October 2013

Occasional Paper

Global Commons: threat or opportunity?

Claudio Catalano (ed.)
Research Community

FINMECCANICA
Research Department

With ”Global Commons: threat or opportunity?” edited by Claudio Catalano and written by various authors of the Research Community of the Research Department, the Occasional Papers of Finmeccanica, edited by the Research Department of the Company, continue the publication.
The initiative is based on the consciousness of Finmeccanica that one of its institutional duties is to help in raising awareness of themes of general interest relating to the economy, technology and industry.
With the Occasional Papers, Finmeccanica aims to provide a practical contribution to current schools of thoughts and to spark debate between the various players in the public and private sectors, in order to contribute to the country’s growth, making it more “conscious”.

Since 2013, the Finmeccanica Research Department Occasional Paper series is edited by Dr. Catalano

Past issues:

“India 2030: security and defence challenges and policies of an emerging world power”, Amitav Acharya, November 2012

“The regularity of irregular war. Counterinsurgency and its implication", Filippo Andreatta, June 2012

“Ristrutturazione del settore aerospaziale e della difesa: tendenze e dinamiche evolutive”, Sara Gentili, May 2012 (available in Italian only)

“BARICENTRI: lo shift globale degli equilibri politici, economici e tecnologici?”, Claudio Catalano e la Comunità Ricercatori, October 2010 (available in Italian only)

“Sovereign investments in sensitive sectors: the case of defence industries”, Katinka Barysch and Clara Marina O’Donnel, March 2010

“Russia to 2020”, Philip Hanson, November 2009

“A new form of entrepreneurial capitalism based on innovation and research in Italy”, Riccardo Varaldo, Alberto di Minin, October 2009

“The need for the network. Internationalisation as a strategy to compete in the global economy”, Paolo Guerrieri, May 2008

“Changing seasons in defence industry and technology strategies: the United Kingdom, and beyond”, Keith Hayward, October 2007

“Impartiality is a pompous name for indifference,
which is an elegant name for ignorance”
(Gilbert K. Chesterton)

In the twentieth century, human conquest of the most extreme parts of the planet have been completed, and the exploration of Outer Space began.

One of the interesting things about these conquests is that, even though they were always accompanied by the flags of sovereign states on behalf of which the explorers where acting, this didn't imply the annexation of visited territories.

When, on the 18th January 1912 commander Scott and his men became second to reach the South Pole, they found the Norwegian flag planted by Amundsen just over a month before, but the Antarctic is still today a land which belongs to everyone and to no country, or better to everyone because it belongs to no country.

The bathyscaphe Trieste, with which the Swiss Jacques Piccard and Lt. Don Walsh from the US Navy touch the ocean bed in the Mariana Trench on 23 January 1960, was built in Italy and later bought by the United States Navy. However, the seabed does not belong to any nation.

And even though the American flag, which from 20 July 1969 stands in the windless sky of the Sea of Tranquillity, was planted on the Moon’s surface as a sign of the important victory in the cold war between enemy nations, it was accompanied by a sign that said: *“Here men from the planet Earth first set foot upon the Moon […] We came in peace for all mankind”.*

All this signifies that the need to better define, within increasing efficiency, the status of Global Commons, and the implications that this status brings with it, comes from the common belief that there are things that cannot be owned exclusively, but that must belong to everyone.

This is also the case for the unique virtual Global Common that is Cyberspace: even though it is something less tangible and therefore less attainable than the more natural Global Commons, it is widely recognised as belonging to everyone.

In fact, the profound nature of Global Commons has much to do with the most fundamental one of them all, i.e. freedom. But freedom to be authentic and be expressed requires space, whether physical or virtual. The protection of Global Commons and the ability to make use of them in the best possible way, and guarantee there accessibility to everyone, is therefore a concrete way as to protect and spread freedom.

Carlo Musso
Head, Research Department

index

GLOBAL COMMONS: THREAT OR OPPORTUNITY?

INTRODUCTION 7
Claudio Catalano

CHAPT. 1
MODES OF GOVERNANCE FOR THE GLOBAL COMMONS 13
Raffaele Marchetti

CHAPT. 2 “AGC”
THE EVOLUTION OF AGC: POWER AND TECHNOLOGY 19
Alessandro Marrone and Alessandro R. Ungaro

CHAPT. 3 “SGC”
GLOBAL WARMING, ICE MELTING AND POLAR SEA: THE ARCTIC SEA LANE, DREAM OR REALITY? 27
Angelantonio Rosato

CHAPT. 4 “SPACE”
UNION IS STRENGTH? EMERGING COUNTRIES’ ACCESS TO ORBITAL SPACE 34
Valerio Briani

CHAPT. 5 “CYBERSPACE”
SECURING CRITICAL INFRASTRUCTURES AGAINST DIRECT ATTACK AND ESPIONAGE 43
Stefano Costalli and Alessandro Fasani

CONCLUSION 52
Claudio Catalano

Authors 66
References 68

October 2013

The opinions expressed are those of the authors and do not necessarily reflect the positions of Finmeccanica SpA.

ACRONYMS

A2/AD	Anti-Access/Area Denial
AAR	Air to Air Refuelling
AGC	Air Global Common
AI	Artificial Intelligence
ALM	Additive Layer Manufacturing
ARPANET	Advanced Research Projects Agency Network
ASTRAEA	Autonomous Systems Technology Related Airborne Evaluation & Assessment
ATM	Air Traffic Management
BRIC	Brazil, Russia, India, China
CAS	Close Air Support
CASD	Centro Alti Studi per la Difesa (Centre for High Defence Studies, Defence Ministry)
CEMISS	Centro Militare Studi Strategici (Military Centre for Strategic Studies, Defence Ministry)
CERT	Computer Emergency Response Team
CIIP	Critical Information Infrastructure Protection
CNI	Critical National Infrastructure
COPUOS	Committee On the Peaceful Uses of Outer Space
DSG	Defence Strategic Guidance
EDA	European Defence Agency
ENISA	European Union Agency for Network and Information Security
FAA	Federal Aviation Administration
GPS	Global Positioning System
HMI	Human-Machine interfaces
IAI	Istituto Affari Internazionali (Italian International Affairs Institute)
IATA	International Air Transport Association
ICANN	Internet Corporation for Assigned Names and Number
ICAO	International Civil Aviation Organization
ICS	Industrial Control Systems
ICT	Information and Communications Technology
III	Insurance Information Institute
IMO	International Maritime Organization
ISTAR	Intelligence, Surveillance, Target Acquisition and Reconnaissance
ITU	International Telecommunication Union
IUCN	International Union for Conservation of Nature and Natural Resources
LDC	Least Developed Country
LNG	Liquefied Natural Gas

MANPADS	Man Portable Air Defence Systems
MARPOL	International Convention for the Prevention of Pollution from Ships
MIT	Massachusetts Institute of Technology
MPA	Maritime Patrol Aircraft
NASA	National Aeronautics and Space Administration
NEC	Network Enabled Capability
NSIDC	National Snow and Ice Data Center
NSR	Northern Sea Route
NWP	North West Passage
PNT	Positioning, Navigation and Timing
QDR	Quadrennial Defence Review
R&D	Research and Development
R&T	Research and Technology
ROK	Republic of Korea
RPAS	Remotely Piloted Aircraft System
RUSI	Royal United Service Institute
SAM	Surface to Air Missile
SATCOM	Satellite Communication
SCADA	Supervisory Control And Data Acquisition
SEAD	Suppression of Enemy Air Defence
SGC	Sea Global Common
SME	Small and Medium Enterprise
TCP/IP	Transmission Control Protocol / Internet Protocol suite
TEU	Twenty-foot Equivalent Unit
TSLV	Taiwan Small Launch Vehicle
UAS	Unmanned Aerial System
UAV	Unmanned Aerial Vehicle
UCAS	Unmanned Combat Aircraft System
UCSD	University of California at San Diego
UNCTAD	United Nations Conference on Trade and Development
UNEP	United Nations Environment Programme
UNESCO	United Nations Educational, Scientific and Cultural Organization
USB	Universal Serial Bus
VLM	Veículo Lançador de Microssatélites (Brazilian microsatellite launcher)
VLS	Vehiculos Lançadores de Satellites (Brazilian satellite launcher)
WDI	World Development Indicator
WWF	World Wildlife Fund

INTRODUCTION

Claudio Catalano

The Global Commons are domains such as Air, Sea, Space and Cyberspace. According to state-of-the-art doctrines these are "areas beyond national jurisdiction that constitute the vital connective tissue of the international system" (DSG, 2012 : 3).

Being the connective tissue of the international system implies that the Global Commons constitute both an opportunity and a threat: "Global security and prosperity are contingent on the free flow of goods shipped by air or sea, as well as information transmitted under the ocean or through space" (QDR 2010 : 8).

A study on the modes of governance of the Global Commons, focusing mainly on State control and international cooperation and agreements, is the main objective of Marchetti's Chapter.

Air includes the segregated and non-segregated airspace and all the aircraft which can fly into it. Though a discrimination shall be done between the national airspace and the AGC, see Marrone and Ungaro's Chapter for this issue.

The sea covers 139,768,200 square miles or more than 70 per cent of Earth's surface. However, not all the sea is a Global Common, the SGC includes only the areas outside State control, which are ever shrinking, such as the High Sea, which has been for a long time historically accepted as an area outside any State sovereignty - formerly known in the seventeenth century legal doctrine as *Mare Liberum* - the Arctic waters, the seabed, and all the seabed infrastructures, such as submarine communication cables and pipelines, and natural resources. Rosato's Chapter focus mainly on the Arctic and the Arctic sea lane (NSR and NWP), their status and their economic and security-related issues.

Space includes the area between the airspace and Outer Space, the Outer Space itself, and also all the Space infrastructures such as communication and imaging satellites, which can act as a support to the other Global Commons, in particular the AGC and SGC - by means of navigating systems, such as GPS - and cyber domain by means of satlinks and internet satellite connection. See the Briani's Chapter for these issues.

Cyberspace is an immaterial Global Common, which act as connective tissue for all the other domains, therefore cyber threats have influence on all the other domains. Cyberspace has

also its physical dimension which is constituted by hardware such as computer, servers and cables including submarine telecommunications cables. These belonging to the physical dimension can be physically attacked. Prof. Silvestri contends that while Cyber is a Global Common, its physical dimension however, that is the hardware is actually owned by private entities (Silvestri : 2013). See also Costalli and Fasani's Chapter for this issue.
As we can see Global Commons are closely interconnected, and the status of these domains is heavily influenced by technological developments and security and economic interests.

A brief history of the Global Commons

The Commons is usually what is publicly-owned as opposed to privately-owned within human society.

In traditional common law, common land or Commons did not mean State-owned or public land, but land that is owned by private individuals or corporations called partition units were areas of land owned collectively or by one person. The Commons could be shared and utilized by residents of the village, who have certain traditional rights on this, such as to allow their livestock to graze upon it, to collect firewood, or to cut turf for fuel. So in general customary law, Commons is public land managed by human communities, generally property that is collectively owned or better common areas or community resources such as public parks, waterway or easements.

Originally, Alfred Thayer Mahan was the first one to formulate the concept of Global Common applying it to the High Sea (Mahan, 1890):

> *"The first and most obvious light in which the sea presents itself from the political and social point of view is that of a great highway; or better, perhaps of a wide common, over which men may pass in all directions, but on which some well-worn paths show that controlling reasons have led them to choose certain lines of travel rather than others. These lines of travel are called trade routes; and the reasons which have determined them are to be sought in the history of the world".*

Mahan also formulate the idea of exclusion by means of State control:

> *"The profound influence of commerce… to secure to one's own people a disproportionate share of such benefits, every effort was made to exclude others, either by the peaceful legislative methods of monopoly or prohibitory regulations, or when these failed, by direct violence. The clash of interest, the angry feelings roused by conflicting attempts thus to appropriate the larger share, if not the whole, of the advantages of commerce, and of distant unsettled commercial regions, led to wars"*

General Giulio Douhet takes inspiration from the "High Sea" Global Common to identify the air as a new domain. The Global Commons is not the atmospheric air itself, but it is the aviation - both military and civilian - or better the aircraft which creates highways (Douhet, 1921 : 89-90):

> *"The airplane has no need of roads in the accepted meaning of the word; all Space is an unlimited road for planes. The sea also is an unlimited roadway for ships; … So can we hardly hope to develop an aerial navigation until we have prepared for air routes…A network of air lines is made up of large links connecting great arteries".*

Douhet see the air routes as responsibility of the State, and an emanation of State control, but leaving space for private initiative in a free Global Common:

> *"Provision for establishing air lines is to the interest of the State as a whole, and therefore is a duty of the State…. This does not, of course, mean that the State should be the entrepreneur of the undertaking, be the active manager of the air lines. On the countrary, the State should merely encourage, see to it that the air lines are created and efficiently run. In view of the doubtful results so far shown by State-controlled undertakings, the management of air lines should indubitably be entrusted to private enterprise. With the right kind of airfields and other ground works accomplished, with well-disposed civilian enterprises encouraged and amply subsidized, with each function of the military air forces differentiated and co-ordinated under competent authorities, with new enthusiasm for adventure and aspiration toward a future that cannot fail, aviation will finally be ready to rise to the freedom of the skies."*

During the Cold War, the NSC 68 (1950), the planning document stressed the idea of building an International system based on free trade, trips and the diffusion of western values so as to fight the expansion of communism by means of individual freedom, democracy and economic development. This was to assure the American lifestyle, and to free Europeans from the Communism thus facilitating trade, individual entrepreneurship and therefore free access to the Global Commons. The Global Commons, in particular the AGC and SGC, were to assure economic prosperity by means of commercial aviation and ship lines.

From Mahan, passing through Douhet, to the NSC, the AGC and SGC have been seen as highways, or better a network of commercial roads, thus introducing the concept of Global Commons opportunities, and to later conceive the Cyberspace as a networked Global Common.

Later on, from a "land of opportunity" of trade and exchanges, the Global Commons became first an environmental concern and then a security threat.

In 1968, the "Tragedy of the Commons" introduced in the sustainable development and economic growth theory, the Malthusian concept that human behavior could depleted the Earth's shared natural resources (Hardin, 1968).

In the 1980s, environmental law started to consider the exploitation of Global Commons. An Environmental Report (IUCN, 1980) published by the IUCN in collaboration with the UNESCO and supported by UNEP whilst WWF defines this as:

> *"A commons is a tract of land or water owned or used jointly by the members of a community. The Global Commons includes those parts of the Earth's surface beyond national jurisdictions - notably the open ocean and the living resources found there - or held in common - notably the atmosphere. The only landmass that may be regarded as part of the Global Commons is Antarctica ...".*

From the late 1990s to the 2000s, the A2/AD military concept, and Space and Cyberspace were included in the Global Commons.

This was due to the new Chinese asymmetric warfare doctrines, the 2006 incidents in the South China Sea, cyber-attacks like those in Estonia or Georgia, maritime piracy which also fuels instability in the Horn of Africa, anti-satellite missiles such as those being developed by China. The US QDR 2010 and the DSG published in January 2012 state that it is in the interest of the United States that Global Commons are "accessible", "free", and "stable" so as to maintain international security and the transfer of goods, capitals and people: For the International economic system is essential to assure:

- **access:** the means and system to accede to the Global Commons, in a sense the technological capabilities
- **freedom:** for the free flow of data, goods, capitals, and people
- **stability:** to assure the status of Global Common, to assure protection and security inside the Global Commons.

Therefore, the United States were the first to develop a military doctrine for the Global Commons:

> *"State and non-state actors pose potential threats to access in the Global Commons, whether through opposition to existing norms or other anti-access approaches. Both state and non-state actors possess the capability and intent to conduct cyber espionage and, potentially, cyber attacks on the United States, with possible severe effects on both our military operations and our homeland. Growth in the number of space-faring nations is also leading to an increasingly congested and contested Space environment, threatening safety and security. The United States will continue to lead global efforts with capable allies and partners to assure access to and use of the Global Commons, both by strengthening international norms of responsible behavior and by maintaining relevant and interoperable military capabilities."* (DSC 2012 : 3)

Global Commons as a technology issue

This study would deal with issues related to the assured access, by means of technological platforms, stability as a legal issue, and the security of the Global Commons, so as the means and systems to maintain the stability, to navigate and protect the goods, data, and people during their transit through the Global Commons.

The Global Commons have legal and economic implications, but first of all come the technological implications. The role of technology is actually twofold, because not only does it ensure access, but also the control of the Global Common, and in particular State control.

A well known example is the range of coastal artillery in defining the territorial waters in the international law of the sea. From the eighteenth century to the First World War, the territorial waters were initially set at 3 (nautical) miles which was at the time the range of coastal guns, or the length of a cannon shot, hence the portion of an ocean that a sovereign State could defend from shore. The territorial sea was then extended to 6 and later to 9 miles, ending up with the 1982 Montego Bay law of the sea Convention to 12 miles, according to the development of the range of guns. Military aircraft, in particular MPAs, and Anti-ship missiles allow the control of 200 miles range of exclusive economic zones. Same thing for the Air domain, whose State control area "usque ad sidera" is defined by anti-aircraft guns and nowadays by missiles. For Space, the technological development has created anti-satellite missiles, the use of which is purely hypothetical and anti-economic though.

State control of Global Commons also implies a cost for it, from the Victorian age right up until the First World War, the Royal Navy absorbed about 20 per cent of the British Empire's GDP. This is why after the First World War, the British Empire to balance the sheets after the war effort, delegated control of the Atlantic Ocean to the US Navy, a young and resourceful country. The same thing could happen now, with the economic crisis and the austerity, the new US strategic doctrine focus on Middle East and Asia-Pacific, thus leaving the Mediterranean and African stability to the Europeans, which are not young countries with sheets in balance. The emerging powers, with all their resources, could make the Asia-Pacific the next "nombril du monde"

The main issue about Global Commons is lack of State sovereignty, thus when States claim a right on these areas, they try to extend their sovereignty on no man's areas. These claims are possible only due to technological capabilities, which allow the interested State to gain control over the area, this being a portion of Air, Sea, Space or virtually of Cyberspace.

In a sense Global Commons will be the residual areas which do not fall under State control, in a mathematical formula (1-S) where "S" is State control. The more the State controlled area grows, the lesser the Global Commons total area are. This is evident in the law of the sea where State controlled waters shrink the High Sea that is defined as waters beyond State jurisdiction.

CHAPTER 1
MODES OF GOVERNANCE FOR THE GLOBAL COMMONS

Raffaele Marchetti

A major challenge for current socio-economic interaction at the global level is constituted by the fragility of the management system of the Global Commons (Nordhaus, 1982). The infrastructural nature of Global Commons is key to understand their value in a globalized world. While most definitions of Global Commons focus on their extra-territorial features, I would argue that their other characteristics in terms of interaction facilitators are of equal if not superior importance. In this vein, Global Commons are first and foremost resources for interchange, are infrastructure for interconnectedness in an ever more globalized world. Following on from this argument, in this article I will understand Global Commons as those domains that 1) serve as channel of transnational intercourse for individuals, goods, and ideas; and 2) are outside the jurisdiction of any specific national sovereignty, and are simply un-owned by any particular state.

In the past centuries, scholars of the law of nature would likely have understood the Global Commons *res nullius*, leaving them to the arbitrariness of the *conquistadores*. Today we have a different understanding that tends to see them rather as belonging to or common heritage of mankind, thereby including both present and future generations. The shift from res nullius to common heritage of mankind is dramatic. It entails overcoming the classic Westphalian system of national sovereignties in the name of a commonly owned domain. The concept itself of common heritage of mankind, despite being still controversial, is by now entrenched in international law. It was first mentioned in the preamble to the 1954 Hague Convention for the Protection of Cultural Property in the Event of Armed Conflict and later associated to specific obligations in the 1967 Outer Space Treaty.

Four domains are usually associated to the notion of the Global Commons: Air, Sea, Space, and more recently Cyberspace. Other domains have been proposed such as the tropical forest, but these remain speculative for the moment. In practice, the designation of these domains is tightly linked to technological developments and strategic interests. Historically speaking, for a long time sea was the only common taken into consideration. Later on with technological innovation and the subsequent possibility for exploitation for the sake of national interest came Antarctica, Air, Outer Space, and just very recently Cyberspace.

Global commons between overuse and free access

Two principal interpretations of the Global Commons are present in the public debate. In the environment-related discourse, the focus is on the conditions to avoid the overuse, the so called over-grazing by free-riding actors. In security studies, the focus is instead on the conditions to guarantee access to these domains for commercial or military reasons. In both interpretations, access to the common is expected to be ultimately unrestricted, and yet somehow paradoxically this may lead to accelerated consumption or degradation of the specific resource so much so that access may end up not being freely available anymore after a while: the classic "tragedy of the common" eloquently depicted by Hardin (Hardin, 1968).

In a world which is ever more integrated, access is a crucial condition for the sustainability of the high level of global interconnectedness. Today over 90 per cent of global trade travels by sea; 2.9 Bn passengers travel through air; enormous quantity of data is exchanged every second on internet and through satellite communications. Were any of these domains disrupted, exorbitant costs would be imposed globally.

Until recently, only localized disruptions took place. Piracy in the Horn of Africa, cyber-attacks to Estonia and Georgia are examples of these kinds of geographically limited troubles. Arguably, the recent scandal on vast scale net of control over data may potentially have a much larger negative impact on the cyber activity worldwide in terms of security closures in the system (as the one suggested by the German government) or the construction of altogether alternative cyber infrastructures (as the one planned by the BRICS governments). This would bring fragmentation to the system, hence it would reduce the free accessibility to it. As much as national borders and passport controls have reduced the possibility for free movement, the compartmentalization of the Cyberspace and the in-built security borders would reduce the free movement in it.

Free access to the Global Commons is crucial. These global infrastructures arguably remain a building block, a fundamental resource of the current global transformations and thus the need to be adequately governed in order to increase the efficiency of the global interactions. At the same time, we cannot stress enough that access to the Global Common has not only the value of free interconnectivity, but also the value of military dominance. In this latter case, access to the common also means control of the common, i.e. the power to let it free and to prevent intrusion of those who would threaten its accessibility. Geopolitical thinkers have long argued for the control of the sea as a key for the control of the world. Part of the American military supremacy of the second half of the twentieth century (but also of the British supremacy of the period between the nineteenth and the twentieth century) was precisely due to the unrivalled control of the commons. Controlling the sea, the airspace, and more recently the Outer Space and especially the Cyberspace proved to be a military enabler of the US global hegemonic power position (Posen, 2003; Denmark, 2010). The two-fold face of the value of the Global Commons needs to always be taken into account when assessing the significance of them. And in both cases, the issue of access is crucial.

A traditional way to solve the issue of access to the common resides is enclosure, which through state control or property right is expected to regulate to free passage in the most effective way. Enclosure constitutes a trend in international affairs and can be better observed in the domain of the sea with the ever growing ambitions of states to enlarge their sovereign rights. But this is no solution for a number of different reasons related to state competition and the subsequent unreliability of the system in terms of access to others.

Global governance mechanisms

A more promising strategy for safeguarding free access to the Global Commons instead consists in the further development of the governance structure already existing in each of the Global Commons. A set of binding treaties, governance mechanisms, and stakeholder initiatives are already in place. The current governance of the Global Commons is the result of a large number of regulatory mechanisms which are at times interlinked and at other time independent one from the other (Vogler, 2000; Koenig-Archibugi, 2006; Hale & Held, 2011; Dodds, 2012; Vogler, 2012; Stang, 2013). Behavior is regulated by a set of prohibitions, norms and rules whose effectiveness depends on a number of different factors. Ultimately what counts is the nature of the agreement. If the agreement is about coordination, i.e. it is a common-aversion mechanism with different points of equilibrium, then actors will have self-incentives to stick to the rules once these are set. On the contrary, if the agreement is about cooperation, i.e. it is a common interests mechanism with no point of equilibrium, then the risk of free riding, of unilateral defection is always present and the need for enforcing measure to attain compliance will consequently be much higher. To sum things up, coordination agreements on issues on which there is a common perception of mutual interdependence are more likely to be effective in regulating state behavior.

These regulatory mechanisms are imperfect. They are incomplete, they are contested, they are developed differently in each common, and yet at the moment they provide a relative good degree of coordination in the protection of the Global Commons. In all Global Commons, High Seas, Airspace, Outer Space, and Cyberspace, a relative high degree of coordination is present. If we simply compare how difficult the usage of any of these commons would be without any shared institutional framework, we can easily realize that we are far from any spontaneous order.

Legitimacy, co-management, and free access

Ultimately the issue of legitimacy remains central in the Global Commons dossier. Both in the classical intergovernmental arrangements and in the more recent hybrid stakeholder formula, what is essential in order to guarantee a viable management of the Global Commons is the input legitimacy. Setting a mechanism in place which excludes important actors from the management of the Global Commons is a recipe for failure. In a world in which power is more and more diffused, the challenge is to create avenues for the inclusion of all major actors involved in any common. Only by doing this, the management of the Global Commons will remain as effective and sustainable as possible. To make a long argument short, it is not enough to guarantee free access to the Global Commons. What is also essential is to guarantee free access to the management itself of the Global Commons. It is on this specific issue that the Global Commons are a terrain of political competition and rivalry. Membership, procedural rules to take decision, financial burden-sharing, and location of international institutions to manage the Global Commons are essential elements of legitimacy. Major issues of current contention on the legitimacy of global governance arrangement for the management of the Global Commons concerns precisely these elements of legitimacy.

Membership and procedural rules are discussed in order to widen the participants to the regulatory and standard setting bodies affecting the management of the Global Commons. For instance, emerging powers complain about the alleged partisanship of some institutions. Typical in this regard is the dispute over the management of the internet standards.

The United States and the EU defend the centrality of the ICANN, a private company based in California that has been running the business since its inception and has allegedly the most up-to-date expertise and flexibility to deal with internet governance. Conversely, other countries such as Russia and China maintain that the ITU, being a universalist intergovernmental organization part of the UN, is better equipped for managing a critical task such as that of internet governance. The dispute is still very much open.

Financial burden sharing is debated in relation to the distributions of costs attached to the control and implementation measures for the policy of free access. The United States (and to some extent the EU) complain for the massive resources they are currently investing in to keep the system going. Also typical of this are the disputes over the NATO budget between the United States and the other (mainly European) partners. In the past, the same case was advanced by the UK before World War I as for the costs of the Royal Navy on its national budget.

Finally, the location of Global Commons institutions is also at the center of political controversies. The current location of most international institutions is based in the West and ultimately derives from the hegemonic stability that the US-led West provided in the last 60 years at the international level. In a de-westernizing context such as the present, signs of increased discontent with the situations are growing. As recently as May this year, the Qatari Government officially submitted a bid to relocate the ICAO to the country in 2016, offering generous financial incentives. ICAO headquarters has been in Montreal since its inception in 1947, but a growing coalition of Arab countries is currently advocating for its relocation to the Middle East. Qatar rallied to put together those 115 votes that are necessary for moving the headquarters, but eventually dropped (at least for the moment) the bid.

These kinds of disputes prove once more that an enhanced perceived legitimacy is crucial in order to provide stability to the management of the Global Commons. In the past, as argued by Posen (Posen, 2003) and Danemark:

> *"The openness and stability of the Global Commons have been protected and sustained by U.S. military dominance and political leadership. The U.S. Navy and Coast Guard have dissuaded naval aggression and fought piracy around the world, ensuring unprecedented freedom of the seas. The United States led the creation of international agreements on air transportation, enabling the creation of a global air industry. Washington also*

> *forged an international consensus on the openness of space, ensuring that all countries with the means to do so can utilize orbital space for scientific, commercial, and military purposes. Lastly, research funded by the U.S. government led to the creation of a decentralized network of connections now called the Internet, which connects physically dispersed markets, capital, and people ….. For the past 65 years, U.S. power has been derived in part from providing global public goods that also service vital U.S. interests, including stability in key regions, a vibrant and interconnected global economy, and open access to the Global Commons."* (Denmark, 2010, 166)

Today, however, in a world that is more and more pluralistic and characterized by the diffusion of power, the issue of legitimacy reacquired centrality becoming as important as the technicalities for access control to the Global Commons (Murphy, 2010). As a consequence, the key characteristics of global governance institutions for the management of the Global Commons should be restructured in order to enhance their legitimacy. First order membership should be maximally inclusive, i.e. all states should be allowed to apply for full membership. Procedural rules should provide room for diffused inputs to reach the final negotiation phase. And finally, also the location of the institution should be decided in order to maximize the representativeness of the institution.

CHAPTER 2 "AGC"
THE EVOLUTION OF AGC: POWER AND TECHNOLOGY

Alessandro Marrone and Alessandro R. Ungaro

The AGC will continue to be fundamental for both global economy and military power. It is currently subject to important trends stemming from both changes in the international security environment and technological innovation, particularly with regards to UAS.[1] These trends particularly influence the access and stability of the AGC by putting them at risk more than in recent years.

Preliminary clarification

A first distinction should be made between the AGC and national airspace, which stretches 60.000 feet over states geographic borders and 12 miles out from their coastlines and it is not part of AGC. It is not by accident that the limit of 12 miles reflect the range of ninteenth century warships: it is another example of how technology contributes to define what is under state authority. At the same time, it should be noticed that since the World War II international air travel requires the use of national airspace for transit on a regular basis, and therefore involves detailed and binding agreements amongst national authorities (Stang, 2013: 2). The UN ICAO is the leading institution in this field, which sets universally recognized standards for air traffic and thus the use of AGC.

Intergovernmental cooperation between national police and security agencies on air security and safety seems to be well established (Stang, 2013: 2) and ICAO standards are regularly enforced, as the access, freedom and stability of AGC is widely recognized as a shared fundamental interest of the international community. In comparison to other Global Commons such as Cyberspace, the governance of AGC has reached a high level of maturity through multilateral and bilateral agreements[2] and international institutions (Martin and Fritz, 2010: 79).

[1] UAS are often called UAV or RPAS. This paper uses the term UAS to stress the fact that the system encompasses not only the uninhabited platform, but also the control system on the ground and associated data-links. In this respect, UAS is truly a system of systems, with the aircraft forming one part of the overall system from which capability is derived.

[2] In 2010, more than 4.000 bilateral air transport agreements were registered at ICAO. See IATA www.iata.org/about.

Trends influencing AGC

The future is unpredictable and this Chapter does not aim to do so. It is rather appropriate to point out the main trends which are likely to influence AGC.
Regarding the international security environment, the tendency towards a multi-polar international system marked by increasingly assertive regional powers will continue also partly due to the on-going globalization process. This implies that more and more medium-sized and large non-Western countries experiencing fast-growing economies – such as Brazil, China, Russia, Saudi Arabia and India - will invest in defence procurement in order to update and upgrade their military capabilities, with a strong emphasis on air capabilities (Ungaro, 2013: 9). There is an ongoing shift of economic, industrial, military and technological power from the traditional North American and Western European regions to other world regions, notably but not only Asia, which is reflected in the international defence market (Dottori and Marrone, 2010: 77-79). This trend will likely also see in the short term major investments into advanced air capabilities, including air defence systems (Denmark, 2010: 167), as well as UAS with many non-Western countries interested in filling the gap with the United States and Israeli products (Arpino, 2011: 1). A recent study estimates that UAS spending will more than double over the next decade from current worldwide expenditures of $5.2 Bn annually to $11.6 Bn, totalling over $89 Bn in the next ten years (Teal Group, 2013: 1). This is particularly important for AGC because its access, freedom and stability has de facto relied in the last decades over the United States overwhelming military power, such as other eventual opponents would certainly loose a military contest for the Global Commons if they attempt to deny them to the United States (Posen, 2003: 8). As far as the US military hegemony – which so far has guaranteed AGC and other Global Commons (Krepinevich, 2010: 7) - is now declining while international system becomes more multi-polar, the key question is whether the access, freedom and stability of AGC will be at risk. In other words, the undisputed Control of the Air enjoyed by the United States in the last decades should not be taken for granted (Martin and Fritz, 2010: 100), and the challenges to such power projection capabilities are likely to threaten the very same access to AGC (Murphy, 2010: 33).

Secondly, non-state actors will continue to play an important a role in the international security environment, also with respect to Global Commons. This is already demonstrated by the importance of Hezbollah in the Syrian crisis and by the capacity of terrorist and criminal groups to take over large parts of Mali - triggering an armed intervention by France at the beginning of 2013. It is likely that large areas of world regions in Africa and Asia will risk falling into a state of anarchy, civil war or failed states (Silvestri et al., 2013: 5) where non-state actors will find safe heavens and sources of manpower and economic resources. These non-state actors will also likely utilize UAS at a tactical level, as done by Hezbollah against Israeli forces in the 2006 Lebanon war, and eventually at a strategic level. Several non-state actors already rely on shoulder-fired anti-air missile known as MANPADS, as well as on increasingly widespread "double-digit" SAMs to threaten the access and stability of AGC.

At the same time, technology will continue to become more cheap, accessible and widespread than in the past, because of ongoing changes in the innovation model (Stankiewitcz et al., 2009: 14-17). This will contribute to empower non-state actors and emerging/regional powers as they will find it easier than in the past to fill the technological and industrial gap with Western countries (Denmark, 2010: 167). The fact that innovation in the civilian market has accelerated and has become global has further reduced the capacity of governments to control transfer of technology to potentially hostile states and non-state actors. Moreover, the current model of innovation paves the way to technological breakthrough and disruptive technologies, which are difficult to foresee but are likely to affect – among other sectors – sensors, telecommunications, electronics, sensors and networks and smart materials (Stankiewitcz et al., 2009: 48). This will obviously influence the activities of R&T and R&D related to air capabilities, including UAS, for example by enabling those actors which will invest significant economic resources into these activities to achieve significant results despite their initial technological gap. In other words, the proliferation of symmetric and asymmetric capabilities allows new powers and non-state actors to increasingly challenge the de facto protector of air commons, the United States (Martin and Fritz, 2010: 80).

The spread of UAS and the AGC

The UAS are not a completely new air capability, but have recently experienced an exponential growth in use. Such system has different degrees of autonomy from the aircrew in the control room: remote controlled UAS, semi-autonomous UAS and fully autonomous platforms. In the first case, the pilot on the ground performs the tasks previously undertaken in the cockpit; in the case of fully autonomous UAS these functions are theoretically performed by the aircraft itself; semi-autonomous UAS have a certain degree of autonomy but remain supervised by the pilot. In practice, a large number of current platforms are remote controlled, and only some have a low level of autonomy. The next generation of UAS is likely to enjoy a higher level of autonomy, depending on developments in control software, microprocessor and data link technology, already in progress: autonomy is measured on a ten-level scale, and by 2025 UAS are expected to reach the 6th level of autonomy (RUSI, 2008: 5). The required mapping radar, threat warning receiver, collision-avoidance systems, will be available by the 2025-2035 timeframe, yet full autonomy can be reached only when AI has been developed and implemented to the extent that it can offer resilient and reliable responses to highly complex and demanding operational demands - a goal that probably will not be reached in the next decade. According to the NATO classification, three classes of UAS are identified on the basis of platform's maximum gross take-off weight: Class I - less than 150kg; Class II - from 150kg to 600kg; Class III - more than 600kg (NATO, 2010: 9). Within the UAS category, the UCAS have the specific ability to engage a target.

Concerning future utilization of UAS, some considerations can be made regarding: endurance and performances; aircrew security and safety; costs and savings; constraints and incentives to launch Air Operations. First, UAS use is likely to increase as these platforms provide a valuable combination of endurance, connectivity, flexibility, autonomy and efficiency. Particularly, endurance is increased as human limitations do not apply: for example the maximum number of hours a pilot can fly per mission is extended by aircrew turnover in the control room. The UAS may utilize AAR as manned aircraft, and by saving the systems and space needed to keep aircrew safe on board UAS can carry more fuel - or equipment or weapons.

One of the main political reasons behind the increased use of UAS is to obviate danger to aircrew - a danger which is increasingly difficult to justify by Western governments in the eye of domestic public opinion. However, there are a number of ethical and legal barriers to be overcome before full UAS deployment, especially in their more lethal forms, will be acceptable to Western governments and people. The disputes occurred over extensive use of UCAS by the Barack Obama administration and the limitations then introduced on their use are a case in point (Marrone, 2013: 1).

A second political argument in favour of UAS is that it could reduce costs, for example by downsizing the foot-print in the theatre required to operate the platform. But it will not necessarily cut the total manpower bill, because so far the extent of personnel savings are questionable. Currently, Class II and Class III UAS aircrew traditionally include a pilot, who is also the mission commander, and a sensor operator to manage and interpret data flows, plus the operational aircrew. Further constraints on the widespread use of UAS may reflect the risk of tactical UAS being jammed or their satellite-based route altered by opponents, including non-state actors utilizing cheap and easily accessible civilian technology, with a consequent loss of control over the system. In addition, the utilization of UAS will depend upon robust NEC and will therefore be subject to a significant risk of cyber attacks, thus requiring careful management of the UAS-cyber nexus.

An important issue is whether the spread of UAS will encourage policy-makers to increase Air Operations in the future merely because aircrew are not put at risk. The trend in American utilization of UCAS between 2009 and 2012 has pointed in this direction. However, European political authorities and public opinion have become used to strict rules of engagement with regards to military operations, and are likely to establish comparably severe limits to the weapons carried on by UCAS and their release, particularly regarding the release of automated weapons.In addition, as mentioned before the use of UCAS made by Obama administration has provoked critics in the United States as well.

Most examples of UAS military utilization so far have come from Air Force-led operations - i.e. Libya - and Army-led operations such as those in Afghanistan and Iraq. In the next few years, it is likely UAS will continue to be used for reconnaissance and surveillance given their capacity to remain in the operational area longer than manned aircraft because they do not suffer the pilot's natural limitation - provided aircrew will ensure turnover in the ground control station. For the same reason, they will probably continue to serve target acquisition, regardless the fact that engagement will be performed by UCAS of by manned fighter aircraft (or helicopters, or missiles). Moreover, it is likely UCAS will be used for CAS, as they have already performed this task by protecting troops on the ground in Afghanistan against enemy forces attacking allied patrols or convoys. A possible, new task could be

SEAD. This task is conducted in the very first phases (day one) of high-intensity military operations against a conventional opponent, in order to destroy its air defence capability, ensure air superiority, and make further operational phases possible, such as targeted bombing or the establishment of a no-fly zone, with near-zero risks for air allied capabilities and aircrews. Obviously, SEAD task is very dangerous, therefore UAS may be preferred to manned aircraft - in conjunction with long-range ballistic missiles - since their destruction by the enemy does not imply allied casualties. Moreover, UAS will probably also be utilized by Navies. For example, UAS are already utilized for ISTAR purposes during border control or anti-piracy operations, and they are likely to be utilized before amphibious operations. UCAS may also be utilized for engagement mission against asymmetric opponent such as pirates. In fact, tests have already been conducted on UAS prototypes with folding wings better suited to be embarked on Navy ships.

All in all, it will be likely we will have a fleet of different UAS able to perform the full spectrum of Air Power roles - Control of the Air, Air Mobility, ISTAR and Engagement. Yet this does not mean UAS are going to replace manned aircraft in the 2015-2025 timeframe, either in Europe or in the United States. They will, rather, contribute to a balanced fleet of both manned and unmanned aircrafts. The proportion of UAS in the force structure will likely vary according to the roles they are expected to perform. Their use will also differ across Western Armed Forces because of military, technological, organizational and budgetary national specificities.

The spread of UAS will be influenced by civil-military coordination on European ATM required to allow UAS flight into non-segregated spaces. In fact, UAS are intrinsically dual-used and by 2025-2035 timeframe are likely to be also widely used for security and civil purposes such as: border control with respect to illicit trafficking and illegal immigration; civil protection purposes by monitoring regions where natural disasters are likely to take place - i.e. risks of floods because of extreme weather phenomena - or have just happened; law enforcement purposes; environmental monitoring; supporting surveillance during international events subject to terrorist threat such as heads of state summits; safety purposes by fire brigades and a number of other security and civilian actors. The main current obstacle to UAS utilization into non-segregated airspace is their airworthiness and their interaction with the European ATM system. Technology allows UAS to transmit the same signal of manned aircraft to ATM ground station, and to interact in a similar way. It also allows the development of systems such as collision avoidance and the necessary redundancy - i.e. triple miniaturized UAS computer system - to reach in the next future the same level of safety guaranteed by manned aircraft. In this regard, on June 2013 a Roadmap for the integration of civil RPAS into the European Aviation System has been delivered to the European Commission from the European RPAS Steering Group.

Access and stability of AGC

The aforementioned trends will particularly influence two aspects of AGC: access and stability.

In fact, a large and growing number of States and non-State actors are likely to invest in UAS - and manned vehicles - to guarantee their individual access to AGC and/or a certain capacity to deny such access to others. To make just but one example, the release of a fleet of unknown UAS in a certain North Atlantic zone of AGC heavily utilized by transatlantic airlines routes may cause the cancellation of scheduled flights because of security reasons, thus denying for a while the use of such portion of AGC.

In case of military confrontation - for example in the South East Asia sea region - it is likely that all powers involved will use UAS and manned vehicles - together with cyber, missiles and naval capabilities - to deny each other access to the AGC in the area of operations. In particular, China would try to deny the United States use of airspace above Taiwan and Taiwan Straits (Murphy, 2010: 37). This scenario is not purely theoretical, as Commander of US Pacific Command addressed this issue in a US Congress testimony (IFPA-Fletcher, 2010: 8).

The aforementioned characters of UAS and their likely diffusion in the next decade pose serious challenges to the capacity to guarantee access and stability within the AGS. First, Class I UAS are relatively cheap and will be produced by a number of companies worldwide - not only the large aerospace industry companies but also SMEs - thus satisfying the demand of a large number of states - not just emerging powers. It is likely that a number of non-NATO countries will start with simple UAS, which will probably lack stealthness, engagement accuracy and advanced navigation systems. Nevertheless they will represent a significant threat at a tactical level, particularly if produced and employed on a large scale in order to make up for quality through quantity. A second element which increases UAS challenge is the facility to control them from relatively cheap and simple devices, similar to a smartphone, which paves the way for non-State actors' utilization of Class I and Class II UAS. Third, the radar cross section of current and future UAS is so small that detection becomes an issue, thus encouraging both state and non-State actors to use them. New technologies to improve UAS tracking at tactical and/or strategic level may be required, coupled with clear and standard procedures to maintain a clear picture of UAS utilized in certain zone of AGC.

Finally, the complex relation of AGC with other commons is beyond the scope of this paper. There is only the space to touch upon the fact that AGC is heavily dependent on both Outer Space and Cyberspace. In the first common, space assets do provide fundamental services such as PNT, together with earth observation and weather forecasting, which contribute to the access, freedom and stability of AGC. In particular, UAS are heavily dependent on PNT and SATCOM since they are somehow remotely piloted by the ground control station. Increased satellite band width will be essential in the most effective deployment on UAS, notwithstanding the development of more autonomous platforms. A key issue for NATO countries will be to develop increasingly secure SATCOM in relation to jamming and other kinds of interference, as well as to ensure interoperability between the set of space and air capabilities. At the same time, activities in AGS - as many others - deeply and increasingly rely on Cyberspace, and are thus extremely vulnerable to cyber attacks. For example. in 2008, 800 "cyber incidents" involved the US FAA (FAA, 2009: 4). In particular, the military trend towards network enabled capabilities will likely lead to greater integration of air operations with surface, cyber and space operations. This will present the challenge of maintaining cyber security and uninterrupted access to space-based systems, as operations are increasingly vulnerable to attack and degradation. It will be essential to build in redundancy and graceful degradation to buy time in the event of hostile action against these complex cyber dependent systems, attacks which may easily affect not just a single node of the net but several. More insidiously, training and planning should not assume unconstrained access to such capabilities: in the future European Air Forces must be capable of operating in less than optimal cyber environments.

CHAPTER 3 "SGC"
GLOBAL WARMING, ICE MELTING AND POLAR SEA:
THE ARCTIC SEA LANE, DREAM OR REALITY?

Angelantonio Rosato

The Arctic is a huge area of almost 30 M squares kilometres, one hundred times Italy, one sixth of planet earth. The Polar Sea has been covered by ice for nine months of the year for a long time. Not anymore: global warming is the driver of an impressive ice melting in the Arctic Ocean, not a new phenomenon, but a continuous trend that has been occurring for many decades. Last year the Arctic has lost more sea ice than at any time since satellite records began in 1979 by the NASA. It is worth stressing the salience of Polar Sea's satellite monitoring: it will be more and more important in the years to come, especially in order to facilitate Arctic access, navigation and incident prevention.

Given the rapid ice melting, the presence of vast untapped natural resources in the Arctic and the geographical strategic position of the Polar Sea, is it possible and economically feasible to build up permanent Arctic routes suited to shorten global maritime traffic and bring Polar natural resources to the world markets, in other words to save and widen the Global Common status (access, movement's freedom, stability) for the Polar Sea? This is the question we will try to answer in this Chapter.

Satellite monitoring & ice melting

NASA's scientists involved in the satellite monitoring say ice melting trend in the Arctic is part of a fundamental change. According to their calculations, between the end of August and the beginning of September 2012 the extent of sea ice was 4.1 M square kilometres, an area smaller compared with a previous low of 4.17 M square kilometres recorded on 18 September 2007, i.e. 6 years ago.

The sea ice cap grows during the cold Arctic winters and shrinks when temperatures climb again. Nevertheless, since the 1980s satellites have recorded a 13 per cent decline per decade in the summertime minimum. What is more, the thickness of the sea ice is also declining. Therefore overall the ice volume has fallen far - though estimates vary about the actual figure.

Joey Comiso - senior research scientist at NASA's Goddard Space Flight Center - affirms that *"this year's [2012] ice retreat was caused by previous warm years reducing the amount of perennial ice - which is more resistant to melting. It's created a self-reinforcing trend". According to the NASA scientist, "unlike 2007, temperatures were not unusually warm in the Arctic this summer"*. But the real problem is that *"we are losing the thick component of the ice cover"* - Comiso says - *"and if you lose that, the ice in the summer becomes very vulnerable"* (Harrabin, 2012). Another scientist from the NSIDC, that collaborates in the measurements, Walt Meier, stated: *"in the context of what's happened in the last several years and throughout the satellite record, it's an indication that the Arctic Sea ice cover is fundamentally changing"* (Harrabin, 2012).

Professor Peter Wadhams, from Cambridge University, says that *"a number of scientists who have actually been working with sea ice measurement had predicted some years ago that the retreat would accelerate and that the summer Arctic would become ice-free by 2015 or 2016"*. Prof. Wadhams was one of the above scientists, and now recognizes those predictions were wrong: *"I was one of those scientists, and of course bore my share of ridicule for daring to make such an alarmist prediction"*. By the way, Prof. Wadhams is convinced that the prediction is now coming true, and the ice is becoming so thin that it will inevitably disappear: *"Measurements from submarines have shown that it has lost at least 40 per cent of its thickness since the 1980s, and if you consider the shrinkage as well it means that the summer ice volume is now only 30 per cent of what it was in the 1980s".* Professor Peter Wadhams states that *"this means an inevitable death for the ice cover, because the summer retreat is now accelerated by the fact that the huge areas of open water already generated allow storms to generate big waves which break up the remaining ice and accelerate its melt".* Cambridge University's scientist thinks that *"the implications are serious: the increased open water lowers the average albedo (reflectivity) of the planet, accelerating global warming; and we are also finding the open water causing seabed permafrost to melt, releasing large amounts of methane, a powerful greenhouse gas, to the atmosphere"* (Harrabin, 2012).

Nothing better in July 2013, according to the NSIDC, in Colorado, United States (Beitler, 2013):

> *"While the rate of Arctic Sea ice loss is normally fastest during July, the warmest month of the year, ice loss was even faster than usual over the first two weeks of July 2013. As a result, on July 15 extent came within 540,000 square kilometers (208,000 square miles) of that seen in 2012 on the same date. The ice loss is dominated by retreat on the Atlantic side of the Arctic, including the East Greenland, Kara and Laptev seas, and Baffin Bay. In the Beaufort and Chukchi seas and much of the Eurasian coast, the ice cover remains fairly extensive, especially compared to recent summers. Compared to the 1981 to 2010 average, ice extent on July 15, 2013 was 1.06 M square kilometers (409,000 square miles) below average. During the first two weeks of July, ice extent declined at a rate of 132,000 square kilometers (51,000 square miles) per day. This was 61 per cent faster than the average rate of decline over the period 1981 to 2010 of 82,000 square kilometers (32,000 square miles) per day. The fast pace of ice loss was dominated by retreat in the Kara and East Greenland Seas, where the ice loss rate from July 1 to 12 was -16,409 and -17,678 square kilometers (-6,336 and -6,826 square miles) per day, respectively. The Laptev Sea ice retreated at about half that rate, at -8,810 square kilometers (-3,402 square miles) per day. In contrast, on the Pacific side, sea ice has been slow to retreat. During the first part of July, the rate of ice loss in the Beaufort and Chukchi seas was only -3,375 and -6,829 square kilometers (-1,303 and -2,637 square miles), respectively. Temperatures at the 925 hPa level for the first two weeks in July were 1 to 3 degrees Celsius (2 to 5 degrees Fahrenheit) above average over much of the Arctic Ocean and as much as 5 degrees Celsius (9 degrees Fahrenheit) above average over the Kara Sea, where ice loss was pronounced"*

It is true that in the summer 2013, Polar ice did not decline at the same spectacular rate of the previous year, the lowest level on record. Nevertheless, according to the last report – first large-scale study in six years by the UN - IPCC, published in September 2013 - *"a nearly ice-free Arctic Ocean in September before mid-century is likely"* (IPCC, 2013).

All this has important consequences: Polar sea is more accessible today, and it will be eve n more so in the near future. That means access to vast untapped energy resources and raw materials. It is believed that 25 per cent of the world energy reserves is under the Polar Sea; these reserves will be more and more attractive thanks to the rising energy world demand. Ice melting also implies access to new shorter sea routes, which might be ice free for a longer part of the year. In fact, "the shortest line between Russia and North America runs across the Arctic. From the northern point of Canada, which lies 4,000 kilometres north of Ottawa, the distance to Murmansk, Russia, is only a little over 2,500 km." (Børresen, 2008: 10). Given that today 90 per cent of international trade is on the sea, the implications for the global economy could be enormous.

Arctic Sea Lane?

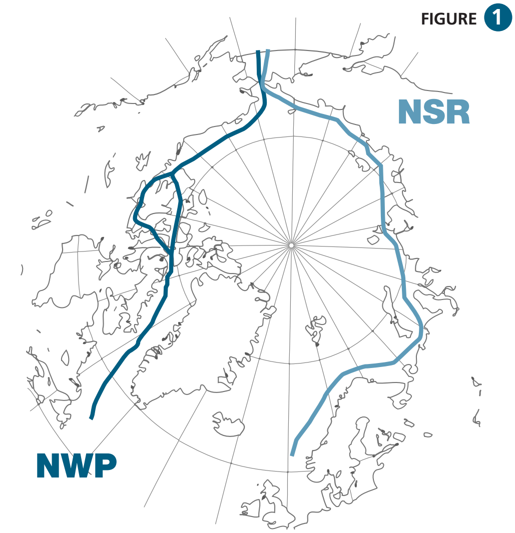
As the ice volume decreases and becomes easier to penetrate, the prospects for a permanent Arctic Sea Lane connecting Asia, North America and Europe seem realistic and attractive to oil and shipping companies. The Lane could result in a substantial reduction of time and costs for energy, people and goods transportation North-South, North-North and Atlantic-Pacific. All this could lead to an Arctic golden age: commercial and civilian shipping would increase, coastal infrastructures would improve, and thus boost the economic and social development of Arctic human communities.

Nevertheless this is a very optimistic picture. In reality, even in case of the most pessimistic global warming scenarios, Polar shipping will continue to be a challenge, both from a physical and an economic point of view. The true story is that the Arctic is scarcely suited for human settlement and activities and is a very fragile ecosystem. It is very hard to believe that the Polar Sea will ever be ice-free all year round. The perennial winter darkness at these latitudes multiplies the ice related dangers for commercial, military and civilian ships. As a matter of fact, a dramatic meltdown will make it even more difficult to predict sea ice and iceberg formation.

Hence Arctic shipping may stay tricky and costly for a long time. It will require enhanced satellite monitoring, icebreakers and ice–reinforced boats, which are twice expensive than ordinary ships; insurance will be always more expensive for vessels operating at these latitudes. Last but not least, delays caused by navigation in ice-infested waters will contribute to make Polar shipping economically disadvantaged compared to the regular routes taken by vessels.

Another major problem will be the greater environmental risks due to increased traffic jam in the Polar Sea: oil spills and toxic materials losses will probably increase and therefore the Polar coastal authorities will have to improve the patrolling and the rapid reaction capability in case of these kind of accidents. These requirements represent relevant costs that will sum up to Polar shipping total costs.

FIGURE 1



The best Arctic Sea Lane scenario would be the Polar Route over the top, the shortest route between the North Atlantic and Pacific Oceans, intersecting the Arctic Ocean and drawing a line from Iceland, over the North Pole to the Bering Strait. Unfortunately the Polar Route is not feasible today, with the rare exception of the most potent icebreakers. A more realist alternative is the route passing closer to the Siberian coast but not so close to be inside the 12 nautical miles of Russian territorial limits. Longer - but not so much - than the Polar Route, it will have the strong advantage of being virtually ice free for three months during the summer, in a decade or two, given global warming and present Arctic melting trends. Considering that multi-year ice is now largely absent in the area towards the Siberian coast, it is reasonable to predict all year navigation in the near future around this Polar Route’s Siberian variant, with a little help from icebreakers.

Avoiding the Russian territorial waters will permit to circumvent the Russian official and grey bureaucracy associated with the NSR transit passage fee; last but not least, there will be no imposed limit to ship size, outside the shallow narrows of the NSR.

On the other hand, the vessels will need special ice-protection and engine power that will make them not economically valuable on other routes. This will open up a market for transhipment ports at both ends of the Polar Route, multiplying the costs associated.

Legal status of the Arctic

Important and controversial issues have to be fixed before Polar shipping could really become commercially competitive. First of all, the legal status of the Arctic, in particular of the NSR along the Siberian coast and the NWP in North America. In accordance with the UN Convention on the Law of the Sea, relevant shipping State actors like the United States. consider them as international straits, therefore not subject to any transit passage fee or national law. On the contrary, Moscow and Ottawa insist that these routes are within their internal waters, hence subject to full national sovereignty. The position of Russia and Canada could weaken the Global Common status of the Polar Sea.

Besides, it is necessary to create a regulatory regime in order to reduce accidents and pollution's hazards. It is true that the MARPOL already exists and applies to the Arctic region, but it is not enough. The region should be designed as a Special Area under MARPOL, following what was proposed by the Arctic Council's working group on the Protection of the Arctic Marine Environment years ago (Børresen, 2008: 37-43).

It is important to enhance the free fundamental principles of Global Common applied to the Polar Sea. Safe, open, reliable maritime routes are indispensable to the geopolitical stability of the area, to the economic development of the Polar region and of the all world. This is especially true for the global energy industry that is always looking for access, stability and movement's freedom for its traffics. The opening of a new, secure, stable transcontinental sea route through the Arctic could help the oil and gas companies to deliver their product to a world that will be more and more energy thirsty.

Conclusions

The growing salience of the Arctic from the strategic and business-related points of view is given by the geographical position of the Polar Sea situated between the North American and the Eurasian continents; the presence of important natural/energy resources; and, last but not least, the chance to build up permanent Arctic routes ideal for commercial aims. In fact, the Polar sea routes to deliver commodities to the world markets are much shorter than the traditional ones, not infested by pirates as in the Red Sea, or crowded by oil tanker traffic jams, such as in the Bosphorus, Hormuz and Malacca straits.

On the other hand, as we stressed, Polar shipping will continue to be a hard challenge, hazardous and very expensive for global commercial traffic. To sum up, the opening of the NSR and the NWP would probably just have a regional importance, at least in the short/medium term. Nevertheless, in the long term and if global warming continues at present trends, the Polar Route - especially the Siberian variant in the North East - may represent a major shift in the global trade that today is passing through Panama, Suez, Hormuz, Malacca etc. In this case, the consequences for the world economy could be enormous. Secure and shorter sea routes are particularly important for the energy industry with a strong appetite for safe, stable and cheap sea transportation of oil and LNG.

The regional economy would benefit, too: the Polar Route will require transhipment ports, rescue and repair services, extra surveillance and all the other services related. This could boost the Arctic economy to an extent never seen before.

A revolutionary Arctic Sea Lane, connecting three different continents in a few days and passing through a geo-politically stable region without piracy and conflicts, is a dream or a reality in the medium term? It will depend on the future trends of global warming and the related Arctic ice meltdown; on the solution of the issues concerning the legal status of the NSR and the NWP, the status of the Arctic region under MARPOL. Last but not least, it will require satellite monitoring extensively applied to Polar Sea navigation; technology improvements in energy exploration/drilling, the construction of special ice-protected ships and the high tech equipment associated with such. Maybe a realistic dream.

CHAPTER 4 “SPACE”
UNION IS STRENGTH?
EMERGING COUNTRIES’ ACCESS TO ORBITAL SPACE

Valerio Briani

Orbital space is a truly unique Global Common. The issues of freedom, stability and access in orbital space must be declined differently from the way they can be conceived in the other Global Commons. “Freedom”, i.e. the free flow of data, goods, capitals, and people in the Sea, Air and Cyber domain is restricted mostly because of regulations and international boundaries: it is States’ political will that interferes with free movement. In space, almost the only factor limiting space-faring States activities are the physical features of the Space domain. Regulations applied to behavior in space are very limited. Freedom of movement is not limited by political choices, but by technological availability.

Regarding “stability”, or the guarantee of protection and security inside the Global Commons, again we find a strong difference between Space and other Global Commons. Rogue actors or conflicts can disrupt the stability of parts of AGC or SGC, or can prevent access to portions of the Web (for example by obscuring selected websites). However, these disruptions remain local in nature, and do not hinder movements in the rest of the domain: Somali pirates may force civilian shipping to avoid the Horn of Africa, but piracy doesn’t make any difference for ships travelling on the Atlantic route from the United States to Europe. On the contrary, an accident in space has the potential to threaten a very wide range of other actors besides those directly involved. For example, collisions between satellites endanger all other satellites in the same orbit through the debris resulting from the collision. The Space “environment” is more delicate than it would seems and requires sophisticated environmental policies (von Prittwitz 2011).

The most important difference between Space and the other Global Commons, however, is to be found in the “Access” area, or the means and system required to accede to the Global Common. Clearly, the resources required to access space are of an incomparable magnitude to those required to access the sGC, AGC or Cyberspace domains.

Having access to Space means having the capability to launch satellites in an independent and reliable manner, for commercial and governmental use. Today, only a handful of countries can do so consistently. However, the launch market is expanding, with the entrance of new actors in the demand and in the supply sides, and with many more to come in the future.

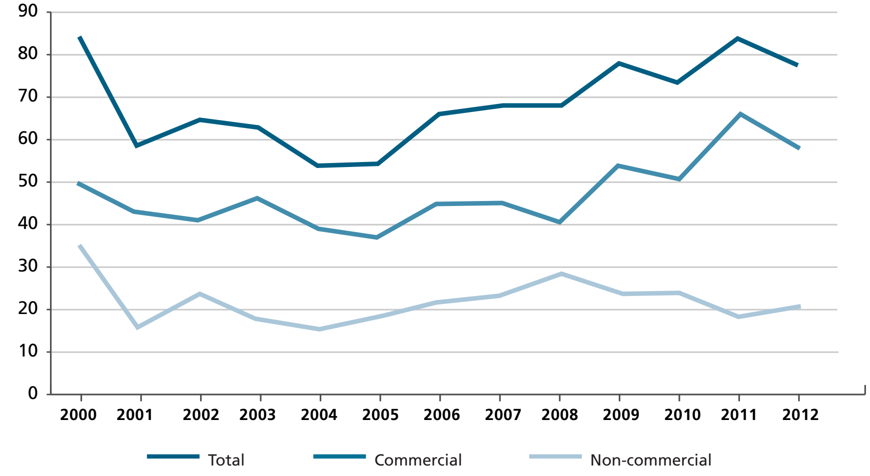
Access to Space has an economic and technological dimension, but also a very strong political and strategic significance. Possessing launch capabilities, in fact, means being able to fully exploit space-based assets to promote one's political and security goals, granting support to friends and allies and obtaining an advantage over hostile countries lacking a similar capability. Cooperation in the field of access to Space, has a strategic significance similar to that of the arms trade. Therefore, it is important to understand the dynamics though which the newcoming space-faring States obtain launch capabilities, and the degree of cooperation they establish with other actors.

This Chapter will provide a review of some of the most recent space-faring State's access to space programs, in particular trying to highlight the degree of international cooperation that might have facilitated the gain of this capability. The first paragraph provide some basic information on the launch market. The second paragraph briefly sketches some new launch-capable countries' access to space programs. The third and final paragraph attempts to draw some conclusions on the issue of cooperation in the field of access to Space.

Access to space today

The access to space "market" is characterized by a specific feature: the commercial component of the market is actually considerably smaller than the non-commercial component (governmental, military, scientific launches). An analysis of data provided by the US FAA in the last five years (FAA, various years) shows that an average of 77 launches were executed annually, only 21 of which were commercial. In 2012,< 78 launches were executed with 20 of them being commercial. Revenues from the 2012 commercial launches were estimated to be around $2.4 Bn, which is also in line with recent trends albeit with an increase of about $500 M. The table 1, based on author's elaboration of FAA data, summarizes the trends of launches in the last decade including both commercial and non-commercial launches.

Number of yearly launches at the global level, 2000-2012 TABLE 1



Recent forecasts do not seem to predict a significant increase in commercial launches. Latest reports attest a number of 31 commercial launches a year throughout 2022 (FAA, 2013). However, the complexity of the market usually forces forecasts to indicate the upper limit of market development. In other words, in the best case scenario according to forecasts, the commercial launch market in 2020 will return to the 2000 level -hardly an exalting market expansion.

On the contrary, most launches today and in the future are and will be non-commercial and in particular "governmental", i.e. the primary payload is owned by a government for official use only. In fact, the main value of possessing launch capabilities is not the commercial value: it is the strategic value of possessing an independent access to space, which allows the autonomous exploitation of the value of space-based assets in order to multiply public policies (including in the defence field).

The "big 4" Russia, Europe, United States and China are the main providers of launch services and currently hold a dominant position in the launch market. Aside from those, private launchers are growing more and more important. The "multinational" data in table 2 in fact refers to international private firms such as Sea Launch, owned by a consortium led by Russia's Energia Overseas Ltd. and Boeing. Other countries such as India, Iran and

Estimated commercial launch revenues (in US$ ms)

TABLE 2

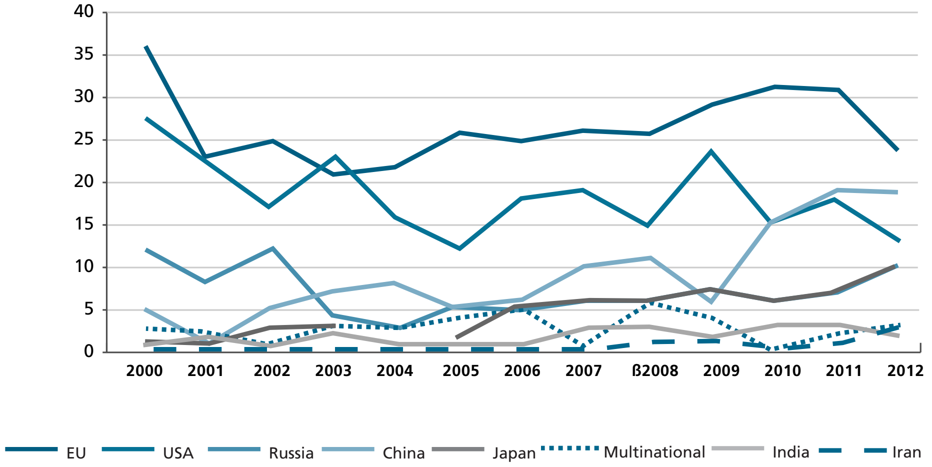
From FAA, Commercial Space Transportation: Year in Review 2103

Country/region	2008	2009	2010	2011	2012
United States	215	298	307	0	108
Russia	581	742	826	707	595
Europe	700	1020	1320	880	1320
China	0	70	0	140	90
Multinational	475	280	0	200	300
Total	1 971	2 410	2 453	1 927	2 413

Japan are slowly building up their own launch capabilities. Their access to Space programs dates back to decades ago, but the difficulty is such that they are still not able to offer a significant number of yearly reliable launches on the market. The table 3, also an elaboration from FAA data, shows graphically the number of launches per country/region.

Number of yearly launches per country/region, 2000-2012

TABLE 3



In addition to those newcomers, other countries are working to obtain independent access to space capabilities. Some conducted limited numbers of launches: North Korea conducted one launch in 2009 and two in 2012 (one of which failed), while ROK conducted two failed launches in 2009-2010 and a successful one in 2013. Israel is able to regularly launch its own satellites but is obliged to resort to foreign launchers in specific occasions. Other countries, such as Argentina or Brazil, have not yet been able to obtain full launch capability. Their cases are described in the following paragraph.

Newcomers

Argentina aims to reach an independent launch capability trought the" Tronador" project which, contrary to the agency's access to Space related programs, is a national effort (De Dicco, 2008). It is entirely possible that the Argentineans benefit from the experience of the Condor II/Badr 2000 short range ballistic missile, developed by Argentina in the 1980s in cooperation with Iraq and Egypt. The first stage of the project, which is ongoing at present, consists of the design and construction of a small ballistic vehicle, Tronador I, which will allows the testing of a liquid combustion rocket motor. Tronador I has already flown successfully in 2007 and 2008 with a payload of 4 Kg. The projected second stage of the program will consist of the design, construction and testing of a bigger vehicle, with a mass ten times that of Tronador I. The new vehicle, called Tronador II, will not be a ballistic one but its path shall be controlled through the corresponding Guidance, Navigation and Control systems designed and produced in Argentina. It should carry a payload of around 300-400 Kg in LEO, and its maiden flight should be in 2015.

Brazil considers independent access to Space as a strategic matter: *"whoever does not matter critical technologies are neither independent for defence nor for development"* (Kasemodel, 2012). Brazil has a long record of developing suborbital vehicles, starting with the SONDA family of the 60s to the VS-30 and -40 and the SVB-30 rockets, currently also used by the European Microgravity program. The current Brazilian effort towards reaching an independent launch capability revolves around the VLS-1 project, the VLM and the *Cruzeiro do Sul* program. The VLS-1 started in 1984. Two flights in 1997 and 1999 were failures, while a third in 2003 resulted in an explosion on the launch pad.

A mockup launch was successful in 2012, while additional VLS-1 V4 launches are scheduled for 2014 and 2015 (this last launch should actually place a satellite in orbit). The VLM started in 2009 and is expected for a first flight in 2015. A simplified VLS-1 rocket comprising only its first stage, should carry up to 150 Kg in orbit from 200 to 700 Km.
Finally, the more ambitious *Cruzeiro do Sul* program envisions five VLS with growing capabilities. The last rocket, VLS Epsilon, should be able to bring a 4 ton payload into geostationary orbit. The completed program should cover 75 per cent of Brazilian launch needs. Interestingly, Brazil is being helped by Russia in this program. Moscow offered technical assistance in the aftermath of the 2003 incident, sending technicians to investigate the site. The Alfa and Beta VLS are currently being developed with Russian liquid-propellant engines, and the Gamma, Delta and Epsilon launchers will be powered by a unit based on the RD-191 engine developed for Russia's new Angara rocket. The upper stage, which will be the same for all Southern Cross rockets, will be driven by an engine which is currently part of Russia's Molniya launcher (Zaitsev, 2008). At the same time, Brasilia also formed a joint venture with Ukraine called Alcantara Cyclone Space. In 2015 the company should start launching Ukrainian Cyclone 4 rockets from the Alcantara facility on Brazil’s east coast.

Israel was the ninth country on Earth to independently launch a satellite into orbit. It is a classic case of searching for an independent capability for access to Space on purely military and strategic grounds. Its Shavit (Comet) launch vehicle is a direct derivation from the Jericho ballistic missile, developed for Israel by French company Dassault in the late 1960s which then became the base for the following generation of Israeli-developed ballistic missiles, the Jericho 2 in the late 1980s. There are strong indication that Jericho 2 was developed in cooperation with Iran and, after the Islamic revolution, South Africa (NTI, 2013). A US official defined the Jericho 2 *“a Shavit minus the upper stage, which is replaced by a warhead”* (Risk Report, 1995). The Shavit, indigenously built by the Israeli Aircraft Industries including the motors, launched a satellite into orbit for the first time in 1988. It then continued with 7 subsequent launches, all carrying Offeq observation satellites designed to offer Israel an independent space-based intelligence capability.

The Taiwan case, interestingly, is quite the opposite from Israel’s and may be a test case of foreign intervention curbing an access to Space program, rather than sustaining it. In

2008, officers from the Taiwan National Space Program Office expressed the intention to a long-term plan for an indigenous launch capability through the TSLV. A test with a 50 Kg payload was supposed to take place in 2010 (clearly the development was in an advanced stage). However, it appears that the United States has been lobbying strongly against the program during its development phase, considering the birth of a Taiwanese indigenous missile capability as an offensive military program sufficient to disrupt the current strategic balance vis a vis China, and contrary to the spirit of the military agreement between Taiwan and the United States which obliges Washington to sustain Taiwan only defensively. A cable which emerged in 2009 would seem to indicate that the United States has effectively lobbied against the TSLV, convincing Taiwan to abandon the program (Cole, 2011). It is a fact, however, that Taiwanese interest in the TSLV evaporated.

The history of Korea's access to space program is also interesting. Both the North and the South of the peninsula started programs to achieve independent access to Space a decade ago. Strategic considerations related to availability of missile technology for military use clearly played a large part in the DRK decision. The very same reasons led the United States, ROK's longtime ally, to forbid any transfer of technology and know-how related to the development of a launch vehicle (Lele, 2013). The United States apparently feared that the ROK's development of a launcher would trigger an arms race in the peninsula. After joining the Missile Technology Control Regime in 2001, ROK was able to sign an agreement with Russia according to which Moscow would provide first stages for three rockets only (Lele, 2013), one of which was used in the first successful launch from ROK in January 2013. A fully Korean launcher should be ready around 2020. However, the rich and technologically advanced ROK was beaten by its poorer Northern neighbor in the run for the first launch. North Korea, a country which is not able to guarantee electricity to all its citizens, was able to successfully deliver a satellite with its Unha II rocket on December 2012, after three consecutive failures (in 1998, 2009 and April 2012). However, it would seem that the Hermit Kingdom's success is due to critical parts of the rocket being manufactured in Russia, in particular the crucial second stage (Wright, 2009), at least in its previous version.

Conclusions

The number of space-faring States will dramatically increase in the next decade. Many emerging countries are in an advanced stage of development of launch capabilities, and many others are working to prepare their first launch. The strategies employed by these countries to build capabilities are varied but many are based on a limited degree of cooperation with other countries.

The way of choice, generally speaking, is to go alone. Most countries analyzed in this Chapter aimed at starting their quest for independent access to Space as national-only endeavors, save recurring to international cooperation if national industrial capabilities proved unable to obtain results. This strategy appears to be closely linked to the military significance of possessing a launch vehicle, which can easily double as a ballistic missile. However other countries, such as Israel, started as clients of foreign producers, becoming producers themselves in a successive stage. This strategy appears to be more typical of countries launching access to space programs during the Cold War, when launch-related technology was less available on the market.

If an emerging country decides to sign up a cooperation agreement, this appear to develop along flexible political lines. Political choices, as obvious, do play a role in this field which is, after all, almost completely dual-use in terms of technology and its applications. However, the analysis of agreement also underlines greater pragmatism in the choice of cooperation: in other words, cooperation in the field of launch technologies is driven by necessity and commercial availability and not by political choices. Russia in particular, one of the main launchers, also seems to be a very active suppliers of key components for missiles. From single stages to raw technologies, Russia signed cooperation agreements with old partners such as India as well as with new associates, such as Brazil, and sold its renowned and proven engines to any country which required them. On the contrary, the United States not only never facilitated any access to space programs of a minor ally, but apparently contributed to stop them. In the case of ROK, US policy did not succeed, but it might have been more efficient in Taiwan’s case. However, it would be difficult to argue that this policy of denial contributed effectively to any political or economic goal.

Europe does not seem to be part of the equation as well. As one of the main providers of launches, it will see its current commercial role challenged by growing competition. This is inevitable. The new space-faring States will develop capabilities, whether Europe is part of the process or not. In fact, technology is today sufficiently widespread to allow for the development of launch capabilities even without European or American assistance, and Moscow proved to be more than ready to help when economic or political reasons suggested so. It would be wise for Europe to start reflecting on the possibility of expanding its already wide range of cooperation agreements to access to space programs.

CHAPTER 5 "CYBERSPACE"
SECURING CRITICAL INFRASTRUCTURES AGAINST DIRECT ATTACK AND ESPIONAGE

Stefano Costalli and Alessandro Fasani

What is Cyberspace? This is the first question that needs to be answered in order to be able to understand all the shades and the implications in the analysis of this delicate subject. Cyberspace is a unique environment, with unique characteristics, that conveys the major transactions nowadays, basically running the world. It is essentially the sum of data packets exchanged, stored and modified through electronics and the electromagnetic spectrum, via network systems and the associated physical infrastructures, such as computers, servers and so on, combined with the software used to run them. In light of this, it is difficult to define a cyberattack. It is clear though that we can consider as such both an attack that uses Cyberspace as a medium and an attack aimed at damaging the infrastructures that support and constitute the material part of Cyberspace, such as underwater cables and other hardware.

Like many other examples of modern technology, the creation of the Internet and Cyberspace started as a military project that then was used solely by government officials and major US universities. Its origins can be traced back to the Cold War, when the United States wanted a telecommunication system that could resist a hypothetical nuclear attack from the USSR. All the studies converged in ARPANET, the prototype of modern Internet that was developed under the auspices of the US Department of Defense and thanks to the previous work of Leonard Kleinrock and JCR Licklider at MIT. ARPANET later evolved to be the Internet that we all know, in the 1970s with the TCP/IP model and the World Wide Web in the 1990s. It is important to underline that "Internet" is not equal to "Cyberspace", as it constitutes only a portion of it, the part of the virtual data exchange made visible to the user and that she could navigate today (Hook and Norman, 2004).

The first example of this technology used for hostile purposes happened in 1982, when, allegedly, a CIA operation was aimed to embed a so-called logic bomb in the Control System of the Urengoy-Surgut-Chelyabinsk (Siberia) gas pipelines, causing a controlled malfunctioning which led to one of the biggest explosions of the past 30 years (Reed, 2005). The story has some shades in it, but two points emerge from it. Firstly, tampering with the SCADA of a critical infrastructure is a modus operandi that has also been found also in the Stuxnet attack, against the Natanz Uranium enrichment facility in Iran. Secondly, the United States gave the USSR defective technologies (Weiss, 1996) and this is one of the main vulnerabilities for critical infrastructures and their ICS even today. This vulnerability has even increased today due to the globalization of the supply chain, where products are designed, manufactured and assembled in different parts of the world, exposing them, for example, to the alteration of modified chips or the implantation of logic bombs.

By the 2000s it was clear that Cyberspace was one of the modern warzones. The attacks on Estonia and Georgia; the Stuxnet virus, Flame, Duqu, Shamoon, Red October and all the other attacks with espionage purposes are clear examples of this trend. It was also clear that the authors of these attacks were not the "nerds" of the collective imagination anymore, but governments' representatives. The proof is that viruses like Stuxnet required a lot of studies and, above all, funds that are normally not available to other actors in Cyberspace (Falliere, Murchu and Chien, 2011). The more interconnected a State is, the more cyberpower it gets but, at the same time, it also becomes more vulnerable to cyberattacks and this brought governments to see Cyberspace as a domain to be controlled.

Cyberspace as a Unique Global Common

Land, sea, air and space are natural environments, which mankind tried to control since the dawn of time. Cyberspace shares some features with these Global Commons but has some unique ones. It is not a natural environment, but an artificial one, manmade, constituted by machines, cables, and network systems. These features allow access, stability and the existence of this Global Common. Theoretically, if the cables get cut and the machines destroyed, Cyberspace would cease to exist. Another unique feature is that individuals or organizations own all the machines constituting Cyberspace and those are placed in some physical location that is under some government’s jurisdiction (Posen, 2003) - except from satellite transmissions and/or undersea cables. Moreover, the biggest slice of the physical part of Cyberspace is privately owned. The private sector has always had a predominant role in the creation of technology for Cyberspace, development of internet policy and defense against network intrusions. An interesting duality emerges: Cyberspace is borderless per se, as far as the virtual part of it is concerned. At the same time however, its physical part is strictly limited by national boundaries and legislations.

Nonetheless, apart from this peculiarity, it can still be considered a Global Common for a number of reasons. Historically, Global Commons permitted the exchange of goods, knowledge, and people. In its own way, Cyberspace does that too. Following Mahan and Douhet, gaining control of a Global Common, and therefore of the routes that pass through it, makes the difference between a superpower and other States. In this Cyberspace is no different: states fight in it and they try to control it. The question is if one actor can dominate in Cyberspace over others. The mainstream view is that today the United States enjoys the command of AGC, SGC and Space. What is the situation in Cyberspace? Briefly, the United States had the biggest technological apparatus in the world. The Stuxnet attack has proved that the United States is capable of attacking infrastructures in other countries (at present, we do not have any other similar reported example) and can also control the major private actors in the Cyberspace arena, such as Apple, Microsoft and also Google, Facebook and Twitter.[3]
This has currently no equals in the world.

Access, Freedom, and Stability

Almost everyone on Earth can access the Cyberspace in this very moment. Desktop PCs, laptops, smart phones, tablets, industrial HMIs: many are the entry points to Cyberspace. Security of access cannot be guaranteed. Recent news history shows us that governments can block access to Cyberspace to their citizens or that governments can access private information of Internet users. These are the two extremes regarding access to Cyberspace. Another feature of Cyberspace is that it has become a sort of Common of the Commons (MNE7, 2013). Cyberspace influences the access to all the other Global Commons and accelerates and broadens the flow of information among them. Nowadays, global com-

[3] Microsoft and Apple are the major software producers in the world today, and Google, Facebook and Twitter are the main vehicle of information nowadays.

munications heavily depend on the interaction between Cyberspace and Outer Space. Satellites permit the connection of cyber environments anywhere in the world, but at the same time space-based systems rely on Cyberspace for information security in communications (we could say that satellites are also part of Cyberspace). Even air traffic controllers, UAV control systems and GPS navigation are influenced by Cyberspace. This flow of data takes place thanks to physical pieces of technology such as command and control systems which are used in various sectors, such as aviation, navy, industry, global finance and commerce or space programs. It is a trade-off, where on the one hand, Cyberspace boosts the capabilities of various actors in different domains, but at the same time the increase in the spread of modern technology widens the borders of the physical and virtual part of Cyberspace itself.

We can conclude that Cyberspace exists as a Global Common in its own, but also that there is an overlap between the Cyber Global Common and the others. In light of that it is important to mention that vulnerabilities in Cyberspace would result in a spillover effect, causing vulnerabilities to spread into the other Global Commons, such as in the possibility of hacking drones, for example (Humphreys, 2012)

For these reasons it is important to have a global degree of security in Cyberspace. Even if now it is an expanding environment, it will become congested as any other common, and this will call for new rules. Since there is already the need for regulatory mechanisms, including Cyberspace in the framework of the Global Commons should help in reaching a global stability, as far as cybersecurity is concerned. (Mather, 2013).

Stability is the most sensitive part to analyze. Cyberspace is globally widespread, it is as complex as it is wide-meshed, so it presents flaws. As it will be further explained afterwards, in Cyberspace the attacker has the upper hand. Unknown flaws in systems can be exploited and can also be sold, these are the famous 0-day exploits. Furthermore the attribution of an attack is not always possible, cyber- resilience is a very difficult status to achieve and deterrence too, given the fact that it relies heavily on the certainty of attribution.

Protection

Recent years have been characterized by an increase in cyber attacks against sovereign States' CNIs, government offices, and economic institutions. The attacks have been both direct, oriented to the control of the infrastructure, and indirect, aimed at espionage and stealing of information, not only of usernames and passwords, but also of sensitive data.

Indeed, cyber attacks are no more bound to a limited scale and the nature of possible targets is increasingly critical. The potential for harmful consequences on civil society is also increasing. Cyber attacks provide low-cost means to exploit vulnerabilities found in most computer networks that run critical infrastructures including power plants, the so-called smart grids, banking systems, and industries that provide goods to society and fuel the global economy. The strategic implications here must not be underestimated. Both direct and indirect attacks constitute capital "cyber issues" for critical infrastructures today. It must be underlined that in this peculiar Global Common there is a huge number of actors and vectors involved. Actors range from the single, isolated, hackers or better "crackers" (in order to distinguish the malicious intent); "organized" groups of hackers such as Anonymous, driven by a common goal; spam and fraudulent groups; criminal organizations that sell illegal drugs and pornography on the internet; private organizations that rely heavily on espionage; cyberterrorists and, in first place, states and governments. The methods obviously vary with the actors and their goal(s). Cyberspace is as a domain that privileges the asymmetry between actors and gives the upper hand to the attacker; in this way single users are capable of causing problems to governmental infrastructures. Moreover, in such an interconnected society, more dependence on Cyberspace means more vulnerability. It is also true that, at the time being, modern cyberattacks have not caused tremendous consequences if compared to traditional attacks (Lindsay 2013). The risks however must not be underestimated, and national and international regulations must be created in order to avoid that those potential risks becoming a reality. As far as direct attacks and Global Commons are concerned, a special mention must go to undersea cables and satellites. Satellite connections are still very high-priced, so the majority of the connectivity between Europe and North America passes through fiber-optic cables on the Atlantic Ocean's seabed. The more "realistic" scenario would be an attack at their endpoints that will disrupt the transatlantic flow of data traffic. (Lacroix et al., 2002) An attack directly onto satellites is however implausible. Nevertheless the locations of these important means of telecommunication are two Global Commons, and must be protected by an international effort, in order to preserve what sustains and fuels modern society at most.

Critical infrastructures

Even though governments are the main actors responsible for the safeguard of societies, the role of the private sector in Cyberspace is heavy and States are facing the challenge of giving some rules for a correct behavior in this Global Common. Critical infrastructures are considered the vital nodes on which modern society is based. They provide electrical supply, waste management and disposal, and water security but this category also includes those organizations that work for the government and its defense and security. Biochem labs, hospitals, public transportation management systems are considered critical infrastructures too. Thus, it is very important to protect these infrastructures in order to protect the nation itself.

The process to obtain protection and, most importantly, resilience of an infrastructure is not simple and it involves two branches: the human component and technology. As far as the human component is concerned, it is important that everyone, from the top management, on which the main responsibilities fall, to the single end user should be aware of the important implications that cyber-misbehavior could have not only inside the infrastructure but on the whole nation. The technological core of the infrastructure is constituted by its ICS. This is responsible of the command and control of the entire infrastructure, and it monitors and manages all the processes that take place inside of it. The largest subgroup of ICS is composed by the SCADA systems.[4]

Obviously, modern infrastructures have state-of-the-art ICS, but infrastructures like some power plants or electric grids were built years, or decades ago, so modern technology adapted to the old one. Updating software, antivirus, and prohibiting the use of personal

[4] See more at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems, last accessed September 17, 2013

USB flashdrives are basic steps that every institution should follow. Nevertheless, the pivotal need is to protect these infrastructures both from the outside and from the inside.

What to Do?

We said at the beginning how Cyberspace was born, and that is basically how we end up here, asking ourselves what are the measures to protect critical infrastructures from cyberattacks. The fact is that Cyberspace, or better the technologies to exploit it, as the Internet, were born as a governmental project. Cyberspace was not born to be a Global Common, neither it was born for being secure, because the security depended on the people who used it, namely governmental scientists and officials. Its nature of an entropic environment, together with the combination of unplanned global access, porous technologies, and weak governance make this new Global Common exceptionally vulnerable (Lewis, 2010). The best would be to avoid a "one size fits all" solution, preferring international engagement and critical infrastructure regulation, instead. In light of the peculiarities of Cyberspace, such as the fact that its "real life" parts are in fact owned by someone at all times, the question is whether Cyberspace can actually be controlled or "dominated", except the portion of machines already under the sovereignty of some nation. One option would be to "share" Cyberspace among current major cyberpowers, a scenario that would be based on multilateral rules and understandings (Silvestri, 2012). The fact is that, as stated before, Cyberspace is an environment that overlaps others, since every day almost everything works thanks to modern technology which exploits, and is part of, Cyberspace. In light of that the best solution would be to adopt a "whole-of-government approach", which should engage all the hierarchies of all the actors involved, whether public or private (MNE7, 2013).

Nevertheless, governments should establish the necessary standards and regulations, and test the defenses put in place in order to ensure a degree of control. It is interesting to mention how, on the one hand, Cyberspace is ruled by a worldwide-accepted standard, another feature of its uniqueness, but on the other hand its national regulation is different from State to State. A multilateral agreement on these matters would help avoid the development of differentiated standards and rules, but this is not the situation we are living in today. Since countries have different degrees of cyber-knowledge, depending on their level of technology penetration, many of them tend to regulate Cyberspace internally. Still, many efforts are put in place both at the national and the international level. At the international level there is a need of norms like for any other Global Common. This is a strong challenge because governments like the Russian or the Chinese one do not condemn cyber attacks and allegedly they largely use them (furthermore they did not sign the Budapest convention in 2008).[5] Another difference is that Russia and China think that the ITU is better suited to help maintain access and stability for Cyberspace, while the EU and the United States are more inclined to give this task to ICANN, a private, California-based body. This, is probably the main example of the public-private struggle in Cyberspace, amongst major cyber powers. Nevertheless, after the 2010 Lisbon summit, in 2011 the North Atlantic Council developed a NATO Cyber Defence Policy, following the request of the heads of state. The main focus of the policy is the protection of communication and information systems. According to the policy, NATO will develop common requirements for all national assets critical to NATO's tasks and help those nations achieve a minimum level of cyberdefence. Moreover, NATO will develop awareness raising programs, tackling the Achilles' heel of cybersecurity, the human factor. Another step taken for international cybersecurity is, for example, the introduction of the IPv6. IPv6 is the new version of the Internet protocol that will simplify the configuration and management of IP networks. With this new protocol every element will occupy a precise location inside the Internet, theoretically easing the problem of attribution.

In the European Union we have the 2008/114/CE directive, for the identification of CNIs and for the evaluation of their needs of security improvement. There is also the ENISA, with a number of interesting initiatives under the CIIP and Resilience Unit, such as the European public-private partnership for resilience (EP3R) co-managed with the European Commission (ENISA, 2013). Furthermore, in January 2013 the European Cybercrime Center (EC3) was launched (EC, 2013), and in February the "EU Cybersecurity plan to protect open internet and online freedom and opportunity" was unveiled (EC, 2013). This is all very positive, it depicts a proactive approach towards critical infrastructure protection and to cybersecurity in general.

So the responses may vary. Iran has a strong data filtering policy, limiting access to content

[5] See more at:http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG

that complies with Islam's laws, plus its encouraging the manufacturing of software locally. Regimes in the Middle East are afraid of Internet as a means of communication, and they shut it down in times of national uprisings (see the recent examples of Egypt, Syria and Turkey). North Korea represents a peculiar example, with basically 0 per cent of Internet penetration for the population, rather they have a national intranet. The access to the Internet is allowed only for military representatives.

Apart from these exceptions, it is straightforward that the main need is a stronger private-public cooperation with a government that should enhance national regulations for critical assets' protection (like the executive order signed by US president Barack Obama in February 2013 "Improving Critical Infrastructure Cybersecurity"), but more importantly the government should make sure that those infrastructures comply with the regulations. The lack of communication and coordination between the public and private sector is slowing down the process of finding national and international regulations. This is also due to the fact that the main responsibilities fall on who owns the infrastructures, and thus establishes a certain degree of cybersecurity. In many cases the incidents are not even reported for the fear that they might go public, leading to a loss in trust from the stakeholders and the general public, that could easily be translated in a financial loss. Given its importance, it should be useful to point out that the private sector is split in pro- and anti-regulation positions. The first argue that only governments have the power to impose rules on the private sector, thus creating and establishing a common level of cybersecurity, since the private sector failed in that. The ones who oppose the establishment of regulations state that rules limit the capability of the private sector of improving cyber response and security and others claim that efficient cybersecurity is too costly and will reduce profits (Clarke, 2005). At the infrastructure level, the aid of a prepared ICT department or a CERT or a more specialized ICS-CERT, is a great help in achieving a status of resilience. These are organizations, generally funded by universities or governments, which collect cyber incidents and vulnerabilities reports. They also provide technical assistance, educational programs, and R&D.

Governments will have to keep up with the fast expansion and evolution of Cyberspace, and this will happen only through strong international collaboration, but maybe more important than that is the need for global awareness on the profound advantages and risks that Cyberspace brings.

CONCLUSION

Claudio Catalano

As you may have noticed in the contributions to the Chapters of this edited occasional paper, the Global Commons have political, legal, economical and technological implications. These are strictly interconnected, and the most interesting implications tend to influence two or more Global Commons altogether.

Access and technology

Technology influences the Global Common: you cannot access the Global Common without the means developed through technology whether this is complex technology (aircraft for the AGC; underwater technologies for the deep sea and seabed; launch vehicles and satellites for Space) or widely available technology (vessels, including small vessels, for the High Sea and simply a point of access for Cyberspace).

For assessing the ‘access’ to the Global Common, we would take into account the complexity and availability of technology, the ownership of the equipment, and the access or flows of persons.

Technological availability allows the individuals to access the Global Common, this is why Cyber domain is the most accessible everyday for anyone living in the advanced economies.

Most common people own the equipment to access the Cyberspace, and navigate everyday into it. In 2013, Internet had reached 2.7 Bn users in the world or 39 per cent of world population. Households internet access is 41 per cent in the world. Household Internet penetration has reached 78 per cent in advanced countries and 28 per cent in developing countries. Europe is the region with the highest Internet penetration rate in the world (75 per cent), followed by the Americas with 61 per cent (ITU, 2013). Norway (95 per cent) Denmark and the Netherlands (93 per cent) have the highest percentage of internet users in the world in 2012, according to the ITU/World Bank WDI.

As Costalli and Fasani argue that a point of access to Cyberspace is easily to be found in everyday use devices. In the near future, internet access will be like digital watches in the

1980s: you could find it in your kitchen furniture, on the top of your night stand, in the display of your mobile phone or video recorder, or your car, and on top of buildings in the main squares of most cities.

SGC and AGC are too close to call: aircraft and ships may be owned by States, airlines and a few individuals. More goods are transported in the SGC, but since the 1950s and in particular following the increase of low-cost airlines people travel more easily by plane than by sea, particularly on transatlantic routes.

However, according to IMO, more than 90 per cent of world trade travels by sea, totaling about 8,4 Bn of tonnes in 2010, but only 18.8 M passengers cruised in 2010 according to European Cruise Council (IMO, 2012). Container port traffic has totaled almost 560 M TEU worldwide in 2011, according to World Bank WDI. The highest values of Liner Shipping Connectivity Index in 2012 were: China (156), Hong Kong (117), Singapore (113), ROK (101), Malaysia (99), United States (91), Germany (90), the Netherlands (88) and the United Kingdom (83) according to UNCTAD/World Bank WDI.[6]
Air cargo traffic in 2012 totaled only 51,4 M tons, but passengers carried by airlines were 2.9 Bn, according to IATA and ICAO. Moreover, air travel totaled more than 30 M registered carrier departures in 2012 according to ICAO/World Bank WDI.

Aeronautics is a high technology sector, and aircraft are very complex platforms with specific design, and include highly sophisticated navigation and communications systems and avionics. Average prices for new commercial airplanes range between $ 70 and 400 M per aircraft in 2013 depending on model and customization. These are the reasons which make aeronautics not a widely available technology. Ships include both medium technology for the platform and high technology for the navigation and communication equipment, and radars. Building costs of new ships in 2010 range from $ 36 M of Oil tankers to over $ 100 M of large containers (IMO, 2012). If we add to the picture, the seabed and Arctic, which require high technologies with limited availabililty owned by States or a few

[6] The Liner Shipping Connectivity Index captures how well countries are connected to global shipping networks. It is computed by the UNCTAD based on 5 components of the maritime transport sector: number of ships, their container-carrying capacity, maximum vessel size, number of services, and number of companies that deploy container ships in a country's ports. The index generates a value of 100 for the country with the highest average index in 2004.

private companies, but not by common citizens, who never travel under the sea or seldom in the Arctic, the SCG becomes less accessible than the AGC.

Space is the least accessible of the Global Commons as High Technology and security restrictions on space technologies, allow only a small number of space-faring States, to be part of the game. Only 500 astronauts have travelled through space till now. Private entrepreneurs are challenging this paradigm, though it is too early to retain Space as being accessible to private citizens.

Global Common	Degree and availability of technology
Space	Highest technology available only to space-faring States. Only 500 astronauts, no passengers yet
SGC	High and Medium technology available to States and private entities, including common citizens. 90% of world trade in 2010: 8,4 Bn T but only 18,8 M passengers. However, seabed and Arctic which imply high technology, and State or private companies ownership, but no private citizens influence, make SGC less accessible than AGC
AGC	High technology very expensive and available to States and private entities, such as airlines, VIP transport. In 2012 flows of 51,4 M T of goods, but 2,9 Bn passengers
Cyberspace	Widely available technology, internet access is available to almost anyone, access points are increasingly growing over time

Freedom (regulation and status)

Marchetti argues that a global governance mechanism for a management system of the Global Commons needs to be achieved through international cooperation, by means of agreements on the cooperation in the Global Commons or agreements on the prohibitions to unlawful activities.

Though some scholars tend to consider general principles of the customary Law of the

Sea to be applicable to general issues regarding State sovereignty or unregulated areas in Global Commons, a specific regulation for each Global Common is often required.

Some Global Commons are highly regulated by widely accepted international agreements and customary international law, such as SGC and AGC, some are formally regulated but in reality are left to the conquest of the sovereign States, such as Space, whose international agreements have the legal status of conventional norms, but they are not always transformed into customary international law, because of persistent objectors. Space law is very similar in this case to Non Proliferation Treaties, where the old traditional space-faring States want to maintain the status quo, while the emerging space-faring States want to create a new situation and acquire increasing space capabilities. On the contrary, Cyberspace is formally an unregulated area, but State control and legal national regulations are increasingly shaping its real legal status.

We may predict that Space, being a domain for space-faring States, will keep on being unregulated and subject to the expansion of sovereign States' control, while Cyberspace, being it a domain for common citizens and private entities, will be increasingly regulated, so as to increase State control to cope with security issues, such as cybercrime.
A general framework is not the panacea for the Global Commons, but each single aspect of each Global Common should be regulated separately. Their very different nature require it, but above all the different ways of economical exploitation, and financial, commercial and security implications of the Commons require it.

For instance, airworthiness is a key issue for the insertion of UAS in the non-segregated civilian airspace, as Marrone and Ungaro argue basing it on the actual UAS experience. Germany has cancelled the Euro Hawk programme on the grounds that it would not obtain airworthiness from EASA. Global Hawks and Predators operating from the NATO and national air bases in Sicily and Southern Italy utilize designated air corridors that allow them to fly around the south coast of Italy and in the Flight Information Region monitored by Italy. The Flight Information Region is an airspace zone over international waters in the Mediterranean. But in the future a more coordinated effort with Eurocontrol, EASA, ICAO and Italian ATM agency (ENAC) is needed for their insertion into the civilian airspace.

UAS which are derived by civilian aircraft platforms, which have already been awarded airworthiness in the manned version, such as the UK-industry-led ASTRAEA project, which utilized an optionally unmanned version of a BAE Jetstream aircraft platform, or the Piaggio Aero/Selex ES P.1HH Hammerhead, a UAS MALE derived from the widely utilized Piaggio P-180 Avanti II, are said to be able to obtain airworthiness more easily.
The general Law of the Sea applies to the Arctic sea lane as Rosato argues, though there are disputes over the legal status as Russia and Canada consider NSR and NWP as internal waters, and the United States as international straits. MARPOL applies to the Arctic region, though the area would require a special status as Rosato argues.

As Costalli and Fasani argue, in Cyberspace there are worldwide-accepted standards or protocols, on which Cyberspace itself is built on, such as TCP/IP, World Wide Web or more recently IPv6. However, the legal regulation is set on a national basis, and is different from State to State.
Some experiments to privately regulate the Global Commons, such as ICANN for the Cyberspace, do not meet the acquiescence of the sovereign States, therefore the international regulation becomes more difficult, either if it is of a prohibitional or cooperative nature, as Marchetti argues.

Stability (security)

As Marchetti argues in his Chapter, unrivalled dominance of the Global Commons - starting with the SGC (Mahan) and AGC (Dohet) - has been the foundation stone of the British empire and later US military doctrine in twentieth century. Those who command the commons command the world (Posen 2003).

The newest Global Commons, such as Space and Cyberspace, will see a more hectic activity with dangers for the stability of the Commons. The emerging space-faring States have started a new space race, but the older States will want to maintain the status quo, this will probably cause instability.
Needless to say, Cyberspace is a breeding ground for cyber crime and illegal activities, in particular in the “deep web”, an unindexed part of World Wide Web, or the “dark net”, a

mostly uncontrolled area of internet accessible by means of TOR tools only, which may cause instability for the whole domain, and a sense of distrust for Cyberspace in the public opinion.

Cooperation applies to the security of the most recent Global Commons. As Costalli and Fasani say, the EU has created in January 2013, the E3C in the Europol framework. However, the E3C is focusing on cyber crime, in particular on cyber fraud, and not on all the cyber threat, such as CNI or SCADA protection. This is because, banks and financial institutions are the main target for the cyber criminals who “follow the money”. While, the CNI is still the domain of national security agencies, while SCADA is under the responsibility of private companies’ logic security departments. Nonetheless, the intranet of banks is more heavily protected than CNI or SCADA systems, because usually these control systems are updated less frequently and are designed by system engineers, not by computer experts, who are less keen on computer security. Therefore, they are more vulnerable to terrorists or criminals.

The cyber security has a key issue in its physical infrastructure security, which is usually less considered than the logic security of the net. Most telecommunications, internet traffic, and all the flows of financial data between the United States and Canada, and Europe, (the UK, Ireland and Iceland in particular) pass through the fiber optic transatlantic communication cables on the Atlantic Ocean seabed. The Global Crossing's AC-1 cable, the current leader of transatlantic communication cables, offers transatlantic connection in 65 milliseconds, the new Hibernian Express cable will do it in 59 milliseconds (the Telegraph, 2011). The Trans-Pacific Express cable was built after the 2006 earthquake in Taiwan that disrupted the older communications infrastructures. It was completed in 2008, at the cost of $500 M. It is 18,000 kilometers long and it connects the United States, China, ROK, and Taiwan. As Costalli and Fasani argue, a terrorist attack to endpoints of these cables would disrupt transatlantic communication, in particular the financial trading between the City of London and New York stock exchanges. Unlike communication satellites, submarine cables are also vulnerable to earthquakes and tsunamis, thus making space technologies more secure than submarine cables.

The most interesting side of Global Commons protection and stability is where two or more Global Commons are interlinked. The EU has created a “networked security” concept by identifying the security nexus between Space and cyber networks (Ashton, 2013). UAS security involve, AGC, Space and Cyberspace. The Satlinks between the UAS and its control station may be theoretically jammed or spoofed. This is easier said than done, all UAS signals are military cipher classified signals, quite resilient to jamming or spoofing, and this operation would require a highly organized group of militaries from a technologically advanced State, not a bunch of kids on the mountains.

Space is the most secure Global commons, only space-faring States could constitute a threat; AGC is the second best; SGC takes the third position, mainly because of the emerging piracy threat in some areas of the world; while Cyberspace is the less secure, because anyone with malicious intent, a cracker, may cause harm, even an amateur, because of the large amount of width widely available technologies. This is because as Costalli and Fasani argue, Cyberspace was not created to be secure: its security depended on the users of ARPANET themselves, who were part of the governmental scientific or security community. Space is not yet a battlefield, but attacks against satellites are a potential threat. In strategic terms, to blind enemy's spatial capability of observation can give a strategic and tactical superiority. However, the only way to blind a satellite is an electromagnetic impulse by means of an atomic explosion in the orbit. This is the only credible threat to satellites, as anti-satellite missiles currently do not have the same degree of efficacy. However, an electromagnetic impulse requires a space-faring State with nuclear weapons, not simply a terrorist group. The fact that the electromagnetic impulse would blind all satellites in orbit, including those of the hostile space-faring State, is also a sufficient dissuasion for this kind of initiative. Therefore, Space seems to be the most secure Global Commons by now.

Insurance costs for third party liability risks give a good measure for Global Commons-related risks. According to a recent report, the US market estimated terrorism reinsurance capacity is in the range between $6 Bn to $8 Bn. Global terrorism reinsurance capacity is estimated to have a value of about $ 9 Bn (Carpenter, 2011). However, this figure includes all kinds of non crime-related violent activities including air-related terrorism, political terrorism, maritime piracy, cyber piracy.

Threats to the AGC are related to technologically advanced threats which can only be performed by State entities, or State-sponsored entities including terrorists. Terrorism has become a lesser perceived threat than in the 9/11 era, due to the small amount of incidents, as compared to other security threats. The economic impact of the terrorist attack of September 11, 2001, has been estimated at about $ 32.5 Bn or $40.0 Bn in 2011 current dollars. Following the 9/11, the Terrorism Risk Insurance Act enacted by Congress in November 2002 did coverage for terrorist attacks, (III, 2012). The Terrorism Risk Insurance Program Reauthorization Act was passed in 2007, extended the federal terrorism insurance program until 2014. Since 9/11, airlines had to insure for Excess Third Party War Liability market, which covers risks of war, terrorism and hijackings. These premiums have declined from $1.7 Bn in 2001 to $0.13 Bn in 2007 (AON, 2007). Since 2007, the market has partially reinstated coverage at a significantly higher cost, but the high end cost of premiums did not exceed 2001 levels.

Maritime piracy is becoming increasingly more dangerous than air-related terrorism. SGC has registered a dramatic increase of maritime piracy in certain areas such as the Horn of Africa, where the fragile states in the areas constitute a safe harbor for piracy and other illegal activities, or South East Asia, as in the strait of Malacca, where the morphological conformation of the coasts and islands is more favorable to the pirates. The International Maritime Bureau estimated the annual cost of piracy as somewhere between $1 Bn and $16 Bn in 2005, with an annual value of maritime trade in 2005 at $7.8 trillion (Chalk, 2008). A more recent estimate in 2011 by shipping companies ranges the cost of piracy between $ 7 Bn and £ 12 Bn a year in insurance premiums, ransom and disruption.
Maritime piracy seems to have reached its climax, and it is now starting to decline, in particular in the horn of Africa.

Cyberspace is the less secure, the World Economic Forum has listed cyber threat in the 2012 top five of global risks in terms of likelihood, and it is the only technological factor. A report from CSIS and a well-known antivirus company estimates the high end of range of probable cost of cyber crime and espionage at around $400 Bn every year. Moreover, the high end estimate of $100 Bn in losses from cyber espionage would translate into the loss of 508,000 jobs. Considering a World Bank estimated global GDP of $70 trillion in 2011, this means a loss of about 0,5 per cent of global GDP, while the report accounts car crashes between 0,7 and 1,2 per cent, maritime piracy between 0,008 and 0,02 per cent, and drug trafficking at 5 per cent (CSIS, 2013).

Global Common	Degree of security
Space	Safest - only space-faring States may be a threat, in particular fro States with nuclear capabilities
AGC	Safe - only technologically advanced threats including insurance costs of War and Terrorism at $1,7 bn to 0,13 bn or 0,002% to 0,0018% of world GDP
SGC	Medium safe - in the last few years piracy has become a key security threat, high end cost up to $ 16 Bn or 0,02% of world GDP
Cyberspace	Unsecure - anyone with malicious intent can be a threat, high end costs of cyber crime up to $ 400 Bn or 0,5% of world GDP

Opportunities

As for the opportunities, Cyberspace is by far the most promising domain, as most of the new technologies are focusing on it. Cyberspace has become the domain in which every financial transaction or information news flows daily Internet contributes to 20 per cent of GDP growth in advanced countries (McKinsey 2011) and eCommerce annual turnover is estimated at $ 8 trillion (McKinsey 2012). Moreover, it has become as the main connecting Global Common to connect all the other Commons. Therefore its influence on the other Commons make it a key opportunity in the Global Commons.
Occupational opportunities also elect the Cyberspace as the Global Common which gives more job opportunities. According to the fifth report of the UCSD on university graduate careers: cyber-related jobs are 4 out of 10 in the top list of hot careers for 2013. The UCSD looked at four criteria, such as: *"current employment in the field, projected growth in the occupation between 2010 and 2020, median annual salary in the occupation, and workplace environment characteristics"*(UCSD, 2013).

AGC has reached its maturity, in 2012 airlines had revenues of $ 600 Bn according to IATA. AGC opportunities are related to the forecasted growth air traffic in airline passengers and cargo traffic between now and 2032, as fuelled by the emerging countries, China in particular. Already in 2016, IATA forecast 3,6 Bn passengers to be carried by airlines or about 600 M persons more than in 2012. Moreover, the insertion of UAS in the non-segregated civilian airspace may boost aeronautics technology, in particular the avionics and navigation and control systems as Marrone and Ungaro argue.

Space is already a challenging area in commercial terms, but as we already stated it is now the least accessible of Global Commons. There are now 'newcomers', or emerging space-faring States, as Briani argues. Space had been very promising in the 1960s and 1970s, but the Space divestment in the United States since the 1980s have reduced space as a business solution. However, by 2020 over 1,213 satellites are to be launched globally (communication, EO, navigation, reconnaissance etc) thus creating multiple innovative applications in many different fields, including civilian logistics, pollution monitoring, natural disasters relief, maritime navigation monitoring etc.

Moreover, it is true that thanks to private entrepreneurs, Space is becoming increasingly accessible to private companies entering the space business, such as Richard Branson's Virgin Galactic or Space X. These companies may revive the space business in the Global Common.

SGC is a mature Global Common, and in the 1950s it has lost some trade traffic, and most of passenger traffic to the AGC. However the multimodal transport and "revolution of containers" since the 1960s have made traditional means of transports such as cargo ships, railways, and trucks regain most of the world traffic of goods. Today, SGC employs 1.5 M seafarers according to IMO. According to Dr Martin Stopford, Managing Director of Clarkson Research Services Ltd by projecting trade growth trend of the last 150 years by 2060 trade transport by sea will amount to 23 Bn tons of cargo (IMO, 2012). However, these estimates take into only fixed technology. On the contrary, new technologies such as ALM or 3D printing may revolutionize the world as we know, and according to some projection the maritime trade in the SGC may be heavily reduced by this new manufacturing technique as you do not need to transport components for end products, but you can print these on site with a 3D printer. However the creation of NSR and NWP are promising for sea lane traffic, if the NSR and NWP succeed in creating an alternative to the usual sea lanes in the Southern Hemisphere.

Global Common	Degree of new opportunities
Cyberspace	Very high - technological opportunities, daily flow of data, and its status as global connector ecommerce estimated at $ 8,000 Bn in 2012 High employment opportunities
AGC	High - new technologies, UAS in particular, and commercial aviation growth forecasted, due to emerging countries. By 2016, 3,6 Bn passengers
Space	Medium - possible growth from emerging space-faring States, launch of new satellites, and new private companies entering the business
SGC	Medium/low - mature technologies, and static sea lanes, unless NSR and NWP create new sea lanes. New technologies such as ALM may even reduce maritime trade. Today SGC employs still 1.5 M seafarers

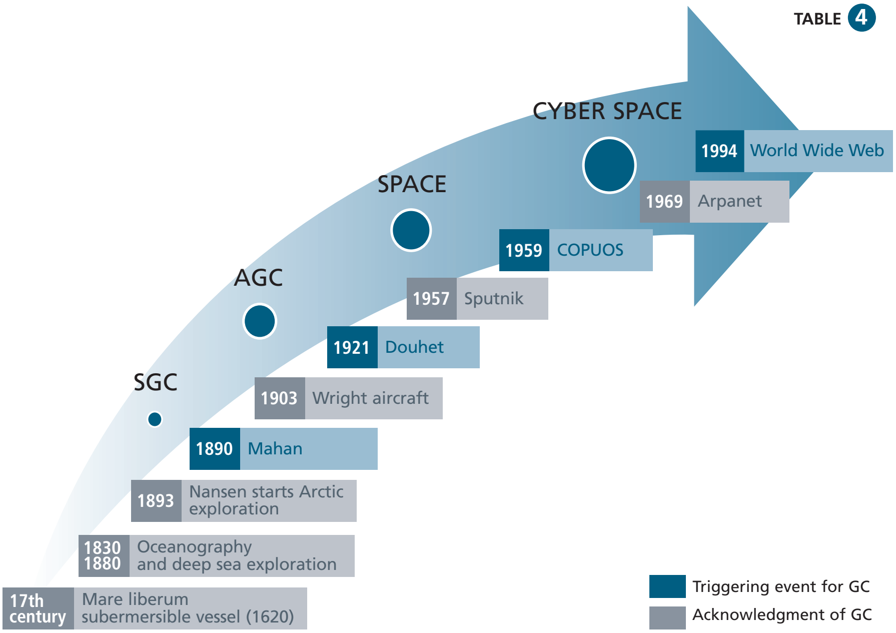
A look into the past and a leap into the future

Technology has created the Global Commons, this is evident for Cyberspace, but it is also true for AGC and Space, while SGC is more the result of a regulatory framework which took into consideration political balance of power and trade customs.

However, we can see the path of technology progress in the creation of SGC too: vessels have travelled through the High Seas for centuries, however the exploration of the undersea and the exploitation of the seabed and the Arctics started at the end of nineteenth century and in the mid-twentieth these were mature technologies, thus starting a new dimension of the SGC.The Air or aeronautical Common began in the early twentieth century and the AGC was first theorized by Douhet. In the late 1950s, the space exploration started. In 1957 the Soviet Union launched the Sputnik and in 1959, the UN created the COPUOS to regulate the Space common. CUPUOS drafted the key Space Law Treaties.

In the 1970s the Cyber domain started to emerge, with Arpanet - the first connections were activated in December 1969 - though it only became a real Global Common with the creation of the World Wide Web in the early 1990s.

TABLE 4



Every Global Common has had a "triggering event" and a point of time in which the "acknowledgement" of the emerging Global Common created it.

The "triggering event" could be a simple fact or theory (like the trade customs and the *"Mare Liberum"* for the SGC) or an emerging technology (underwater technologies for the SGC, aeronautics for AGC, space technologies, computer networks such as ARPANET for Cyberspace).

The "acknowledgment", which is when the Global Common is actually born, may coincide with the start of its theorization or its regulatory framework (Mahan, Douhet, and COPUOS) or just the public acknowledgment of the existence of a new Global Common such as for the World Wide Web for Cyberspace. "Triggering events" may be many, as shown by the history of SGC, but the "acknowledgment" is only one single time in history.

By taking into account the “acknowledgements” illustrated in table 4, and by utilizing a ‘trend analysis’ methodology - which is not always an exact science - we may estimate that about every 30-35 years (in average) a new domain is born. Should we expect a new Global Common to be created just before the 2030s?

What this will be, is a matter of future studies, or better science fiction, rather than technology pace, though it is acknowledged that technological progress is mostly a result of technological leapfrogging.
A new Global Common could be the result of technology progress or of simple events, but the trends should be already be emerging right now.
For instance, Climate change may make the Arctics emerge as a distinct Global Common separating it from the SGC. This trend is already evident, but as Rosato argues, we do not know whether this will be a “dream or reality”. A couple of years ago, ice melting seemed more a reality than we know now by reading the 2013 IPCC report.

However, we may try to be imaginative and we may find in the current science fiction literature what a future Global Common will be like.
In the nineteenth century, a heavier-than-air aircraft seemed a dream, but balloon airship have been flying since the end of eighteenth century. In late nineteenth century, Jules Verne dreamt of flying to the moon in a missile, this was accomplished a few years later.
In the 1950s, space travels and inhabiting other planets in the outer space seemed to be the next frontier. This dream, which could seem realistic at the start of the space race, was not made possible by subsequent space divestment. In fact, science fiction first started to conceive the Cyber domain when the first military networks were developed.

If the future Global Common is the result of a new emerging technologies we should have a look at the current cutting-edge technologies such as: modeling and simulation, unmanned technologies and smart technologies.
Future advancement in modeling & simulation may create a “virtual reality” dimension, thus making you living a second life in a virtual dimension in which you interact through avatars. This “virtual reality” should be different from Cyberspace, as rather than navigate the web you can actually interact in the virtual domain.

Unmanned technologies or AI are going to transform the AGC as we know it today, as Marrone and Ungaro argue. Unmanned technologies may also conquer the SGC, in particular the deep sea, and Space, but these would not create a distinct Global Common from those already existing. Though unmanned and space technologies, such as unmanned space and ground vehicles, may help in exploring and exploiting the moon, which could become "a province of all mankind" (UN,1979) or a new Global Common.

Smart technologies are going to transform the way in which we actually live, by creating smart cities, smart grids and smart transports. Megacities are a key macro trend, and these would easily fulfill the requirement of being a "connective tissue", but it is difficult for a megacity to become a Global Common because it should be no longer under State control, though science fiction imagines these to become unruled or self-ruled areas in the longer term.

These assumptions seem to be unrealistic right now, but so it was Cyberspace some 35 years ago, when the computer networks were already an emerging technology.

Today, a few economists are already defining "Wikis" or "open-source" softwares as "digital commons" or "knowlegde commons" to be owned and shared by internet communities (Stadler, 2010). Our more risk-averse prediction is that the Arctic could emerge as a separate Global Common or become a disputed area for neighboring States.

However also this assumption may be tricky as our more imaginative solutions.

In this edited occasional paper we only made assumptions from a qualitative observation of the last few years. This is considering the technology available now. The future may be quite different from what we know, and this depends on the future key technologies and the priority of R&D investments, or it could just be the same as we know today.

AUTHORS

Valerio Briani (Laurea Roma Tre) is Associate Fellow at IAI and he has been working as a research consultant for institutions, such as the European Commission, the Italian and the European Parliament, the Centro Studi sul Federalismo (Turin) and CEMISS (Rome). His main focus is the European Common Security and Defence Policy and the EU defence industry and market, as well as European and Italian defence policies. Among his recent publications: *The Development of an European Defence and Technological Industrial Base* (European Parliament, 2013), *La Politica di sicurezza e difesa comune e il nodo delle capacità dell'Ue*, (in G. Amato, ed., *"Le istituzioni europee alla prova di Lisbona"*, 2013).

Stefano Costalli (Laurea, University of Florence; PhD, IMT - Lucca) is Research Fellow in International Relations and teaches Strategic studies at the Catholic University of the Sacred Heart, Milan. His studies have been published in Italian and international journals, including *British Journal of Political Science, Ethnic and Racial Studies, Journal of Peace Research, Rivista Italiana di Scienza Politica*. His research interests concern the study of civil wars, ethnic conflicts, democratic transitions, political realism, and the politics of the Mediterranean region.

Alessandro Fasani (Laurea, Università Cattolica del Sacro Cuore) was Assistant Project Manager in the framework of the LNCV Science and Technology for Non Proliferation Programme at the Landau Network - Centro Volta (Como). His research interests concern mainly cyberspace and related sub-fields, such as cybersecurity and cybercrime. He co-authored several papers on the subject, among others: "Cyber Security And Resilience Of Industrial Control Systems And Critical Infrastructures" and "From Fortress to Resilience" in *Cyber Security, Deterrence and IT Protection for Critical Infrastructures:* (Springer, 2013); "Securing the Systems" in Omega Science Review (UK) 1, pp. 38-41, March 2013.

Raffaele Marchetti (Laurea, La Sapienza; PhD, LSE) is assistant professor in *International Relations* at LUISS where he holds a Jean Monnet Module on *EU's Engagement with Civil Society.* His research interest concerns global politics and governance, transnational civil society, political risk, and democracy. In 2005, he received the *Lawrence S. Finkelstein*

Award by the International Studies Association-ISA, Section on International Organization. Among his recent publications: La politica della globalizzazione (Mondadori, forth. 2014); *Global Democracy: Normative and Empirical Perspectives* (co-ed. Cambridge University Press, 2011), *Civil Society, Ethnic Conflicts, and the Politicization of Human Rights* (co-ed. United Nations University Press, 2011).

Alessandro Marrone (Laurea, LUISS; Master of Science, LSE) is Researcher in the Security and Defence Area at IAI and member of the editorial board of the webmagazine AffarInternazionali. His research interest concerns security and defence issues, including military capabilities, dual use technologies, defence industry and market, NATO and EU common security and defence policy. Among his recent publications: "Italy", (co-authored) in Biehl, H., et al. (Eds.) *Strategic Cultures in Europe. Security and Defence Policies Across the Continent* (Springer VS, 2013); *The Transformation of the Armed Forces: the Forza NEC Program*, (co-ed. Nuova Cultura, 2012).

Angelantonio Rosato (Laurea, Political Science, International Relations, LUISS) is energy security and Eurasia analyst, professional journalist, Board Member at Limes–Italian Review of Geopolitics. His research interest concerns Russia, Caucasus, Central Asia, China, Shale Gas American Revolution, Arctic Region, Climate Change. He was Fulbright-Schuman Research Scholar at Pittsburgh University, 2009. He is member of AISSECO – *Associazione Italiana Studi di Storia dell'Europa Centrale e Orientale*. He is frequently interviewed by Italian/international media i.e. TG2 RAI, Russia Today, Skytg24, Rainews 24, Radio 24 (Sole-24 ore), TV Sat2000, Radio3rai, Radio in blù, Radio Popolare.

Alessandro R. Ungaro (Laurea; Cattolica) is junior researcher at IAI, Security and Defence Area. He works on research projects funded by the European Commission and by the EDA. He published a book on offset policy in the defence market, considering the EU, the US and the Indian case studies. His main research interests focused on defence industry, market and procurement. Among his recent publications: *Trends in the Defence Offsets Market, paper presented at the SIPRI 17th* ICES 2013; *Developments in and Obstacles to the US Pivot to Asia: What Alternatives for Europe?* (IAI, 2012); *Le compensazioni industriali nel mercato della difesa e il caso indiano* (IAI, 2012).

References

AON (2007). Airline Insurance Market Review 2007, AON
http://insight.aon.com/?elqPURLPage=1090

Arpino, M. (2011). "L'irresistibile ascesa dei velivoli senza pilota", in AffarInternazionali, 18 October 2011. http://www.affarinternazionali.it/articolo.asp?ID=1885

Arrigo, K. R. et al. (2008). 'Impact of a shrinking Arctic ice cover on marine primary production' in: Geophysical Research Letters, Volume 35, Issue 19.

Ashton, C. (2013). Preparing the December 2013 European Council on Security and Defence: Final Report by the High Representative/Head of the EDA on the Common Security and Defence Policy, Brussels, 15 October 2013

Beitler, J (2013). 'A change of pace', in: 'Arctic Sea Ice News & Analysis', National Snow and Ice Data Center (NSIDC), updated online 17 July 2013.
http://nsidc.org/arcticseaicenews/2013/07/a-change-of-pace/

Boike, J. et al. (2009). 'The International Polar Year 2007-08; Part 22, Permafrost and global climate change' in: Polarforschung, 78(3).

Brown, J. (2006). 'Permafrost and the International Polar Year' in: Proceedings of the International Symposium on Cold Regions Engineering, Vol.13.

Børresen, J. (2008). 'The Great Arctic Game' in: 'The Polar Game', Heartland - Eurasian Review of Geopolitics, no. 2.

Carpenter, G. (2011). Terrorism: Terror Market Continues to Provide Abundant Cover.
http://www.scor.com/en/sgrc/pac/terrorism/item/1815.html?lout=sgrc

Chalk, P. (2008). *The Maritime Dimension of International Security Terrorism, Piracy, and Challenges for the United States*. Santa Monica, CA: RAND.
http://www.rand.org/pubs/monographs/MG697.html

Clarke, R. (2003). Interview for Frontline. Frontline website.
http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/clarke.html

Cole, M. (2011). 'US qualms may have nixed Taiwan space launch program'. in "Taipei Times", 19 December 2011.

Critical Information Infrastructure Protection in the European Newtork and Information and Security Agency Website.
http://www.enisa.europa.eu/activities/Resilience-and-CIIP

CSIS (2013). *The Economic Impact Of Cybercrime And Cyber Espionage*. July 2013. Santa Clara, CA: McAfee Inc.
http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf

De Dicco, R. (2008). *Accesso al Espacio, Centro Latinoamericano de Investigaciones Cientificas y Tecnicas*, August 2008.

Denmark, A. H. (2010). 'Managing the Global Commons'. The Washington Quarterly, 33(3), 165 182, July 2010.
http://csisdev.forumone.com/files/publication/twq10julydenmark.pdf

Dodds, K. (2012). 'Introduction: The Governance of the Global Commons: Much Unfinished Business?' Global Policy, 3(1), 58-60.

Dottori G. and Marrone A. (2010). "Il mercato mondiale della difesa tra geopolitica e globalizzazione", in Catalano C. et al. *Baricentri: lo shift globale degli equilibri politici, economici e tecnologici?*, Occasional Paper Finmeccanica.
http://www.finmeccanica.com/siamo-finmeccanica-we-are/ufficio-studi/pubblicazioni-publications

Douhet, G. (1921). *Il dominio dell'aria. Command of the Air* (English translation). Washington DC: Air Force Historical Studies Office.
www.afhso.af.mil/shared/media/document/AFD-100924-017.pdf

DSG (2012). "Sustaining US global leadership: priorities for 21 century defense" January 2012.

European Commission (2013). 'European Cybercrime Centre (EC3) opens on 11 January' Commission Press Release IP/13/13.
http://europa.eu/rapid/press-release_IP-13-13_en.htm

European Commission (2013). 'EU Cybersecurity plan to protect open internet and online freedom and opportunity' Commission Press Release IP/13/94.
http://europa.eu/rapid/press-release_IP-13-94_en.htm.

EU Military Staff (2011). *Draft concept for Air Operations in support of the EU CSDP*, 2011.

FAA (2009), 'Review of Web Applications Security and Intrusion Detection in Air Traffic Control Systems'. Report Number: FI-2009-049," May 2009.
http://www.oig.dot.gov/StreamFile?file=/data/pdfdocs/ATC_Web_Report.pdf.

FAA (2013). Commercial Space Transportation Forecast, May 2013.

Falliere, N., O Murchu, L., Chien, E. (2011). 'W32.Stuxnet Dossier", Symantec Security Response Whitepaper, February 2011.
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

Hale, T., & Held, D. (Eds.). (2011). *Handbook of Transnational Governance. New Institutions and Innovations*. Cambridge: Polity.

Hardin, G. (1968). 'The tragedy of Commons'. Science, 162(3859), 1243-1248.

Harrabin, R. (2012). 'Arctic sea ice reaches record low, Nasa says' in: BBC News, updated online 27 August 2012 .
http://www.bbc.co.uk/news/science-environment-19393075

Holland, M. M. et al. (2006). 'Future abrupt reductions in the summer Arctic sea ice' in: Geophysical Research Letters, Volume 33, Issue 23.

Humphreys, T. (2012). 'Drone Hack Explained: Professor details UAV hijacking' RT.com,
http://rt.com/usa/texas-professor-drone-hacking-249/ Last accessed October 3, 2013.

IFPA-Fletcher (2010). 'Final Report of Conference on National Security Strategy and Policy, Air, Space, and Cyberspace Power in the Twenty-First Century', January 2010.
http://www.ifpa.org/pdf/USAFreportweb.pdf

III (2012). 'Terrorism Risk: A Continuing Threat: Impacts for Property/Casualty Insurers'. September 2012.
http://www.lockton.com/Resource_/PageResource/MKT/iii%20Terrorism%20Risk%20February%2013.pdf

IMO (2012). 'International Shipping Facts and Figures - Information Resources on Trade, Safety, Security, Environment', Maritime Knowledge Centre, 6 March 2012.
http://www.imo.org/KnowledgeCentre/ShipsAndShippingFactsAndFigures/Statisticalresources/MaritimeTransport/Pages/default.aspx

IPCC (2013). 'Fifth Assessment Report (AR5)' in: UN Intergovernmental Panel on Climate Change, (September, 30, 2013.
www.ipcc.ch/

ITU (2013). 'The world in 2013, ICT Facts and Figures', February 2013.
http://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx

IUCN (1980). 'International Union for Conservation of Nature and Natural Resources, World Conservation Strategy, Living Resource Conservation for Sustainable Development'. 1980.

Kasemodel, C. (2012). 'Access to space in Brazil: current and future scenarios' in Journal of Aerospace Technology and Management, vol. 04, n. 04, October-December 2012.

Koenig-Archibugi, M. (2006). 'Introduction: Institutional Diversity in Global Governance'. In M.Koenig-Archibugi & M. Zürn (Eds.), *New Modes of Governance in the Global System*. Houndmills, Basingstoke, Hampshire; New York: Palgrave Macmillan.

Krepinevich, A. F. (2010). ‘Why AirSea Battle?’, Center for Strategic and Budgetary Assessments, 2010.

Laxon, S. et al. (2003). ‘High interannual variability of sea ice thickness in the Arctic region’ in: Nature. International Weekly Journal of Science, 425.

Lele, C. (2013). ‘How geopolitical factors overshadow South Korea’s space success’. In “The Space Review”, February 2013.

Lindsay, J. R. (2013). ‘Stuxnet and the Limits of Cyber Warfare’. In Security Studies, 22:365-404, 2013.

Mahan, A.T (1890). *The Influence of Sea Power Upon History: 1660-1783*. 12th Edition, Boston: Little, Brown and Company.

Marrone A. (2013). “La spina dei droni nel fianco di Obama”, in AffarInternazionali.
http://www.affarinternazionali.it/articolo.asp?ID=2311

Martin K. and Fritz O. (2010). “Sustaining the Air Common”. In: Center for a New American Security. Contested Commons: *The Future of American Power in a Multipolar World*. January 2010.
http://www.cnas.org/files/documents/publications/CNAS%20Contested%20Commons_1.pdf

Mather, M. (2013). ‘How Space and Cyberspace are Merging to Become the Primary Battlefield of the 21st Century’. In Space Quarterly Magazine. March 2013.

McKinsey (2011). ‘Internet matters: The Net's sweeping impact on growth, jobs, and prosperity’ McKinsey Global Institute, May 2011.
http://www.mckinsey.com/insights/high_tech_telecoms_internet/internet_matters_

McKinsey (2012). ‘Internet matters: Essays in digital transformation’, McKinsey Global Institute March 2012.
http://www.mckinsey.com/insights/business_technology/essays_in_digital_transformation_

Murphy, T. (2010). Security Challenges in the 21st Century Global Commons. Yale Journal of International Affairs, 5(2).

Murphy, T. (2010).’Security Challenges in the 21st Century Global Commons’. In Yale Journal of International Affairs. Summer 2010.
http://yalejournal.org/wp-content/uploads/2010/09/105205murphy.pdf

NATO Joint Air Power Competence Centre (2010). Strategic Concept of Employment for Unmanned Aircraft Systems in NATO.
http://www.japcc.de/fileadmin/user_upload/projects/nato_flight_plan_for_uas/NATO_UAS_CONEMP_Final.pdf

Nordhaus, W. (1982). ‘How far should we graze the global commons?’. In American Economic Review, 72(2), 242-246.

Nuclear Threat Initiative (2013). ‘Israel Country Profile’. February 2013

Posen, B. R. (2003). ‘Command of the Commons: The Military Foundations of US Hegemony’. In International Security, 28(1), 5-46. åSummer 2003.
http://belfercenter.ksg.harvard.edu/files/posen_summer_2003.pdf

Quintana, E. (2008). The ethics and legal implications of Unmanned Aerial Vehicles. RUSI.
http://www.rusi.org/downloads/assets/RUSI_ethics.pdf

Risk Report (1995). ‘Israel: How Far Can Its Missiles Fly?’. In: Risk Report, volume 1, n. 5, June 1995.

Silvestri, S. (2013). ‘A Better Cybersecurity? Some Considerations’ (unpublished).

Silvestri S., Nones M. and Marrone A. (2013). “How to carry out a successful retreat”. In: Marrone A. and Nones M. (eds) *More Europe on Defence or No Europe*, DOCI IAI 13 03E, July 2013. http://www.iai.it/pdf/DocIAI/iai1303e.pdf

Stalder, F. (2010). “Digital Commons”. In: Hart, K.; Laville, J.L.; Cattani, A. D. (eds). *The Human Economy: A World Citizen's Guide*. Cambridge, UK: Polity Press, pp. 313-324.

Stang, G. (2013). ‘Global commons: Between cooperation and competition’. EUISS-Brief Issue No. 17. April 2013.
http://www.iss.europa.eu/uploads/media/Brief__17.pdf

Stankiewitcz R. et al. (2013). ‘Knowledge Dynamics Scoping Paper’. Paper published within the research project SANDERA funded by FP7.
https://sandera.portals.mbs.ac.uk/Portals/65/docs/KNOWLEDGE%20Dynamics%20Scoping%20Paper-D2.1.2.pdf

Teal Group (2013). ‘Teal Group Predicts Worldwide UAV Market Will Total $89 Billion in its 2013’ UAV Market Profile and Forecast.
http://tealgroup.com/index.php/about-teal-group-corporation/press-releases/94-2013-uav-press-release

The Telegraph (2011). ‘The $300m cable that will save traders milliseconds’. 11 September 2011. http://www.telegraph.co.uk/technology/news/8753784/The-300m-cable-that-will-save-traders-milliseconds.html

UCSD (2013). ‘Special Report for Recent and Mid-Career College Graduates: Hot Careers for College Graduates for College Grads and Returning Students 2013’ fifth edition, June 2012. UCSD Extension.
http://extension.ucsd.edu/about/images/careerReport.pdf

UN (1979). United Nation General Assembly resolution 34/68. ’Agreement Governing the Activities of States on the Moon and Other Celestial Bodies’. 5 December 1979.

Ungaro A. R. (2013). ‘Trends in the defence offsets market’. Paper presented at the SIPRI 17th Annual International Conference on Economics and Security (ICES), Stockholm, June 2013. http://www.sipri.org/research/armaments/milex/ICES2013/papers/archive/ungaro-trends-in-the-defence-offsets-market

VV.AA. (2013). ‘Concept of Employment for Cyber Situational Awareness Within the Global Commons’. Multinational Experiment (MNE) 7 Website.
http://mne.oslo.mil.no:8080/Multinatio/MNE7produk/35CyberCon/file/3.5%20Concept%20of%20Employment.pdf

Vogler, J. (2000). *The Global Commons. A Regime Analysis*. London: Wiley.

Vogler, J. (2012). ‘Global Commons Revisited’. Global Policy, 3(1), 61-71.

Von Prittwitz, V. (2011). ‘Space as Environment: On the Way to Sustainable Space Policy?’ ESPI Perspectives no. 50, August 2011.

Wright, D. (2009). ‘North Korea’s Missile Program. Union of concerned Scientist’. Paper produced as part of the project “Improving Regional Security and Denuclearizing the Korean Peninsula: U.S. Policy Interests and Options.”, April 2009

Zaitsev, Y. (2008). Russia begins elbowing Ukraine out from Brazil's space program’. RIA Novosti, September 2008.
http://en.ria.ru/analysis/20080917/116874710.html

The authors would like to thank Gen. Vincenzo Camporini, *IAI Vice President*; Lorenzo Fiori, *SVP Strategy Finmeccanica SpA*; Adm Guido Venturoni, *Deputy Chairman Finmeccanica SpA*; Giuseppe Viriglio, *Vice President Telespazio SpA*, for their suggestions and for delivering seminars to the Research Community.

FINMECCANICA RESEARCH DEPARTMENT

Carlo Musso - *Head*
Graduated in physics, he has been researcher at the Cosmic Physics Institute of the Consiglio Nazionale delle Ricerche and coordinator of the science program of the Italian Space Agency. He is member delegate of the Board of ISPI, member of the executive Board of IAI and member of Chatham House. He is author of five novels.

Claudio Catalano - *Senior Analyst*
Graduated in Political Sciences at the University of Rome "La Sapienza", he has obtained a PhD (Dr. Eur.) at the IMT High Studies, a master degree in Strategic Studies at LUISS and a master at the College of Europe in Bruges. He is a journalist and he has been visiting fellow at the Universities of Cambridge (UK) and Heidelberg, and at the EU-ISS in Paris. Since 2013, he is adjunct fellow in "History of international relations" at the University of Rome "La Sapienza" and "European Defence" expert for the CeMiSS.

Andrea Mignogna - *Senior Analyst*
Graduated in Economics of Institutions and Financial Markets at the University of Rome "Tor Vergata", he has obtained the master degree BEST in General Management provided by Finmeccanica in collaboration with IRI Management. Since January 2012 he coordinates the Finmeccanica Working Group managing the relations with information companies like EIU, IHS, F&S, Aviation Week, Flight International. He worked in the Strategy Department of Finmeccanica. He won the 2008 Finmeccanica Innovation Award.

Eleonora Nicoletti - *Assistant*

The Research Department refers to the Executive VP Strategy, Business Development and Innovation **Giovanni Soccodato**

Finmeccanica
Piazza Monte Grappa, 4 - 00195 Rome, Italy - Tel. 06.3247321