71

FIIA Working Paper
June 2011

Mika Aaltola
The Finnish Institute of International Affairs

Joonas Sipilä
Finnish National Defence University

Valtteri Vuorisalo
Tampere University School of Management

SECURING GLOBAL COMMONS

A SMALL STATE PERSPECTIVE

ULKOPOLIITTINEN INSTITUUTTI
UTRIKESPOLITISKA INSTITUTET
THE FINNISH INSTITUTE OF INTERNATIONAL AFFAIRS

The Finnish Institute of International Affairs
Kruunuvuorenkatu 4
FI-00160 Helsinki
tel. +358 9 432 7000
fax. +358 9 432 7799
www.fiia.fi

ISBN: 978-951-769-305-9
ISSN: 1456-1360

Language editing: Lynn Nikkanen

Contents

SECURING GLOBAL COMMONS
A SMALL STATE PERSPECTIVE

Mika Aaltola
Programme Director
The Finnish Institute of International Affairs

Joonas Sipilä
Senior Researcher
Department of Strategic and Defence Studies
Finnish National Defence University

Valtteri Vuorisalo
Researcher
Tampere University School of Management

Abstract

This report examines the increasing importance of the global commons. It argues that the securing of the sea-, air-, space-, and cyber-based global flows solidifies the vital structures of global interdependence. For a small state with a highly specialized economy, the multilateral frameworks for securing global flows are crucial. Each global domain highlights different aspects of power and requires unique forms of international cooperation. Whereas the maintenance of sea, air, and space flows are resource-intensive, cyberpower demands de-territorial agility and innovativeness and, therefore, evens out power disparities. It is also noted that, although individual global domains are usually considered separately, they are intimately connected and characterized by cross-domain dependency. This report focuses on the cyber domain because of its novel cross-domain impact. The CD&E and MNE processes and their relation to military transformation and patterns of political discourse are approached. It is argued that a small state can utilize the MNE forum to gain important situational awareness over the domains and cross-domain issues, as well as facilitate the formulation of multilateral normative frameworks. This multilateral work on solidifying and securing global flows offers a more stable foundation for the main networks of global interdependence.

Introduction

Consistent and stable access to the global commons is vital for the regular and intensifying flows of information, trade and people. Securing access to these flows can be seen as crucial for a small state, which is relatively more dependent on global interlinkages due to its more specialized economy. Ultimately, the key thematic behind "securing access to the global commons" has to do with the future shape of the underlying global network of interdependence. Until now, the dynamics of deepening global interlinkages have been based on increased mutual dependency and specialization. These dynamics have created a global community that is defined by knowledge, technology, financing, and production-based structures of capability. There is a vital need to solidify these underlying loose networks and to develop a more coherent and up-to-date normative framework concerning access to the global commons. For a small state in particular, deepening interdependence has meant that not only the economy but also the security sectors have become reliant on the existence of multilateral connections. Because of this relatively high degree of interdependency, there are inherent dangers and risks if the structures supporting the interdependence are not more adequately developed and institutionalized. Globalization implies that the strategic interests of small states also extend far beyond their borders. At the same time, it is important to internationalize efforts to maintain access since the situation in which some states enjoy a commanding position over flow security is undesirable and risky.

Different global commons have qualitatively distinct implications for the global distribution of security and power. On the one hand, all global commons emphasize the need for better international cooperation and institution building. However, there is also a need to consider the changing nature of states and their power, especially when dealing with the challenge posed by the cyber dimension. Similar to the sea, air and space dimensions, which each challenged the prevalent geopolitical axioms of their time, the cyber dimension does not only reflect the current global power hierarchy. Instead of being customary power politics by other means, the cyber dimension has fundamental implications for the nature of power and states. Moreover, different states face different adaptive needs and requirements for

capabilities that need to be considered in developing normative and institutional frameworks. From the small state perspective, globalization has been particularly problematic. In general, power has been flowing away from all states to structural forces such as the financial markets, and from small states to big states. To counteract this loss of power, small states have traditionally concentrated their efforts on building multilateral institutions and on participating in key international forums where collective decisions are being taken.

Bearing the importance of multilateral institutions in mind, the changing nature of state practices in the different global domains is the key to understanding the ramifications of Multinational Experiment (MNE) 7. The cyber domain is particularly important because it affects the traditional notions of power and the distribution of military capabilities. But what is meant by defence in the cyber domain? What type of actor does cyberspace favour? How can customary state features and services be maintained in cyberspace? It is clear that a range of activities – from popular protests, and skirmishes between nations, to terror attacks – are going to have a cyber dimension. The consequences of this aspect are still being debated: Some argue for the possibility of cyber wars that would cause widespread havoc comparable to that caused by actual physical war or a pandemic[1], while others claim that the effects of the cyber dimension are less drastic and should not be treated with hyperbole[2]. Despite the debate over the right metaphors and frameworks for assessing the implications of the cyber dimension, it is clear that the realm of state power is going to undergo a major transformation as much of people's lives increasingly takes place in and through cyberspace. Cyberspace enables the creation of communities, patterns of political loyalty, and forms of legitimacy irrespective of territorial distance. How will these new social formations interact with traditional territorial arrangements such as the state? How to create situational awareness of these new types of actors? How do they interact with different groupings such as terror networks, which constitute sources of insecurity? There needs to be a better understanding of the changing nature of power in the global context. When distance and territory matter less, attention should turn to dynamics, flows, and mobility. This calls for a better appreciation of the dynamic paradigm.

[1] e.g. Clark and Knake 2010
[2] Sommer and Brown 2010

During Roman times, the outer boundary of the empire was in constant flux. It was more of a zone or an interstitial area, as opposed to one which could be precisely defined. Roads were far more important for the Romans as the defining feature of their empire. They expended considerable resources on their defence in order to maintain regular connections between the centre and the peripheries. In a way, the roads were the limits of Rome. This historical anecdote illustrates how the global flows through the global commons can be understood as the main objects of securing, instead of the usual territorial entities. These flows need to be made resilient and their regularity guaranteed for the global community to flourish. In some cases, the emphasis is more on securing the flows than on the continued viability of territorial states. For example, the massive global flow through Suez to the Indian Ocean and beyond is being secured even when Somalia's state failure poses considerable piracy challenges. It is clear that a technologically developed and economically specialized state like Finland has much at stake in maintaining flow security and the resilience of the global flows. This stake requires active participation in the multilateral management of the global commons. The centrality of this challenge is further accentuated by the likelihood of the following two future scenarios: 1. The US-led Western hegemony is likely to decline and give rise to an era of state fragility, failures, and interventions; 2. The rise of new powers will challenge the systems of global governance that have been built by the transatlantic community. The overriding scenario is that global flows will become increasingly contested as access to them is becoming constrained by technological problems, sheer volume congestion, and political disruptions.

Securing the global commons

Global commons can be understood as a reiterative game. Multiple players (that is, states), based on their self-interest, tend to deplete a shared resource despite the fact that it is not in anyone's interest. This "tragedy of commons" impacts small states in particular as their agency and power depend on the existence of shared resources and governing norms. The global commons (sea, air, space, and cyber domains) benefit all actors. However, access to these commons can easily become an object of competition where one (or more) actor(s) can gain a commanding position. For a small state like Finland, participating in international normative and governance structures that secure access to the global commons is the preferred option. It should be noted that the institutional and normative foundation of the global commons is, in some cases, based on regional alliances. Over time, these alliances can develop their own competing legal and policy frameworks. For example, a rising power like China can spearhead the development of its own normative framework to rival the US-centric one. A situation in which the frameworks for the global commons are less than global would make the situation very cumbersome for a small state that is reliant on long-distance commerce.

Global commons are domains that are not controlled by any single state; rather, they are universally needed and thus should be shared. These areas, or functions, of cooperation deemed to be central to life have traditionally included the high seas, airspace, and outer space. However, new issue areas, for example cyberspace, have recently been added to the list of global commons.[3] The term "global commons" is derived from old English law where the commons refer to tracts of land shared by villagers (such as the village square or common grazing land), and without which the village as an assemblage of people could not have come together.

An organism's basic needs are fulfilled by resources. An important conceptual distinction can be drawn between *natural resources* and *spatial extension resources*.[4] Natural resources refer to materials that can be extracted from nature and

[3] Many include the polar areas and the electromagnetic spectrum in this listing.
[4] Buck 1998, 3.

which have biological, economic, social, and political value (such as minerals). Spatial extension resources are valuable because of their location, irrespective of whether they can be extracted, converted, and refined. For example, it is evident that in the global age global connectedness is a fundamental need. This connectedness has to occur somewhere – for example on the high seas – with the result that these spatial places and locations can be seen as central *resource domains*. The root concept has been extended to cover the common functions between sovereign territorial states. Global commons are not only functions, they are also international practices that are focused on the basic needs of modern sovereign states. As a key contemporary practice, "global commons" is an evolving concept. As the needs and functions of states expand and evolve, the practice of global commons is duly extended and becomes stronger.[5]

[5] In order to further conceptualize the meaning of global commons, it is important to consider the legal practice of property and ownership. Property can be understood in terms of property rights where an individual or state has rights over certain resources guaranteed by a specific legal regime. The legal context of *res publica*, deriving from Roman law, stipulates that certain properties were held by public authorities for the benefit of the public. *Res publica* rights have covered roads, public places, territorial waters, and rivers. However, certain resources have been regarded as falling outside property rights altogether (i.e. *res communes*) such as air, abandoned objects, and property that has not been acquired by any entity. The idea of global commons also includes realms and domains that are hard to conceive of as being acquirable by any agent so as to exclude others from them. Furthermore, these commons would have a high subtractability – more specifically, their use by a single entity would subtract much of the inherent value of the "common" (Buck 1998, 5).

Global domains and power

During the 1990s, the conceptualizations of global governance structures became increasingly risk-sensitive. This need to gain awareness and control over multi-level sources of vulnerability and insecurity led to the development of institutions geared towards comprehensive resource management. The global commons increasingly came to be seen as public spaces to be monitored, measured, administrated, and regulated. Due to the multiple sources of perceived risks – ranging from pandemics and global warming to nuclear proliferation – the emerging governance solutions were global and multi-level in nature. The deepening and enlarging European Union embodied these new governance trends, and constitutes a complex system of institutional arrangements today. Fundamentally, the institutional solutions delegate and spin off state-based sovereignty upwards, downwards, and sideways. The result is an emergent networked sovereignty system, or a network state where sovereignty is shared. This networked sovereignty system involves the territorial dimension as well as various functional fields such as global health, transportation, trade, and economy. At the same time, the states have continued to coexist with other emerging forms of authority. However, as parts of the networks, the states have become qualitatively different as different states operate in an increasingly complex network society held together by overlapping interests, institutions, regimes, and norms. The overlapping network fabrics are not evenly spread throughout the global space. They cluster and nest in some places more than others. This means that the access to global networks is conditional on the proximity to the global hubs or network clusters which represent the main portals to the multi-dimensional global interconnectedness.[6]

Different global commons have distinct domain-specific consequences for the clustering of the global networks and for the emergence of global hubs. For example, the political patterns formed by the system of territorial states do not translate one to one to global commons. Qualities such as sovereignty do not have clear-cut correspondence in sea and air domains, and in space and cyberspace the

[6] The centres of interconnectedness – i.e. hubs – can be thought of as the command and control centres around which diverse networks of actors coordinate and manage their intertwined activities.

situation is even more ambiguous. Most importantly, power is manifested via different dynamics outside the system of sovereign territorial states. Joseph Nye notes a distinct difference. Power can be seen as having a historical continuity in the state system: the rise of one predominant power follows the decline of another. Thus, power remains constant from the historical perspective. However, the power dynamics of the new domains such as cyberspace are distinct from this historical pattern: "*The problem for all states in today's information age is that more things are happening outside the control of even the most powerful states.*[7] The cyber domain tends to flatten state-based power hierarchies. Its inherent dynamic favours swarms of collaborative networks instead of the usual hierarchical distribution of military capabilities.

Thus, it seems that the new global commons as power domains can give rise to tendencies that have not hitherto been present in the post-Cold War American moment. Nye further notes that the cyber domain tends to distribute power in a more diffuse way. In other words, relative power is not transferred from one state to another. Rather, in the domain of cyberspace, power favours asymmetrical actors and discounts the economies of size of the predominant states: "*States will become much less central to people's lives. People will live by multiple voluntary contracts and drop in and out of communities at the click of a mouse"*.[8] The resulting "politics of mouse clicks" and the power associated with them cannot be controlled by the traditional ideas of state sovereignty. The power of such new young urban cyber-aware people was demonstrated by the pattern of contagion that spread from Tunisia to Egypt and to other regional states during the spring of 2011. The contagions of sudden political mobilization are relatively impervious to state borders, although they still tend to take state-specific forms unique to the conditions in each state. Importantly, cyberspace can be seen to favour power flows away from states to markets and other structures composed of circulations of information. Whereas this tendency can be somewhat controlled by the bigger states – such as the Chinese system of controlling the internet – it poses a formidable challenge to smaller states with fewer resources and less bargaining power against major internet providers.

[7] Nye 2010, 1.
[8] Ibid.

It seems that the existing patterns of state power are not easily translatable into some of the global commons. This problem of incompatible power contexts forces a rethinking of the traditional notion of state-based power. The most traditional notion of power was crystallized by Robert Dahl in the 1950s. His idea was that power is an ability to cause others to do something that they would not otherwise do. This *coercive* type of power is characterized by the force, status, and influence possessed by a single unitary actor. The classical realist Hans Morgenthau saw power as having two faces: force and influence. Influence refers to the gaining of sympathy through spontaneous sentiments of mutuality, whereas force refers to situations of unilateral forceful imposition. The goal of sympathy-based power is to impose order on the other actor(s), which does not require further force and effort on the part of the first actor. Morgenthau's thinking reflected an idea of power as an ability to frame, which became increasingly important in the 1960s.[9] Other actors can identify with a particular framing in a way that they need not be coerced. In a more interest-based way, the actors can learn to co-opt a frame or agenda in a way that allows them to carry out their own preferences. Another much-quoted distinction that parallels these two faces of power is the distinction between hard and soft power.

In a more detailed review of the different facets of "power", Michael Barnett and Raymond Duvall present four different ways of understanding power: *"The concept of power is central to international relations. Yet disciplinary discussions tend to privilege only one, albeit important, form: an actor controlling another to do what that other would not otherwise do"*.[10] The authors point out that this one-dimensional view of power prevents the development of more *"sophisticated understandings of how global outcomes are produced and how actors are differentially enabled and constrained to determine their fates."* The authors emphasize that power is produced through social relations. The effects of such power constitute the capacities that actors have to influence their circumstances and fate. Depending on different types of interrelations, power can be compulsory, institutional, structural, or productive. *Compulsory power* refers to the Dahlian definition of direct control over another; *Institutional power* refers to the ability to control socially distant others through rules and procedures constituting an

[9] *Cf.* Baldwin 2002.
[10] Barnett and Duvall 2005, 39.

institution; *Structural power* refers to the direct and mutual constitution of the capacities of actors; *Productive power* refers to the continuous and agile production of actor-ness through often diffuse and ad-hoc social relations. These distinctions offer a more fine-tuned understanding of the power-related repercussions that different global commons entail.

The fourth type, productive power, is the least known. Yet, it seems to be particularly pertinent to the cyberspace domain which Nye defines as tending to flatten and diffuse power. Whereas structures produce hierarchical superiority and subordination among actors, productive power stems from much more tacit, diffuse, and situational knowledge formations. These formations are often ad hoc, spontaneous, and fleeting in ways that cannot be captured by formal institutions or structures. Productive power requires situational awareness over the rapidly changing scenarios. Strict adherence to static institutional settings and structural formations is anathema to this kind of power.

The debate on the different faces of power and the power-related repercussions of the distinct global commons can elaborate how the global commons change traditional power and how power is going to evolve in the future. Nye articulates a type of power that is specific to the cyber domain, cyberpower.[11] This power is based on the ability to exploit flows of information in the interconnected networks, which have spread exponentially since the late 1960s. These expanding networks have altered the way people associate, what is meant by the concepts of political and social, and how territory and distance are framed. The idea of state-produced cyber security is a relatively recent phenomenon. The physical nature of the underlying technology – servers and infrastructures – provides obvious yet traditional clues about how to control cyberspace. However, although the physicality of the information networks is a tempting bridgehead into cyber security, the virtual dimensions can be regarded as an emergent, constantly evolving quality which, to a degree, challenges an approach based on the physicality of cyberspace. Nye defines cyberpower as the ability to obtain preferred outcomes by strategically using the

[11] Nye 2010, 3.

virtually interlinked information resources.[12] Cyberpower can refer to the ability to produce such outcomes within the cyber domain and/or draw capacities outside of the cyber domain. For example, the Stuxnet virus that targeted the Iranian nuclear programme in 2010 shows how assumingly state-based agencies could use cyberpower to realize their national security interests.

[12] Nye 2010, 4.

Characteristics of power, mobility and flows

Cyberspace can be said to have its own domain-specific power consequences. The other global domains have similar power-related dynamics. One common element is that power becomes "flow-like" instead of referring solely to a spatial distribution of military capabilities. The ability to secure and/or command global flows of goods, people, and information becomes a key ingredient of what is meant by power in the context of global commons. For a small state acting alone, such production of power is increasingly difficult. At the minimum, it calls for a new type of thinking that goes beyond the traditional state imagery highlighting territorial sovereignty.

Although the relationship is still under-examined, power and mobility are highly interchangeable concepts in the Western security-related thinking. Supported by the recent focus on networks, power is increasingly seen as being on the move, as a movable property, and mobile entities are similarly regarded as powerful. The effects of this nexus are seen in various global flows and circulations that intertwine with the power of various territorial states. As a result, it is increasingly difficult to conceive of any power, military or political, that is lacking in these dynamics.

The flows and moves of global power accord with different trajectories in different global domains. Cyberspace was presented as an example of a domain that has its own type of power dynamic. The other domains discussed in this section – space, sea, and air – all have their unique tendencies that determine how power flows through them. These dynamic flows are relatively unbound by territorial boundaries. Any meaningful utilization of power in any of the aforementioned four domains is affected by the patterns and logics of the flow specificity. Any action has to tap into the resource pool of these flows. This is even more pertinent in a world where states and their security structures are increasingly dependent on the flow of information in cyberspace. This means that the flow cannot easily be turned off through kinetically destroying the underlying physical infrastructure. States need to use cyberpower to influence and create the desired forms of flow security. Moreover, action and reaction sequences easily generate vortexes and turbulences in the vital flows that influence international politics and create sources of security and insecurity.

Modern transportation infrastructures and technologies have allowed for increasing control over distance and territory. These land, sea, air, space, and cyber networks have made distance a relatively manageable obstacle.[13] In this new dynamic context, power becomes as movable as possible with the result that such "movability" becomes a crucial marker or signifier of power. For example, a cyber attack that interferes with the flow of information derives much of its power from its ability to signify actual or potential failures of regular "movability". Because power has become mobile, any disruptions to the flows signify power failures and, therefore, become security concerns.

It seems that the recent expansion of political horizons was not any physical barrier or territorial extension, but a breakthrough in making power as movable as possible and, in practice, engineering various technologies of mobility to solve the obstacles to the emergence of a truly mobile form of political power. This logic of Western movable power has led to the establishment of a relatively de-territorial and de-centralized structure based on a network structure of political power.[14] From this perspective, it should be noted that there is a need to move beyond spatiality, which is inherent in the "network" metaphor. The emergent power-political context is not static; instead it is a dynamic flow where nodal points may move. Perhaps the most tangible embodiment of mobile power has been the crafting of the air carrier battle groups. Kaplan describes aircraft carriers as *"the supreme icon of American wealth and power"*[15] and Horowitz declares that *"short of the atomic bomb, nothing signifies the power of a great nation like ... a fleet of aircraft carriers"*[16]. This spectacle of "power on the move" conveys strong symbolic meanings and emotional experiences.

Air carrier battle groups embody what can be termed cross-domain entities. Such entities draw on synergic interaction from multiple domains. The cross-domain features are present in many contemporary tactics. For example, the aforementioned

[13] E.g. Daileda 2008, 225.
[14] Hardt and Negri 2001, xi-xiii, 160.
[15] Kaplan 2005, 53.
[16] Horowitz 2010, 65.

Stuxnet virus that contaminated Iranian nuclear facilities in late 2009 and again in 2010 was part of a larger coordinated covert operation launched to sabotage the Iranian nuclear programme. It is likely that cyber tools will be used in combination with other efforts in the future to maximize their effectiveness and to undermine the probability of retaliation, although it is likely that the Stuxnet breed of tools will be quickly adapted by states like Iran as well as diverse transnational actors.

One way of understanding the cross-domain interactions between various tools, such as sea, air, space, and cyber-based applications, is to compare them with swarming tactics. Swarming refers to the splitting of large units and turning them into a larger number of self-sufficient, highly mobile, and autonomous units. These swarming units form situational networks that may assemble and disassemble as specific needs, contexts, and goals change. The swarming approach is based on the idea that one needs to be aware of, respond and adapt to changes in situational dynamics. These entities are characterized by continual reflexivity, self-monitoring, and self-repair. It is possible to see how the coordination of the interaction between different swarming entities can bring about huge situational benefits. For example, the Stuxnet virus can be seen as a swarming unit. Its effectiveness was, according to some sources, reinforced by other simultaneous activities *vis-à-vis* Iran that used more traditional methods of sabotage and undercover warfare. Such interactions can bring unforeseen and serendipitous benefits.

An examination of flow security can seek to shed light on the wider entanglements of contemporary power mobility with the dynamics of power(s) on the move in and across various global domains. These entanglements with status, influence and power were very much in play, for example, during the volcanic ash episode of late April 2010 that closed much of the European airspace. Peoples' lives became interconnected across territorial boundaries. The stoppage of air flow demonstrated how highly dependent political life is on smooth global flows.

This could suggest that, as people and information flow, power is on the move and finds its expressive language in the perceived tempos of the mobility. For example, the humming regularity of the flows within national, regional, and global aeromobility systems constitute and signify the power of the "movers" in global

politics. The opposite is equally expressive: The regular disturbances in the hub-and-spoke dynamics translate into a lack of, or decrease in, power.[17] Related to this idea, the trajectories of power in the contemporary world are comparable to successes and failures of mobility. For a flow to catch on and convey power, it has to produce a sense of moving smoothly. For a global actor to demonstrate its status, it is vital to visibly meet the challenges posed by the perceived hostile or rogue elements, which in the case of aeromobility range from terrorism and pandemics to volcanic ash.

Global circulations are increasingly energetic flows: Although they are fragile, they possess vigour. The security of the air flows and circuitry – namely flow security[18] – is dependent on the underlying hub-and-spoke structure. Paradoxically, this highly directed circulation cannot eliminate the factor of being exposed to complex sources of "eddies". These eddies create over-flows, by-flows, and side-whirls that may even run counter to and interfere with the intended directionality of the overall dynamic. We have all experienced these as delays, cancellations, temper tantrums as well as flights hitting turbulence. The sources of flow insecurity are complex, and many of them are very hard to predict. For example, few of us have experienced the link between air travel and the violent eruptions of the earth's underground magma chambers. Yet the potential consequences of this link have changed in magnitude due to the exponential growth in modern aeromobility circuitry. This change went largely unrecognized until the 2010 Icelandic eruption. The facts of the case are well known. The eruption of the Eyjafjallajökull volcano in Iceland in late April 2010, although relatively small, caused the largest air travel disruption in Europe since the Second World War. In the end, the ash particles, which can occasionally cause rough, and even dangerous, flights, engendered complex entanglements that

[17] The tight conceptual bridge between imperial governance structures and hub-and-spoke political architecture is often referred to in the research literature (e.g. Motryl 1999; Hafner-Burton et al. 2009; Kelly 2007; Smith 2005). For example, Phillips (2005, 3) sees a distinctly "hub and spoke" set of regionalist arrangements in the Americas as having allowed the U.S. to "capture control of the governance agenda and to ensure that the regional economic regime takes a form consistent with U.S. interest and preferences".

[18] E.g. "Without necessarily making territorial security less important, I would argue that "flow security" is the true challenge for the decades to come." Swedish Foreign Minister Carl Bildt, Mexico City, 8 February 2010; www.sweden.gov.se/sb/d/7417/a/139273.

reinforced the sense that aeromobility flow is as fragile as it is crucial for the interdependent Western economies and polities.

Moving further beyond the spatial imagery of the network, the mobility paradigm[19] is increasingly useful because it highlights fluidities and circulations. Without a due understanding of time, mobility as a function of both time and space cannot be adequately described. Qualitatively different velocities, accelerations, and decelerations bring necessary elements to the understanding of circular fluidities. The aeromobility network can be seen as a dynamic kinesthetic context. Knox et al.[20] citing Castells[21] call them "spaces of flows" that emphasize temporal qualities such as process, speed, improvisation, and flexibility over more spatial notions of space and networks. Castells defined a flow as a "*purposeful, repetitive, programmable sequence of exchange and interaction between physically disjointed positions held by social actors".*[22]

It seems that Castells' remark concerning the sequential character of the flow is quite correct: The aeromobility flow contains a step-by-step and move-by-move type of pattern. Aeromobility is in a perpetually reactive mode of experiencing different types of disruptions – eddies. This agitation has been referred to as "constant-shock syndrome": "*There is no doubt that the public has become highly sensitized to risk, both real and perceived. Besides the passengers, the airport itself has emerged as a dynamic context of continual reflexivity, self-monitoring, and self-repair".*[23] The flow dynamic is seen as having *resilience*. The key question in this context is how to increase the resilience of the central global flow. The flow's underlying mechanisms fail here and there, yet the flow also interacts with other circulations in a fashion that may appear random to a casual observer. The rhythmic pulse of the flow is such that, besides producing a sense of sequential monotony, it brings forth the contrivances within a broader temporal context of social interaction: "*The accumulation of factors – 9/11, the bombings in Bali and the Philippines, the Iraq war – meant that the arrival of the 'killer mystery virus [SARS]' hit a nerve that was well and truly*

[19] e.g. Urry 2008
[20] Knox et al. 2007, 265.
[21] Castells, 1996.
[22] Castells 1996, 412.
[23] Knox et al. 2007, 266.

exposed".[24] Airlines are vulnerable to world economic (e.g. the 2008 recession) and geo-political (e.g. 9/11) events as well as to pandemics (e.g. SARS), natural catastrophes (e.g. the ash cloud episode), and accidents (e.g. the crash of the plane carrying the Polish political elite).

The dynamic network models that stem from the studies of modernity's central infrastructure tend to highlight the paradigm of resilience. The way in which public bodies are integrated into different global commons has to be based on rethinking the processes for assessing risk. This rethinking should be informed by an ability to withstand and recover from crises and emergencies. In building resilient societies, there is much to be learnt from the adaptive capabilities of the airspace infrastructures. Indeed, they can be used as a model for more resilient societies. Comprehensive security and effective defence require adapting a more holistic perspective that focuses on the dynamic interactions between different interacting global flows.

Without the monitoring and awareness systems granting overall access to information concerning the changing situational flows, one is left perilously blind and uncoordinated. One needs to develop situational awareness over situationally changing patterns or pulses in the complex global flows. Such productive or ad-hoc knowhow provides a foundation of resilient entities that can flourish in the complexities of global circulations. These global pulses are often ad hoc, spontaneous and fleeting in ways that cannot be captured by formal institutions or decision-making procedures. For a small state to have the requisite productive power, it needs to develop situational awareness over the rapidly changing situational scenarios. The opposite of this is a strict adherence to static institutional settings and structural formations. In many ways, the realm of productive power is becoming increasingly important for a number of reasons, including the shortening news cycle, more complex vulnerabilities, sudden shocks, and the need for more resilient systems. However, the most relevant reason for such productive agility is the need to tap into one of the central global resources, into global flows.

[24] Thomas 2003, 30.

The cyber challenge

The main difference between the cyber domain and other global commons is that the cyber domain is entirely a human creation. It is layered and contains physical infrastructure and systems as well as logical systems. According to Zimet & Skoudis, the cyber domain can be divided into the Systems domain (technical foundation, infrastructure, architecture); the Content and application domain (information base and mechanisms for accessing and processing that info); the People and social domain; and the Governance domain, which overlays the others.[25]

This division reflects the character of cyberspace. The Systems domain resides mostly in the physical world, in national territories or global commons of sea and space. These parts of the cyber domain can be affected by direct physical acts. The other subdomains, on the other hand, transcend territorial borders and make geographical distance irrelevant. As such, the cyber domain provides new channels for human interaction. This transcendent nature of the cyber domain also makes it difficult to govern. At the same time, even some basic concepts have not been unequivocally defined. What, for example, is the precise relationship between the internet and the cyber domain? Are they synonymous or do they denote different things?

Computer and software trends promise more (computing) power for the machines that are constitutive elements of the cyber domain.[26] This allows for even more extensive utilization of the cyber domain for different purposes. Combined with digital convergence, which is connecting everything from household appliances to the internet, it gives rise to new possibilities, but also to increased risks. More and more systems are becoming increasingly dependent on the functioning of the internet and cyber domain-based services. Any disturbance has significant potential ramifications for states and societies, making the cyber domain a source of risks.[27]

[25] Zimet & Skoudis 2009.
[26] Skoudis 2009.
[27] For example, the Finnish Security Strategy for Society (*Yhteiskunnan turvallisuusstrategia*) enacted in late 2010 (available in Finnish at: www.defmin.fi/files/1696/Yhteiskunnan_turvallisuusstrategia_2010.pdf) enumerates

In addition, different, albeit benign, attempts in the developed countries to provide an ever larger proportion of the population with high speed internet access underline the need to swiftly create clear rules and effective governance for the cyber domain.

Key characteristics of the cyber domain

Distance has no meaning in cyberspace. Cyberspace negates physical distance, which has hitherto been the basis of human commonality. Because of this, cyberspace changes the way that people come together, associate, and form communities. It is a domain of high connectivity that transcends physical distance and space. This non-existence of physical distance in the cyber domain is one of its most distinct features. There is no space in cyberspace in the spatial sense. Intangible, yet connected to the physical world through nodes and "portals" (cables in the sea, and so forth), the nature of the cyber domain encourages and facilitates global communications, connectedness, and commonality. For example, news reporting cycles have shortened and ordinary people also have the possibility to broadcast to global audiences. Global economics and trade are also relying more and more on smooth flows of information – now increasingly carried in the cyber domain.

The potential disruptions to information flows increase the fragility of the developed states. At the same time, the inequality of the technological infrastructures highlights power disparities as developed economies can benefit from highly efficient information sharing systems. Opportunities as well as risks have duly grown.

The rapid development and inherent risks highlight the need for better governance and regulatory frameworks. Governance of the cyber domain is still in its infancy and despite the best efforts of national governments, this domain remains under-governed as no state can impose its will on the global commons. Despite being hailed as the domain of free speech, many governments, including those in the

14 different threat models for the vital functions of society. At least 12 of these include the cyber dimension as one of the elements constituting the particular threat model.

Western world, often choose to restrict the internet in various ways.[28] In addition to direct control, indirect methods of internal control are applied. For example, it has been argued that China's massive use of cyber units or "cyber militia" is an indirect way to control and involve people active in the cyber domain, and potentially dangerous, who "are thus co-opted by the state and become less likely to turn against the regime".[29]

No formal channels exist to coherently arbitrate issues arising in the cyber domain. Questions abound, like the extent to which a state is responsible for cyber attacks emanating from or directed through servers physically located in its territory. In the case of small states, such governance issues are accentuated for the very reason that almost any cyber infringement easily acquires a transnational dimension.

Nye[30] has rightly observed that the cyber domain is a factor transforming state-based power hierarchies. Although the domain can be seen to distribute power more widely, and flatten the power hierarchies, the point should not be overstressed as modern nations still exercise power that is incredible in scale and pervasiveness compared to their historical predecessors just a century or two ago. Many Western powers have much greater capacity for control and surveillance than they had previously. However, the ability to process and centralize a massive amount of information might increase the inherent risks, as the Wikileaks incidents illustrate. Furthermore, the cyber realm is just one more realm for the pervasive (mostly soft) power of states. While the cyber domain redistributes and changes some of the ways power is localized, it can still be argued that this domain can add to state power rather than diminish it in any significant way.

Nevertheless, the cyber domain challenges traditional key concepts such as those related to sovereignty and freedom of access. Can traffic in the cyber domain be controlled effectively, and should such an attempt even be made? Can a state mirror itself in the cyber domain in its familiar form or are the specifics of the cyber domain going to radically alter the way in which we regard states, their security,

[28] Nye 2010, 8.
[29] Klimburg 2011, 44–48.
[30] Nye 2010, 1–2.

power, and defence? Questions like these are becoming increasingly critical as more and more functions of society at every level rely on the smooth functioning of and access to the cyber domain. This creates new potential risks that have to be thwarted. A risk-aware society is concerned about risks that carry with them severe consequences if realized. Flows in the global commons must consequently be ascertained, which increases the need for risk management and preventive action.[31]

Types of cyber attack and the problem of attribution

Malicious activities that can be carried out in the cyber domain, so-called cyber attacks, include cyber warfare and cyber crime, with its subsets of cyber vandalism, cyber espionage and cyber terrorism. Preventing access to the cyber domain altogether could also be characterized as a cyber attack.

Typologies of cyber attacks have been developed[32], but classifications remain somewhat vague and are still under-defined, reflecting the evolving praxis. One aim for international cooperation could be to clearly define and differentiate between different types of cyber attacks. On the other hand, net activism or cyber demonstrations, such as electronic civil disobedience[33], should not automatically be classified as cyber crime or worse.

Because distance is conflated in the cyber domain, problems related to cyber warfare and other forms of malicious cyber activity are connected to a complete absence of warning and the short timeframes involved when under attack or under a malign influence. Possible malicious activities are hard to anticipate, and even harder to deter, making effective preventive measures and responses difficult to coordinate and initiate in a timely fashion.

When it comes to cyber attacks, the most pressing issue is that of attribution. Was the harm/destruction-causing event (virtual or otherwise) in the cyber domain an attack or an accident? What was the intent behind the action if it was intentional?

[31] cf. Heng 2006; Coker 2009.
[32] e.g. Lachow 2009; cf. Palojärvi 2009, 27–45.
[33] cf. Meikle 2009.

Where did the attack originate from? Who is responsible? In the cyber domain it is exceedingly difficult to identify the perpetrator or even, at times, to distinguish an attack from an accident.

Collaborative international mechanisms for investigating cyber attacks (and for laying blame) are needed, especially from a small-state perspective. Capabilities for real-time attribution when under attack are also needed for the offence that is an integral part of defence in the cyber domain. There can be no defence in cyberspace without offensive capabilities.

Societal effects

The cyber domain has created new social domains and new activism, giving rise to political online communities that are easy to take part in and easy to depart from. Willing non-governmental groupings may even develop or gain access to cyber weapons. On the net, likeminded people can always be located – for better or for worse, generating beneficial movements but also cyber extremism.[34] For example, unhealthy ways of showing nationalistic feelings can be found in the cyber domain, as demonstrated in October 2009 when Egyptian and Algerian activists fought in cyberspace before a football World Cup qualifying match between their respective countries.[35]

Through online forums and websites, radical and extremist individuals may be connected to relatively non-state-centric and de-territorialized global societal spaces. State-based authoritarian socialization and guidance is missing in these new contexts, and there is no clear authority presiding over the complex networks. Blogs and other swift and novel ways to bypass and complement traditional newsfeed decrease the power of states to define and frame issues.[36] The cyber domain also creates new political discourse because, as Shirky puts it, "[a]ccess to information is far less important, politically, than access to conversation".[37]

[34] E.g. Egerton 2009.
[35] Michael 2010, 17.
[36] Touri 2009.
[37] Shirky 2011, 35.

States have tried to develop different solutions to "moderate" the different internet sites. In the absence of an overarching moderating authority, the state preference is for surveillance. If carried out collectively at the international level, the ability to control and moderate cyber domain activity is clearly distributed unevenly among states. Small states may not have the means to control internet traffic, which might be routed through servers which are not in their territory.

Online communities are often forged across national borders. These spontaneous and instant online communities or movements, which can dissolve as quickly as they spread, create new modes of interaction and influence that formal institutions and structures struggle to adapt to. In this sense, the cyber domain favours individuals over organizations.[38] On the other hand, people, companies, and so forth, often concentrate on themselves and fail to see cyber disturbances as problems that affect everyone. Unlike a mugging in one's neighbourhood, cyber breaches against one's neighbours do not cause consternation.

The ease of access to the cyber domain, coupled with the speed of information transfer, has multiplied the opportunities for small groups to reach large audiences and, by extension, to exert considerable influence. The cyber domain provides unprecedented potential global access to information. An example of how the speed and ease of access to the cyber domain can flatten traditional power relations can be seen in the Wikileaks case. In particular, the leaking of 250,000 US State Department diplomatic documents in late 2010 marked the advent of a new era in the flow of information.[39] Before advanced computers and the internet, no one could have acquired such massive numbers of classified documents. Moreover, the internet facilitates the availability of these stolen documents. All leaks of classified documents are symptoms of the new unprecedented vulnerability of governmental functions. These hard to trace leaks are having a sharp societal impact, not least in the sphere of bureaucracy and diplomacy.

[38] cf. Nye 2010, 13.
[39] Heisbourg 2011.

Any successful national cyber strategy also has to deal with governmental information security. It is clear that all classified material could leak into the cyber domain and thus be made available to hundreds of millions of people. Administrative actions must take such eventualities into account. This newfound, potentially public nature of documents means more closed systems (and fragmentation of the cyber domain) and better protected data as well as potential complications for the established diplomatic practices and discourse. This may inadvertently lead to a certain reluctance to commit the background of decisions to writing – gradually altering the character of documents produced by bureaucracies. In the future, public archives, although open to all, may contain fewer documents of real value and explanatory power.[40] If such a development were to occur, it would serve neither the democratic ideal nor the public – not to mention blight the historians of the future.

The military perspective

The advent of the cyber domain also poses more fundamental questions related to war and warfare. The problems of attribution and the nature of damage pose further questions: What is war? How to define it in the context of cyberspace? What, for example, constitutes military action in the cyber domain? The relative ease of access to the means for rudimentary cyber attacks offers even a motivated group of computer-literate laypeople the possibility to conduct operations that could be regarded as acts of war. Opposing sides in a future war in the cyber domain need not be states, meaning that new actors have the potential to emerge.[41]

From the military point of view, the cyber domain is now in the same situation as the air domain was after World War I. During the 1920s, many theorists, like the Italian Giulio Douhet or William Mitchell of the United States tried to conceptualize and predict, as well as devise, optimal strategies for the use of the air domain by the military, while at the same time being involved in the politics and process of shaping

[40] The so-called "empty archives" phenomenon, cf. Eriksson & Östberg 2009, 118–124.
[41] For cyber warfare, see e.g. Miller & Kuehl 2009; Palojärvi 2009, 47–74; Cavelty 2010; Clarke & Knake 2010; Cornish et al. 2010; Farwell & Rohozinski 2011.

the emergent air component of the armed forces.[42] Cyber warfare and the capabilities and forces developed around it are now faced with a situation analogous to the emergent air forces back then, which was characterized by questions like: Shall we develop strategic bomber fleets to crack the enemy's will to resist, or tactical, integrated support for advancing ground forces? Or just rely on defensive short-range fighter planes and anti-aircraft artillery? In 1921, Douhet took sides in the argument about the status of future air power, calling for an independent air force completely detached from the Army and the Navy.[43] In a similar vein, should the cyber domain have its own independent cyber arm, parallel to the Air Force, Army and Navy?

Military involvement in the cyber domain also creates the potential problem of drifting into a constantly widening and more undefined, discursive use of the term "war". If everything is war, or can be interpreted and construed as such, what is to become of ordinary political struggle and debate? Can the cyber domain governance issues and questions of "defence", access and protection militarize politics if these issues are framed primarily in a military context or by using warfighting concepts? What organization or actor at the national level should take the lead in cyber-related issues? To what extent should the military be involved in securing access to the cyber domain?

[42] Douhet 1999 [1921]; Mitchell 1999 [1925]; cf. Kerttunen 2010, 26–27.
[43] e.g. Douhet 1999 [1921], 304–306.

Military transformation and political influence (CD&E and MNE)

Having examined the characteristics of the global commons in general, and the cyber domain in particular, we will discuss one way in which the international military community is seeking to ensure and develop its influence over the commons.

"Securing access to the commons" has been raised as a study theme of the Multinational Experimentation (MNE) cycle that began in 2011, thus forming the essence of MNE7. In this section, the methodological framework of MNE will be briefly introduced, namely Concept Development and Experimentation (CDE). Then, a short history of MNE will be provided. First, however, we will sketch a brief historical overview of the US-NATO transformation, as both MNE and CDE have their roots here.

Military transformation

The first Gulf War in 1991 has been identified as a catalyst for the use of information technology as the basis for military development. Raitasalo ties this to the decline of the Soviet threat. High technology, and information technology in particular, was seen to change the nature of war. The marketing of this vision to Europe started in the late 1990s. In the 1999 NATO summit, the Defense Capabilities Initiative (DCI) was launched to ensure interoperability amongst the allies and to update capabilities in the face of perceived threats. Although the DCI was not noticeably successful, the perceived change in the security environment a year after 9/11 led to a transformational process within the alliance (Raitasalo, 2008: 44-51; cf. NATO, 2001: 50-52). Although the transformation process had already begun prior to 9/11, it led to a new sense of urgency in the United States.[44]

[44] For example, to quote President Bush: "The need for military transformation was clear before the conflict in Afghanistan, and before September the 11th …What's different today is our sense of urgency – the need to build this future force while fighting a present war. It's like overhauling an engine while you're going at 80 miles an hour. Yet we have no other choice." Bush, G. W. 2001. *President Speaks on War Effort to Citadel Cadets* [Online]. Washington DC: Office of the Press Secretary. Available at:

These developments naturally had an impact on NATO as well. As a consequence, and with the aim of addressing security issues in a global context, NATO began to recognize the need for "softer" crisis management mechanisms, including humanitarian relief. Moreover, NATO saw asymmetrical threats, often stemming from the underdeveloped, crisis-ridden areas of the world, as its source of future threat. In response, NATO realized a need for new ways of thinking to ensure success in these missions. Success was seen to be achievable only if military ways and means were coordinated and supported with the application of the political, civil and economic instruments of the allied nations' power.[45]

The key elements of the transformation are rapid reaction forces and an increase in the quality of the Alliance's military capabilities. These elements were encapsulated in the Prague Capabilities Commitment (PCC), and the NATO Response Force (NRF), which have been utilized by European powers to increase their technological capabilities and used by the US government to pressure European governments into doing so. To ensure that NATO is influenced by the transformational processes that had started in the US a few years earlier, NATO Allied Command Transformation was relocated next to the US Military's transformational command.[46]

Despite the fact that the technological revolution in military affairs is not without its problems, advanced information technology remains one of the most, if not the most important indicator of military capability today.[47] The transformational approach focuses on the technical revolution in military affairs (RMA); the effects-based approach to operations (EBAO); and network-centric warfare (NCW).[48] Today, militaries are perceived to be in a state of constant adaptation (and thus also transformation).[49]

---

http://georgewbush-whitehouse.archives.gov/news/releases/2001/12/20011211-6.html [Accessed 26 November 2010].

[45] NATOACT: §5.

[46] Raitasalo, 2008: 52-53, NATOACT: §1–4.

[47] Raitasalo and Sipilä, 2008: 57–58.

[48] Nurmela, 2010: 18, cf. Smith, 2002, Alberts et al., 1999.

[49] Dillon and Reid, 2009: 109. Indeed, the new 2010 NATO strategic concept states: "…Allies will engage in a continuous process of reform, modernization and transformation." NATO 2010. Strategic Concept For the Defence and Security of The

Concept Development and Experimentation

The purpose of Concept Development and Experimentation (CD&E) is to serve as a tool for the aforementioned transformation process. The most important function of this tool is to provide the intellectual association for future capabilities. CD&E is rapidly gaining relevance in many military structures[50], including Finland, via the creation of the "Network Enabled Defense Development Center"[51] , which held its opening event on 1 October 2010.[52]

As a transformational tool, CD&E functions primarily by providing fillers for capability gaps, thereby supporting capability development. Capability development covers strategic analysis, identification of capability requirements, solution identification and solution implementation. CD&E is particularly instrumental when innovative answers to capability gaps are required. CD&E primarily develops conceptual solutions for capability shortfalls which have already been identified by other processes. However, it can also contribute to capability development through the introduction of previously unknown capabilities.[53] There is some debate over which of these two CD&E functions should be primary.[54]

Members of the North Atlantic Treaty Organisation. Lisbon: NATO. Additionally, as the key spokesman on US military transformation and Director of Force Transformation Arthur K. Cebrowski put it*:* "Today, when you buy a military, either you buy transformation or you buy irrelevance". Cebrowski, A. 2004. Statement of the Director of Force Transformation, Office of the Secretary of Defence, Before The Subcommittee on Terrorism Unconventional Threats and Capabilities, February 26, 2004. *Armed Services Committee, United States House of Representatives.* Washington D.C. On the other hand, the transformation discourse, a low level of experienced threats, and the limited expeditionary involvement of small states may lead to small-state military doctrines at the strategic level becoming detached from issues of operational effectiveness (Bjerga & Haaland 2010).

[50] A few examples include: the US, the UK, France, Australia, Canada, Sweden – to name a few. In Singapore, for example, CD&E is seen to provide "great competitive advantage, yielding great operational advantages and providing its practitioner with a management tool to optimize finite resources." Wah, L. K., Ong, T. & Fan, K. 2006. Experimenting with Experimentation. *Pointer,* 32.

[51] Vuorisalo's translation of: Verkostopuolustuksen Kehittämiskeskus, VPKK.

[52] FDF, 2010, Takkunen, 2010.

[53] de Nijs, 2010: 3.

[54] cf. Wah et al., 2006.

All concepts share the problem-solving aspect, which is the underlying characteristic of CD&E. This "problem" might be a non-existent military capability, or an identified need to improve an existing capability. Moreover, it can be identified or anticipated – stimulated by changes or disruptions in the security environment.[55] The problem may be solved through any action deemed necessary. Thus, a concept in the military world focuses on how a capability might be used in the future. This forward-looking feature of concepts is underlined with the notion that a concept can be developed in advance of policy or may envisage changes to current policy. The purpose of concepts is thus to be transformation-enablers and, as such, they should provide solutions to perceived problems.

Six CD&E requirements shed more light on the characteristics of the methodology. First, innovation: amongst the proponents of the methodology, CD&E has established itself as an innovative and flexible methodology for capability development. Second, resource efficiency: CD&E is seen to ensure the greatest benefit for a given investment in an environment characterized by rapid change and limited resources. Third, CD&E must provide a linkage to other processes, primarily to the capability development process. Fourth, transparency: The CD&E process should be fully transparent and involve multiple stakeholders. Fifth, coordination and integration: CD&E is a cooperative approach that contributes to organizational cohesion. Sixth and lastly, flexibility and balance: CD&E should be able to react quickly, without abandoning long- term challenges.

All concepts in CD&E should contain 1) a description of the future environment and the problem that this environment contains, 2) an analysis of problem-influencing issues, and 3) a proposal for a solution within a coherent framework. Military concepts can be viewed in terms of ways, ends and means as they are primarily descriptions of *how* things are done. The method is the essence of a concept.

[55] For example, changes in the political, social, or economic sectors; advances in technology; changes in doctrine; new objectives in an existing crisis situation or operation (due to altered political expectations for example); or other factors.

For management purposes (to help define the scope, effort, content, and relationships to and dependencies on other projects), concepts have been divided into different types. Nonetheless, an outcome in any category of concept can run across the strategic, operational, and tactical levels of warfare. The types are: 1) Strategic Level Concepts, which focus on the political and military levels of planning, decision-making, direction and execution of operations. Details of specific operational activities are omitted. 2) Operational Level Concepts that develop or improve military capabilities, and which will be utilized to accomplish strategic objectives in operations. Operational level concepts can be further divided into three sub-types: a Capstone Concept – broad operational descriptions and strategic objective requirements; an Operating Concept – provides commander-level descriptions of how to perform a military function; and a Functional Concept – identifies solutions and methodologies to solve explicit or practical capability problems.[56]

In addition, concepts have some clear requirements. First, a concept must be consistent with the vision of the war/crisis and the military's role in it, while providing sound reasoning and evidence to support its arguments. Second, the provenance (origin/source) of a concept should be clear. Since the concept might be a reaction to a change in policy, doctrine, strategic circumstances, technology or politics, concepts should clarify what shortfall is being sought and what are the contextual circumstances under which the concepts are developed. Third, a concept should seek authority by sufficient review and endorsement. Fourth, a clear writing style (language and terminology, for example) should be used in order to provide clarity. Fifth, the context of a concept should be defined in order to ascertain the relationship between the concept and existing doctrine. Sixth, a concept must be argued well and bear scrutiny, for which experimentation is the primary method. Seventh, a concept must be developed within a realistic time frame in order to be able to respond to a specific need in time. Eighth and lastly, a concept needs to

[56] de Nijs, 2010: 3. Compare this classification with that of Schmitt, who discusses military, institutional, operating, functional, and future operating concepts in: Schmitt, J. 2002. A Practical Guide for Developing and Writing Military Concepts. *DART Working Paper* [Online], 2. Available at: www.au.af.mil/au/awc/awcgate/dod/dart_guide.pdf [Accessed 19 October 2010].

justify the time and resources that were spent developing it. In other words, it must have sufficient merit.

It is important to define what experimentation is not. First, experimentation is not test and evaluation; experimentation is not research and development; and experimentation should not be equated to long-term studies. In its simplest form, experimentation is a "trial and error" methodology. Its role is primarily to determine whether a concept will be successful. This determination is carried out by providing information on whether the concept is successful or flawed (totally or partly). Thus, experimentation reduces uncertainty in the utility of the concept. Furthermore, experimentation helps identify potential issues in the concept and provides solutions for these. Experimentation can occur at each stage of concept development, including implementation. In other words, the two go hand in hand.

The process of experimentation comprises many aspects, which are categorized into three themes. The first theme (of experimentation) sets the stage for how to design valid experiments. Within the second theme, it is recognized that a campaign of experiments (including analytical activities) will generally be required to achieve successful capability development. The third and final theme discusses considerations for success in order to support the practical implementations of experiments. These themes are then sub-divided into fourteen principles.[57]

MNE: A short history

Multinational Experimentation (MNE) is a US Joint Forces Command-led (JFCOM) process which aims to create/discover crisis management capabilities to alleviate force transformation pressures that arise from operational theatres with CD&E. Moreover, it aims to create crisis management knowledge, and crisis management processes, that is, perceived best practices. Subsequently, it distributes these creations amongst participants and beyond. Participation in this "community of interest" is voluntary amongst coalition-friendly states.

[57] cf.TTCP, 2006.

Since 2001, the MNE process has been used by participating states and organizations to investigate crisis management concepts and capabilities within a frame of common interest. Instead of investigating these concepts and capabilities in live operations, MNE provides a controlled experiment scenario in which participants may test a new crisis management hypothesis iteratively. Thus, it provides a virtual scenario-setting which may be based on reality in some aspects – or can be completely artificial *vis-à-vis* current events. Moreover, MNE facilitates the development of multinational inter-agency operation models or procedures as early as the planning phase of a crisis management operation, utilizing the knowhow and material resources of the participants. As a result, MNE has been viewed as a cost-effective and safe method to create crisis management capabilities in problem areas where the participants share a common interest.[58] MNE has steadily increased its popularity in creating crisis management capabilities for the future. MNE can be seen as a process to develop capabilities, with which a coalition accomplishes its political goals and influences the adversaries' activities with the full force of the coalition's capabilities, including diplomatic, information, military, and economic activities.[59]

The MNE process began in 2001 with MNE1. At that time, the focus of the investigation was a joint force's capability for collaborative military planning in a technically distributed environment. The participants in MNE1 were Australia, Germany, the UK, and the USA. The second cycle of MNE, MNE2, began in 2003 when Canada and NATO joined the process. The research interest of MNE2 was to examine what influences the effectiveness of information distribution in a multinational environment. Then, in 2004, France joined the core MNE group and MNE3 got underway. In this third cycle, effects-based planning was at the heart of the investigation.

One result of MNE3 was that stability operations are indisputably multinational in nature and require the utilization of all resources at the disposal of a nation. This work was continued in 2006 when MNE4 examined how a multinational coalition can coordinate effects-based military planning with a multinational inter-agency

[58] MNE5, 2009.
[59] Blank et al. 2006: 4–1.

coordination group, and how to make the most of this coordination. This was the first significant attempt in the MNE process to expand "comprehensiveness" and the number of actors in coalition operations. In June 2006 (and until the end of 2008), the MNE community decided to unite previous MNE results and experiences from operations in MNE5. The goal was to examine the interdependencies between different actors within a comprehensive framework. A further aim was to develop effective interoperability between all crisis management actors for the purpose of crisis management planning and implementation. Eighteen countries participated in MNE5, along with NATO and the EU. The main aim of MNE5 was to broaden (utilizing national and international capabilities) the understanding of pre-crisis assessment, strategic policy development and planning, implementation planning, management and evaluation. The scenario used in the MNE5 experiment was an imagined regional crisis in West Africa.[60]

In MNE6 (2009–2010), the MNE community wanted to: "Improve the coalition commander's capabilities to counter irregular adversaries through harmonizing multinational civilian and military planning, execution and assessment efforts." This impact was achieved via outcomes in the study segments of cultural awareness, strategic communication, the evaluation of crisis management operations, and situational awareness.[61]

The next cycle, MNE7, began in January 2011 with the theme of "Access to the Global Commons".[62] For example, NATO considers that: "Adversaries will take the initiative and exploit Alliance vulnerabilities in both the virtual and physical domains of the global commons, including the realms of sea, air, space, and cyberspace." Access to, and "unfettered[63] use" of the commons must be ensured. Access in particular is seen as "pivotal to the success of all Alliance operations". In other words, the flows of commerce, communication and information, military capability, and governance – indeed the functioning of the global (western, liberal-democratic) system – must be ensured. One step in achieving this is to ensure safe

[60] MNE5, 2009: Chapter I (1–2), Chapter II (8–11).
[61] USJFCOM, 2009.
[62] See: http://mne.oslo.mil.no:8080/Multinatio/MNE7/MNE7Access
[63] Released from physical or mental bonds; unrestrained.

access to the commons. Thus, MNE7 is focusing its attention on the interconnections of the system, rather than on the objects of the system. Building on the logic of past MNE cycles, “flow-security” in MNE7 will be developed as a multinational inter-agency framework, as the sheer complexity of these tasks requires intensive orchestration and synchronization amongst different actors.

The cyber domain, small states and MNE

The cyber domain is a recent newcomer to the list of global commons. The smooth functioning of developed states increasingly relies on assured access to this particular domain. Yet, it is an interconnected network based and built on technologies that were not designed in the first instance for such widespread use, nor for information of such value and magnitude. It is important and challenging to create rules for the cyber domain that transcend territorial borders in many ways. Societal effects may lead to fragmentation of the cyber domain, which cannot be reversed, giving rise to more closed and protected environments. At the same time, the traditional concepts of national security tied to the state system do not transfer well to the cyber domain context.

It is easy to argue that securing access to the cyber commons and guaranteeing its usability calls for transnational action, as the cyber domain transcends national borders. Transnational collective mechanisms of investigation and attribution are also essential for any kind of credible deterrence in cyberspace (towards anyone). Also, the question of the way in which transnational arbitration in cyber-related issues could be arranged is worth pondering, as is the question of a state's responsibility for unwanted cyber activity channelling through its "virtual territory".

What sort of denial of access to, or action in, the cyber domain constitutes such an infringement that military action (also outside the cyber domain) might be warranted? Another question concerns the need to define sovereignty in the cyber domain. The militarization of cyberspace is to be avoided (without foregoing the development of effective cyber capabilities for military-related uses). Political engagement with issues related to the cyber domain would be desirable in order to create rules, if only to increase one's normative power and to sanction security measures. Soft power means may give rise to opportunities to positively affect groupings and communities in the cyber domain. A key challenge for a state is to secure the cooperation of non-state actors, be they businesses, private societies, humanitarian organizations or whatever. Change and development in the cyber domain will be a constant. Nations

must anticipate changes and be ready to adapt to the ever-evolving cyber environment.

Furthermore, the question of language and metaphors is important in connection with the cyber domain. How to define the central concepts related to this domain in a way that advances cooperation and mutual understanding? What metaphors should we use when discussing cyberspace, when the concept of "space" is already misleading in this context? Metaphors matter in that they will serve to direct our thinking and influence our perceptions of and attitudes towards the cyber domain. For example, approaching the cyber domain and cyber security via the language and metaphors of public healthcare[64] frames the issues quite differently in comparison with using the language of military security.

Previously, we discussed how power can be seen as an ability to frame (for example, the power to set the agenda). More specifically, we described how power in international politics can be seen to have four overlapping and interdependent dimensions: compulsory power, institutional power, structural power, and productive power.[65] Through multinational and multi-actor participation, MNE places some aspects of the crisis management *problematique* in the foreground, while simultaneously excluding others. Thus, through the presented understanding of power, it can be argued that as MNE is able to set an agenda, it therefore also demonstrates the use of power. Without going into a detailed account of every specific variation of power, two brief examples of productive power[66] can be given. First, it can be argued that MNE uses productive power, as it assigns understandings of subjectivity in the crisis imagery (among participants, in crisis areas). For example, which nations are depicted as "compliant" and "capable", and which nations are not? Who is the adversary and who is defined as friendly? What are these definitions exactly, and how were they arrived at? Second, it can be argued that MNE is an aspect of the "capability-gap bridging" debate, where the United States

[64] Rattray, Evans & Healey 2010.
[65] cf. Barnett and Duvall, 2005: 39–57.
[66] Productive power (indirect, constitutional): the socially diffuse production of subjectivity in systems of meaning and signification.

most certainly sets an agenda for Europe (capable and non-capable subjectivities produced).

The MNE process, and its methodological basis of CD&E, were created as products of the military transformation project, championed by the United States and facilitated by NATO. Therefore, some MNE critics have claimed that the MNE process is, in essence, agenda-setting, and thus a power demonstration by major MNE actors (the US, NATO), especially towards small, non-coalition actors. To the critical mind, MNE can be seen as a pedagogical project of the great powers, whereby the methodology of conducting military transformation is taught to the small and non-influential actors. The products of these transformations and "best practices" are then used to conduct liberalism's societal transformation projects elsewhere, for example in the Third World, via the convergence of the humanitarian and military establishments.[67] Despite the fact that MNE critics point out that participation in a great powers-led multinational military network is not really a voluntary option, it can be identified that small states choose to participate, often willingly, and even enthusiastically, for various reasons.

Through the framework presented earlier, it was seen that participation in the governing networks and processes of international politics is in the interest of small states. Finland, a small non-coalition state, has participated in the MNE process since 2004 with an extensive and cross-organizational list of participants, including the Ministries of Defence, Justice, the Interior, Transport and Communications, and Foreign Affairs, as well as the Defence Command and the Prime Minister's Office. Through the above-mentioned framework, the motive for participation can be seen to derive primarily from the political dimension, rather than from a strict domestic interpretation of capability needs. Four specific interests and goals in the MNE process have been discussed: participation products and practices should support national capability goals; they should support the development of national research and development; they should support the development of international interoperability; and finally, they should influence the development of international crisis management.

[67] Cf. Duffield, 2001; 2007.

For national decision-making, two central issues emerge here. First, the learning opportunities MNE provides and second, the development of national crisis management capabilities. The latter in particular directly affects where and how Finland can participate in crisis management operations in the future. Therefore, although it can be argued by some that MNE is a demonstration of power where the established crisis management actors set the stage for the smaller actors, MNE also provides small states with a forum in which they can pursue and refine their own political-strategic interests.[68] Areas where such interests have actualized include increased synergy, and the avoidance of development overlaps.[69] It should be remembered, however, that the resources of small states are very limited. Thus, finding a way to save resources and simultaneously develop national capabilities is often welcomed.

Moreover, as an informal community of interest which focuses on future realizations of crisis management, MNE is yet another forum in which a small state can strive to facilitate its own perceived best practices. Furthermore, a small state can utilize this forum to frame itself within a politically preferred subjectivity (e.g. coalition-friendly, responsible, and technologically adept) within a framework of major international crisis management actors.

[68] It should be remembered that the room for manoeuvre is not limitless and not without inner restrictions and control.

[69] Interests like these can manifest themselves in serendipitous ways, and via different levels of participation. For example, at times it may be beneficial to acquire a major developmental role in the MNE process, whereas, at other times, even a small participatory role can facilitate learning tremendously. This observation demonstrates the utility and versatility that the MNE process can provide for a small state.

References

ALBERTS, D., GARSTKA, J. & STEIN, F. 1999. Network Centric Warfare. CCRP.

BARNETT, M. & DUVALL, R. 2005. Power in International Politics. *International Organization*, 59**,** 39-75.

BLANK, J., SNYDER, D. & OSEN, D. 2006. *Using the Multinational Experiment 4 (MNE4) Modeling and Simulation Federation to Support Joint Experimentation* [Online]. Available at: http://ftp.rta.nato.int/Public/PubFullText/RTO/MP/RTO-MP-MSG-045/MP-MSG-045-04.pdf [Accessed 29 July 2010].

BALDWIN, D.A. 2002. Power and International Relations. In: W. CARLSNAES, T. RISSE, B.A. SIMMONS (eds.) *Handbook of International Relations*. SAGE Publications.

BJERGA, K.I. & HAALAND, T.L. 2010 Development of Military Doctrine: The Particular Case of Small States. *The Journal of Strategic Studies* vol. 33, no. 4, 505-533.

BUSH, G. W. 2001. *President Speaks on War Effort to Citadel Cadets* [Online]. Washington DC: Office of the Press Secretary. Available at: http://georgewbush-whitehouse.archives.gov/news/releases/2001/12/20011211-6.html [Accessed 26 November 2010].

CAVELTY, M.D. 2010 Cyberwar. *The Ashgate Research Companion to Modern Warfare*. G. Kassimeris & J. Buckley. Ashgate.

CEBROWSKI, A. 2004. Statement of the Director of Force Transformation, Office of the Secretary of Defence, Before The Subcommittee on Terrorism Unconventional Threats and Capabilities, February 26, 2004. *Armed Services Committee, United States House of Representatives.* Washington D.C.

CLARK, R. and Knake, R. 2010. *Cyber War: The Next Threat to National Security and What to Do About It*. New York: Ecco.

COKER, S. 2009. *War in an age of risk*. Polity.

CORNISH, P., LIVINGSTONE, D., CLEMENTE, D. & YORKE, C. 2010. *On Cyber Warfare*. A Chatham House Report. Available at: www.chathamhouse.org.uk.

DE NIJS, H. 2010. Concept Development and Experimentation Policy and Process: How Analysis Provides Rigour Available at: http://ftp.rta.nato.int/public/PubFullText/RTO/MP/RTO-MP-SAS-081/MP-SAS-081-21.doc.

DENMARK, A. M. & MULVENON, J. (eds.) 2010. *Contested Commons: The Future of American Power in a Multipolar World*. Center for a New American Security.

DILLON, M. & REID, J. 2009. *The Liberal Way of War. Killing to Make Life Live*, London and New York, Routledge.

DOUHET, G. 1999 [1921]. Command of the Air. In: D. Jablonsky (ed.) *Roots of Strategy* 4. Stackpole Books.

DUFFIELD, M. 2001. *Global Governance and the New Wars: The Merging of Development and Security*, London and New York, Zed Books.

DUFFIELD, M. 2007. *Development, Security and Unending War. Governing the world of the Peoples.*, Cambridge, Polity Press.

EGERTON, F. 2009. The Internet and militant jihadism. Global to local re-imaginings. *In*: A. KARATZOGIANNI (ed.) *Cyber Conflict and Global Politics*. Routledge.

ERIKSSON, F. & ÖSTBERG, K. 2009. The problematic freedom of information principle. The Swedish experience. In: A. FLINN & H. JONES (eds.) *Freedom of Information. Open Access, Empty Archives?* Routledge.

FARWELL, J.P. & ROHOZINSKI, R. 2011. Stuxnet and the Future of Cyber War. *Survival* vol. 53 no. 1, 23-40.

FDF. 2010. Verkostopuolustuksen Kehittämiskeskus (VPKK) viettää avajaisiaan 1.10.2010. Available at: www.puolustusvoimat.fi/fi/Puolustusvoimat/Laitokset/?urile=wcm%3Apath%3A/su%20puolustusvoimat.fi/Puolustusvoimat.fi/Puolustusvoimat/Laitokset/ [Accessed 2 November 2010].

HEISBOURG, F. 2011. Leaks and Lessons. *Survival* vol. 53 no. 1, 207-216.

HENG, Y-K 2006. *War as Risk Management. Strategy and Conflict in an Age of Globalised Risks*. Routledge.

KERTTUNEN, M. 2010. *Kuinka sota voitetaan. Sotilasstrategiasta ja sen tutkimisesta*. Maanpuolustuskorkeakoulu: Strategian laitos. Julkaisusarja 2, no 45.

KLIMBURG, A. 2011. Mobilising Cyber Power. *Survival* vol. 53 no. 1, 41-60.

LACHOW, I. 2009. Cyber Terrorism: Menace or Myth? *In*: F.D. KRAMER, S.H. STARR, L. WENTZ (eds.), C*yberpower and National Security*. National Defense University.

MEIKLE, G. 2009. Electronic civil disobedience and symbolic power. In: A. KARATZOGIANNI (ed.) *Cyber Conflict and Global Politics*. Routledge.

MICHAEL, A. 2010. *Cyber Probing: The Politicisation of Virtual Attack*. Special Series. Defence Academy of the United Kingdom.

MILLER, R.A. & KUEHL, D.T 2009. Cyberspace and the "First Battle" in 21st-century War. *Defense Horizons* 68.

MITCHELL, W. 1999 [1925]. Winged Defense. In: D. JABLONSKY (ed.). *Roots of Strategy* 4. Stackpole Books.

MNE5. 2009. *Multinational Experiment 5 - Key Elements of a Comprehensive Approach: A Compendium of Solutions* [Online]. The United States Joint Forces Command (USJFCOM). Available at: www.defmin.fi/files/1433/ MNE5_Compendium_Mar2009_PUBLIC.pdf [Accessed 29 July 2010].

NATO 2001. NATO Handbook 2001. *Chapter 2: The Transformation of the Alliance*. Brussels: NATO Office of Information and Press.

NATO 2010. Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation. Lisbon: NATO.

NATOACT Understanding NATO Military Transformation.

NURMELA, T. 2010. *The Social Battlespace of Stabilization Operations - action amongst the People,* Helsinki, Edita Prima Oy.

NYE, J. S. 2010, *Cyber Power*. Harvard Kennedy School, Belfer Center.

PALOJÄRVI, P. 2009. *A Battle in Bits and Bytes: Computer Network Attacks and the Law of Armed Conflict*. The Erik Castrén Research Reports 27/2009.

RAITASALO, J. 2008. Sodankäynnin vallankumous - realistinen visio vai virhearvio? In: RAITASALO, J. & SIPILÄ, J. (eds.) *Sota – teoria ja todellisuus. Näkökulmia sodan muutokseen.* Helsinki: Edita Prima Oy.

RAITASALO, J. & SIPILÄ, J. (eds.) 2008. *Sota - teoria ja todellisuus. Näkökulmia sodan muutokseen,* Helsinki: Edita Prima Oy.

RATTRAY, G., EVANS, C. & HEALEY, J. 2010. American Security in the Cyber Commons. In: A. M DENMARK, & J. MULVENON (eds.) *Contested Commons: The Future of American Power in a Multipolar World*. Center for a New American Security.

SCHMITT, J. 2002. A Practical Guide for Developing and Writing Military Concepts. *DART Working Paper* [Online], 2. Available at: www.au.af.mil/au/awc/awcgate/dod/dart_guide.pdf [Accessed 19 October 2010].

SHIRKY, C. 2011 The Political Power of Social Media. Technology, the Public Sphere, and Political Change. *Foreign Affairs* vol. 90, no. 1, 28–41.

SKOUDIS, E. 2009 Evolutionary Trends in Cyberspace. In: F.D. KRAMER, S.H. STARR, L. WENTZ (eds.), C*yberpower and National Security*. National Defense University.

SMITH, E. 2002. Effects Based Operations. Applying Network Centric Warfare in Peace, Crisis, and War. *Information Age Transformation Series.* CCPR Publication Series.

SOMMER, Peter and BROWN, Ian (2010). *Reducing Systemic Cybersecurity Risk.* London: OEDC report.

TAKKUNEN, J. 2010. Analyyttisyyttä puolustusjärjestelmän kehittämiseen. *Ruotuväki*.

TOURI, M. 2009. Transparency and accountability in the age of cyberpolitics: the role of blogs in framing conflict. In: A. KARATZOGIANNI (ed.) *Cyber Conflict and Global Politics.* Routledge.

TTCP 2006. Guide for Understanding and Implementing Defense Experimentation. Ottawa: The Technical Cooperation Program.

USJFCOM. 2009. Multinational Experiment 6. The Irregular Challenge: A comprehensive approach to a complex problem. Available at: http://mne.oslo.mil.no:8080/Multinatio/GeneralInf/MNE6USJFCO/file/MNE%206%20Rev%20--%20JCDE%20Spotlight%20--%2019May091.pdf [Accessed 09 August 2010].

WAH, L. K., ONG, T. & FAN, K. 2006. Experimenting with Experimentation. *Pointer,* 32.

ZIMET, E. & SKOUDIS, E. 2009. A Graphical Introduction to the Structural Elements of Cyberspace. In: F.D. KRAMER, S.H. STARR, L. WENTZ (eds.), C*yberpower and National Security*. National Defense University.