2011/811

ISSN 1797-3457 (verkkojulkaisu)
ISBN (PDF) 978-951-25-2294-1

TIIVISTELMÄRAPORTTI (SUMMARY REPORT)

Securing the Access to Global Commons

Mika Aaltola, The Finnish Institute of International Affairs
Juha Käpylä, The Finnish Institute of International Affairs /
The University of Tampere, School of Management
Charly Pasternak-Salonius, The Finnish Institute of International Affairs
Joonas Sipilä, The Finnish Defense University
Valtteri Vuorisalo, The University of Tampere, School of Management

Tiivistelmä / Abstract

1. Introduction

PROJECT THEME: GLOBAL COMMONS - A NEW STRATEGIC FOCUS

The Global Commons refer to areas or domains that fall outside the direct jurisdiction of sovereign states, and thus can be used by anyone. Traditionally, such areas include the high seas, air, space, and most recently the man-made cyberspace. These domains, even if outside the direct responsibility and governance of sovereign entities, are of crucial interest for the contemporary international order. In fact, so great is their importance that they are said to be “the connective tissue around our globe upon which all nations’ security and prosperity depend.” In a sense, then, the Global Commons constitute the arteries that make possible the heightened states of global connectivity and circulations of the liberal international order. Today, in a world that is perceived to be increasingly interconnected and interdependent, the security of these arteries is of crucial interest.
Recently, the security of the Global Commons has emerged an important topic in the strategic planning of major actors of international relations, including leading state actors such as the United States, and international organizations, such as the NATO. The United States has led this discursive move to (re)secure the global commons. The 2010 *US National Security Strategy* (NSS) has defined the “Safeguarding the Global Commons” as one of the “Key Global Challenges” that require the attention of both the United States but also the international community as a whole. In a similar vain, the 2010 *US Quadrennial Defence Review* (QDR) and the 2011 *US National Military Strategy* (NMS) have highlighted the growing importance of the Global Commons. The 2010 *QDR* has stated that the assured access to the Global Commons “will take on added importance” in future in the shifting operational landscapes of the US armed forces, and indeed security and foreign policy more broadly. Echoing this, the 2011 *NMS* has defined the “Global Commons and the Globally Connected Domains” as a key feature of the current and future strategic environment. According to *NMS*, “[...] assured access to the global commons and cyberspace constitutes a core aspect of U.S. national security [...].”
It is especially the latest of the Global Commons - the cyberspace - that is drawing an increasing amount of attention in the US today. As the 2010 *NSS* stated, “[c]ybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a nation.” The increased importance of the cyberspace was made apparent with the release of the first ever US Department of Defence *Strategy for Operating in Cyberspace* (SOC) in July 2011 where cyberspace was deemed as a “defining

Postiosoite	MATINE Puolustusministeriö PL 31 00131 HELSINKI	Sähköposti	matine@defmin.fi
Käyntiosoite Puhelinvaihde	Eteläinen Makasiinikatu 8 00130 HELSINKI (09) 16001	WWW-sivut Y-tunnus	www.defmin.fi/matine FI01460105
Pääsihteeri	(09) 160 88310	OVT-tunnus/verkkolaskuosoite Itellan operaattorivälittäjätunnus	003701460105 003710948874
Suunnittelusihteeri Toimistosihteeri	(09) 160 88314 050 5555 837	Verkkolaskuoperaattori Yhteyshenkilö/Itella	Itella Information Oy helpdesk@itella.net
Faksi kirjaamo	(09) 160 88244		

feature of modern life", and as such, a critical infrastructure for civilian, commercial and military interests alike.

The focus on the Global Commons has not remained the sole purview of the United States. Increasingly, international organizations have also started to pay strategic attention to the Commons. Most notably, the NATO 2011 Report *Assured Access to the Global Commons* (AAGC) has claimed that "the security and prosperity of our nations, individually and for the Alliance as a whole, rely on assured access to and use of the maritime, air, space, and cyberspace domains." In fact, according to the report, the concept of the Global Commons provides a "useful lens" through which it is possible to view the world "as a complex, globalized whole that depends for its security and prosperity on access to all four domains." Due to the complex nature of the Global Commons – e.g. in terms of the opportunities, vulnerabilities and risks therein that all actors of contemporary life experience – the governance of the Global Commons cannot be achieved in isolation. The complexity of the cyberspace domain is a good example of this. Like most modern organizations, NATO is "highly networked at every level, from governance to command and control, from document handling to military operations." As a result, NATO is not only a "major target of hackers", but also "an important global resource for new research and thinking on cyber defence." However, the security of the cyberspace – or of any other domain for that matter – is not a problem that the NATO can or should solve alone. Quite the contrary, according to it the "assured access to and use of the cyber commons is a *global concern*, and while we [the NATO] believe the Alliance can play a role in promoting security and best practices, it is not and never will be the sole contributor."

Perhaps the latest of international efforts that highlights the growing strategic importance of the Global Commons is the on-going Multinational Experiment 7 (MNE7) project *Access to Global Commons* (ACG). The MNE7 project is a "two-year multinational and interagency concept development and experimentation (CD&E) effort to improve coalition capabilities to ensure access to, and freedom of action within, the Global Commons domains [...]."As such, the MNE7 project has an explicit military focus; it is "an attempt to [...] cover the most relevant issues and scenarios where military forces are given tasks and may be utilized as preferred means of action." Related to the specific interests of this working paper, one of the MNE7 research tracks focuses on the important maritime Global Commons. The 2011 *Access to the Global Commons: Maritime Domain Baseline Assessment Report (ACGMDBR)* summarizes the importance of the Maritime domain for the broader international order; it is a huge and critical domain that consists of "139 million square miles of ocean and corridors that connect widely dispersed markets and manufacturers around the globe." As such, these waterways are "essential to a healthy international economic system," and "vital to most nations' security interests." Crucially, it is also a domain that is becoming increasingly contested around the globe, and in fact is said to experience a "maritime security deficit" due to lack of functional maritime security regimes, international disputes related to conflicting legal interpretations and behavior at sea, and increased "anti-access" or "area-denial" threats, including maritime piracy.

2. Research objectives and accomplishment plan

Given the increasing high-level strategic interest in the Global Commons discussed above, what is notable and worth highlighting here briefly is the somewhat curious lack of strategic level focus on the Commons by the European Union (EU). While the 2003 *European Security Strategy* (ESS) starts with the diagnosis of a globalized world in which Europe is dependent on "an interconnected infrastructure in transport, energy, information and other fields", the specific focus and language of the Global Commons was still - quite understandably given the impact of the 9/11 - missing in early 2000. Similarly, while the 2008 follow-up *Report on the Implementation of the European Security Strategy* (RIESS) also highlights globalization and the importance of “the arteries of our society” that include, for example, “information systems and energy supplies”, the specific language and focus on the Global Commons remains absent in the EU strategy.

However, there are some elements that can be read to point towards an emerging even if still unspecified recognition of the importance of the Global Commons by the EU. First of all, the 2008 report does highlight the importance of cyber security as a critical infrastructure of the European space. This is also supported by the adoption of a separate *EU Strategy for a Secure Information Society* in 2006. Secondly, the 2008 report also highlights the importance of energy security, for example in relation to the need for the diversification of transit routes – some of which are land-based and some maritime - through which the European demand for energy is met. Lastly, the problem of maritime piracy around the Horn of Africa is highlighted as a potential source of disruption to world economy since most of the world trade is conducted through maritime transport in the high seas. With the launch of the first-ever EU naval mission *EUNAFOR Somalia: Operation ATALANTA* in 2008, the problem of piracy and the security of the maritime domain more broadly seem to have become specific strategic interests for the EU.

Despite the recent maritime activity by the EU, the European high-level military strategy does not fare any better than the security strategy, as a whole. For example, the 2006 European Defence Agency’s *An Initial Long-Term Vision for European Defence Capability and Capacity Needs* (LTV) does not explicitly highlight or focus on the strategic importance of the Global Commons. While it does point out the importance of the cyberspace (both in terms of opportunities and vulnerabilities), the growing threat of asymmetric warfare (for example in the cyberspace), and the need for joint operations that utilize all domains (interoperability), the *LTV* is focused, for the most part, on comprehensive *land-based crisis management operations.* These operations aim to produce social and political stability that is seen as the pre-requisite for comprehensive social engineering, including the promotion of rule of law, human rights, and democratic structures in a post-conflict situation on land. More specifically, the strategy sets out two specific types of operations for the future EU engagement: first, the “separation of warring factions by force”; and secondly, “stabilising operations in a failed state in the face of a determined and capable asymmetric threat.” Neither of these is precisely tailored for the specific task of governing or securing Global Commons – be it the securing a free access to, and use of, the maritime domain (e.g. securing transport routes from pirates) or the cyberspace (e.g. non-kinetic cyber war against states or non-state actors, protecting critical infrastructure from hackers).

Similarly, the more political EU *Headline Goal 2010 (HG2010),* first approved in 2004 in support of the 2003 *ESS*, has its focus on land-based crisis management operations. In the *HG2010,* the member states “decided to commit themselves to be able by 2010 to respond with rapid and decisive action applying a fully coherent approach to the whole spectrum of crisis management operations covered by the Treaty on the European Union.” The operations reflect the full range of the so called “Petersberg Tasks” that include “humanitarian and rescue tasks, peace-keeping tasks, tasks of combat forces in crisis management, including peacemaking.” To accomplish these tasks, the *HG2010* set out to develop the EU Rapid Response force based on the “Battlegroup concept” – that is, to come up with rapidly deployable *land-based* Battlegroups that consist of “a combined arms battalion sized force package with Combat Support and Combat Service Support.”

This claim of land-based bias on the part of the EU, however, requires a reservation. It is important to point out an explicit observation in the *LTV* according to which future operations may, indeed, have a “reduced theatre footprints” on land, and instead they “may require an emphasis on the sea as a sphere for maneuver and sustainment.” This potential transformation of European crisis management operations, claims the report, “reflects the problems that civilian opposition and insurrectionary movements can pose for the land as a military base, and political sensitivities over deployment and host nation support of troops in the territory of allies." If accurate, this could result, in the future, in an explicit strategic shift from securing and stabilizing land-based conflict zones towards an increasing focus on securing the Global Commons, including the Maritime Domain. In fact, when interpreted through this lens, the EU *Operation ATALANTA* around the Horn of Africa is a first reflection of this trend to detach from, or avoid, both operationally and politically complex land-based operations, and to place emphasis on securing the Global Commons and the critical flows of the European and global markets therein from the symptoms – here maritime piracy - of land-based complex crises. As such, the emergence of a strategic focus on Global Commons, while not explicitly expressed in strategy but executed in practice, could mark the first step towards a broader shift of European crisis management operations from a comprehensive agenda of social transformation towards a more limited goal of securing critical flows and infrastructures, and containing crises.

Given that the Global Commons have been recently identified as a new and emerging strategic focus by various key actors -- including the US, the NATO, the multinational MNE7 process, and to a limited extent also the EU -- we are still a bit in the dark as to *why* exactly this is so for these actors. While the above has already hinted at some possibilities, it is worthwhile to illuminate some of the answers to this question on the basis of the documentation through which the discursive move to secure Global Commons is conducted. The high-level strategic documentation points towards three inter-related reasons: first, it is increasingly recognized that that these domains are of crucial *importance* for the current liberal international order; secondly, and as a result, they also present some of the key *vulnerabilities* of the contemporary order; and thirdly, related to this, there is a recognition of a set of current and potential future *threats* that the domain-dependent liberal international order faces.

The *importance* of the Global Commons to the liberal international order is connected to the critical activities that take place in various domains, and between them. As already pointed out, the Global Commons constitute the arteries of today's interconnected world through which commerce, capital, information, people but also military force flow (still relatively) freely. In terms of *commerce*, a rough 90 percent of global trade travels by maritime routes in the sea domain, amounting up to $14 trillion in value in 2008 alone. This leads easily to the conclusion that "free trade and free access to the Maritime Global Commons Domain are key features of the present world order." The assured access to, and free use of, maritime routes is especially important in certain strategic parts of the world, including critical sea lanes and potential choking points, such as the Gulf of Aden, the Strait of Hormuz or the Strait of Malacca, through which a large portion of trade goods and especially oil are transported for the global markets. The same goes for the air domain; free and assured access to air domain is crucial for global commerce since an estimated 6 million tonnes of international freight and as many as 2.75 billion passengers will travel by air in 2011. Without fast inter-continental flight services, global commercial and business interests would not be properly served.

The global *finance* sector is also highly dependent on the Global Commons, and especially of the cyber-domain. The nearly-instantaneous transactions of the financial markets rely on the free and safe flow of digitized information and capital in the cyberspace, but also on the safety of its constitutive systemic components divided into other common domains, including the sea (cables) and space (satellite technology), but also relying on the crucial land domain that remains under the jurisdiction of sovereign states (the server infrastructure). Likewise, individuals, civilian organizations and corporations of all kinds also rely on the free, secure and fast flow of *information* – text, imagery, video, and so on - in the cyber domain.

What is crucial to notice is the fact that it is also the *military* that relies on the assured access to, and free use of, the Global Commons. For example, the US Department of Defence (DoD) cannot function without access to cyberspace. It operates "over 15,000 networks and seven million computing devices across hundreds of installations in dozens of countries around the globe." Furthermore, the DoD "uses the cyberspace to enable its military, intelligence, and business operations, including the movement of personnel and material and the command and control of the full spectrum of military operations." What is even more crucial to notice - albeit only briefly here - is the fact that the military rely not on a single but multiple Commons domains in (almost) any given operation. From the perspective of maritime activities, contemporary navies are "dependent on digital communication and satellite reconnaissance and navigation for deployed operations, maritime related flight data, and missile guidance." For example, the NATO anti-terrorist naval mission *Operation Active Endeavour* in the Mediterranean Sea relies much of its operation capability to its "strong maritime situational awareness" that utilizes "an array of surveillance and intercept assets on land and sea, and in space and cyberspace." The same goes for the recent European Union anti-piracy operation *EUNAVOR Somalia: Operation ATALANTA* in the waters around the Horn of Africa. For example, the maintenance of the *Maritime Security Centre – Horn of Africa* (MSCHOA)[1] that supports the provision of an international transport corridor for commercial ships through the Gulf of Aden relies on, and utilizes, the free access to various domains to provide a scheduled and systematic escort service to ships passing the Gulf of Aden. This includes, for example, assured and free access to air domain to make possible radio communication between and among commercial and military ships at sea; access to space domain for satellite surveillance, targeting of ships, and communication purposes; and to cyberspace for an internet-based service for commercial ships.

The strategic focus on the Global Commons is also made apparent by the potential *vulnerabilities* that the importance of, and reliance on, the Global Commons produces. As the 2011 MNE7 *AGCMBR* clearly claims, the current liberal world order is based on free trade and free access to the Global Commons, e.g. to the high seas and critical sea lanes in the maritime domain or to the internet in the cyberspace. It is from this ever-flowing economic order that the political and military might of its backbone, the United States, but also of other liberal powers, is drawn. Given that both commerce and finance sectors utilize the free and assured access to the Global Commons, it naturally follows from this that the Commons become the very vulnerability of the current liberal world order. This is the so called "irony of the commons" - namely that while the various Commons domains play a powerful role in enhancing economic prosperity, the exchange of information, the flow of goods and services, and even the efficient projection of military power in a globalized world, they are, at the same time, the vary basis of increased insecurity today.

In addition to these considerations of importance, vulnerability and threats, it is almost impossible not to consider the possibility that *recent long-term engagements* by the US-led coalitions of the willing in Iraq and Afghanistan have had an impact on the way in which robust and comprehensive operations on land are viewed today. Not only have these engagements become extremely costly, but they have turned out to be extremely difficult in terms of achieving the set objectives, whether operationally or politically. This, in turn, might be reflected in the increasing willingness to keep major Western/Coalition forces away from land-based engagements, especially in the less strategic parts of the world on the African continent, and to emphasize more feasible and less costly strategy of governing and securing the Global Commons from the negative symptoms of land-based crises. As discussed above, this is something that the European *LTV* had already considered explicitly.

[1] For more information on the Maritime Security Centre – Horn of Africa (MSCHOA), see http://www.mschoa.org/pages/default.aspx.

3.Materials and methods

METHOD: DOMAIN INTERRELATIONSHIPS AND COMPLEXITY - TOWARDS A HOLISTIC APPROACH

Traditionally, the Global Commons are conceptualized through a *spatial* metaphor, as the geographic and/or virtual spaces of international waters, airspace, space and the cyberspace. More specifically, they are a sub-set of the broader maritime, aerospace, and cyber domains insofar as they refer to those sub-domains that are accessible to all but owned by none. In a historical perspective, and following this spatial conceptualization, man-made innovations have tended to emerge within one of these domains, even if having wider impact on larger human activities. This is especially the case in the military where “the emergence of human activity within each of the sea, air, space and cyberspace domains has produced a fundamental transformation in the nature of warfare and military operations.” It is this spatial and geographic understanding of warfare that has remained central for the Western understanding and conceptualization of war; for example, it has “remained a cornerstone of for the U.S. military approach to development of military power theory and operating concepts.”

This spatial understanding of warfare, and more broadly of man-made activities, in the various domains of the Global Commons is based on what Redden and Hughes call the “traditional approach.” It is a micro view with a reductionist and bottom-up methodology through which the Global Commons are conceptualized in a linear and dogmatic fashion, on domain-by-domain basis. It tends to pay close attention to single domain exploitation that is only secondarily related to activities that cross domain borders, let alone to the evaluation of their wider implications. In short, intra-domain focus trumps inter-domain analysis and conceptualization. A close variant of this traditional approach is what Redden and Hughes call “bi-domain theoretical initiatives” to understand activities in various domains. These bi-domain approaches are characterized by hierarchical conceptualization of domains in which one domain is dominant and the others are relegated to a subordinate or supporting role, as potential force multipliers of activities that take place in the dominant domain.

These intra- or bi-domain approaches that conceptualize activities through a spatial lens tend to lag behind the current realities of the Global Commons. In particular, it is the *emergence of domain interrelationships* that tends to challenge the traditional approaches. With the introduction of space and cyberspace into the equation, the *multiplication* of interrelationships across and between domains in activities in the Global Commons brings with it the associated *increase in seams between domains.* It is these seams that, in turn, offer both opportunities and vulnerabilities to agents that operate in the Global Commons, whether friendly or adversary, commercial or military. For example, the reliance on satellite technology in space by Western naval forces acting in the maritime domain enables an efficient and long-range projection of force in distant waters, but also brings along new extra-maritime domain vulnerabilities to the successful execution of naval activities. The loss of space systems - including global positioning, communications, or intelligence, surveillance and reconnaissance systems - would be potentially incapacitating, as the negative effects of the loss would cascade down on operating platforms and systems in other domains.

Moreover, the cross-domain dependencies and interrelationships have not only increased with the introduction of new domains and technologies to harness them, but they have also become increasingly *complex*. This complexity is a double-edged sword. On the one hand, the increased reliance on domain interrelationships brings a potentially non-linear growth in the *value* for any activity that utilizes such connectivities and capabilities. The introduction of satellite technology in space and computer networks in the cyberspace have created complex chains of dependencies that have dramatically improved the efficiency of military operations in recent decades, for example by improving command and control systems or making possible the use of precision weaponry from a distance. Similarly, the reliance on satellite phones and GPS gadgets has increased the efficiency and range of piracy operations in the waters around the Horn of Africa.

On the other hand, the increase in complexity of cross-domain dependencies also brings along a potentially non-linear growth in *vulnerabilities* on activities and systems that utilize them. As pointed out above, vulnerabilities in the space and/or cyber domains may have fundamental consequences for activities in air or maritime domains. From a military perspective, to counter the use of advanced fighter in air might be achieved through adversary behavior in other domains, for example in space (disruption of satellite) or cyberspace (cyber attack against relevant computer systems on ground), or in both. Similarly, to disrupt the free flow of information in cyberspace might be achieved through kinetic adversary behavior at sea (e.g. against major network cables) or in space (e.g. against satellite relays). From an adversary perspective, piracy operations at sea could be severely hampered if not prevented by activities in the space domain to prevent the use of satellite phones or GPS gadgets.

It is because of these changing realities in the Global Commons that the traditional domain-centric approach is increasingly cumbersome and out of date. By focusing on intra-domain activities alone there is a heightened risk that domain dependencies and the resulting seams, opportunities and vulnerabilities will be inadequately addressed, both in theory and practice.

Instead of the traditional approach, then, it has been recently suggested that it might be worthwhile to start conceptualize the Global Commons through what Redden and Hughes call the “holistic approach”. This macro approach would eschew the domain-by-domain focus, and instead would take into consideration the complex nature of the *interactive system* of the Global Commons and especially the *complex relationships* across domain borders that various activities or platforms rely on when operating within the various domains. In short, it would treat the Global Commons not as a “set of distinct geographies, but rather as a complex, interactive system.” In practice, then, this would mean the adoption of not only a *systemic* but also an increasingly *functional* metaphor of the Global Commons, instead of the traditional spatial one. The importance of this approach is being increasingly appreciated by the Western military community. This is because of the realization that domain interrelationships are ubiquitous; they start precisely “at the most fundamental levels of military operations and capabilities and yield effects throughout the whole spectrum of military power as the totality of interrelationships is integrated across each level of warfare.”

Within the military, the so called “join operating concepts” – e.g. the United States sponsored AirSea Battle - are a step into this direction. However, even these have a tendency to fall short of a truly holistic approach, mostly because an “analysis that [still] envisions one or possibly two domains and considers others as enablers ignores the need to consider the totality of the global commons and the domains’ evolving interdependent nature.” As such, thinking on the Global Commons or activities therein should clearly depart from the domain-centric and spatial mind-set and adopt a broader, holistic approach.

From the military perspective, the holistic approach should provide a *synoptic overview* of the Global Commons. It should, first of all, *quantify* the nature of domain relationships; secondly, it should *identify* (friendly and/or adversary) vulnerabilities and opportunities associated with domain seams; and lastly, it should *illuminate* fundamental principles of military power employment that will mitigate the risks associated with seam vulnerabilities and exploit inherent seam opportunities.

While it is correct to claim that the holistic approach does provide a way to elevate theoretical conceptualization of the Global Commons beyond the traditional intra-domain mind-set that, at best, can lead to insights about the inter-relatedness of domains from the dominant perspective of a single domain, it is not so clear whether a holistic approach is able to deliver on being a better – in the sense more accurate - account of the interactive and complex reality of the Global Commons system. This is because of the fact that complex systems are *in a constant state of transformation,* and hence they tend to avoid systematic efforts to map them out. This, in turn, is especially because they exhibit or produce entities, properties, patterns or phenomena that are *emergent*.

Stemming from this, the general thesis of emergentism usually entails three assumptions about complex systemic interaction that are pertinent to the discussion here. The first of them claims that emergent entities, properties, patterns or phenomena of a complex system are not simple resultants; they are not *reductively explainable* on the basis of their basal conditions out of which they emerge. Secondly, this is often coupled with the claim that they are also not *predictable* on the basis of even the most complete and exhaustive knowledge of their emergence base. Together, these point to the conclusion that emergent entities are more than the sum of their constituent parts. Thirdly, it also often suggested that since emergent entities are not merely novel but possess causal powers of their own (i.e. powers that their constituents did not have), they may exert downward causality to the interactions out of which they emerged; this *feedback loop* can then change their nature and dynamics.

Within the inter-domain space of the Global Commons, this could mean that even the relatively simple interactions between domains can lead to the unexpected and unpredictable emergence of novel and complex systems or patterns that may feedback to the interactions and change their nature and dynamics. For example, the complex system of the Global Commons has the potential to facilitate the emergence of new friendly vulnerabilities in the cross-domain interaction between the maritime, cyber and space domains. When a commercial oil tanker at sea relies increasingly on satellite systems in space, computer networks and systems in the cyberspace and communication systems in the air domain, some or many of these dependencies *may* become a new source of vulnerability. The emergence and apprehension of these vulnerabilities *may* have an impact on both friendly and adversary behavior. The adversary behavior may seek to transform to exploit these novel vulnerabilities, where as friendly activities may seek to transform in order to prevent such exploitation.

Naturally, the complexities of the inter-domain system may vary. Some of the interactions are weak in their emergent nature. Such interactions can be analytically reducible to elemental characteristics of a single dominant domain. In these cases, it may be possible to claim that the system supervenes on its components without being reducible to them. However, the developing nature of the inter-domain practices in the Global Commons may at time lead to the emergence of contingent new properties that are not specific to any single domain, but are based on the interaction between multiple characteristics. Moreover, since these emergents have the capacity to exert influence - or downward causality - on the constituent activities at the “basal level”, the very nature of the system becomes flux-like and irreducible to any particular representation of it.

This has implications for the holistic approach to the Global Commons. As pointed out, the holistic approach pays a close attention to the systemic nature of the Global Commons, and is thus a counter-move against the encapsulating stove-pipe tendencies of the more traditional intra-domain approach. Within the holistic approach, the synoptic or system-oriented overviews of complex systems are commonly crafted for two general reasons: an overview can, first of all, *moderate the sense of perplexity* due to complexity by an initial mapping of inter-domain knowledge (about the existing relationships and dependencies) so as to better allow for a subsequent *analytical explanation*. The key to this was the double move of quantifying domain interrelationships and identifying related vulnerabilities. However, this two-step approach might not make sense if the domains are not fundamentally neatly interlocking processes, but consist of an open-ended bundle of

complex, multifarious, and irreducible processes, some of which may end up feeding back to the system and thus transforming the very basal conditions of present and future systemic interaction. In this transforming and emergent systemic environment, synoptic overviews that aim to quantify interaction and interrelations that cross domain borders and identify related vulnerabilities are bound to be *insufficient* at best, but probably *misleading* and *untimely* at worst.
This partial shift of conceptual focus from a *systemic* to *sub-systemic* analysis, from the sole and general focus on complex interrelationships towards actual (and sometimes conflicting) communities of practice and their historically patterned but gradually transforming capabilities to exploit vulnerabilities or to counter them in the meta-space of the Global Commons, requires some ground work in terms of theoretical elaboration. In particular, the notions of practice, communities of practice and constellations of communities of practice need to be elaborated in some detail. For this task, we now turn to discuss a methodology that contemporary social science knows as practice theory. This practice approach to the Global Commons could be seen as a conceptual effort to complement – and to some extent also to moderate - the holistic and complex approach to the Global Commons.

4. Results and discussion

FINDINGS
To recap our discussion, this approach has two central methodological implications for the *conceptual understanding* of contemporary Global Commons as a meta-space characterized by inter-domain relationships that are worth re-iterating here. First of all, while appreciating the focus on domain interrelationships and activities, lessons learned from practice theory can help limit the potential over-complexities and conceptual entanglements that stem from a holistic, systemic and complex approach to the Global Commons; this is especially the case with vulnerability and threat scenarios therein. Secondly, and closely related to the above, it can also help us approach the Global Commons through the social ontology of practice instead of spatiality; in this regard, a special focus can be placed on communities of practice with relatively patterned and recurrent practices and capabilities, some of which may cross domain borders.

This conceptual elaboration can also bear fruit in terms of a more *concrete method* through which communities of practice and their inter-domain capabilities and footprint in the Global Commons can be studied and identified. For this task we propose the following preliminary heuristic:

1. The state of community of practice: Established / Embryonic
2. Technological sophistication of the community of practice: Know-how in one / Many domains
3. The networked nature of the community of practice: Open / Closed
4. Geographical spread of the community of practice: Localized / Regional / Global
5. Compositional intensity of the community of practice: Diffuse / Concentrated
6. Transformational ability of the community of practice: Innovative / Rigid
7. Vulnerability of the community of practice: High / Low
8. Disruptive and exploitative capability of the community of practice: Advanced / Rudimentary
9. The nature of (background) knowledge of the community of practice: Sticky and Non-transferrable / Flexible and Transferrable

Lastly, it is also possible to reflect on some of the potential *political implications* that are related to the holistic approach to the Global Commons that emphasizes complexity in relation to the practice approach with a specific focus on communities of practice and their relatively patterned (inter-domain) capabilities. First of all, the conceptualization and identification of communities of practice allows for the *detection of political dynamics* and points of contestation between communities of practice. This might not be possible in a systemic overview that maps all the possible domain interrelationships without due attention to actual political actors, their existing capabilities or political intentions and motivations. Secondly, the reduction of complexity in the Global Commons through a practice-based approach also reduces - in a sense, *moderates - the conceptualization of potential vulnerabilities* therein. This could help to avoid potential moves to over-secure the Global Commons as a meta-space of complex and unpredictable vulnerabilities. This may be especially pertinent if juxtaposed with the post 9/11 Global War on Terror in which potential vulnerabilities and related threat scenarios were based on the existence of mostly invisible and emergent acts of terror that led to the near establishment of a global and permanent state of exception. Similar possibilities, while not probable, could become a reality in the Global Commons if vulnerabilities are seen not only complex but ubiquitous. This political reading of the over-securitization of the Global Commons may be especially relevant for small liberal states that rely on international law and institutions for their security. From a small state perspective, tendencies to establish complex vulnerabilities and the related discursive moves to secure them may be problematic; such moves may not respect exiting international law, especially if complex and systemic vulnerabilities are seen as existential threats. Moreover, such drastic moves to securitize the complex system of the Global Commons may also call for robust military activities that might not advance the promotion and adherence of universal human rights. In fact, and in the worst case scenario, they might jeopardize the fundamental right to have rights in the first place, as was the case in Guantanamo Bay, Abu Ghraib and elsewhere. Finally, potentially robust military activities might not fit to the broadly accepted and legitimate framework of Comprehensive Crisis Management in Europe.

5. Conclusions

6. Scientific publishing and other reports produced by the research project

Reports:

1. Global Commons: Small State Perspective. Working Paper. The Finnish Institute of International Affairs.
2. Securing the Access to Global Commons: Practices Based Analysis. MNE7 Concept Development Report
3. U.S. Changing Geopolitics: Governing the Global Commons and Flows. Working Paper. The Finnish Institute of International Affairs
4. The Security of the Finnish Global Flows. Working Paper. The Finnish Institute International Affairs (forthcoming spring 2012).

Events:

1. Kyberturvallisuus, April 2011, The Finnish Institute of International Affairs
2. Cross border flows: November 2011, The Finnish Institute of International Affairs
3. Numerous other events were used to report the results of the project.