazard to jet engines, and when dispersed at higher altitudes can be difficult for pilots to detect and avoid. In the 1980s, the International Civil Aviation Organization[57] created the International Airways Volcano Watch to monitor volcanic activity, issue advisories to aviation, and develop mitigation procedures. In the extremely dense Western European and trans-Atlantic air corridors, even with advance warning, however, the cascading effects of shutting down airspace quickly became overwhelming, and took officials several weeks to resolve. Models and procedures exist to deal with such contingencies; one example is the Russian-US agreement in the Northwest Pacific that allows rapid, almost real-time re-routing of international air traffic.

Over the past year, the EU has accelerated its open sky initiative, based on what it calls functional airspace blocks (FABs). These blocks apportion European airspace into functional sectors according to operational requirements rather than national airspace. The purpose is to rationalize and integrate airspace, improve air traffic control and safety, and eliminate inefficiency. In a recent report, the European Commission stated: "Airspace is a common resource. The key to a more rational organisation of airspace is integration across borders through FABs in order to improve capacity, enhance security and lower costs of air traffic services. These FABs should be based on operational requirements – in particular traffic flows – rather than existing national borders."[58]

The world has yet to experience a large-scale attack on the air traffic system, with widespread infrastructure damage that put one or more major international airports out of commission for a period of time. The bombing that took place at Moscow's Domodyedovo Airport on 24 January 2011, multiplied a half dozen times across Western Europe and North America in a series of concerted attacks, would strike a serious blow not only to the economies of the Alliance, but also to global trade. If public reluctance to fly because the risks of terrorism or other disruptive actions became too high, as occurred after the terrorist attacks of 9/11, the commercial air industry would suffer another recessionary wave of cutbacks that, given growing trade deficits, would be hard to overcome.

What would an air anti-access campaign against NATO look like? NATO and its allies now exercise air superiority across the globe, a situation that has gone unchallenged since the end of the Cold War.[59] This superiority is based on a strong civil-military partnership, the coordinated use of cyber and space technologies, and access to precision weaponry. The stability of the air domain may be eroding in some parts of the world, however, as national air forces grow in size and sophistication. Furthermore, air superiority per se does not offer its traditional significant advantages against campaigns of interruption and exploitation in the air domain by non-state adversaries using asymmetric methods and tactics. In other words, an adversary need not establish air superiority to mount an effective challenge to NATO's ability to operate freely in airspace. This could present a serious vulnerability to NATO land operations, which depend heavily on strong air support to limit risks to troops on the ground.

There are three major likely developments that will challenge NATO's access to international and littoral airspace in the near-term to mid-term:

- The continued proliferation of long range surface-to-air (SAM) and advanced fourth generation air-to-air missile technologies will challenge NATO and its partners. Combined with long range precision-guided ballistic missiles, these high-end capabilities will put forward air-basing and deployed carrier-based air operations at risk.

- Persistent disruption to the command and control (C2) of aviation infrastructure through attacks in space and cyberspace60 would have profound implications for civil and military air operations.
- The increasing lethality and affordability of unpiloted aerial systems is changing the fundamental nature of air operations, and over time will dilute what has been a competitive advantage for the Alliance.

These trends and the spread of such capabilities will put both military and commercial communications and C2 networks at risk, and will force NATO to rethink ways by which to defend its forward-deployed operations.

The new reality of resource constraints and budget cuts are forcing air force leaders to think carefully about how to allocate scarce resources. As air forces become more effective through the use of advanced technology, they are also becoming smaller, while new aircraft are increasingly expensive. One important innovation has been the development of unmanned aerial systems (UAS), from micro- to large air vehicles, for intelligence, surveillance, and reconnaissance, and a long-range strike capability, as a technological hedge to complement "high-end, manned power projection platforms."[61] These systems are fragile, however, and require relatively secure airspace (and especially the continuity of secure communications) in order to operate. Furthermore, every technological advance that benefits the Alliance comes with a cost. Widespread proliferation of platforms and military technologies and the spread of dual-use technologies have made missiles faster and more lethal. SAMs, available world-wide on the black market, are smarter, more mobile, and easier to conceal than ever before, which makes them potentially dangerous to modern air operations.[62]

Air anti-access systems will operate in, from, and through all domains of the Global Commons, plus, of course, terrestrial locations. Space and cyberspace, as noted above, are intrinsic to the operations of modern aircraft, both military and civil, and the maritime domain is an essential component of Alliance air operations. National and non-state opponents know this and are planning accordingly; in the meantime they can be expected to take advantage of the lack of effective technology and weapons control regimes. For instance, in the near future, the anti-ship missile systems now being designed to launch from ship-borne containers are expected to include a surface-to-air version.[63] Able to move freely in the vast maritime domain, these FEU-based anti-air platforms will be exceedingly hard to identify and track. As more and more nations develop naval capabilities that incorporate relatively cheap and available cruise missiles, ballistic missiles, and advanced UAS technologies, unencumbered access to airspace will come under increasing pressure from those who seek to deny it.[64]

NATO's Future in the Air Domain

Access to international airspace is a vital aspect of NATO's ability to fulfil its Level of Ambition and to defend itself. As the Alliance continues to expand and build partnerships, it must be prepared to see its interests expand as well, and to understand the requirements for training and interoperability that will allow new partners to participate in air operations. Regional cooperative air surveillance efforts such as BALTNET are helping NATO members manage the burden of air policing, and may serve as one way to integrate air assets.

Air defence and joint air operations are continuing roles for NATO. The more Alliance nations can set the example by finding ways to cooperate and coordinate their activities in national airspace, such as is being done with FABs, the better they will be able to assure access to international airspace and the national corridors and airports that are the system's vital nodes. An important question for NATO will be whether it can, or should, help member nations better coordinate and secure international air traffic as it relates to air defence and joint logistical operations, in order to increase resiliency and avoid major disruptions.

As adversaries develop increasingly sophisticated and effective anti-access systems, they are likely to find UAS an attractive choice. If so, these systems may come to play a greater role in the missions of surveillance and precision strike. While UAS and their command systems are at present expensive and hard to use effectively, the enabling technology is rapidly improving, and many experts believe the coming decade will witness a geometric explosion in their deployment. NATO needs to determine what roles and missions it envisions for this new class of vehicle, and then develop standards of use and interoperability for the Alliance.

The lessons of modern warfare, missile proliferation, and the realities of resource constraints are encouraging air forces increasingly to move away from strategies that rely on short-range weapon delivery to more capable stand-off forces and long-range precision.[65] Naturally, this will require improved intelligence, surveillance, and reconnaissance capabilities that are more dependent on assured access to the space and cyberspace domains. When evaluating how an adversary might view anti-access strategies, they may find it to be more cost effective to target space and cyberspace, given the heavy reliance modern air defences have on terrestrial and space-based advanced information technologies. Therefore, the potential effects such strategies may have on access and use of the air domain is something NATO will need to evaluate and understand if it is to develop effective counter-strategies.

Space

"The massive bulk of the earth does indeed shrink to insignificance in comparison with the size of the heavens."

Nicolaus Copernicus

Space, popularly referred to as "the final frontier," has been brought much closer to Earth in recent decades, with continual discoveries in astronomy, advances in space-faring technology, and the digital revolution in cyberspace. Over a thousand orbiting satellites collect, transmit and transfer data, such as telecommunications, meteorological imagery, surveillance, global positioning, and timing, all of which have both commercial and security applications. Whether deciding what to watch on television or if weather conditions are safe to deploy aircraft, space capabilities that include satellite-enabled telecommunications have become indispensable to contemporary life. Only when the signal disappears, or a satellite falls to Earth, are we reminded about the importance of space to our daily lives.

Unlike the world's oceans and airspace, no part of outer space falls under sovereign rule. Therefore the term "domain" as used in this discussion refers to all of outer space. Assured access to and use of space, for all who have the means to reach it, was codified in the 1967 Outer Space Treaty and its follow-on agreements.[66] The most basic question of what constitutes the space domain, however, is not answered in international law. Although the Treaty does not specify the boundaries that differentiate space from the upper reaches of national airspace, a norm has developed that defines space as the point above the Earth at which satellites stay in orbit.[67]

Like the maritime and air domains, the space domain, in tandem with cyberspace, is a vital part of the intricate web of trade and information that characterizes globalization. Air traffic control has become far more efficient with global positioning systems (GPS), as have seaborne and land navigation. The just-in-time global supply chain depends on world-wide telecommunications and GPS data from satellite systems to manage its complex operations. Space thus is one of the critical enablers of the globalized economy and military command and control, operations, and logistics.

> **In the early 20th Century, Admiral Alfred Thayer Mahan was adamant in his belief that sea power was not only naval power, and not even mostly military power. He insisted the greatest military utility of sea power was a healthy and profitable sea commerce which would produce the wealth necessary to sustain a nation at war...Military space strategy should be intended to produce space power in times of peace as well as in times of war, in all of its forms. Therefore, not only military space theorists, but all military space leaders must be always cognizant of civil and private space programs.[68]**

The ability of satellites to monitor conditions on Earth allows researchers to anticipate changes in terrestrial and atmospheric conditions by tracking large-scale patterns as they emerge over time. We have become used to planning our personal, economic, and military activities according to remarkably accurate multi-day meteorological predictions that were unobtainable a generation ago. Satellite data also is vital to the opening of the waterways and sea-beds of the Arctic Ocean for transit and exploration, as nations seek to determine and predict the annual melting and formation of ice packs, and their movements across the Arctic Ocean. The ever-increasing acuity of satellite imagery allows interested parties with access to the data to track maritime activities in real time and monitor compliance with international regulations.

Nor is the space domain limited solely to orbiting satellites. Access to space includes the ground facilities that both manage orbiting satellites, and receive and disseminate the data stream. Like shipping ports, airports, and computer servers, these critical nodes lie on sovereign territory, are often commercially owned and operated, and in many nations, are likely to be shared by the public and private sectors. Unlike ports and airports, which are usually located according to geographic necessity or convenience, the location of an orbital tracking station is constrained by the orbit, and the nature of the satellite's mission. The placement of these facilities therefore frequently involves negotiated use agreements, leases, and financial arrangements among governments and commercial enterprises across the globe.

Several participants in the Global Commons space workshop, held at the Joint Air Power Competence Centre (JAPCC) in Kalkar, Germany, characterized space as a "centre of gravity" for NATO. Twenty-three of the 28 Alliance members have a space program of some kind. In 2009, a total of 78 orbital launches took place from over 17 spaceports around the world, carrying 111 payloads for militaries, government civilian sectors, commercial entities, and universities. This brought the total number of functioning satellites circling the Earth in various orbits to approximately 1100.[69] In the civil sector of the most developed nations, loss of space and its cyber-enabled backbone would bring certain areas of commerce, finance and government to a halt for the days or weeks it would take to devise work-around systems. While ground-based nodes using fibre-optic cable and wireless technologies can replace some satellite services, they cover a limited territory, and the cost of access can be prohibitive. Command and control of military forces, precise air power, missile guidance, troop movements, environmental reconnaissance, and missile warning all have come to depend, to a large degree, on information relayed by satellites.

The present architecture of assets in space is an amalgam of private and state-owned and -operated systems. The rapid growth of commercial space activity over the past quarter century has, however, outpaced the development of rules and procedures to govern access, use, debris mitigation, hostilities, information sharing, and many other aspects of space management. Despite its seeming vastness, the useful geo-orbital region of space is a surprisingly fragile environment, and the pressure of human activity threatens to overwhelm parts of it. As the use of space to support and enable private, commercial, and military enterprises has increased, so have the vulnerabilities, and the need for a coordinated body of updated space policy.

For over fifty years, since the advent of the Space Age, attempts to write rules for the use of space have generally followed two approaches: top-down laws and treaties created by nations, and bottom-up initiatives developed by national groups, international organizations (IOs), think tanks, and others.[70] The Outer Space Treaty is an example of a broad, multi-lateral top-down approach that

codifies agreed laws and limits on both equipment and activities in space.[71] Bottom-up initiatives, by contrast, are more likely to focus on narrow areas of interest, and are often aimed toward developing a set of norms and confidence-building measures.

Excluding the Anti-Ballistic Missile (ABM) Treaty, the bottom-up approach to arms negotiations that developed between the United States and the Soviet Union during the Cold War focused on narrowly targeted initiatives, backed by mutually accepted verification measures. These first steps gradually expanded into a nuclear arms control regime and disarmament process that continues to this day. As verification became more important, satellites increasingly replaced clandestine spy planes, driving both sides to accept certain infringements on their sovereignty, such as over-flight by objects in orbit.

One of the subsequent conventions on outer space ensures freedom of access to the Moon and all "celestial bodies," for exploration. Because objects in orbit eventually fall to Earth, another agreement defines the responsibilities of space-faring nations for the things they put in space, although there is no specified governing body with the authority and power to enforce this provision.[72] The activities and liabilities of commercial space enterprises are regulated at the national level. States are required to keep a registry of objects launched into space, submit data on launches to the UN International Telecommunications Union, and inform that body when objects leave orbit.

The finite capacity of the useful radio spectrum, which is under increasing pressure from rapidly expanding commercial and military space activities, is a further concern for space governance.[73] All users, including militaries, are enjoined to avoid harmful interference in one another's bandwidth and orbital tracks. Enforcement, however, has been weak, a shortfall that is likely to become more noticeable as the spectrum becomes more congested.

NATO Activities in the Space Domain

At the present time, assured access to space is threatened only on a relative, rather than absolute, level. NATO's membership comprises several of the most advanced space-faring nations in the world, whose combined assets far outstrip any known competitor. NATO relies on its space-faring members and the commercial sector for services on an as-required basis, an arrangement that is likely to continue for the foreseeable future. The services that member nations choose to make available, are not, however, considered to be common assets. In NATO, most surveillance, reconnaissance, and remote-sensing satellites are dual-use, used by both the military and the commercial sector.[74] The availability of commercial satellite assets means that much of the imagery, information, communications, and GPS data coming from space is widely available. This openness benefits NATO and its allies and partners by making it easy to share information. On the downside, this data is equally available to adversaries and competitors alike.

Though NATO depends on space to perform its tasks and missions, it does not have a policy that guides its expectations and access to capabilities in space, a military space strategy, or a dedicated cadre of experts from among the nations to sustain its space-based support. ISAF forces, for example, are highly dependent on space for data, intelligence, and telecommunications. This capability allows commanders to make decisions, both before and after action, based on accurate and timely information. In the absence of a host network, expeditionary forces rely on satellites for

their online activities, including communications with support bases.[75] Commercial satellite imagery is also a vital tool for NATO's disaster response and humanitarian relief operations, allowing responders to evaluate conditions on the ground prior to arrival. Using the information from space, commanders can make better decisions about where to drop supplies, which ports or airstrips are usable, and which areas remain inaccessible.

If NATO were to lose access to space, its operational plan to defend itself or to deploy forward would be compromised, and the Alliance would be forced to revert to crude, pre-space era technologies and tactics. In some cases, such as precision-guided weapons and the synchronization of communication networks, there would be no going back, as these technologies require GPS to operate. Their loss would have a significant impact on the Alliance's ability to project power, exert command and control, and resupply its forces. Some researchers have theorized, based on extensive "day without space" modelling and simulations, that the human and economic costs of fighting such a war, without the "smart" weaponry and real-time situational awareness modern militaries have come to rely on, would be staggering.[76]

Putting a satellite into space and maintaining it there remains costly. Because of the high cost of entry and diminishing availability of useful orbits and bandwidth, the radio frequency spectrum of one commercial satellite constellation is often divided and leased to a variety of private and public users. The clear trend among space-faring nations is to rely on the commercial sector for a considerable portion of their space activity, including manufacturing, launch, hardware maintenance, and data management.[77] While this introduces a level of uncertainty into the system by subjecting space access to the vagaries of market-based interests and possible disruption in the supply chain, it also provides resiliency by spreading research, funding, and knowledge across a large industrial sector.

Several European nations have developed satellite consortiums that combine public-private strategies and investment to run their space programs. The European Space Agency (ESA) has the mission to develop use of space and actively promote European industry, by granting contracts to each member in proportion to the country's contribution to the agency.[78] A goal of the ESA's policy is to apportion scarce resources to avoid duplication of effort. The EU also has taken the lead in fostering the development of a European space policy and a code of conduct for operations, as emphasized in the Lisbon Treaty.[79]

The U.S. government, including the military to a lesser degree, works extensively with commercial and civil-space organizations such as the National Aeronautics and Space Administration (NASA) to operate its space programs. Many of the large aerospace companies that are headquartered in Europe and the United States share people, ideas, and organizational practices in an increasingly borderless environment where cooperation and competition are seen as complementary. This decade-long interaction between the continents has led to a significant increase in space capabilities that are interoperable.

The decision to support the international space station with a hybrid of private and government-backed services that are modular and interoperable is just one recent example of this trend towards privatization. On 8 December 2010, the Space Exploration Corporation (known as Space X) launched a spaceship from Cape Canaveral aboard a Falcon 9 rocket. The craft successfully went into low Earth orbit and descended to a soft landing in the Pacific Ocean, the first time a

commercial enterprise in the United States has achieved this goal. Space X has signed a $1.6 billion contract with NASA, under the new Commercial Orbital Transportation Services program, to replace the retiring space shuttles with privately owned and operated craft that can transport cargo to the International Space Station.[80]

As the commercial sector takes over more of the activity in space, the Outer Space Treaty has in some regards been overtaken by technology.[81] On 22 May 2007, the European Space Agency, working together with the European Commission, unveiled a simple policy that seeks to clarify certain questions regarding the responsible uses of space.[82]

> **[T]he European Space Policy sets out a basic vision and strategy for the space sector, and tackles issues such as science, applications including security and defence, access to space and exploration. Based on that European Space Policy, the Resolution adopted by the "Space Council" of ESA and European Union ministers defines a vision for Europe in space and provides guidelines for implementing that vision.[83]**

The new policy also promotes increased cooperation between civil and defence space programmes and technologies. Importantly, it calls on members to ensure sustained funding for space applications, in particular the flagship initiative Global Monitoring for Environment and Security. Further, it describes space as a driver for growth, innovation, and employment, and a valuable source of new opportunities for European industry. To support these goals, the EU and ESA are planning to develop a joint strategy for international relations regarding space activities.

Changing Conditions and Emerging Concerns

Threats to access in the space domain fall into two broad categories: kinetic damage to space assets on the ground or in orbit, and activities that, deliberately or not, disrupt the transmission or reception of satellite signals without direct physical damage to the components. Either kind would be harmful to commercial and military activities on Earth. A space-capable adversary intent on achieving the greatest effects would be likely to use both. Invariably, as more nations and non-state actors develop counter-space capabilities, challenges to stability and security in space will continue.[84]

It does not require a specially designed weapon to destroy a satellite in space, as was seen when a defunct Russian satellite accidentally struck and destroyed an active communications satellite in 2009.[85] Technically, any object with a guidance system and fuel to manoeuvre can become a "space mine." What is more, objects travel at such high velocities in space that even a scrap the size of a pen can inflict serious damage on valuable machinery. The sheer numbers of man-made objects orbiting the Earth, estimated at some 21 thousand individual pieces,[86] have made it nearly impossible to determine with certainty whether or not a collision was intentional. This is true even for the space situational awareness (SSA) capabilities of Air Force Space Command in the United States. This growing congestion problem is threatening to render some of the most desirable orbital paths essentially useless.[87]

It is important to note, however, that although the new commercial players make space more congested, it is the states themselves that have been the most egregious violators of accepted space

conduct, especially when it comes to the generation of space flotsam.[88] An anti-satellite (ASAT) test by China in 2007 left a large debris field behind that will take many decades to fall back to Earth. Meanwhile, each of these thousands of shards, from a few centimetres to several metres in size, becomes an unguided missile that must be tracked from Earth and avoided by the active satellites that share that orbital path.[89] Likewise, the Soviet Union and United States both tested nuclear warheads in space during the Cold War. The resulting electromagnetic pulse and radiation from the blasts indiscriminately destroyed or damaged a string of satellites that happened to be nearby at the time of detonation. This alarming experience led directly to the 1963 Limited Test Ban Treaty outlawing the testing of nuclear devices in space, and the 1967 Outer Space Treaty banning the placement of weapons of mass destruction in space.[90] Unfortunately, while research is underway, the technology to actually clean up space is still years in the future.[91]

It is this persistent quality of space pollution that certain adversaries may find attractive, particularly non-space-faring states or actors that seek the most damage with the lowest input, and have no concern for long-term consequences. North Korea, for example, has no space assets and little digital infrastructure, and correspondingly has little incentive to preserve access to space. The North Korean regime is actively developing both nuclear weapons and long-range missile capabilities, which would put the possibility of a nuclear attack in space within Pyongyang's reach, or the reach of anyone who managed to acquire similar technologies.[92] There is no practical way to differentiate between commercial and military launch vehicles; both the United States and Russia have successfully converted Cold War-era ballistic missile launchers, originally designed to deliver nuclear warheads, into satellite launchers.[93]

Terrorist groups, for their part, are unlikely to view anti-access activities in space with much interest. The first and most obvious reason is that terrorists who acquire a missile and/or a nuclear device are unlikely to use them against targets in space, when they could be used to far greater physical and psychological effect against targets on Earth. Second, despite technological advances, access is still prohibitively costly for anyone below the state or corporate level. Third, launches are high-profile events, thanks in large part to satellite surveillance. Any country that allowed terrorists to launch an anti-satellite weapon, especially a nuclear device, would be a clear target for retaliation. A launch from the vast stretches of the maritime commons, however, could be difficult to attribute.

The proliferation of anti-satellite technologies among a number of nations is a far greater threat to access to space, and is forcing changes in the way satellites are designed and launched. Although large, complex communication satellites will continue to be the norm for the foreseeable future, there is a trend to develop smaller, more adaptable devices that are easier to launch, harder to hit, more manoeuvrable, and more capable. The U.S. Operationally Responsive Space Office is working on a modular satellite that can be reconfigured on demand to meet specific operational requirements. The same idea is being applied to command and control software designed to improve interoperability between Alliance members by enabling satellites, like personal computers, to recognize and accommodate new firmware.[94] Other nations and commercial enterprises are following suit as advanced technology continues to lower the bar to entry to space.

The expense of launching satellites is being addressed in a number of ways, including the use of modified jumbo jets and fighter aircraft. Innovative entrepreneurs are engineering and marketing so-called "cubesats," constellations of shoebox-sized satellites that can be launched essentially as

ballast on large rockets, significantly reducing their launch costs.[95] The French firm Dassault Aviation, in partnership with German and Spanish firms, is testing a satellite-launching rocket that can be fired from a carrier-based version of the Rafale fighter jet. In the event of a conflict or other major event that disrupted existing satellite communications, "This would allow naval fleets...to launch their own satellites if needed."[96] Even without the actual "weaponization" of space, it is easy to imagine how a terrestrial war that grew to involve the destruction or disabling of satellites, and subsequent quick launches of emergency "cubesat" constellations, could make specific low-Earth orbital paths even more congested and less useful.

There are other ways to disrupt, disable, or destroy satellites in space, through the use of directed energy weapons and microwaves. Today the means to carry out these attacks are in the hands of states rather than non-state actors, and several NATO nations are among the most advanced developers of such devices. Over the next decade, an array of anti-satellite warfare capabilities, including space-based weapons, will emerge.[97] At the current pace of technological change, and with the inevitable proliferation of enabling technologies, NATO should expect these capabilities to be used in future conflicts, and plan for the consequences of that eventuality.

Simpler methods, such as jamming and spoofing, can be directed against the information output of satellites or the control systems of spacecraft, rather than the hardware. Jamming disrupts the connection between a satellite and its ground station through a high-power electronic signal; spoofing is the cyber hijacking of a space system's control signal.[98] In 2010 and 2011, the Iranian and Libyan governments both used signal jamming techniques in an attempt to stop news media from broadcasting coverage of pro-democracy movements within their countries. In each case, the news sources were forced to transfer their signals from one satellite to another in attempts to evade the jamming.[99] Although, technically speaking, these activities fall into the cyber domain, their effects occur in both space and cyberspace, and demonstrate the complex interrelationship of the two domains. A successful large-scale, long-term jamming attack would wreak immediate havoc across all four of the highly interconnected domains of the Commons. Ships and aircraft would lose the ability to navigate precisely, satellites would not be able to update their positions, and retaliatory cyber-attacks would very likely proliferate. Jamming and spoofing techniques, which require only widely available technology and computer programming skills, are now within the reach of many non-state, as well as state, actors.

Just as in cyberspace, discerning intent and attributing specific actions are still major obstacles to security in space. One of the key findings of the Schriever Wargame 2010[100] underscored that observation: The interweaving of civil, commercial, and military space capabilities has become so complex that it was difficult, if not impossible, for participants to attribute an attack, or in some cases understand when, or even if, an attack had started, or whether it had ended. Uncertainty about the source or scale of an attack produces instability in the international system, and instability can trigger escalation.[101] The mitigation of uncertainty in the space domain requires both communications information, which helps to define intent, and detailed space situational awareness (SSA), which provides tracking and environmental data. France and Britain both are investing in the development of SSA systems that will be compatible with and enhance existing U.S. capabilities. Within the next decade, China, India, and Russia are expected to make significant progress in the development of their own sophisticated tracking systems as they invest billions of dollars in new technologies.

The military-civil-commercial interface that is a chief characteristic of the space domain makes it imperative that any discussion of new norms, regulations, and initiatives regarding space brings all stakeholders into the process. The new ESA policy can be a good starting point for a larger international discussion on some critical questions regarding the responsible use of space.

NATO's Future in the Space Domain

The space domain has undergone a number of changes over the past two decades that, left unaddressed, will gradually undermine its usefulness, increase instability, and render space less accessible. Crowding of orbital paths and radio frequencies will only increase as more new actors, both state and commercial, take advantage of less costly technology to develop programs in space. Some states are actively developing anti-satellite capabilities, using both kinetic and cyber techniques that have the potential to deny and disrupt access to the critical information enabled by capabilities in space. These new developments are putting pressure on the Outer Space Treaty, and compelling many countries and international organizations to either originate new policy or rethink existing policy. There are at least five major areas of concern for NATO in space: evaluating, determining, and articulating NATO's needs in space; planning and training for access denial and operations in a degraded environment; improved space situational awareness and protocols for sharing information; developing agreed policy for NATO's use of national assets in space; and the accrual of a dedicated cadre of space experts, along with the creation of a NATO space office.

What would a day without space look like? It is possible to imagine a future scenario in which the nations that make their space assets available to NATO have lost access to space or need their assets to defend themselves against a series of highly capable adversaries. Does the present arrangement in the face of such a threat leave the Alliance vulnerable, and equally important, is NATO willing to accept that vulnerability? It is important that NATO study, understand, and articulate to its members what the loss of commercial and/or military satellite telecommunications, whether deliberately or by cyber-attack, or unintentionally by space debris, would mean for the security of the Alliance.[102] Only then can NATO make a realistic determination of its critical needs in space, and plan to meet those needs.

Given those possible scenarios and the trend toward further commercialization in space, planning needs to be done well in advance of operations, to identify and integrate space requirements into the strategic and operational phases. Such planning will help identify uncertainties that can have an effect on capabilities-based planning. Does NATO need an integrated space picture that allows it to see the status of all Alliance space assets, both military and commercial? Should NATO be working with allies and partners to better coordinate and integrate space assets for future contingencies? Does the Alliance require a dedicated space surveillance network to enhance deterrence and security?

It is important to keep in mind that most satellite ground stations belong to commercial enterprises that tend to calculate risk in economic/criminal, versus military/adversarial, terms. An adversary determined to deny access to space may well target commercial ground stations along with the satellites themselves. Nations will need to evaluate the importance of these assets and nodes, and consider whether certain space (and cyber) facilities are so valuable that they merit special protection under a national defence program. Doing so would likely require nations to develop

public-private partnerships that share information, intelligence, and access to combined military and law enforcement capabilities.

During the Cold War, space imagery allowed the United States and the Soviet Union to verify compliance with nuclear arms treaties, a capability that made the treaties themselves possible in an age of "trust but verify."[103] Today the ability to see what is happening on the ground half a world away is vital not only to military situational awareness and treaty compliance, but also to civilian-led disaster mitigation and crisis management.

Similarly, accurate, timely space situational awareness is a critical tool for determining priorities and promoting responsible behaviour in space. One of the larger questions NATO needs to address is what SSA information it needs, how and where will the data be distributed, and who will receive it. This could be done through the creation of a space-situational information sharing centre, or possibly through a series of formal Memoranda of Understanding with space-faring nations, which would provide such information.

Several nations are moving to develop their own operational space capabilities. The French government, which has taken the lead in fostering improved space awareness across the EU, established a joint space command in 2010, and recently signed an agreement to share data with the United States on space debris.[104] Germany, the Netherlands, and Spain are considering improvements that would establish a series of situational, operational, and satellite monitoring centres. For its part, the commercial sector is working hard to monitor and track commercial satellites in space, through the Space Data Association, which performs conjunction screening of over 300 satellites.[105]

Lack of a comprehensive space policy that addresses these and other issues is a growing vulnerability for the Alliance. Without a well-conceived and articulated policy, planning, preparation, and training suffer from uncertainty. Commanders of ISAF, the NATO mission in Afghanistan, routinely have urged NATO to draft and promulgate a policy that addresses the need for integration and coordination of national assets in space, including appropriate training and education. Moreover, personnel from those NATO nations that do not have any operational space capability frequently lack the specialized training and knowledge they need to properly utilize assets in space when participating in deployed joint operations.[106] When polled, experts from across the Alliance cited the need for a clear, coherent policy as their most pressing concern with regard to NATO's future in the space domain.

The value of all four domains of the Commons is linked intrinsically to accessibility and use. Unlike the maritime or air domains, however, access to space is only partially about the freedom to launch an object into orbit. The more important aspect is access to the "product" of space, which is primarily in the form of digitized information. Without the cyber domain, the space domain loses some of its value. Thus, one critical facet of a viable space policy is to understand this critical interface between space and cyberspace, and plan for the simultaneous defence of both.

This will require that nations with established space programs take a leadership position and recognize it is in their long-term interests to increase cooperation and promote best practices that maximize safety and ensure access and responsible use. "Verification, compliance, and enforcement will carry the greatest political and policy risks but also the largest upside potential in keeping space

safe and secure" as a critical domain of the Global Commons.[107] Normally, policy should be written within known rules and regulations. Because this is at times difficult in the case of space, NATO may find it easier to first develop a policy framework among member nations that codifies agreed activities, behaviours, and methods. The new ESA Space Code of Conduct, which has been accepted by several NATO members, may serve as a good template for such an agreement.[108]

To assure its own access to space, the Alliance should consider developing a cadre of space experts who can guide the process of evaluating NATO's capability needs in space, advise senior leaders on policy and strategy, and most importantly, support commanders in the field. Another step for NATO to consider as it evaluates its requirements in the space domain is the establishment of a dedicated space office. Participants at the Kalkar workshop on space agreed that NATO does not need to create another centre of excellence devoted to space, as long as issues and concerns, especially those related to training and education, were addressed appropriately through existing structures.

In a competitive environment, private companies and governmental organizations can find it difficult to advocate for a "community of interest" that fosters sharing and best practices for the benefit of all members. The most practical way to address stability and assured access in this increasingly complex and competitive domain is through an approach to governance that allows stakeholders from across the military, civil, and commercial sectors to meet regularly, address concerns, and agree on constructive change.

Cyberspace

"It is not down in any map; true places never are."
Herman Melville

Cyberspace is a unique domain in that it does not itself occupy a discrete physical space in the same way that the maritime, air, and space domains do. The term cyberspace itself was only coined in 1982, yet access to this newest domain has come to characterize modern life.[109] There still is no standard, universally accepted definition for cyberspace. The narrow meaning of the term is the electromagnetic spectrum by which digital data are transmitted. In general usage, however, the domain also encompasses the digitized information itself, as well as the infrastructure of cables and towers, satellite telecommunications on the terrestrial side, server networks, computers, and especially the internet, that make the spectrum useful. More than the other domains, we tend to define cyberspace by how we use it, which for most people means the internet and the World Wide Web.

The internet is essentially an international network of servers that send "packets" of digitized information, such as email, from one address to one another. It was originally created by the Pentagon's Advanced Research Projects Agency (ARPA) in the 1960s for military use. ARPA later partnered with research organizations like RAND and several large universities to make it easier for institutions and facilities to share information across linked networks. Based on the belief that an open architecture would encourage creative networking, the internet was designed specifically so that anyone could add functionality, without having to adhere to a specified design structure. Users could create networks to suit their own needs, and then integrate them into the larger "network of networks." Another specific principle of the original design was that there would be no global control at the operational level. The prototype ARPANET was first demonstrated in 1972. The first email application was added later that same year. In 1980, the U.S. military officially separated its network, MILNET, from the ARPANET; other militaries around the world followed suit, and the internet as we now know it was born.[110]

The World Wide Web was invented by a British software engineer as a means to collect information in hypertext documents, and then link these documents in a digital "web." This web of information was made accessible over the internet through the parallel invention of the hypertext browser. The World Wide Web was launched in 1991, according to the same principles of open access as the internet, which has allowed it to undergo continual refinement and expansion since its creation.[111] The critical nodes, or "gateways" to cyberspace, however, are almost entirely in the hands of commercial enterprises. Internet service providers (ISPs) connect computers to the internet, while web hosting services maintain websites on the World Wide Web. Browsers such as Internet Explorer, Safari, Chrome, and Firefox make the content accessible.

There are parallel, sequestered regions of the internet, such as military networks and virtual private networks (known as VPNs) that are not part of the Commons, but even these remain linked at critical nodes, in the same way that nations' territorial waters are linked to the international

shipping lanes of the maritime domain. While cyberspace, unlike the other domains, can in principle be physically shut down or dismantled, in reality, especially in the democratic nations that comprise the Alliance, it is far too entrenched for this to happen short of some much larger global calamity. Nor can it be used up like the others; to the contrary, the more people add to it, the larger and generally more useful it becomes. Nevertheless, the data that give cyberspace its value can be compromised, and the best means to assure access and protect use are by no means clear.

From 2003 to 2009, use of the internet expanded globally at an average annual rate of 290%. Currently about 1.8 billion people, an estimated quarter of the world's population, have access to a network. While internet penetration in developed countries reached nearly two-thirds of all citizens by the end of 2009, in developing countries it reached only 18 per cent (and only 14 per cent if China, which has established restrictive internet access policies, is excluded).[112] As the developed world becomes increasingly networked, the importance of access to the cyber domain for developing nations will only continue to grow.

The vast amount of digitized information that travels across the electromagnetic spectrum is the "payload" of cyberspace, and is available to anyone with the technological means, such as a computer or a smart phone, to gain access. The infrastructure of cyberspace, however, depends on physical nodes such as servers and terminals, and the wires and cables that connect them, which are located in nations that exert control and, in some cases, ownership. For example, a discrete transmission may start via cell tower (USA terrestrial), be converted to a trans-Atlantic fibre-optic signal (maritime), then be relayed via microwave tower (European terrestrial) to a French satellite in space, ending moments later as a SATCOM signal to a Chinese cargo ship at sea. Transmissions like this occur millions of times each day, illustrating not only the ubiquitous nature of cyberspace, but also the complexity of the global telecommunications system we rely on to make it accessible.

Cyberspace has become a centre of gravity for the globalized world. For the military, the value of cyberspace depends to a large degree on simultaneous access to space. From a civil perspective, the information that networks convey almost instantaneously across the globe is the lifeblood of the global supply chain. Without both of these domains, trade as we know it would slow considerably, global financial markets would struggle to function, and modern militaries would be forced to revert to the command, control, logistical, communications, and precision strike methods of three generations ago. In the 21st century, missions and the network have become intrinsically linked; as things stand, without the network the mission will fail.

From a military perspective, one of the complexities of cyberspace is that it does not depend primarily on state power for security; over 90% of networks are private and competitive in nature. Most Web content is privately owned, and subject to national and international copyright laws similar to those that cover other creative works including journalism, music, screen plays, and printed matter like books and newspapers. The right to post content and view or download it is typically governed according to local laws.[113] Commercial enterprises, including ISPs and web hosts, treat content as a commodity, while users often regard access to content as a right. Most of the cyber domain is accessible to anyone with even the most minimum skills and equipment to use it, a traditional aspect of the internet that is cherished and staunchly defended by its "netizens." In this environment, both providers and users have resisted the imposition of government regulation, as many prefer market solutions to security that weigh risk against cost.

These aspects of internet culture can lead to "cyber skirmishes" among groups of internet users, who use tactics such as distributed denial-of-service attacks to disrupt access to certain websites.[114] Retaliatory escalations can continue across the Web for weeks. A major incident flared when several companies that do business on the Web stopped servicing the website Wikileaks, after it made a large cache of classified documents public in December 2010.[115] Freedom-of-access activists quickly launched protest attacks against these businesses, in particular Visa, MasterCard, PayPal, and Amazon. Opponents of Wikileaks also launched distributed denial-of-service attacks against any service provider that hosted the Wikileaks website. Meanwhile, hundreds of other sites stepped in and picked up Wikileaks' content, so that within a week the material had "gone viral" across the Web.[116]

This event highlights two important points that have implications for the wider discussion of assured access to cyberspace. First, it is an example of the internet culture of instant "justice," where users feel free to organize offensive measures against content or practices they find objectionable. While denial-of-service attacks cause only temporary problems and do no permanent damage to a website, they are a costly nuisance and are becoming more common.

Second, these attacks involved the creation of voluntary "botnets," large networks of PCs whose users willingly turned partial control of their computers over to anonymous hackers, who organized the attacks.[117] Without the proper security in place, such an *ad hoc* network makes these linked computers vulnerable to clandestine penetration. Botnets, hard to detect and nearly impossible to attribute, are a common tool for both espionage and criminal activity across the internet.

As this example shows, humans are one of the weak links in any network security system. At the development end, hundreds of thousands of programmers, some with little formal training in software security, are busily creating the software for games and applications, and they make mistakes. As one cyber security expert emphasized, poorly planned or written code incorporates vulnerabilities – what programmers call "bugs" – which the developer later "patches" only after some hacker has discovered and exploited it.[118] In some cases, these vulnerabilities may be intentionally created. At the user end, most people log onto the internet as easily as they once picked up a newspaper, yet relatively few know very much about computers or have any training in cyber security. Assurance in such an environment is difficult, because in general, the greater the ease of access for the legitimate user, the easier it is for criminals or spies to steal information. Removable drives, for instance, are highly convenient, but they have been implicated in a number of viral infections in cyberspace, including the W32.Stuxnet worm and an attack on military networks in 2008.

Some authoritarian regimes restrict access to the internet, and use limits on information as a means to control their internal message and shape national identity. The leaders of such regimes are increasingly likely to view open access to the internet as an existential threat. "Google, Twitter, YouTube and Facebook," an observer noted, "have changed society by giving people the means to control the fidelity and frequency of the information they transmit and receive."[119] The so-called "Green Revolution" that shook Iran after disputed elections in 2009, and especially the violent crackdown that followed, was broadcast to the world by cell phones, using the social networking sites Twitter and YouTube. It is sometimes even called the Twitter Revolution, although more for the novelty of the communications than for any change the protests accomplished.[120] In January 2011, anger at worsening economic conditions quickly spread through Tunisia's social media.

Within days, protestors, mobilizing in part through Facebook, took to the streets and ended the autocratic Tunisian president's 23-year hold on power.[121] When similar cyber-enabled protests ignited in Cairo only days later, Egypt's government reacted by shutting down the internet almost entirely for a week. Only pro-government messages were allowed. Subtracting an entire country from cyberspace was unprecedented, and possible only because Egypt's relatively rudimentary cyber infrastructure is state controlled.[122] The Organization for Economic Cooperation and Development estimated the cost of the shutdown for Egyptian commerce, which is as dependent on the global supply chain as any other country, at about $18 million per day, or 3-4% of economic output.[123]

Digital media and social networking, like the telegraph and telephone in their time, are emerging as a new factor in world politics, for better or for worse. As one expert put it, "This does not mean the nation-state has been consigned to irrelevance. But within the cyber domain, [the nation-state] is now only one actor on a rather crowded stage, and not necessarily the most significant."[124]

NATO Activities in the Cyber Domain

Like most modern organizations, NATO is highly networked at every level, from governance to command and control, from document handling to military operations. As such, it is a major target of hackers, but it is also becoming an important global resource for new research and thinking on cyber defence. The new Strategic Concept characterizes the cyber domain as a stabilizing medium that can help NATO members communicate, share information, and work together. Seeing assured access to the cyber domain in the context of the Global Commons can help the Alliance understand the size and complexity of the problems the domain faces. By no means, however, do we think this problem is NATO's alone to solve. Quite the contrary: assured access to and use of the cyber commons is a global concern, and while we believe the Alliance can play a role in promoting security and best practices, it is not and never will be the sole contributor.

Disruption or loss of access to cyberspace would have an immediate effect on NATO's ability to carry out its missions. Disruption could be as simple as manipulating information in a way that might embarrass leaders, possibly with the intent to spark divisions within the Alliance. In one recent example, Wikileaks published classified documents that detailed NATO contingency planning to defend the Baltic States against hypothetical Russian aggression.[125] This revelation, while probably no real surprise to Moscow, proved embarrassing to NATO leaders in light of progress made in Russia-NATO relations at the 2010 Lisbon Summit. At the operational end, malicious hacking could deny access to vital situational data; alter data to make it useless or even dangerous to those depending on it; or divert sensitive information to adversaries. NATO's Cyber Defence Concept warns that, "due to the globalization within the communications field, there is now no guarantee that NATO information is routed only through 'friendly' networks."[126]

NATO has taken several important steps toward defining, understanding, and addressing the Alliance's vulnerabilities in cyber space, including the development of the Cyber Defence Concept to describe the problems and provide guidance on the way forward. The Concept will propose an approach called "layered defence" or "defence-in-depth," which applies an array of different defences between the attacker and the target, both to slow or stop the attack and to increase the ease of detection. One important aspect of this is a defence methodology called Detect, Respond, Recover, and Feedback, a constantly evolving process that, when followed properly, improves

information assurance. Each level in this system incorporates data, checks for validity, generates continuous feedback, and promotes near instantaneous learning that can be fed back into the system.[127] In the coming decades, new generations of computers will be far better at pattern recognition, which they can use to seek out and isolate malevolent code, and thus help assure the security of data without human intervention.[128] New kinds of analysis software are making it possible to detect unauthorized intruders, similar in concept to the submarine sensor networks of the Cold War.[129] Until that time, constant training, modification of protocols and procedures, troubleshooting systems, and human learning will continue to be critical aspects of any cyber defence. NATO is also looking for the best means and channels to share appropriate kinds of information in order to strengthen cyber security at several levels: among cyber specialists, with members of the Alliance, and with partners in the private, organizational, academic, and governmental sectors.[130]

The Cooperative Cyber Defence Centre of Excellence (CCD COE) was established in Tallinn, Estonia to provide technical expertise; improve cyber defence training, including a simulation capability; and improve data analysis, in part through the use of artificial intelligence. The experts at CCD COE are also helping NATO "develop a plan for defending against cyber-attacks, or cyber war based on Estonia's experience with the 2007 cyber-attacks directed against their government and financial industry."[131] Participants in a workshop on NATO's role in the cyber domain, held at the CCD COE, pondered the question of what would happen to a globalized society in the event that it lost most or all access to cyberspace.[132] Some suggested that the consequences of a major cyber-attack could be resisted by the developed economies for up to three days without crippling damage if, within this period, authorities were able to take appropriate measures to respond to the attack. After three days, however, the consequences would become increasingly serious. Thus, while the damage from a cyber-attack that disrupted operations at a major port like Rotterdam or an international airport like Heathrow would be less immediate than, say, a missile strike, an unmitigated attack that shut down the information infrastructure of a highly networked nation would, over the long term, have much larger consequences.[133] This finding raises the question of how ready NATO forces are to operate in a degraded environment, without access to the data flow and command and control that cyber networks provide.

The more cyber defence policy and planning can be normalized at the international level, the easier it will be for nations to absorb and share rules and best practices, and thus isolate those who choose to operate outside the international norm. States are cooperating at the bilateral and multilateral levels to work out protocols for dealing with cyber security. For example, Australia's military intelligence gathering agency, the Defence Signals Directorate, which leads that country's development of cyber warfare techniques and defences, is working closely with its counterparts in the United States and Great Britain to enhance mutual security. Law enforcement agencies are also continuing to make significant progress in developing responses to cyber-crime. In the United States, the FBI (through Operation Bot Roast) and the courts, in cooperation with information technology firms, have had some success dismantling criminal botnets and prosecuting those involved. The United Kingdom has undertaken similar arrests. While these kinds of judicial actions will not end cyber-crime, they do serve to raise the stakes for would-be criminals, who can no longer be certain of impunity.

Changing Conditions and Emerging Concerns

At least two things are clear about cyberspace: first, the global economy and modern militaries are deeply dependent on assured access to cyberspace; and second, access is increasingly threatened by hackers (state and non-state) and malicious software ("malware"). NATO for its part is constantly fending off attacks against its systems at all levels, ranging from the annoying defacement of websites to extremely sophisticated data mining. Many experts believe a number of these attacks are state-sponsored. Besides stealing secrets and causing damage to networks, a cyber-attack may generate a lack of trust in the systems that support globalization, such as banking, the stock markets, medical research and collaboration, and academic exchange, to name just a few. The danger that virtual attacks might escalate into deadly hostilities is real, especially if an attack against a power grid or an air traffic management system, for example, cascades out of control and causes severe economic damage or loss of life.

The distributed denial-of-service attack on Estonia in 2007 is generally regarded as the first full-scale cyber-attack against a state, although it did no long-term damage and was arguably not state-sponsored.[134] Ghostnet, an espionage botnet that forensics determined had originated from Chinese territory, infected computers in the government offices of 103 countries around the globe during 2008. Despite very strong circumstantial evidence, however, that attack also cannot be officially attributed.[135] Beijing makes no secret of its intention to win "informationised wars by the mid-21st century," and is assumed to be developing offensive cyber capabilities, but it is not unique in this regard.[136] Technical attribution, as mentioned already, is one of the most difficult aspects of cyber-attacks. Forensic work can take months, while the very act of "hacking back" through code in an attempt to find its source can be a violation of trust, treaties, and even the Law of Armed Conflict.137

On a very different level, the computer worm called W32.Stuxnet did actual physical damage to Iran's nearly completed Natanz nuclear complex in 2010, by causing the centrifuges used for uranium enrichment to run erratically and, over time, self-destruct. Most of the uranium that came from the centrifuges proved useless as well. Stuxnet also was able to completely hide any traces of its activity from the systems used by technicians to monitor the centrifuges. The instruments showed everything to be working normally, even as the machines were destroying themselves.

Unlike previous cyber-attacks, Stuxnet did not go after information, it went after physical infrastructure.[138] Despite Iran's initial claims that the attack was not serious, there is evidence that it succeeded in disrupting the plant's operations for at least a year before it was detected. The incident apparently also led to serious repercussions among Natanz's technicians, even possibly some executions.[139] Command and control of the worm was traced back to servers in Denmark and Indonesia, to which access has been blocked, but attribution of the attack remains speculative.

Scientists first learned of vulnerabilities in the Supervisory Control and Data Acquisition (SCADA) system, the same operating system that was targeted by Stuxnet, in 2008, when they were asked by the developer for help in detecting and correcting security problems in a similar system. Many critical infrastructure facilities throughout the world, such as dams and electrical grids, run on these same SCADA systems, and there is now concern that they may be vulnerable to attack, possibly from a manipulated or next-generation version of Stuxnet.

Even the most sensitive state and commercial facilities rely to some extent on proprietary commercial technologies like SCADA. There is already speculation that some components

available on the open market may contain spyware or logic bombs, which, when triggered, will render the system useless or worse, vulnerable to espionage or sabotage.[140] These and other vulnerabilities may not become apparent until the systems are under attack. When that happens, fixing the problem will require coordination between both supplier and user, which, in the case of a military end-user, raises its own questions regarding the limitations of trade restrictions, or laws that govern potentially dual-use technologies.

A cyber-attack may be defined as a malicious cyber activity, which can vary from unauthorized intrusion, espionage, or the corruption of data, to a large-scale offensive action (as yet undefined) that might trigger an Article 5 response. "Cyber war" is a loaded term that is heard more frequently, especially in the media, whenever a new incident comes to light. At present, however, there are few, if any, commonly shared definitions or agreements between nations describing what war in cyberspace means.[141] It has been applied to everything from the denial-of-service skirmishes described earlier to Stuxnet, yet the only thing these two types of attack have in common is that they occurred in cyberspace.

Some representatives at the 2011 Munich Security Conference, which took place in early February, called for states to agree on "rules of engagement for cyberspace." Their draft document took note of the fact that nation-states are not the main players in cyberspace, and that "perhaps the idea of 'peace' and 'war' is too simple in the internet age when the world could find itself in a third, 'other than war,' mode."[142] Similar to the space domain, some speculate that a real cyber war between states could also involve kinetic attacks on the physical nodes of the network infrastructure, such as cutting cables or bombing large server facilities. If a cyber-attack simultaneously disabled situational awareness and the communications ability of a responder, the effects could be far more damaging than either one alone. An early lesson from the Japanese tsunami in 2011 was that, as the electric grid went down, so did much of the cyber network, which was no longer available to help facilitate the movement and staging of emergency responders.

At the same time, we tend to fear the most what we understand the least. Cyber security itself has grown into a multi-billion dollar industry, with its own entrenched interests, lobbyists, and critics.[143] This "industrialization" further complicates the process of discerning those threats that require our full attention from those that are merely irritants. Even corporations and industries that are liable to suffer significantly in the event of a serious attack are wary of allowing governmental surveillance of their networks for security purposes. Because they depend on the trust of their customers, they tend to handle their own breaches of security with as little publicity as possible.[144] Effective cyber security, however, cannot be "stove-piped." As Gen. Abrial emphasized in a recent New York Times article, it will require collaborative information-sharing and problem-solving among commerce, academia, government, and the military.

> **Today, a critical element of any cyberdefense strategy is the understanding that cyberspace is international by nature. No one country can deal effectively with cyberthreats on its own.... The concept of "in-depth cyberdefense," which was endorsed at the Lisbon summit, is not intended to be a military-only, or even a military-centric, strategy. It necessarily cuts across the portfolios of a variety of actors, as it spans the technology employed, the awareness of users, and the physical protection of key elements of our hardware.[145]**

We have yet to see evidence of terrorist groups launching a major disruptive attack, perhaps because the effects of such attacks are regarded as too subtle and slow. To spread sudden fear and confusion, a printer, underwear, or shoe bomb will be much more effective than a logic bomb. Furthermore, terrorist groups are heavily dependent on the Web for recruiting, command and control, and fundraising. As in space, many adversaries, state and non-state, depend on access to cyberspace, and may be reluctant to launch attacks that could rebound on their own networks. For this same reason, however, the ubiquity and importance of the cyber domain is a major constraint on choosing the means for its defence. The "nuclear option" of shutting down the internet to keep it safe, in other words, is not actually an option.

The latest trend in data storage, "cloud" computing, represents another significant shift in the way people are thinking about security. Individual computers connected to a cloud will become much less tempting targets for hacking or espionage, because data will be stored on multiple virtual servers rather than on a single server or a local hard drive. NATO is working with IBM on a "private cloud" test project at headquarters SACT, which commenced in early 2011. The on-site cloud will be used to "test and develop network solutions for command, control, intelligence, surveillance and reconnaissance projects," and IT infrastructure interoperability, as a way of improving information collecting and sharing among the Alliance nations.[146] Some experts are concerned that use of the cloud is growing faster than measures to ensure its security, but most see it as a positive way to solve the problem of easy access versus strong security, because it removes much of the burden of security from the ordinary user.

At the universal level, the language of the internet is currently undergoing a major revision (from IPV [internet protocol version] 4 to IPV 6), which leaves behind many of the vulnerabilities of the original version. Besides fixing the known problems of the old version, this change means far fewer people, especially ordinary hackers, will know how to take advantage of it. The changeover represents a unique opportunity for stakeholders in the world of cyberspace to increase the security of their systems. [147]

Another obstacle to retaliation is that many effects in cyberspace are unintentional, as anyone who has accidentally forwarded an email knows. Early hackers who set the first experimental viruses loose often had no idea or intention that their creations would shut down entire portions of the internet. A hacker can be prosecuted for his activities, but should an accident be interpreted as an act of espionage, or even war? In other cases, anonymous programmers may be willing to infect thousands of non-targets as collateral damage to get to one specific target. Even the most tailored attacks can have unintended effects that may not be discovered for some time, or understood to be a result of the attack. Furthermore, if a victim is able to determine with reasonable certainty that an attack came from a particular source, the accused source can just as reasonably claim that its system was used for the attack without consent or knowledge. The original victim has no way of proving beyond a doubt whether the suspected source is lying or telling the truth. States may, for this very reason, even use the services of dummy corporations, criminals, or other non-state actors to carry out an attack that was in fact planned and designed by the state.

As with terrorists who carry out physical attacks, states that harbour sources of cyber-attacks could be identified as "sanctuary states," and thus be held responsible for aggressive cyber activity coming from their territory. The issue would then be to determine an appropriate response, both to compel that state to stop the activity, and/or punish it for the damage that was caused. This

approach could help spread responsibility for cyber security, like other forms of international security, among all states rather than only the defenders. This, however, will require states to agree that such collective action is in their interest.[148]

NATO's Future in the Cyber Domain

As the above discussion has shown, "cyber space is a realm where national interests – military, diplomatic, economic and social – co-mingle and by doing so share risk and vulnerabilities in sometimes chaotic and complex ways."[149] Most governments, large organizations, and corporations currently experience dozens, even hundreds, of cyber-attacks every day, primarily of the nuisance, lone-hacker type, but increasingly from criminals and spies out to steal or corrupt sensitive information, or cripple infrastructure. Given these trends and the explosion of cyber-enabled functions and devices, both commercial and military, we can only expect attacks to escalate in number and sophistication.

Effective cyber defence has three interdependent aspects: cooperation, policy, and preparedness. Progress in these areas must be simultaneous and continual, to keep up with the speed of change in the cyber domain. To be effective for the Alliance, NATO's efforts in all three areas must extend outside the Alliance, to include all responsible stakeholders. "Defence in depth," as described in NATO's Cyber Defence Concept, is an important aspect of this cooperation.[150] Such a policy will cross as many layers of the domain as possible, from international organizations like NATO, the EU, and the UN, to states and the commercial sector, down to the individual user.

Cooperation is improving in some areas, particularly in public-private sector initiatives like NATO's collaboration with IBM on cloud computing. Again at the international level, there are several efforts underway to develop mechanisms that will allow governments to coordinate their cyber security efforts. NATO and the EU, with a large overlapping membership, should be able to collaborate effectively on a comprehensive approach to cyber security. This would help eliminate duplication, improve capacity and sharing, and satisfy the needs of both organizations to enhance cyber security.

The development of a strong, rational, and mutually acceptable policy on cyber security must occur in tandem with other cooperative activities. There is some concern that, on cyber issues, national interests and priorities can sometimes prevent NATO from facing new security challenges as they arise, and delay important decisions on what needs to be solved, researched, secured, or procured. Until recently, with regard to cyber security, nations have tended to act bilaterally rather than push for an Alliance-wide policy.[151] Fortunately, with impetus from the new Strategic Concept and guidance from the upcoming Cyber Defence Concept, this is changing. The distributed denial-of-service attack against Estonia in 2007 led NATO nations to step in with technical assistance, and for the Alliance as a whole to reaffirm its commitment to Article 5 in the event of a cyber-attack. What this would mean in the event of an attack that caused physical damage or loss of life, however, given all the complexities of cyber warfare, will require clarification, perhaps on a continuing basis, starting at the policy level.

Nations need to consider what are the rule-sets and behaviours that will best serve the interest of all sectors. Defence and assurance of the cyber domain has been a top-down process with regard to setting policy, but bottom-up in developing standards and good practices. Even among allies,

different standards, policies, and cultures can lead to friction in cyberspace. The EU has developed a Policy on Computer Network Operations, which promotes an integrated approach to cyber issues, from information sharing to traditional cooperation and defence, while eschewing offensive capabilities.

As a political-military alliance of nations that are among the most highly integrated, cyber-enabled, and therefore vulnerable, countries in the world, NATO must take active steps to develop and inculcate cyber security throughout the Alliance. Planning, preparation, training, and education are the fruits of effective cooperation and good policy. In this discussion of vulnerabilities to cyberspace, it is important to ask what would be the consequences if adversaries were to succeed at destroying, or denying access to, a significant part of cyberspace. This should not be a rhetorical question for any sector, governmental, military, or commercial, that depends on reliable access to the cyber domain. Are NATO forces prepared to operate in a degraded environment, without access to the web of near-instantaneous reconnaissance and surveillance information they have come to expect? Something as simple as navigation in the absence of GPS can become a significant vulnerability. Nations obviously have managed their defence and security without cyberspace until only recently. Yet, having adapted to this new "net-centric" environment, are operational planners and field commanders thinking about, and training for, command and control in its absence?

The new Strategic Concept commits NATO to a strong defence posture in cyberspace, by calling for the coordination of defensive capabilities, education, and training across the Alliance, and "bringing all NATO bodies under centralized cyber protection."[152] It goes on to assure that NATO will be "at the front edge in assessing the security impact of emerging technologies." Recognizing the need to develop a defensive cyberspace policy, the Alliance has created several entities to address various aspects of policy and capability, including the CCD COE, which focuses on research and training in cyber warfare, and the Cyber Defence Management Authority, which coordinates cyber defence across the Alliance.[153] Due to the intertwined, highly complex international architecture of cyberspace, any incident such as a distributed denial-of-service attack will involve a number of internet service providers, probably in many countries, each of which will need to be included in an investigation. Therefore, it is important that NATO establish collaborative mechanisms within and outside the Alliance for these kinds of events in advance. The Alliance also needs to consider how to monitor adversary networks, as a means to improve attribution and defence.

One important question is whether the Alliance should concentrate on countering intrusive behaviour over capability, or should it consider both? If so, how can NATO help the international community to establish training and education that sets codes for conduct and standards for interoperability? To the extent possible without compromising Alliance security, NATO has made clear that it will share its experience and expertise with partners and international organizations to help them improve their cyber defences, with the understanding that such sharing will be reciprocated.[154] This is an important means to divide responsibility and resources to counter common security concerns in cyberspace:

> **NATO must accelerate efforts to respond to the danger of cyber-attacks by protecting its own communications and command systems, helping Allies to improve their ability to prevent and recover from attacks, and developing an array of cyber defence capabilities aimed at effective detection and deterrence.[155]**

In an organization as complex as NATO, which depends on the security of large amounts of information, the education and training of all users must be continuous, and updated regularly to reflect the changing security environment. In the wider world, security will depend on better education, but it also will require technical means that bypass the user, such as high-quality application software and effective virus scanning and cleaning software. As computers, cellular phones, and other devices become increasingly "smart" and capable, the requirement to set standards between developers and large end-users, such as NATO, will be vital to continued, unlimited, secure access and use of information.

The forthcoming NATO Cyber Defence Concept should clarify the basic principles and provide direction to NATO's civil and military bodies, to ensure a consolidated approach to cyber defence, and coordinated responses to cyber-attacks.[156] The process should have the following characteristics:

- It should be supported by a well-defined cyber defence and intelligence information exchange;
- it should be standardized to the maximum extent to meet any common requirements and be independent from any specific implementation; and,
- it should be derived from NATO's evolving cyber defence policy, which will define respective roles in managing the NATO network, especially in case of cyber-attacks.[157]

These, then, are the most basic questions that will need answering if we are to assure access to cyberspace:

- What is freedom of access in cyberspace? How can it be assured for those who use it responsibly, but defended against those who seek to limit or deny it?
- How do we prepare to function at all levels, in the event that we lose access to cyberspace?
- How much does cyberspace need to be regulated? Where is the proper balance between an open internet and a secure internet?
- How do nations develop (and share with NATO) network monitoring and intrusion detection capabilities that can be used to positively attribute attacks in cyberspace?
- How do we categorize levels of attack in cyberspace, and how do we determine the appropriate level of response? Who should retaliate, how, and with what authority?
- Among all the architects, providers, and users in every sector of cyberspace, who has the right or responsibility to defend themselves, and how?
- What are the norms, best practices, and regulations we want to support and promote across the cyber domain?

"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,* BookIII

Conclusion:

A Role for the Alliance in the Global Commons

The Global Commons of maritime, air, space, and cyberspace are key enablers of the globalized economy and prosperous world. Disruptions to the integrated global supply chain, whether through piracy, missile proliferation, treaty violations, natural disasters, or malicious digital code, ripple through the system and touch every shore. The members of NATO are among the most networked and globally integrated nations in the world, and are therefore highly susceptible to military, economic and social damage from loss of access to and use of the Commons. It is not enough, however, to protect an isolated sector of the Commons, or to divide the domains up and assign individual value to them. Their value lies in their accessibility, commonality, and ubiquity as a system of systems. Therefore, the efforts nations put into keeping the Commons accessible must be for the good of all responsible users, equally and without exception.

Most users of the Commons do so responsibly and lawfully, mindful that their continued individual prosperity depends on the health and prosperity of the global system. What this report shows, however, is that the laws and regulations of the domains need to be developed further and updated where appropriate. This should be a continuous process, as we learn to better manage the increasing levels of use, new means of exploitation, and heightened competition – all hallmarks of globalization. In the case of the cyber domain, regulation is *ad hoc*, in part because increased use of the internet adds to its value. Unfortunately, as its accessibility grows, so do the numbers of those ready to take advantage of inefficient regulatory mechanisms and ineffective security. Where there are no rules, as the truism goes, there are no rule-breakers. What is less clear is the best mechanism to establish and enforce rules, whether at the international, national, or subnational level, or among the users themselves.

There are also, of course, the deliberate rule-breakers, both state and non-state, who take advantage of assured access to the Commons for immediate short-term gain, without regard for long-term consequences. Modern piracy is one example of this problem. While the roots of piracy and its consequences in the Gulf of Aden and the Strait of Malacca are complex, they are not new. This is an area in which NATO can work with partners like the UN and the EU, to look for ways to alleviate the causes by addressing complex social and cultural issues. While this is not a report on piracy, one thing is clear: piracy left unattended will continue to cause disruptions to the maritime commons, and those disruptions come at a cost. Meanwhile, the navies of Alliance members, working with partners from around the world, are cooperating to create a credible deterrence through patrols, interdictions, and arrests, but given the alarming trends of the past three years, we must do better.

Even the most law-abiding users of the Commons can cause harm, if the rules and agreements they follow are inadequate. Therefore, a vital first step to assuring access to the Global Commons is to support interested stake-holders as they work together to find common ground on their future interests, roles, and responsibilities. The opening of the Arctic to increased exploration, for example, is an area where competition for resources, if left unaddressed, may lead to irresponsible behaviour. NATO, as an alliance of globalized nations, has a natural leadership role to play in

promoting dialogue and consultation where and as appropriate. Representatives of Brazil, Russia, India, and China (BRIC), who attended a recent project workshop on the Global Commons, indicated that thoughtful leadership, advocating best practices and formal agreements that assure access to the Commons for all legitimate users, would be welcome.158

Historically, dialogue and cooperative action have led to more formal Memorandums of Understanding and treaties, across a wide range of issues in the maritime, air, and space domains. This cannot, however, be only, or even mostly, a top-down process. While powerful nations such as the members of the G-20 have historically been the primary stake-holders in the Commons, that is no longer true as both developed and developing countries rush to join the globalized economy. Like the most promising current efforts to regulate the space domain, initiatives need to come from the community of users. In some parts of the world, for example, we are witnessing the beginning of a movement that makes access and use of the internet a human right.

By definition, state sovereignty does not extend to the Commons. Increasingly, however, states, state-level organizations like NATO, the UN, and the EU, NGOs, commercial entities, and academia are partnering to look for solutions to problems in the Commons. This is fuelling a growing recognition that in order to preserve the intrinsic value of the Commons, nations and groups might have to cede some freedom of action, the same way that individuals have to observe limits on their behaviour when using a shared resource. The creation of excessive space debris, for example, is threatening to diminish access to the space domain for all users. Responsible use promotes norms and best practices for long-term sustainability, as opposed to unilateral measures that bring only short-term gain.

Throughout history, adversaries have looked to gain strategic advantage by restricting or preventing the movement of others. A future adversary may attempt to deter and/or deny access to the Commons in a manner that harms the strategic interests of the Alliance. From a military perspective, there are several questions NATO and its partners and allies should consider in order to prepare for such an eventuality:

- Do we have the right doctrine and policy?
- Do we have contingency plans and do we exercise those plans?
- Do we conduct planning scenarios and table-top war games with our Joint Force Commanders based on access to the Commons?
- If yes, are defence planners evaluating the results and considering the capabilities required to conduct such operations in complex environments far from home?
- Do our maritime forces have the right Rules of Engagement and capabilities required to forcibly open a closed strait or canal?
- Are our regular and special forces properly networked and integrated?
- Do we know how to operate, lead, and empower a complex network – a diverse collection of organizations, personalities, and cultures – to accomplish assigned roles and missions?
- Are we prepared to operate without support from space or cyberspace, without GPS and without global communications? One of the conclusions of our report is that in today's complex environment, if our highly networked forces lose access to the network, the mission may be jeopardized.
- Are NATO forces prepared to operate in an environment where they are denied access to and use of the Global Commons?

These are not trivial questions. NATO relies on access to all four domains of the Commons to fulfil its essential core tasks of collective defence, crisis management, and cooperative security. Strong modern sea and air power in support of ground forces, linked through space and cyberspace, remain the primary means by which the Alliance maintains stability and a credible deterrence, projects power, and responds to crises both natural and man-made. The loss of access to any of these domains would seriously affect its ability to operate effectively in any of the others.

In the introduction to this report, we proposed that the report would analyse the domains separately and jointly. While we offered over a dozen examples that depict the interwoven and complex nature of the four domains, a systematic description of the ways in which they blend and interact proved beyond the scope of this work. We must leave this important aspect of the Global Commons to later studies. It is our hope that Multi-National Experiment 7 can take on this important work, and provide needed clarity as it proceeds over the coming eighteen months.

The *Assured Access to the Global Commons* project developed a number of observations and findings that can help guide discussion and planning as the Alliance moves forward with implementation of the new Strategic Concept. By viewing the Alliance as one important actor in the global web of relationships that make up the Commons, nations will better understand how NATO can fulfil its current roles and possibly take on new ones as the 21st century unfolds. 48

In conclusion, it is important to note that the ideas presented here are not universally accepted. Clearly nations will need time to study and consider the implications of assuring access to the Global Commons. We believe, however, that the ideas expressed have utility for NATO, because they highlight the shared interest that all responsible nations have in developing capabilities that ensure access to these domains, in ways consistent with international norms, practice, and law. Further, this understanding of shared interests can be promoted by NATO to encourage countries that are not formal partners of NATO to cooperate with the Alliance. Finally, and most importantly, they can be used to encourage nations to improve governance of these spaces, and to strengthen international norms of responsible behaviour.

"Wir leben alle unter dem gleichen Himmel, aber wir haben nicht alle den gleichen Horizont."
"All of us live under the same sky, but we don't all have the same horizon."

Konrad Adenauer
Chancellor of the Federal Republic of Germany (1949-1963)

Endnotes

Executive Summary

1 Frank Hoffman, "The Maritime Commons in the Neo-Mahanian Era," in *Contested Commons: The Future of American Power in a Multipolar World*, Center for a New American Security, January 2010: p. 51; http://www.cnas.org/files/documents/publications/CNAS%20Contested%20Commons_1.pdf

2 Ibid.

Introduction

3 Grant Hammond, "Transformation: An Assessment," in Derrick Neal, Henrik Friman, Ralph Doughty, and Linton Wells II, eds., *Crosscutting Issues in International Transformation* (Washington, D.C.: National Defense University Press, 2009), p. 10.

4 Susan J. Buck, *The Global Commons: An Introduction* (Washington, D.C.: Island Press), p. 6.

5 This report therefore is not concerned with wilderness or environmental issues, except as they affect security and access to the Commons for NATO and its members.

Maritime

6 Wendy Kaufman, "How the iPhone Figures in the U.S.-China Trade Gap," interview with Glenn Fleishman on "All Things Considered," *National Public Radio*, 18 January 2011; http://www.npr.org/templates/transcript/transcript. php?storyId=133029198

7 See Shipping Facts, Value of Volume of World Trade by Sea; http://www.marisec.org/shippingfacts/worldtrade/

8 Hoffman, "The Maritime Commons in the Neo-Mahanian Era."

9 Alliance Maritime Strategy, Annex 1, C-M(2011)0023, 18 March 2011: p. 1-2, para. 5.

10 Grotius's treatise, "On the Law of War and Peace," published in 1625 in response to the devastation of the Thirty Years' War was another important milestone in the evolution of principles in international law.

11 James Kraska, "Indistinct Legal Regimes," in Scott Jasper, ed., *Securing Freedom in the Global Commons* (Stanford: Stanford University Press, 2010), p. 51.

12 Flag states have ships, coastal states have shorelines; most coastal states are also flag states, and vice versa. Coastal states may also choose to become port states, by developing port facilities. Kraska, "Indistinct Legal Regimes," p. 51.

13 Ibid., p. 52.

14 Japan, of course, has been able to rely on its alliance with the United States as a proxy for an indigenous fleet; China's economi rise, however, preceded its current naval buildup.

15 Alliance Maritime Strategy: p. 1-4, para. 11.

16 Diego A. Ruiz, "The End of the Naval Era?" *NATO Review* (2010); http://www.nato.int/docu/review/2010/Maritime_ Security/EN/index.htm

17 Alliance Maritime Strategy: p. 1-3, paras. 9, 10.

18 The interdependencies and vulnerabilities of these domains are discussed at length in the space and cyberspace sections of this report, and therefore will not be repeated here.

19 NATO in the Maritime Commons, final report from the third ACT workshop, Norfolk, Virginia, 30 September 2010; http:// www.act.nato.int/globalcommons-reports

20 Alliance Maritime Strategy: p. 1-1, para. 1.

21 The EEZ was introduced in UNCLOS III, 1982, with a 200-nautical mile limit to protect the fishing rights of coastal states. United Nations Convention on the Law of the Sea, 30 April 1982, UN Doc. A/CONF.62/122 (1982), 10 December 1982, 1833 U.N.T.S. 3, 397, 21 I.L.M. 1261 (1982) (entered into force on 16 November 1994), United Nations, New York.

22 Customary international law is the other main source of international law besides treaties. It grows out of a customary practice that is accepted by the larger community as carrying a legal obligation. See Anthea Elizabeth Roberts, "Traditional and Modern Approaches to Customary International Law: A Reconciliation," *American Journal of International Law* 95 (2001): p. 757.

23 See Ninian Carter, Tonia Cowan, Mark MacKinnon, and Danielle Adams, "Where China's Navy Operates," an "infographic map" that provides an arresting overview of China's naval activities, *The Globe and Mail*, 14 January 2011; http://www. the globe and mail.com/news/world/asia-pacific/where-chinas-navy-operates/article1870900/

24 See "Strait of Hormuz," Robert S. Strauss Center, University of Texas, Austin, 2007; http://hormuz.robertstrausscenter.org.

25 Hoffman, "The Maritime Commons," p. 55.

26 Robert D. Kaplan, *Monsoon: The Indian Ocean and the Future of American Power* (New York: Random House, 2010), p. 15.

27 "New Russian weapons system hides missiles in shipping container," *Homeland Security Newswire*, 28 April 2010.

28 Jack Izzard, "Italian police find smuggled explosives," *BBC News Online*, 22 September 2010.

29 "Report on Container Transport Security Across Modes," Organization for Economic Cooperation and Development (OECD), Paris, May 2004: p. 1; http://www.oecd.org/dataoecd/29/8/31839546.pdf

30 Alliance Maritime Strategy: p. 1-2, para. 6.

31 Michael Schuman, "How to Defeat Pirates: Success in the Strait," *Time*, 22 April 2009; http://www.time.com/time/world/ article/0,8599,1893032,00.html

32 The littoral states of Malacca are Indonesia, Malaysia, and Singapore.

33 Global Commons: Asia Perspective, final report from the sixth ACT workshop, Singapore, 15 November 2010; http://www. act.nato.int/globalcommons-reports

34 These statistics come from the International Maritime Bureau: "Hostage-taking at sea rises to record levels, says IMB," ICC Commercial Crime Services, 17 January 2011: http://www.icc-ccs.org/news/429-hostage-taking-at-sea-rises-to-record- levels-says-imb

35 An American couple sailing into the Gulf tried to evade pirates by limiting use of their radio and satellite systems, but pirates were able to track the transmissions and interdict them. The couple and their two passengers were murdered. Jim Sciutto and Martha Raddatz, "Four Americans Captured by Pirates Killed," *ABC News,* 22 February 2011; http://abcnews.go.com/ International/somali-pirates-kill-american-hostages-yacht-hijacked/story? id=12971097

36 James Bone, "US flies 11 Somali 'pirates' to stand trial in Virginia," *Times of London,* 24 April 2010; http://www.timesonline. co.uk/tol/news/world/africa/article7106414.ece

37 Ibid.

38 John M. Glionna, "South Korean forces storm hijacked ship, free hostages," *Los Angeles Times,* 21 Jan 2011,; http://articles. latimes.com/2011/jan/21/world/la-fgw-south-korea-rescue-20110122

39 Security Council Resolution 1918(2010) [on acts of piracy and armed robbery against vessels in the waters off the coast of Somalia] 27 April 2010, S/RES/1918 (2010).

40 "Spain proposes international piracy tribunal," *Radio Netherlands,* 9 December 2010; http://www.rnw.nl/international-justice/ article/spain-proposes-international-anti-piracy-tribunal

41 See "Climate Change 2007: Synthesis Report," Intergovernmental Panel on Climate Change (IPCC), Geneva:; http://www. ipcc.ch/publications_and_data/ar4/syr/en/contents.html

42 These nations, so far, include Russia, the United States, Canada, Norway, and Denmark.

43 "Russia's Arctic Circle Claims Worry NATO," *UPI.com,* 2 October 2009: http://www.upi.com/Top_News/2009/10/02/ Russias-Arctic-Circle-claims-worry-NATO/UPI-55371254525955/

44 Ibid.

45 Alliance Maritime Strategy: p. 1-1, para. 2.

46 Ibid.: p. 1-1, para. 1.

47 Ibid.: p. 1-4, para. 11.

Air

48 Mort Rolleston, "Air Superiority," in *Securing Freedom in the Global Commons,* Scott Jasper, ed. (Stanford: Stanford University Press, 2010), p. 132.

49 Ibid.

50 Kraska, "Indistinct Legal Regimes," p. 57.

51 En route (i.e., military aircraft in flight) and transiting (i.e., temporarily at an airfield) military aircraft "commanded by a member of the armed forces and manned by a crew subject to regular armed forces discipline" have immunity from searches and seizure, whether in national or international airspace (This provision includes unmanned aerial vehicles and government spacecraft, such as the U.S. space shuttle). Nor are they required to identify themselves or file a flight plan if they do not intend to enter national airspace, although many do as a matter of policy when on routine flights. Ibid., p. 57. Rules for civil aircraft in international airspace are codified in Annex 2 (Rules of the Air) to the Convention on International Civil Aviation, Ninth Edition - July 1990 (14 November 1991).

52 Kraska, "Indistinct Legal Regimes," p. 58.

53 From "NATO's Air Policing Mission Challenges," read-ahead material for the JAPPC conference, Kalkar, Germany, 13-15 October 2010.

54 Ibid.

55 USGS/ICAO Eruption Source Parameters; http://esp.images.alaska.edu/background.php

56 Graeme Wearden, "Ash cloud costing airlines £130 million a day," *The Guardian*, 16 April 2010.

57 The International Civil Aviation Organization (ICAO) sets standards and recommended practices for the safe and orderly development of international civil aviation. 190 nations are members.

58 See the "Report on Evaluation of Functional Airspace Block (FABs) Initiatives and their Contribution to Performance Improvement of October 2008," EUROCONTROL Performance Review Commission, Brussels, Belgium, 31 October 2008; http://ec.europa.eu/transport/air/single_european_sky/functional_airspace_blocks_en.htm

59 Air superiority means an adversary cannot deny NATO forces access to airspace, but itself can be denied by NATO's forces.

60 Threats to space and cyberspace are detailed in the following sections on those domains, and so will not be repeated here.

61 The National Military Strategy of the United States of America, draft, 2010: p. 16.

62 Rolleston, "Air Superiority," pp. 136-7.

63 "New Russian Weapons System Hides Missiles in Shipping Container," *Homeland Security Newswire*, 28 April 2010.

64 For a snapshot of SAM proliferation during and after the Cold War, see "Surface to Air Missile Systems and Integrated Air Defence Systems," Air Power Australia, last updated 16 December 2010: http://www.ausairpower.net/sams-iads.html

65 Rolleston, "Air Superiority," p. 141.

Space

66 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies (known as the Outer Space Treaty), UN GA resolution 2222 (XXI); http://www.oosa.unvienna. org/oosa/SpaceLaw/outerspt.html

67 The Fédération Aéronautique Internationale has proposed an altitude of 100km, called the Karman Line, as a working boundary. UK Military Space Primer, June 2010: pp. 1-1, 1-2, para. 104.

68 Captain Brent D. Ziarnic, USAF, "To Command the Stars: The Rise of Foundational Space Power Theory," *High Frontier* 3, no. 4 (2007): pp. 63-66; nmsu.edu/~bziarnic/theory.pdf

69 "The Space Report 2010," Space Foundation, pp. 62, 77. 2009 is the last year for which official data is available. It can be assumed the numbers are higher in 2011.

70 Jana Robinson, "The Role of Transparency and Confidence-Building Measures in Advancing Space Security," Report 28, European Space Policy Institute (ESPI), September 2010: p. 5.

71 See the Outer Space Treaty.

72 Kraska, "Indistinct Legal Regimes," pp. 59-60.

73 For information on management of the space-based spectrum, see the Space Services Department section of the UN's International Telecommunications Union website: http://www.itu.int/ITU-R/go/space/en

74 Major Tom "Solo" Single, USAF, "What is NATO's Position on Space?" *JAPCC Journal* 7 (2008): p. 38.

75 Ibid.

76 See Dana Johnson, James Lewis, H. Baker Spring, Tommy Brazie, and David Graham, "A Day Without Space: National Security Implications," Marshall Institute, 12 February 2009; http://www.marshall.org/article.php?id=660

77 An example is SES, one of the world's largest commercial satellite companies, headquartered in Luxembourg and with locations on every habitable continent. The company has two subdivisions that are devoted to government services, and a third that is exclusively for U.S. government contracts. See http://www.ses.com/ses/siteSections/services/government/index.php

78 See the ESA homepage: http://www.esa.int/SPECIALS/About_ESA/SEMW16ARR1F_0.html

79 Research and Technological Development and Space, Title XIX, Treaty of Lisbon, entered into force on 1 December 2009: http://ec.europa.eu/enterprise/policies/space/files/policy/lisbon_treaty_space_en.pdf

80 "Dragon spacecraft completes low-Earth orbit flight," *The Engineer*, 9 December 2010; http://www.theengineer.co.uk/video/ dragon-spacecraft-completes-low-Earth-orbit-flight/1006482.article

81 The UN Office of Outer Space Activities acknowledged the need to revisit the Outer Space Treaty in a report released in June 2009: "This proposal for a UN Space Policy charts a course toward the UN regaining an important place in the global space context as the current arrangements are not fully satisfactory and a far more proactive approach is necessary.... Too much is at stake...for the United Nations to watch from the sidelines...." "Towards a UN Space Policy," A/AC. 105/2009/CRP.12, UN Committee on the Peaceful Uses of Outer Space, 52nd session, 3-12 June 2009: p. 4; www.unoosa.org/pdf/limited/l/ AC105_2009_CRP12E.pdf

82 See "Resolution on the European Space Policy: ESA Director General's Proposal for the European Space Policy," ESA Communications, The Netherlands, 2007.

83 Ibid., p. 3.

84 National Security Strategy of the United States, January 2011: p. 3.

85 Bobbie Johnson, "NASA alert as Russian and US satellites crash in space," *The Guardian*, 12 February 2009; http://www. guardian.co.uk/world/2009/feb/12/nasa-alert-as-satellites-collide

86 Alex Sciuto, "Air Force Plans to Track 21,000 Pieces of Space Trash," *Talking Points Memo*, 25 January 2011; http:// tpmlivewire.talkingpointsmemo.com/2011/01/air-force-looking-to-track-20000-pieces-of-space-trash.php?ref=fpi

87 Certain desirable orbital paths are likely to lose their usefulness before others, rather than all going at once, e.g., geosynchronous orbits become useless while medium Earth orbits remain available, if more costly. Maj. Phil Verroco, USAF, Point Paper on Global Commons Air and Space Workshop, 5 October 2010, presented to the workshop on 15 October 2010.

88 "Satellite Wars: Endangered Birds: Space technology: Concern over anti-satellite weapons is changing the way satellites are designed, built and launched," *The Economist*, 9 December 2010; http://www.economist.com/node/17647639?story_ id=17647639

89 Robinson, "The Role of Transparency:" p. 35.

90 Ibid.: 37.

91 In late 2010, the U.S. Air Force offered contracts totalling $214m USD for designs to improve the so-called Space Fence – an array of S-band radars, originally operated by the U.S. Navy, that track space debris down to 10 centimetres in diameter over the United States. Sciuto, "Air Force Plans to Track 21,000 Pieces."

92 Fortunately, there is evidence that nonproliferation measures such as the Missile Technology Control Regime have been effective at slowing down long-range missile development in such countries as North Korea and Iran, which have been seeking them for some 25 years. Dennis M. Gormley, "Winning on Ballistic Missiles but Losing on Cruise: The Missile Proliferation Battle," *Arms Control Today* (December 2009); www.armscontrol.org/act/2009_12/Gormley

93 Robinson, "The Role of Transparency:" p. 36.

94 "Satellite Wars: Endangered Birds: Space technology: Concern over anti-satellite weapons is changing the way satellites are designed, built and launched," *The Economist*, 9 December 2010; http://www.economist.com/node/17647639?story_ id=17647639 "Satellite Wars: Endangered Birds."

95 Ibid.

96 Ibid.

97 China Update, 7 February 2011, *Chinascope* [translation of an article published in Quishi Journal on 10 December 2010] paragraph B-4; http://www.chinascope.org/main/content/view/3291/92

98 Robinson, "The Role of Transparency:" p. 38.

99 Peter B. de Selding, "ITU Implores Iran to Help Stop Jamming," *Space News*, 26 March 2010; Peter B. de Selding, "Thuraya Accuses Libya of Jamming Satellite Signals," *Space News*, 25 February 2011.

100 This was the sixth in a series of such games sponsored by the U.S. Air Force Space Command, at Nellis AFB in Nevada. Set in the year 2022, "the game stressed space and cyberspace planning and deterrence in the context of a future global conflict," according to a press release. "Schriever wargame concludes," Air Force Space Command website, 27 May 2010; http://www.afspc.af.mil/news/story.asp?id=123206668.

101 The stability of the Cold War nuclear standoff, for the most cogent example, depended on both sides' being assured of their enemy's destruction in the event of war, which is why anti-ballistic missile systems were considered destabilizing. Geoffrey Forden, Pavel Podvig, and Theodore A. Postol, "False Alarm, Nuclear Danger," *IEEE Spectrum* (Center for Arms Control, Energy, and Environmental Studies) 37, no. 3 (March 2000); http://www.armscontrol.ru/start/publications/spectrum-ews.htm

102 The commercial sector has begun to study this scenario as well. See, for instance, Edward Morris, Director, Office of Space Commercialization, U.S. Chamber of Commerce, "A Day Without Space," remarks to Public Discussion Forum, U.S. Chamber of Commerce, 16 October 2008; http://www.space.commerce.gov/library/speeches/2008-10-daywospace.shtml

103 The UK Military Space Primer, para. 205.b.(3): Other Regulations Relating to Space, Development, Concepts, and Doctrine Centre, UK Ministry of Defence, June 2010: p. 2-6.

104 "Accord franco-américain pour surveiller les débris spatiaux," *Le Monde,* 8 February 2011; http://www.lemonde.fr/imprimer/ article/2011/02/08/1477152.html

105 SDA was established to improve the safety and proficiency of space operations, providing a proximity assessment for more than 60% of all operational satellites in geosynchronous Earth orbit. "SDA Now Performs Conjunction Screening for More than 300 Satellites," *Space Daily*, 24 January 2011; www.spacedaily.com/reports/SDA_Now_Performs_Conjunction_Screening_For_More_Than_300_Satellites_999.html

106 Lt. Col. Tom Single, email correspondence re: RC Space Planner ISAF, 30 November 2010.

107 Robinson, "The Role of Transparency:" p. 61.

108 The draft ESA Code of Conduct for Outer Space Activities was distributed by the Council of the European Union on 11 October 2010. It can be downloaded at: http://www.spacepolicyonline.com/pages/images/stories/EU_revised_draft_code_of_conduct_Oct_2010.pdf

Cyber-space

109 Science fiction author William Gibson first used the term in a short story, "Burning Chrome." It entered widespread use upon publication of Gibson's novel *Neuromancer* (1984).

110 See Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, and Stephen Wolff, "A Brief History of the Internet," Internet Society; http://www.isoc.org/ internet/history/brief.shtml#Initial_Concepts

111 Unlike many subsequent cyber inventors, Timothy Berners-Lee, the Web's creator, did not copyright his work or become a billionaire. He is credited with the creation of HyperText Markup Language (html); HyperText Transfer Protocol (http); and the webpage identifiers called URLs. See a short biography on the MIT website: http://web.mit.edu/invent/iow/berners- lee.html

112 Usage data from "Measuring the Information Society 2010," report, International Telecommunications Union (ITU), Geneva; http://www.itu.int/ITU-D/ict/publications/idi/2010/Material/MIS_2010_Summary_E.pdf

113 Wikipedia, for instance, which is the fifth most popular website in the world, remains bound by the laws of the U.S. state of Florida, where it was founded, although its headquarters are now in

California. Jimmy Wales, founder of Wikipedia, in an interview on *The Daily Show with Jon Stewart*, broadcast 5 January 2011; http://www.thedailyshow.com/watch/wed- january-5-2011/

114 A distributed denial-of-service attack occurs when a large number of computers deliberately seek to log onto a target website all at once, with the goal of causing it to crash and thus become unavailable to legitimate users.

115 Wikileaks is a website that, in the name of democracy and free speech, publishes classified documents that have been leaked to it. The incident in question involved some 250 thousand confidential U.S. State Department emails and cables. "Wikileaks: NATO's Baltic Plan Against Russia," *Euronews,* 7 December 2010; http://www.euronews.net/2010/12/07/wikileaks-nato-s-baltic-plan-against-russia/

116 Ryan Singel, "Vigilantes Take Offensive in Wikileaks Censorship Battle," *Wired,* 9 December 2010; http://www.wired.co.uk/ news/archive/2010-12/09/vigilantes-take-on-wikileaks-deserters

117 An organizer even installed a simple JavaScript button on a website, so that would-be attackers did not have to download software to join the botnet. They could just click the button and their computer would join the attack. This also, however, made them easy for authorities to trace. Ryan Singel, "Joining Pro-Wikileaks Attacks as Easy is as Clicking a Button," *Wired,* 13 December 2010; http://www.wired.co.uk/news/archive/2010-12/09/vigilantes-take-on-wikileaks-deserters

118 Global Commons: Asia Pacific Perspective, Final Report from the sixth ACT workshop, Singapore, 15 November 2010; http://www.act.nato.int/globalcommons-reports

119 Dick Bedford, "The Changing Security Environment," in *Securing Freedom in the Global Commons* (Stanford: Stanford University Press, 2010), pp. 39-40.

120 Matthew Weaver, "Iran's 'Twitter revolution' was exaggerated, says editor," *The Guardian,* 9 June 2010; http://www.guardian. co.uk/world/2010/jun/09/iran-twitter-revolution-protests

121 "World responds to Tunisia uprising," *Aljazeera Africa,* 15 January 2011; http://english.aljazeera.net/news/ africa/2011/01/201111422472746065 8.html

122 Christopher Williams, "How Egypt Shut Down the Internet," *The Telegraph,* 28 January 2011; http://www.telegraph.co.uk/ news/worldnews/africaandindianocean/egypt/8288163/How-Egypt-shut-down-the-internet.html. On 11 February 2011, President Hosni Mubarak ended his 30-year authoritarian rule, following 18 days of increasing protest in the streets of Cairo and other cities.

123 Matthew J. Schwartz, "Egypt Takes $90 Million Hit from Internet Blackout," *Information Week,* 3 February 2011; http:// www.informationweek.com/news/security/management/showArticle.jhtml?articleID=229201128

124 Nigel Inkster, "Power in Cyberspace," speech to the International Institute for Strategic Studies (IISS) Middle East Global Perspective Series, Bahrain, 18 January 2011: p. 2; http://www.iiss.org/middle-east/global-perspectives-series/power-in- cyberspace/

125 "Wikileaks: NATO's Baltic Plan."

126 Draft NATO Cyber Defence Concept, Annex A to SH/J6/COI/07-203139 TI-3/TT-1162/Ser: NU, dated 4 October 2007.

127 Ibid.: pp. 9-11.

128 Humans are estimated to process information at 10^{16} computations per second. Ray Kurzweil, *The Singularity is Near* (New York: Penguin Group, 2005), p. 125.

129 "The Comprehensive National Cybersecurity Initiative," the White House, Washington, D.C. [no date]: pp. 2-3; http://www. whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative

130 Draft NATO Cyber Defence Concept: pp. 10-11.

131 Ibid: p. 2-2.

132 NATO in the Cyber Commons, Final Report from the fifth ACT workshop, Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, 19 October 2010; http://www.act.nato.int/globalcommons-reports

133 Ibid. As mentioned, Egypt has only a small infrastructure, and the January shutdown at least partially ended within 24 hours, so this incident does not provide a real case study.

134 When Estonia relocated a Soviet war memorial from its capital, Russian hackers all over the world quickly organized to shut down Estonia's government websites. There is no proof of official involvement by Moscow.

135 John Markoff, "Vast Spy System Loots Computers in 103 Countries," *New York Times,* 28 March 2009.

136 Jeffrey Hunker, "Cyber War and Cyber Power: Issues for NATO Doctrine," *Research Paper no. 62,* Research Division, NATO Defense College, Rome, November 2010.: p. 3.

137 Ibid., p. 6.

138 See Nicolas Falliere, Liam O Murchu, and Eric Chien, "W32.Stuxnet Dossier," v. 1.3, *Symantec Security Response,* Symantec Corp., November 2010; http://www.symantec.com/connect/blogs/w32stuxnet-dossier

139 Like all cyber-attacks, the intention of the attackers can only be inferred from the worm's behavior. Given the unprecedented design of Stuxnet, and the fact that Iran's enrichment facility is the only location that suffered actual damage, it is assumed by most that the plant was the true target.

140 A logic bomb is a set of malicious code embedded in software and programmed to activate when triggered, either by the user or the attacker.

141 Susan Watts, "Cyber ar Geneva Conventions call," *BBC News,* 3 February 2011; http://news.bbc.co.uk/go/pr/fr/-/2/hi/ programmes/9386445.stm. Hunker, "Cyber War and Cyber Power:" p. 1.

142 Watts, "Cyber War Geneva Conventions Call."

143 Seymour M. Hersh, "The Online Threat: Should We be Worried about a Cyber War?" *The New Yorker,* 1 November 2010.

144 Ibid.

145 General Stéphane Abrial, NATO Supreme Allied Commander Transformation, "NATO Builds its Cyberdefenses," *New York Times,* 27 February 2011.

146 Vance McCarthy, "NATO, IBM Explore Private Cloud for Command & Control," *Integration Developer News*, 7 January 2011.

147 Ibid.

148 Compelling a state to take action it does not deem in its best interest presents a set of problems that is beyond the scope of this report.

149 Hunker, "Cyber War and Cyber Power," p. 3.

150 Draft NATO Cyber Defence Concept: p. 9.

151 Ibid.

152 Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation," adopted in Lisbon on 20 November 2010: paragraph 19, subparagraph 8 and subparagraph 11.

153 Hunker, "Cyber War and Cyber Power," p. 9.

154 See "NATO's Cyber Defence Policy and Activities;" http://www.nato.int/cps/en/natolive/topics_49193.htm

155 "NATO 2020: Assured Security; Dynamic Engagement: Analysis and Recommendations of the Group of Experts on a New Strategic Concept for NATO," 17 May 2010; http://www.nato.int/cps/en/natolive/official_texts_63654.htm

156 See "Defending Against Cyber-attacks" on the NATO website: http://www.nato.int/cps/en/natolive/topics_49193.htm

157 Draft NATO Cyber Defence Concept: p. 5.

158 NATO in the Global Commons: Global Perspective, Washington, D.C., 3 February 2011. This was the seventh of the ACT workshops held to prepare for this report; http://www.act.nato.int/globalcommons-reports

Participants and Contributors

Arbor Networks
ASEAN Studies Centre
Astrium
Atlantic Council of the United States
Belgium Ministry of Defence
Boeing
Bundeswehr
Center for a New American Security
Center for Intelligence, Research and Analysis
Center for Naval Analyses
Center for Strategic & International Studies
Center for Technology and Society
Centre for International Law
Charles River Associates International
Chicago Council on Global Affairs
Combined Joint Operations from the Sea CoE
Cooperative Cyber Defence CoE
Council for Security Cooperation in the Asia Pacific
Council on Foreign Relations
Defence Research and Technology Office
Delegation of France to NATO
Delegation of Turkey to Europe
Deloitte
Delta Risk
Developement, Concepts and Doctrine Centre
Diplomatic Academy of Vietnam
Embassy of Australia in the USA
Embassy of Canada in the USA
Embassy of Finland in the USA
Embassy of France in the USA
Embassy of India in the USA
Embassy of Japan in the USA
Embassy of Portugal in the USA
Embassy of Sweden in the USA
Embassy of the Czech Republic in the USA
Embassy of the Netherlands in the USA
European Space Agency
European Space Policy Institute
European Union Satellite Centre
Finnish Ministry of Defence
Fudan University
German Ministry of Defence
Global Strategies & Transformation

Global Trade Systems
Hague Centre for Strategic Studies
Heritage Foundation
IBM - Netherlands B.V.
IBM - Singapore
Institut de Recherche Stratégique de l'Ecole Militaire
Joint Air Power Competence Centre
Maersk Line, Limited
Maritime Institute of Malaysia
Mission of Sweden to NATO
Mission of the Russian Federation to NATO
Mission of Ukraine to the EU
National Defense University, USA
National Maritime Institute
National Security Coordination Secretariat
National Security Council, USA
National Security Space Office
NATO Allied Command Transformation
NATO C3 Agency
NATO CC Air Ramstein
NATO Defence College
NATO HQ ESCD
NATO Watch
Navy Warfare Development Command
Netherlands Intelligence Studies Association
Peace Research Institute Oslo
People's Republic of China Mission to the EU
Project 2049 Institute
QinetiQ Group
RAND Corporation
Raytheon International Europe
Republic of Austria Mission to NATO
Royal United Services Institute
S. Rajaratnam School of International Studies
Saab AB
School of Advanced International Studies, JHU
School of Management Studies NIT Calicut
Secure World Foundation
Security and Defence Agenda
Security Art
Singapore Ministry of Defence
Space Innovation and Development Center
Stevens Institute of Technology
Stockholm International Peace Research Institute
Thales Group
Turck Strategic Communication

United States Mission to NATO
University of Brasilia
University of Pennsylvania
US Army War College
US Coast Guard
US Department of Defense
US Department of State
US Naval War College
US-CREST
USS Enterprise