Freedom and Control Networks in Military Environments

Paul T, Mitchell

2006

Paul T Mitchell. (2006). Freedom and Control Networks in Military Environments. (RSIS Working Paper, No. 112). Singapore: Nanyang Technological University.

https://hdl.handle.net/10356/82390

No. 112

Freedom and Control Networks in Military Environments

Paul T Mitchell

Institute of Defence and Strategic Studies

Singapore

May 2006

With Compliments

The Institute of Defence and Strategic Studies (IDSS) was established in July 1996 as an autonomous research institute within the Nanyang Technological University. Its objectives are to:

- Conduct research on security, strategic and international issues.
- Provide general and graduate education in strategic studies, international relations, defence management and defence technology.
- Promote joint and exchange programmes with similar regional and international institutions; and organise seminars/conferences on topics salient to the strategic and policy communities of the Asia-Pacific.

Constituents of IDSS include the International Centre for Political Violence and Terrorism Research (ICPVTR), the Centre of Excellence for National Security (CENS) and the Asian Programme for Negotiation and Conflict Management (APNCM).

Research

Through its Working Paper Series, *IDSS Commentaries* and other publications, the Institute seeks to share its research findings with the strategic studies and defence policy communities. The Institute's researchers are also encouraged to publish their writings in refereed journals. The focus of research is on issues relating to the security and stability of the Asia-Pacific region and their implications for Singapore and other countries in the region. The Institute has also established the S. Rajaratnam Professorship in Strategic Studies (named after Singapore's first Foreign Minister), to bring distinguished scholars to participate in the work of the Institute. Previous holders of the Chair include Professors Stephen Walt (Harvard University), Jack Snyder (Columbia University), Wang Jisi (Chinese Academy of Social Sciences), Alastair Iain Johnston (Harvard University) and John Mearsheimer (University of Chicago). A Visiting Research Fellow Programme also enables overseas scholars to carry out related research in the Institute.

Teaching

The Institute provides educational opportunities at an advanced level to professionals from both the private and public sectors in Singapore as well as overseas through graduate programmes, namely, the Master of Science in Strategic Studies, the Master of Science in International Relations and the Master of Science in International Political Economy. These programmes are conducted full-time and part-time by an international faculty. The Institute also has a Doctoral programme for research in these fields of study. In addition to these graduate programmes, the Institute also teaches various modules in courses conducted by the SAFTI Military Institute, SAF Warrant Officers' School, Civil Defence Academy, and the Defence and Home Affairs Ministries. The Institute also runs a one-semester course on '*The International Relations of the Asia Pacific'* for undergraduates in NTU.

Networking

The Institute convenes workshops, seminars and colloquia on aspects of international relations and security development that are of contemporary and historical significance. Highlights of the Institute's activities include a regular Colloquium on Strategic Trends in the 21st Century, the annual Asia Pacific Programme for Senior Military Officers (APPSMO) and the biennial Asia Pacific Security Conference. IDSS staff participate in Track II security dialogues and scholarly conferences in the Asia-Pacific. IDSS has contacts and collaborations with many international think tanks and research institutes throughout Asia, Europe and the United States. The Institute has also participated in research projects funded by the Ford Foundation and the Sasakawa Peace Foundation. It also serves as the Secretariat for the Council for Security Cooperation in the Asia-Pacific (CSCAP), Singapore. Through these activities, the Institute aims to develop and nurture a network of researchers whose collaborative efforts will yield new insights into security issues of interest to Singapore and the region.

ABSTRACT

Militaries around the world are pursuing the idea of Network Centric Warfare as the fundamental basis for how they will conduct operations in the future. NCW suggests that "a robustly networked force improves information sharing and collaboration, which enhances the quality of information and shared situational awareness. This enables further collaboration and self-synchronization and improves sustainability and speed of command, which ultimately result in dramatically increased mission effectiveness." In many respects, NCW seeks to develop military power in the same way that the Internet has enhanced both business and individual knowledge.

This article explores the development of this concept of information sharing particularly with regard to the possibility of enhancing information sharing within military coalition environments. It suggests that there is a fundamental dialectical tension between the enhanced freedom of action sought by NCW and the need to protect information on networks. The nature of this tension will resolve itself in unpredictable fashions, however, its essence reveals that it is highly unlikely that NCW will enhance coalition operations in the same way it might enhance national operations.

****

Dr Paul T. Mitchell was the Director of Academics at the Canadian Forces College, Toronto, for four years where he helped to establish the Masters in Defence Studies for the Command and Staff Course taught there. His research interests are in US military policy and operations, especially in the area of transformation and emerging operational concepts. In 2003, he was awarded the United States Naval Institute's Literary Award for the best article on surface naval warfare for his article in the Naval War College Review, "Network Centric Warfare and Small Navies, is there a role?". He has published in Journal of Strategic Studies, Armed Forces and Society, US Naval Institute Proceedings, US Naval War College Review, and the Canadian Military Journal. In 1997, he co-edited "Multinational Naval Cooperation and Foreign Policy in the 21st Century. He has taught at Queen's University Kingston, Dalhousie University in Halifax, the Pearson Peacekeeping Centre, Royal Military College, and the Canadian Forces College. He has a Ph.D from Queen's University in political studies and a MA from King's College London in War Studies.

Freedom and Control
Networks in Military Environments

Claims to the establishment of revolutionary ideas are difficult to verify in the present. Only the passage of time can truly confirm the impact an idea will have on history and events. For example, immediately after the Second World War, nuclear weapons were widely believed to have revolutionized war. Nevertheless, their role in warfare has to date been latent rather than direct and it still remains to be seen precisely what their role will ultimately be. Secondly, as Colin Gray points out, the concept of a revolution in military affairs is essentially an interpretation placed on the unfolding of events by historians, as opposed to an objectively verifiable occurrence with a time and place attached to it. Thus, debates over the meaning of military developments in the sixteenth century have a never ending quality to them simply because their existence is ultimately dependant upon the subjective interpretation of a series of historical events and trends.[1]

The purpose of this chapter is not to establish the revolutionary nature of the emergence of Network Centric Warfare (NCW); it is too soon to predict its influence and longevity as a concept. As in the case of nuclear weapons, the demands of information technologies may ultimately prove to be militarily impossible to implement in the manner predicted by the early proponents. Likewise, there is no predicting if alternate approaches may be devised for their use by other forces[2] just as the combined use of armored forces, wireless communications, and aircraft took much trial and error before being perfected in the Second World War.[3]

There is much that is promisingly novel about the role that Information and Communication Technologies (ICT) may play in a military context to warrant the label revolutionary, even at this early date. Still, at the heart of NCW lies a fundamental dialectical tension in concepts. NCW promises faster, more precise,

[1] Colin S. Gray, *Strategy for Chaos*, (London: Frank Cass, 2002), pp. 13-17.
[2] Eliot Cohen, "Change and Transformation in Military Affairs", *Journal of Strategic Studies*, Vol. 27, No. 3, September 2004.
[3] See, Williamson Murray, "May 1940: Contingency and Fragility of the German RMA", *The Dynamics of Military Revolution, 1300-2050*, MacGregor Knox, Williamson Murray (ed.s), (Cambridge: Cambridge University Press, 2001);Thomas G. Mahnken, "Beyond Blitzkreig: Allied Responses to Combined-Arms Armoured Warfare during World War II", *The Diffusion of Military Technology and Ideas*, Emily O. Goldman, Leslie C. Eliason (ed.s), (Stanford Ca: Stanford University Press, 2003); Williamson Murray, "Armored Warfare: The British, French, and German Experiences", *Military Innovation in the Interwar Period*, Williamson Murray, Allan R. Millet (ed.s), (Cambridge: Cambridge University Press, 1996); Barry R. Posen, "The Battles of 1940", *The Sources of Military Doctrine*, (Cornell: Cornell University Press, 1984).

more decisive operations due to the effects of information sharing. In this regard, NCW is oriented around increasing the operational freedom of choice for military commanders such that they can avoid or efficiently surmount the barriers war creates either through the active resistance of the enemy or through the ignorance generated by the danger and chaos of operations. At the same time, because military operations are ultimately undertaken to ensure the security of the state, the military context is an environment of strict control and direction. The criticality of this operational dimension is made even more so by the dangerous quality war poses to human life. These two aspects, then, freedom and control, sharing and security, circle each other warily within the nature of NCW.

Even as they pose distinct questions on how networks will influence both traditional military organization (will networked militaries flatten or will they remain in their traditional hierarchical shape?), networks raise significant questions for coalitions and how they will operate in networked environments. Coalitions are all about sharing and thus should be open to the use of networks. However, while the premise of the information age is founded upon the power generated through information sharing, networks can also be exclusionary and it is here that US military primacy, and the role national security still plays in shaping state and military behaviour that suggests networks and coalitions may not be as amenable as hoped.

Origins of NCW

NCW is a relatively new concept, first appearing in the literature in 1998 in a United States Naval Institute *Proceedings* article authored by VAdm. Arthur Cebrowski and John Gartska.[4] However, the idea of networking information amongst naval platforms is one that began to emerge in the midst of the Second World War. The challenge presented to surface ships by aircraft, widely ubiquitous at sea for the first time with the appearance of modern aircraft carriers, required considerably more coordination amongst fighting platforms than traditional naval gunnery.[5] The

[4] VAdm. Arthur K. Cebrowski, John J. Gartska, "Network Centric Warfare: Its Origins and Future", *Proceedings*, Vol. 124, No. 1, January 1998, pp. 28-35.

[5] One need only think of the Battle of Midway and the challenges presented to naval commanders in terms of locating the enemy's carriers, launching strikes of various aircraft types, all armed with different weaponry, while maintaining combat air patrols of friendly fighters and keeping task force ships all in formation. The challenges of three dimensional warfare presents far more complex

coordination of these many different missions and platforms resulted in the development of modern Combat Information Centres, or Operations Rooms, and airborne radars.[6] Modern tactical data exchange systems such as Link and GCCS can also trace their origins to developments of that period.[7] Finally, cybernetic theory, which forms the basis for much thinking on information and control, was developed as a side product of ballistics research into the problems of anti-aircraft weaponry.[8]

Following the close of the Second World War, both the US Navy and the US Air Force continued to develop the role that information played in the conduct of war; by the end of the 1970s, the US Army had joined them as well. Information plays a natural role in naval strategy; navigation and location of the enemy are central to all naval battle. However, the Maritime Strategy of the 1980s exploited fundamentally information based technologies such as *Aegis* and advanced sonar to threaten the Soviet Union's coastline, thus potentially globalizing any struggle over Western Europe.[9] Likewise, airborne and 'spaceborne' technologies emerged at a steady pace following the close of the Second World War, including advanced airborne radars and command and control systems, precision guided munitions, stealth, and satellite

---

command and control issues than the traditional naval battleline. Karl Lautenschlager, *International Security*

[6] In the spring of 1942, Adm. Ernest J. King asked Vannevar Bush of the Office of Scientific Research and Development to examine the possible development of a system of radar relays that would permit ships to share radar information thus expanding the range of awareness commanders had of the tactical situation. The project later switched to a system of air based radars that ultimately saw the development of the first airborne early warning aircraft in the form of modified Grumman Avengers carrying APS-20 radars. Edwin Leigh Armistead, *AWACS and Hawkeyes*, (St. Paul Mn: MBI Publishing co., 2002), pp. 3-7.

[7] In 1957, after three years of deliberation, the CANUKUS Naval Data Transmission Working Group ratified the technical standard for data exchange. Originally named the Tactical International Data Exchange (or TIDE, "good for cleaning up messy tactical pictures"), it later became known as Link 2 (given as "II" in roman numerals) in the Royal Navy, which was already using forms of data sharing technology to distribute tactical information among its ships. As other NATO links became established, Link II became known as "Link 11" (i.e., eleven). Norman Friedman, *World Naval Weapons Systems 1997–1998* (Annapolis, Md.: Naval Institute Press, 1997), p. 28

[8] Robert Burnett, P. David Marshall, *Web Theory: An Introduction*, (London: Routledge, 2003), p. 25; Norbert Weiner, *Cybernetics; Or, Control and Communication in the Animal and the Machine*, (New York: Wiley, 1948).

[9] Tacticians anticipated that Soviet bombers would mass their aircraft in "regimental" attacks, launching masses of missiles towards naval formations in the hopes of overwhelming their defences. In this type of tactical environment, it would no longer be possible to coordinate the defence of a task force through voice reporting, nor could the resources of any single ship hope to defend against such an attack. The threat posed by this challenge meant that the area that had to come under positive control by Western surface and air assets expanded considerably. Norman Friedman, *The US Maritime Strategy*, (London: Janes Publishing, 1988), pp. 162-164, 174. Scott L. Nicholas, "Anti-carrier Warfare", *The Soviet Navy: Strengths and Liabilities* Bruce W. Watson, Susan M. Watson (ed.s), (Boulder Co.: Westview, 1986), p. 146. Norman Friedman, *US Destroyers Revised Edition*, (Arlington Va: Naval Institute Press, 2004), pp. 391-392.

imaging.[10] Finally, the growing interest of the US Army in operational theories of warfare, after the end of the Vietnam War, spawned concepts such as Airland Battle. Projected operations deep in Soviet rear areas required significant intelligence and the dissemination of information between Army and Air Force units in order to coordinate deep strikes so as to create a level of operational paralysis.[11]

From the end of the Second World War, then, and with increasing velocity in the mid-1970s, each service pursued independent strategies with similar themes converging on the growing importance of information and its transmission and sharing. This serendipitous evolution was noticed by the Soviets in the 1970s, who first raised the issue of a "military technical revolution" occurring within the United States military.[12]

In some respects, the close of the Cold War not only marks the end of a political era as well as that of a military one. The "strategic" developments of operational theories like the "Maritime Strategy" by the USN, "Global Reach; Global Strike" by the USAF, and "AirLand Battle" by the US Army all point to the ultimate expansion of the battlefield to something beyond what had been well understood, to that point, by "Operational Art." Operational Art first appeared during the military changes of the early 19th century where the steady enlargement of the battlefield, its growing complexity due to the rapid introduction of new technologies, and the growing role of the State's economic power in fielding and sustaining military forces led to both long military "campaigns" as well as "theatre warfare".[13] Aside from a solid grounding in tactics, successful military commanders needed to come to terms with the time and space dimensions of moving numerous large and internally complex military formations to achieve the ends of strategy. In the eyes of many strategic analysts, operational art reached its acme in the closing years of the First World War.[14] Jonathon Bailey makes the bold assertion:

---

[10] Jacob Neufeld, George M. Watson jr., David Chenoweth (ed.s), *Technology and the Air Force: A Retrospective Assessment*, (Washington DC: USAF, 1997).

[11] See, for example, Col. Thomas A. Cardwell (USAF), *Airland Combat: An Organization for Joint Warfare*, (Maxwell Al: Air University Press, 1992), pp. 75-80; the concept of "Agility", defined as "the ability of friendly forces to act faster than the enemy" is clearly derived from Col. John Boyd's OODA loop. Dept. of the Army, *US Army Field Manual 100-5 Blueprint for the AirLand Battle*, (Washington DC: Brassey's (US) Inc., 1991), pp. 16-17.

[12] Norman Friedman, "The Computer Bomb", *The Fifty Year War: Conflict and Strategy in the Cold War*, (Annapolis: United States Naval Institute Press, 2000), pp. 445-451.

[13] Milan Vego, *Operational Warfare*, (Newport RI: Naval War College, 2000), pp. 1-2.

[14] Timothy Travers, *The Killing Ground: The British Army, the Western Front, and the Emergence of Modern Warfare, 1900-1918*, (London: Allen Unwin, 1987); Murray, "Armored Warfare (1996);

> Three dimensional conflict was so revolutionary that the tumultuous development of armor and air power in 1939-45 *and the advent of the information age* in the decades that followed amounted to no more than complementary and incremental improvements upon the conceptual model laid down in 1917-1918.[15]

The operations projected by the US military at the close of the Cold War were inherently global in nature, however. The ability to deal with the complexity of this battlefield was greater than the individual competency of any single service, recognized by the introduction of the term "battlespace".[16] In a fashion to how business was dealing with the increasingly large global market by exploiting ICT, American military forces were dealing with similarly sized operational challenges, looking to exploit the same technology. By the mid-1990's, the US military began to put these new developments into doctrinal perspective.

Emergence of the Concept

In 1996, Adm. William A. Owens published in National Defense University's *Strategic Forum* "The Emerging System of Systems" in which he described a concatenation of sensors, command and control systems, and precision weaponry. The result was the development of "dominant battlespace knowledge".[17] In the same year, *Joint Vision 2010* appeared which described the "conceptual template … for achieving dominance across the range of military operations through the application of new operational concepts…." *JV2010* introduced the concepts of Dominant Manoeuvre, Precision Engagement, Focused Logistics, and Full Spectrum Protection

---

Jonathan B.A. Bailey, "The First World War and the Birth of Modern Warfare", *The Dynamics of Military Revolution, 1300-2050*, MacGregor Knox, Williamson Murray (ed.s), (Cambridge: Cambridge University Press, 2001); Gray, *Strategy for Chaos*, (2002).

[15] Bailey (2001), p. 132. Emphasis added.

[16] Defined by the Department of Defense as "The environment, factors, and conditions that must be understood to successfully apply combat power, protect the force, or complete the mission. This includes the air, land, sea, space, and the included enemy and friendly forces; facilities; weather; terrain; the electromagnetic spectrum; and the information environment within the operational areas and areas of interest. Department of Defense*, Joint Publication 1-02, "DOD Dictionary of Military and Associated Terms*, http://www.dtic.mil/doctrine/jel/doddict/data/b/00700.html, as amended through 31 August 2005.

[17] Adm. William A. Owens (USN) "The Emerging System of Systems", *Stragtegic Forum*, No. 63, Feb. 1996.

to achieve "massed effects". In essence, *JV2010* represents the first distillate of twenty years of technological advance and operationally focused thinking. Yet it was clear that at the base of these novel operational concepts lay "information superiority".

As much an advance that the introduction of these concepts represent, they are basically a more elaborate re-statement of the 1980s era Airland Battle concepts. *JV2010* encorporates the advances of manoevrist warfare concepts and the advance of technology, but operations are still fundamentally derivative of what has preceded before. While *JV2010* speaks to the emergence of the revolution in military affairs, a further step was required before one could begin to call these developments revolutionary in nature. In 1998, the concept of Network Centric Warfare burst on to the conceptual landscape, first in Cebrowski and Gartska's seminal article and later in book form jointly authored by Gartska, David S. Alberts, and Frederick P. Stein.

Elaboration of NCW

NCW is basically fleshed out by three semi-official publications: *Network Centric Warfare*, published in 1999, *Understanding Information Age Warfare* by Alberts, Gartska, Richard E. Hayes, and David A. Signori in 2001, and *Power to the Edge: Command and Control in the Information Age*, by Alberts and Hayes in 2003.[18] Together, these three works form the kernel from which most thinking on NCW has sprung. In general, *Network Centric Warfare* introduces the idea that networks generate power through the distribution of information through a series of business case studies. *Understanding Information Age Warfare* takes the idea of NCW and develops a theory on how information, knowledge, and awareness interact in a military environment. *Power to the Edge* is more of a conceptual piece ruminating on the implications that information and networks will have on military organizations and their operations.

[18] The three books are published by the Command and Control Research Project managed by Evidence Based Research (EBR). While EBR is an arms length independent think tank, the presence of Dr. David Alberts speaks to the authority of these works. At the time, Alberts was Director Research and Strategic Planning in the Office of the Assistant Secretary of Defence (C3I). David S. Alberts, John J. Gartska, Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority 2nd ed.*, (Washington DC: Command and Control Research Program, 1999); David S. Alberts, John J. Gartska, Richard E. Hayes, David A. Signori, *Understanding Information Age Warfare*, (Washington DC: Command and Control Research Program, 2001); David S. Alberts, Richard E. Hayes, *Power to the Edge: Command and Control in the Information Age*, (Washington DC: Command and Control Research Program, 2003).

In its exploration of how computer networks are altering the economic and business activities of corporations in the United States, *Network Centric Warfare* (1999)shows its lineage to earlier works by Alvin and Heidi Toffler, who suggested in their influential *War and Anti-war* that "the way we make wealth is… the way we make war."[19] Corporations, by linking together "knowledgeable entities" (the various sub-units within the organization) through computer networks, can take advantage of the shared awareness thus generated in order to make decisions faster, more efficient, and improve the accuracy of business predictions. In addition to these advantages, networked businesses improve collaboration between sub-units and ultimately generate a level of self-synchronisation in planning for future events that enable them to create efficiencies in their supply chains and customer relations. Alberts *et al.* suggested that the compression of time and space caused by this shift would also impact the battlespace. In essence, the same processes so important to creating better business decisions would also enable military commanders to create a condition of "information superiority", analogous to earlier concepts of air superiority or sea control. As they stated,

> Information superiority is a state that is achieved when competitive advantage (eg. Full Spectrum Dominance) is derived from the ability to exploit a superior information position. In military operations this superior information position is, in part, gained from information operations that protect our ability to collect, process, and disseminate an uninterrupted flow of information while exploiting and/or denying an adversary to do the same.[20]

Such capabilities would be increasingly important because of the greater complexity of the modern battlefield.[21] However, this new approach would produce a series of remarkable outcomes changing the very nature of warfare. Networks would permit the generation of combat power from highly dispersed yet agile entities because of their ability to enhance awareness. They argued that both the "fog of war" and friction in military operations, while not eliminated completely, would be

[19] Alvin and Heidi Toffler, *War and Anti-war: Survival at the Dawn of the 21st Century*, Boston: Little and Brown, 1993, p. 80.
[20] Alberts, *et al.* (1999), p.54.
[21] *Ibid,* pp. 60-65.

dramatically reduced.[22] As enhanced awareness would reduce risk, the cost of operations would decline, just as networks permitted businesses to reduce cost.[23] The combination of these assets would permit networked militaries to "mass effects" instead of massing forces.

> As the range of our sensors and weapons increase and as our ability to move information rapidly improves, we are no longer geographically constrained. Hence in order to generate a concentrated effect, it is no longer necessary to concentrate forces.[24]

In *Understanding Information Age Warfare*, the ideas that had been introduced previously are fleshed out into a fully formed theory of operations. Alberts, *et al.* begin with a series of assumptions regarding how experience translates ultimately into awareness and extrapolates from them a theory of warfare in networked environments. They suggest that we consider the manner in which we obtain information about the external environment through the interaction of what they call primitives. Sensory impressions of the environment can be directly inferred (as in directly seeing an event take place for example) or indirectly (through the interpretation of data returned by a sensor such as a radar). These impressions are then translated into "information" by putting the impressions into a "meaningful social context" through the identification of patterns interpolated between the sensed data and the purported social context. These patterns represent "knowledge" and comparisons between what is "known" about the world (prior knowledge) and what is currently being sensed generates "awareness". Finally, with sufficient levels of knowledge, the observer can draw inferences about what is likely to happen through identification of patterns in development. As such, awareness permits the observer to identify what is known about the past and present, however, "understanding" permits the observer to identify "what the situation is becoming." At the end of this sensing process, the observer is now capable of deciding what to do and they perform an action based on that decision. The whole process replicates the famous "OODA" loop developed by Col. John Boyd in that once an action is performed, the process can then repeat itself through the analysis by the observer of the impact his or her action has

[22] *Ibid,* pp. 71-72.
[23] *Ibid,* p. 41.
[24] *Ibid,* p. 90.

had on the world.[25] Although these assumptions are eminently debateable in terms of how humans ultimately perceive the world,[26] for the purposes of this paper, these assumptions will be taken as true.

The world in which this sensing and interpretation of data takes place is described as a series of interconnected "Domains". Three principal domains are posited, (although a fourth "Social Domain" is added to the theory in *Power to the Edge*). The "Physical Domain" is described as the scene where all action takes place. It is the location where military forces manoeuvre, strike, and defend themselves, and action, being directly observable here, can be measured through a variety of means (as in direct and indirect sensing). The "Information Domain" is the place where information is created, manipulated, and shared. Unlike the physical domain, it is not a "real" space but rather a virtual environment in which data is transferred and shared amongst actors through technology, and software; at its heart, it is a medium for communication. Last, the "Cognitive Domain" resides in the minds of actors participating on the network. In here, understanding is created through the interpretation of the data being communicated from the physical domain through the information domain. It is in the cognitive domain that information is evaluated, judged, and decisions made from the conclusions arrived at therein.[27] The social domain envelops these three others. The social domain mediates the evaluations, judgements and decisions that are developed in the cognitive domain. This recent addition to the theory has yet to be as firmly described as the previous three.

As Alberts points out, NCW is principally about the sharing of information and awareness.

> The concept of sharing lies at the core of both information superiority and NCW. Sharing data, information, and knowledge creates increased awareness because different actors in the battlespace have different elements of the situation, abilities to fuse them, and experience within which to interpret what is known. At the same time, sharing is an essential process for creating shared awareness.

[25] Alberts, *et al.* (2001), pp. 14-21.
[26] Darryn J. Reid, Graham Goodman, Wayne Johnson, Ralph Giffen, "All that Glisters: Is Network Centric Warfare Really Scientific?", *Defense and Security Analysis*, Dec. 2005.
[27] Alberts, *et al.* (2001), pp. 12-13.

> Obviously, shared awareness is essential if actors are ultimately to be synchronized in the battlespace.[28]

NCW facilitates sharing, then, enabling the development of superior awareness that ultimately translates into information superiority. This is described as the "NCW Value Chain", first elaborated in *Network Centric Warfare*, shown below:

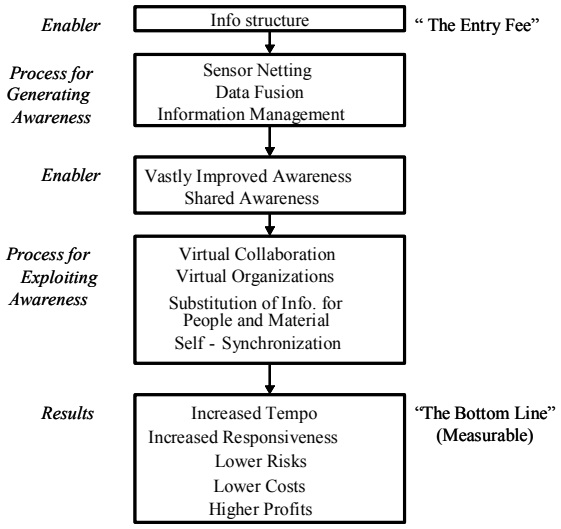

Figure 6. The Network Centric Enterprise

NCW Foundation (1999)

P 36, Network Centric Warfare: Developing and Leveraging Information Superiority. CCRP. 1999

The diagram graphically shows the series of inferences that lead ultimately to the establishment of increased combat power. By lowering the costs and risks associated with military operations, greater effects can be generated. Essentially, then, as the "Tenets of Network Centric Warfare" assert:

> a robustly networked force improves information sharing and collaboration, which enhances the quality of information and shared situational awareness. This enables further collaboration and self-synchronization and improves sustainability and speed of command, which ultimately result in dramatically increased mission effectiveness.[29]

[28] *Ibid*, pp. 15-18.
[29] Department of Defense. *Network Centric Warfare Report to Congress*. July 2001.

Shared knowledge becomes a critical keystone then for forces participating in a networked operation.

> The degree to which shared knowledge can be developed has a significant influence on the nature of command and control that can be employed, the nature and amount of communications that are needed to develop and maintain shared awareness, and the ease and degree to which forces can be synchronized.[30]

The end result of this sharing of information and awareness is the creation of additional combat power through enhancing the utility of information provided to decision makers. Information can be characterized by its richness (or the quality of the information), and its reach (or its ability to permeate every area on the network). Typically in most scenarios, the higher the level of richness, the less reach it has. We see this in the case of classified information, which is generally closely held by those with a "need to know".

However, those in the field with proper clearances may be unable to access this information because of their distance from those who control it. Lower level information will spread much further along a network than the most highly classified material. This is depicted graphically below in *Figure 1*:

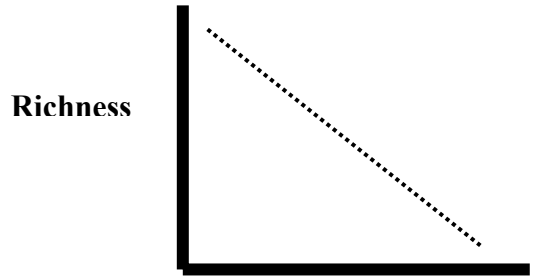

Figure 1: The Traditional Battlespace Information Richness and Reach

Figure 1

[30] Alberts, *et al.*, (2001), p. 26.

In a functioning network centric environment, richness no longer has any barrier in terms of its reach. Those with the proper credentials in the field will be able to access even highly classified information in real time. As a result, the "traditional business space" is now transformed into a whole "new competitive space" which in turn, generates additional combat power.[31] A "common operating picture" permits greater unity of command and purpose, de-conflicted missions, avoidance of any duplication of effort, enhanced early warning (and thus greater force protection), and the ability to use scarce resources more economically.[32] This change is represented graphically below in *Figure 2*:

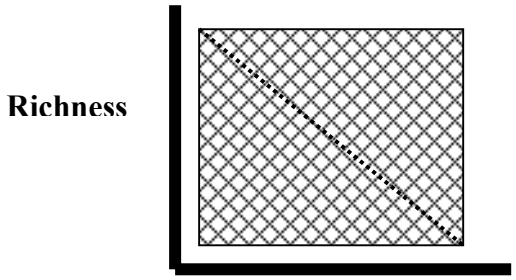

Figure 2: The New Competitive Space

Figure 2

The requirements for this outcome are high. In the physical domain, all elements of a military force are connected together "achieving secure and seamless connectivity and interoperability." In the information domain, persons and platforms must be capable of sharing, accessing, and most importantly, *protecting* "information to a degree that it can establish and maintain an information advantage over an adversary." Last, in the cognitive domain, forces must be capable of using the shared information to develop an awareness of the environment surrounding them as well as sharing that awareness with other participants on the network. Unless these objectives

[31] *Ibid*, p. 60.

[32] George K. Gramer [Col.USA], " Optimizing Intelligence Sharing in a Coalition Environment: Why US Operational Commanders have an Intelligence Dissemination Problem, (Course Paper, Department of Joint Military Operations, US Naval War college, Newport RI, 17 May 1999), pp. 2-3.

are accomplished, military forces will be unable to self synchronize and thus take advantage of the benefits conferred by networking together.[33]

While it is the combined effect of the four domains that permit the establishment of shared awareness and self-synchronization, it seems clear that the lynchpin to the whole enterprise is the *security* of the information domain. Establishment of a combat advantage depends on information superiority. This superiority must be protected, however:

> it is increasingly the information domain that must be protected and defended to enable a force to generate combat power in the face of offensive actions taken by an adversary. *And in the all-important battle for information superiority, the information domain is ground zero*.[34]

With the development of a theory describing the relationships between information, knowledge and awareness in place, development proceeded on the implications of theory for the practice of military operations in this new environment. The conclusions of this research emerged in *Power to the Edge* in 2003. Explicitly, Alberts and Hayes argued that in order to take advantage of the opportunities offered by NCW, militaries would have to "focus on C2, where information is translated into actionable knowledge." In the modern battlespace, traditional procedures and organizations established to practice the command and control of military forces will be unable to cope with the complexity that they will face. Alberts and Hayes argue that to date, militaries have been able to adapt by using "work around" procedures that are typically unique to the time and place of specific operations. Increasingly, however, complexity will defy traditional, industrial age organizations to mobilize their potential power through their inefficient knowledge sharing. Decision makers in these challenging global arenas cannot possibly anticipate every outcome, nor possess complete knowledge about the environment in which they will operate. In order to maximise the potential offered by information, *"information age"* organizations and processes will have to be founded on interoperability, so as to enhance the sharing of awareness.[35] Furthermore, since they cannot know who they will work with, nor

[33] Alberts, *et al.*, (2001), pp. 57-58.
[34] *Ibid* pp. 12-13. Emphasis added.
[35] Alberts, Hayes, (2003), p. 56.

which systems may be relevant to the solution of problems, a high degree of agility will be necessary "in terms of who participates as well as who plays what roles."[36]

Given these observations on the demands of the modern military environment, the centralization of command and control is increasingly impractical. Instead, power needs to be devolved to "edge entities",

> Power to the Edge is about changing the way individuals, organizations, and systems relate to one another and work. Power to the Edge involves the empowerment of individuals at the edge of an organization (where an organization interacts with its operating environment to have an impact or effect in that environment) or, in the case of systems, edge devices. Empowerment involves expanding access to information and the elimination of unnecessary constraints. For example, empowerment involves providing access to available information and expertise and the elimination of procedural constraints previously needed to deconflict elements of the force in the absence of quality information.[37]

It goes without saying that the vision that is encapsulated by this simple quotation is markedly revolutionary in terms of its organizational and procedural impacts. If ultimately realized, it suggests Bailey's link between the First World War and the Information Age is somewhat overstated as it strikes directly at the hierarchical nature that militaries have always relied on for command and control. It remains to be seen whether these militaries will be capable of adapting to such a wide ranging vision. Nevertheless, as demonstration of DOD's commitment to it, Albert and Hayes discuss the development of the "Global Information Grid", or GIG as an example of this emerging philosophy. "The GIG itself will increasingly become an adaptive entity that integrates communication and computer systems into a secure, seamless infostructure, one that provides access to a variety of information sources and information management resources."[38]

[36] *Ibid*, p. 59.
[37] *Ibid*, pp.4-5.
[38] *Ibid*, p. 187.

The Emergence of the GIG: Networks and Global Military Operations

The introduction of the GIG as a fundamental structural component of American defence[39] points to the role that information technologies have had in transforming modern societies. Comparisons are easy to make between the military GIG and the civilian Internet. Transformation itself seems to be guided by an "Internet paradigm" in terms of its overall vision.[40] In testimony before the House Armed Services Committee, the Assistant Secretary of Defense for Networks and Information Integration, John Stenbit describes the GIG as a "private world wide web":

> In the same manner that the World Wide Web is transforming industry and societies on a global scale, the GIG will support the transformation of our warfighting and business practices.[41]

Under present plans, the GIG will establish its core capabilities for US defence by 2010 through an overall investment of $21 billion through that time period. However, full implementation of the infrastructure is not expected to be until 2020. By then, the GIG will "integrate all DOD's information systems, service applications, and data into one seamless and reliable network."[42] Structurally, the GIG will be realized through four related endeavours. These include the "Global Information Grid Bandwidth Expansion" (GIG-BE)[43], "Transformation Communications System" (TCS)[44], "Network Centric Enterprise Services" (NCES)[45], and the "Cryptological Transformational Initiative" (CTI).

---

[39] Paul Wolfowitz, "Global Information Grid (GIG) Overarching Policy", *Department of Defense Directive 8100.1*, Sept. 19, 2002, accessible at http://www.dtic.mil/whs/directives/corres/html2/d81001x.htm.

[40] Committee on Network-Centric Naval Forces, Naval Studies Board, *Network Centric Naval Forces: A Transition Strategy for Enhancing Operational Capabilities*, (Washington DC: National Academy Press, 2000), p. 31.

[41] Statement by John P. Stenbit before the Committee on Armed Services, United States House of Representatives, Terrorism, Unconventional Threats and Capabilities Subcommittee, February 11, 2004.

[42] Robert E. Levin, *The Global Information Grid and Challenges Facing its Implementation*, GAO 84-858, (Washington DC: Government Accounting Office, July 2004), p. 1

[43] The GIG-BE is a world wide ground based fiber optic network, using IP protocols, to expand the connectivity and interoperability of DOD installations. Six sites achieved IOC on Sept. 30, 2004. "Global Information Grid (GIG) Bandwidth Expansion (GIG-BE), http://www.globalsecurity.org/space/systems/gig-be.htm, accessed April 7, 2006. See also, Stenbit, *op cit*.

[44] The TCS is composed of space based and ground based segments. Space based segments include the Transformation Satellite (TSAT) and Advanced Polar System (APS) satellites, a laser based SATCOM

Several developments all come together in order to make this appear "inevitable".[46] Geographical issues in terms of both the steady expansion of the operational battlespace since the eighteenth century and the globalization of American defence tasks have all demanded greater coordination amongst armed services. Missions such as close air strike, suppression of enemy defences, tactical missile defence, and deep strike operations all require a high degree of coordination amongst highly disparate force elements, many of them crossing service boundaries, and some crossing traditional theater and command boundaries. In order to accomplish missions such as these, simple deconfliction of efforts requires a high degree of communication and coordination between participating units. To go the next step of ensuring joint coordination, rather than simple deconfliction demands highly integrated planning[47]. Second, given the cost of forward deployment and the capital and human costs of continuous forward operations, an increasing number of US forces since the end of the Cold War have been redeployed to the North American continent. The cost in human, economic, political, and social terms of sending US forces abroad is increasing. Moving information instead of forces allows many support elements, such as administrative, logistical, and intelligence, to remain deployed in the US, even during periods of combat.[48] Even the force providers themselves need not deploy in the "massive" fashion of traditional combat operations, relying on the speed, agility,

---

constellation allowing global IP routing and addressing of information, even in areas with no pre-existing communications infrastructure. The ground based segment is composed of the Joint Tactical Radio System (JTRS), a software based radio that will be programmable to imitate other types of radios thus enhancing overall communications interoperability within the US military. Able to transmit voice, data, and video, it is hoped that JTRS will enable seamless communication, hypothetically between fighter pilot to soldier to sailor. See, Jefferson Morris, Rich Tuttle. "Contractors lining up to compete for Transformational Communications Network", *Aerospace Daily*, Vol. 207, No. 38, p. 1; GAO 2004, pp. 11-12; Johnny Kegler, "Pathways to Enlightenment" *Armada International*, Vol. 29, No. 5, Oct./Nov. 2005, pp. 10-14; ; Johnathon Karp, Andy Pasztor. "Pentagon Week: High Tech has High Risk", *Wall Street Journal*, May 2, 2005, p. B2; "Transformational Communications Architecture", http://www.globalsecurity.org/space/systems/tca.htm; "Transformational SATCOM (TSAT) Advanced Wideband System", http://www.globalsecurity.org/space/systems/tsat.htm.

[45] NCES are the integrated series of applications that will reside on the GIG permitting the military to access, send, store, and protect information. In effect, this will create the software nervous system that will operate the GIG. By establishing IP protocols on the GIG, NCES will enable US forces to forego the typical "point to point" interfaces between systems, ending the duplication of efforts and multiplication of incompatible systems. Levin, (2004), p. 11; "Global Information Grid (GIG)", http://www.globalsecurity.org/space/systems/gig.htm.

[46] *Network Centric Naval Forces*, p. 3.

[47] Committee to Review DOD C4I Plans and Programs, Computer Science and Telecommunications Board, National Research Council, *Realizing the Potential of C4I*, (Washington DC: National Research Council, 1999), p. 70

[48] *Realizing the Potential of C4I*, p. 27, Alberts, *et al.*, (1999), pp. 60-65.

and manoeuvrability brought about by rapid and ubiquitous information sharing.[49] Last, the importance of building stability in regions torn by civil war and social breakdown has made for the complex battlefield identified by former Commandant of the Marine Corps, Gen Victor Krulak as the "three block war".[50]

The high degree of complexity in these three areas defies any one person or organization being able to remain in complete awareness about all critical aspects affecting operations. Geographically dispersed, numerically small, and organizationally complex operations require extensive information sharing. Networks assist in the planning and conduct of operations in many ways. Relatively instantaneous communications have the impact of rendering the constants of geography less important, at least in terms of sharing information and knowledge. This also has the concomitant effect of compressing time given that information is available upon request and thus decision cycles can by accelerated.[51]

In this complex global environment, the very malleability of networks is also highly attractive. Castells has pointed out that "nodes" on a network vary in terms of their overall relevance. The importance of any given node on the network stems not from its function or features, but for its ability to contribute to the goals established by the network. Nodes can be added or deleted from network architecture as their importance changes or as the missions alter. This nature permits a high degree of flexibility (in determining the paths that information can be sent along), scalability (in terms of growth or contraction of the architecture without having a significant operational disruptions), and survivability.[52] The advantage this allows is the easy access of information "anytime, anyplace, with attendant security."[53] "Perhaps the single most transformational and operationally significant attribute presented by the GIG vision will be that US servicemen and women 'at the edge' will no longer be at the mercy of someone remote from the fight determining what information they need."[54]

---

[49] Cohen, (2004), p. 395; Alberts *et al.* (2004), p. 88.
[50] Charles C. Krulak, "The Strategic Corporal: Leadership in the Three Block War", *Marines Magazine*, January 1999.
[51] Alberts *et al.* (1999), pp. 20-21; *Network Centric Naval Forces*, p. 3.
[52] Manuel Castells, "Informationalism, Networks and the Network Society: A Theoretical Blueprint", *The Network Society: A Cross-cultural Perspective,* Manuel Castells, (ed.), (Cheltenham UK: Edgar Elgar, 2004), pp. 3, 5-6.
[53] Stenbit, *opcit.*
[54] "Global Information Grid (GIG)", http;//www.globalsecurity.org/space/systems/gig.htm. Alberts and Hayes point out in their book *Power to the Edge*, that expanding access to information permits the

Just as information superiority formed the base on which *Joint Vision 2010's* advanced concepts rested, *information sharing* forms the base on which the entire edifice of military transformation rests. The "fog of war" is commonly blamed for both the waste associated with battle, and the failure of forces to achieve their purposes; the authors of *Network Centric Warfare* assert that any such fog is largely caused by the lack of battlespace awareness. Fog results from "our inability to tap into our collective knowledge or the ability to assemble existing information, reconcile differences, and construct a common picture." [55] While the US *Transformation Planning Guidance* blandly defines transformation in highly general terms,[56] the transformation necessary to overcome the fog of war and achieve the vision portrayed above clearly revolves around "seamless" information sharing.[57] As *Network Centric Warfare* points out, information superiority is "in part gained by information operations that protect our ability to collect, process, and disseminate an uninterrupted flow if information while exploiting and/or denying an adversary the ability to do the same." [58] Ultimately, the ability to build a *collective* awareness upon the *collected* limitations of platforms and individuals operating in the battlespace constitutes the basis of America's transformation plans.[59] In the words of one USAF officer "IP brings global connectivity to the kill chain."[60]

Information Vulnerabilities

That which makes this a powerful vision for warfighting also contains within it an equally powerful vulnerability. The same technology that enables dispersed and small formations to magnify their operational power through information sharing, also enables an adversary to both read the intentions and plans of a military force as well as to alter the information to accomplish a variety of ends. The problems of

---

elimination of "unnecessary constraints previously needed to deconflict elements of the force in the absence of quality information. Alberts and Hayes (2003), p. 5.

[55] Alberts *et al.* (1999), p. 71.

[56] "A process that shapes the changing nature of military competition and cooperation through new combinations and concepts, capabilities, people, and organizations that exploit our nation's advantages, protect against our asymmetric vulnerabilities to sustain our strategic position which helps underpin peace and stability in the world. Department of Defense, *Transformation Planning Guidance*, April 2003, p. 3.

[57] Levin 2004, p.1

[58] Alberts *et al.* (1999), p. 54.

[59] *Network Centric Naval Forces*, p. 59.

[60] Charlotte Adams, "Network Centric Rush to Connect", *Aviation Today*, Sept. 1, 2004.

unauthorized access to secure information sites is so widely understood as to have infiltrated popular culture; similarly, we are increasingly familiar with the threat posed by identity fraud, at least as far as our own credit records extends, if not in terms of national security. The threats of information denial and clandestine alteration of stored data are less commonly appreciated in general although just as damaging.[61] With the exception of a Denial of Service attack, all of these methods share in common the problem of malicious penetrations of secure systems. Identity fraud, in particular, assumes the proportions of introducing a "mole" into a secure organization. The damage that "malicious insiders" can cause to information systems points to a fundamental alteration of warfare – the reversal of the relationship between offence and defence. Traditionally, defence has always been the stronger form of warfare, for a variety of reasons. The asymmetry between offence and defence is reversed in terms of information security. As one study by the National Academy of Sciences described it:

> Imagine a situation in which truck bombers in a red truck attempt entry to a military base. The bomb is discovered and they are turned away at the front gate, but allowed to go away in peace to refine their attack. They return later that day with a bomb in a yellow truck, are again turned away and again go away in peace to refine their attack. They return still later with a stolen military truck. This time the bomb is undetected, they penetrate the defenses and they succeed in their attack. A base commander taking this approach to security would be justly criticized and held accountable for the penetration.[62]

Nevertheless, the difficulty of establishing identity in a digital environment[63] highlights the danger of such penetrations to the security and integrity of the context within a secure information environment.

A second challenge testing information security on the GIG comes not from a malicious insider, but rather from authorized users of a system, compromising information from simple ignorance. In its essence, digital information is persistent

[61] *Realizing the Potential of C4I*, p. 135.
[62] *Ibid*, p. 143.
[63] One is tempted to argue against the possibility of establishing a digital identity. Human beings in their endlessly variable forms are essentially analogue entities – unique and discrete. Digital entities through their ordinal precision and endlessly replicable nature means such a fundamental identification will prove elusive in its very essence.

and transportable. Persistence reflects the fact that digital information is easily copied, archived, and shared. While this is generally only a problem for those caught in compromising circumstances by paparazzi, the implications for inadvertent disclosure and subsequent propagation of classified information are evident. The Google search engine routinely archives all information it categorizes, permitting users to view material that has since disappeared from the original web pages. The same miniaturization developments that have enabled electronic communications, the same compression of time and space that have enable dispersed military operations have also eased the problem of transporting large amounts of data over distance. Networks permit the rapid replication and translocation of information in ways that spies could only dream of years ago.[64]

Control versus Anarchy: The Problem of Information Assurance

These essential issues of information vulnerability have not been un-noticed by national security agencies within the US defence community. Nevertheless, the lack of fundamental progress on information assurance, as opposed to the rapid developments in communication links and information sharing made in the last decade, point to real difficulties in resolving the issue. In the 1990's the "Defense Information Assurance Program" (DIAP), according to the GAO made limited progress, although ultimately failed to meet its goals.[65] In its examination of the GIG, the GAO has identified similar operational challenges. It noted three issues in particular: deciding when and how much information should be posted; establishing rules to ensure the GIG would work securely without compromising the benefits of flexible and dynamic information sharing; and convincing data owners of the value of sharing data with a broader audience and trusting the network enough to post data.[66] Again, the essential security of information in a digital environment appears to lie at the basis of the operational challenges confronting the GIG.

---

[64] Maj. Joshua Reitz, *Untangling the Web: Balancing Security, Prosperity, and Freedom in the Information Age*, MDS dissertation, (Toronto: Canadian Forces College, May 2005), pp. 11-14.
[65] According to the GAO, draft readiness metrics went untested, and organizational policies and procedures for managing information assurance were not fully defined across the DOD. Each of these issues points to the real problem in terms of preserving both the power enabled by information sharing while protecting the organizational security from the effects of unauthorized information release. See Robert F. Dacey, *Progress and Challenges to an Effective Defense-wide Information Assurance Program*, GAO-01-307, (Washington DC: GAO, March 2001), p. 4.
[66] Levin, p. 19.

As noted above, the GIG's development involves the "Cryptological Transformation Initiative", a $4.8 billion NSA funded project. The CTI involves both the development of advanced firewalls, multilevel security protection, and high assurance IP encryptors that would encrypt digital communications at the packet level.[67] Any information assurance system, however, will have to accomplish a variety of goals. As defined by the US Dept. of Defense, information assurance is "information operations that protect, and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation (which) … includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities."[68] In order to accomplish these missions, however, the essential nature of digital information confronts the systems engineer. "Availability" of information is for "*authorized*" users only. "Integrity" of information means protection from "*unauthorized*" change. "Authentication" involves verifying the identity of the originator (of a request for/author of data). "Confidentiality" involved protection from "*unauthorized*" disclosure. Finally, "non-repudiation" involves undeniable proof of participation.[69] Each of these aspects relates either to the fundamental control over the meaning of data or the identity of participants.

In effect, the nature of security casts an enormous shadow on the nature of digital collaboration in military environments. Control of information in terms of both its security as well as its meaning is of paramount importance in this environment.[70] The GAO report on the GIG summarises the nature of this control very effectively:

> Establishing network and system security safeguards – such as firewalls, identifying the sender and recipient of information, protecting information from unauthorized access, and safeguarding

[67] Charlotte Adams, "Network Centric Rush to Connect", *Aviation Today*, Sept. 1, 2004. Reportedly, JTRS radios would be able to firewall information within transmissions if included data at different security levels. In this way, information would be double encrypted in terms of both data and transmission.

[68] Paul Wolfowitz, "Information Assurance", *Department of Defense Directive 8500.1*, October 24, 2004, p. 20.

[69] Dacey, p. 6.

[70] As one study examining the impact of networks on naval forces argued: "Strict controls will be necessary at the connection points between tactical and non-tactical potions of the Naval Command and Information Infrastructure. These controls will ensure that only authorized types of traffic are allowed onto the tactical networks, and hence they will provide continued guarantees that the tactical networks can provide highly reliable, low latency data services. These controls will also aid in providing security boundaries." *Network Centric Naval Forces*, p. 33.

> data to prevent accident and deliberate alterations will be essential but difficult. … (T)he complexity and magnitude of enabling hundreds of systems and applications to operate in a secure web based environment will require careful planning and coordination. Comprehensive plans will be needed to ensure that sensitive data and communications are safeguarded across diverse platforms. This will require DOD to identify sensitive data as well as applications, databases, storage subsystems, and media used to process and store the data. Once systems have been examined, data access models must be applied to determine proper security levels for information and how integration can occur across platforms without disrupting network and near-real time operations.[71]

A simple overview of these requirements suggests a fundamentally different orientation to information and its place in society as compared to the movements that spawned the communications revolutions that permit this style of military operations in the first place. Indeed, the control necessary to ensure that a single point of failure in information security suggests elements of a police state where "every node is a sensor that can relate security information to those tasked with securing the network."[72] In many respects, this vision of near totalitarian control of information clashes with the fundamentally anarchic nature of the Internet itself.

At its most basic level, the Internet is an anarchical society in the manner in which Hedley Bull described the nature of international society.[73] Like the international environment, there is no single authority that controls the Internet. Despite this absence, there is a degree of order in that protocol for the transmission and sharing of information that have developed to enable its ubiquitous communication (TCP/IP and HTML and its variants for example). While legal regimes are steadily being established, in a global communications environment, they depend largely on self interested enforcement and compliance in a manner similar to international law. These developments all permit a considerable amount of industry

[71] Levin, pp. 28-29.
[72] Joe Pappalardo, "Protecting GIG Requires a New Strategy", *National Defence*, October 2005.
[73] Hedley Bull, *The Anarchical Society, A study of order in world politics*, (London: MacMillan, 1977).

and business to be conducted in a global fashion in this electronic environment just as international anarchy does not prevent the conduct of business between states.

The internet is also anarchical in terms of the meaning ascribed to the information that is placed there. There are no gate-keeping features on the Internet.[74] The introduction of web sites like Wikipedia takes advantage of this aspect as well as the dynamic, malleable aspect of digital information.[75] The popularity of "blogs" and their growing influence on news reporting within the media is a similar issue. The ability of sites like the "Drudge Report" to unearth key political scandals in Washington is due to the fact of differing approaches to how truth is mediated between it and traditional news organizations. The commitment to professional standards of reporting by mainstream publications like the *Washington Post* ensured that rumours of an affair between White House interns and the President were unpublishable without iron clad sources. Wikipedia itself has been criticized by the journal *Nature* in terms of its accuracy.[76] In many respects, the web becomes a location for debate over truth owing to the multiplicity of sites presenting differing slices of what is depicted as real, permitting the web surfer to arrive at their own unique conclusions. In many respects, the aspect of information overload that is commonly associated with the web reveals in its essence the impact of editorial decisions made in terms of the representation of truth in news stories and frees the individual to make independent judgments on its nature. The side effect of this is of course the development of obscure communities convinced of the existence of ghosts or American possession of UFO technology at its base in Groom Lake ("Area 51").[77] Irrespective of these charges, the interpretation of truth on the Internet is similar to how abstract terms such as justice and freedom are interpreted in the international environment: each of these *problematiques* owe their origin to the anarchical setting in which they are situated.[78]

---

[74] Although this is not strictly true in some parts of Asia where the state has retained a degree of control over Internet communications.

[75] Robert Burnett, P. David Marshall, *Web Theory: An Introduction*, (Routledge: London, 2003), pp. 32-33; http://news.bbc.co.uk/2/hi/technology/4840340.stm

[76] http://www.nature.com/nature/journal/v438/n7070/full/438900a.html

[77] For example, http://www.ghosts.org, http://www.aliensthetruth.com/, http://www.anomalies.net/area51/faq/.

[78] As Morgenthau puts it, "Where the insecurity of human existence challenges the wisdom of man, there is the meeting point of fate and freedom, of necessity and chance. Here, then, is the battlefield where man takes up the challenge and joins battle with the forces of nature, his fellow-men's lust for power, and the corruption of his own soul. Hans Morgenthau, *Scientific Man vs. Power Politics*, (Chicago: University of Chicago Press, 1946), p. 223; See also E.H. Carr. *The Twenty Years Crisis*

That the Internet should display these anarchical features is not entirely surprising, according to Manuel Castells. In his analysis of what he calls the "Network Society", its emergence was influenced by three key features, including the culture of individual freedom inculcated in both America campus environments and the counter-culture movements of the 1960s. The peace movement, civil rights struggle, and growth of environmentalism during this period were founded on opposition to traditional sources of authority. Similarly, the academic culture of universities, especially those in the United States, was that of shared discovery in which interpersonal professional communication was the basis for academic progress and the advancement of truth. Each of these movements "stood in sharp contrast to the world of corporations and governmental bureaucracies that had made secrecy and intellectual property rights the source of power and wealth."[79]

Pekka Himanen asserts that the information sharing on which the "network society" and its electronic sinews are based has permitted the establishment of a "culture of innovation", sometimes referred to controversially as the "hacker ethic".[80] The spirit of this culture is one of innovation, individuality, and networking. It approaches work as a child does play and emphasizes the value of creation over the spirit of the profit motive. "Money centredness leads to the closing off of information. Innovation lives on the open flow of information."[81] This orientation towards information, freedom, and innovation has also inspired technological movements such as the Open Source Initiative and the associated developments of the Linux Operating system.[82]

1919-1939 (New York: Harper & Row, 1964), pp. 63-88; Michael Howard, "Morality and Force in International Politics", *Studies in War and Peace,* (London: Temple Smith, 1970), pp. 235-250.

[79] Castells, (2004), pp. 17 – 21.

[80] Himanen uses the term Hacker Ethic, although notes that the negative connotations that come with the term Hacker, due to is appropriation by destructive individuals bent on criminal activity have distorted its original meaning as a informal society of technologically savvy and artfully creative individuals intent on the propagation of truth through the free sharing of information. See Pekka Himanen, "The Hacker Ethic as the Culture of the Information Age", *The Network Society: A Cross-cultural Perspective*, Manuel Castells (ed.), (Cheltenham UK: Edward Elgar Publishing, 2004), P. 424.

[81] Himanen, p. 423.

[82] See, for example, http://www.opensource.org/, and http://www.linux.org/lininfo/index.html.

Fundamental Dialectical Tension within the Network Centric Vision

> *As we prepare for the future, we must think differently and develop the kinds of forces and capabilities that can adapt quickly to new challenges and to unexpected circumstances. We must transform not only the capabilities at our disposal, but also the way we think, the way we train, the way we execute, and the way we fight.*
>
> *Donald Rumsfeld* [83]

This necessarily limited discussion of the role of information and networks in modern military thinking, and the development of the GIG emerging from the nature of Network Centric Warfare as contrasted with the development of the Internet and its impact on modern society suggests the tensions that underlie these developments. On the one hand, we can note that the role that information exchange has played within military contexts is an aspect of warfare that has a long history and hardly constitutes a revolutionary development. What does seem to be revolutionary is the near instantaneous networking of information sharing on a global basis due to developments in micro-electronics and their concomitant impact on ICTs. The potential offered by these technological developments seem to suggest new approaches to both how time and space operate in military operations, and reflect changes in terms of fundamental principles such as that of mass and concentration.

The power that militaries may derive from networks comes at a price of ensuring the security of the information domain from direct attack or clandestine infiltration in order to either mine its secrets or to surreptitiously alter its contents. The complexity of accomplishing this mission in a digital environment where concrete identities are difficult to establish suggests a level of control over information that contrasts starkly with speculative writings on the larger nature of networks for civil society. In effect, the conflations of military and civil uses of ICTs seem to establish a dialectical tension in terms of the fundamental concepts directing technological and social developments. Military uses of ICTs seek to replicate the power they lend to civil society in terms of their impact on innovation, creativity, and expansion of knowledge. Nevertheless, in order to protect the competitive advantages

[83] *Transformation Planning Guidance*, (2003), p. 1.

afforded to networked militaries, a level of control on networked information and its access is necessary to the extent of possibly squashing the very features that were sought after in the first place.

To a certain degree, one must be careful of accepting at face value the mythologies [84] that surround both the Internet and military use of networked technologies. The Open Source Movement itself accepts the positive role that trade secrets play in some product development where competitive advantage is generated through research and development that must be protected against competitors.[85] As such, the need to protect corporate competitive advantages in the business environment equates closely with the state's need to protect national security (or, indeed, the individual's need to protect their own privacy). The growing development of e-commerce points to the ability to use information in a proprietary manner as opposed to its open, anarchical exploitation.

Similarly, an examination of the principals that underlie the Open Source Movement and, indeed, Hinamen's culture of innovation itself call to mind the military principle of *auftragstaktik.* As described by Richard Hunter, Open Source development is guided by "extraordinary talent, clear vision of the goal, a deadly enemy, extraordinary tools, and autonomy and responsibility."[86] This compares remarkably with the observations of Germany's 1933 doctrine handbook for infantry operations, the *Truppenfuhrung*, which noted that:

1. The conduct of war is an art, a free creative activity that rests on scientific foundations. It makes the most extreme demands on the individual.
2. The conduct of war is based on continuous ongoing development. New tools of war give armed conflict an ever-changing shape.[87]

Auftragstaktik's decentralized approach to operations devolves a significant amount of creative freedom all down the command hierarchy even into the ranks of non-

[84] See Vincent Moscoe, "Myth and Cyberspace", *The Digital Sublime: Myth, Power, and Cyberspace*, (Cambridge Ma: MIT Press, 2004).
[85] See http://www.opensource.org/advocacy/secrets.php for example. The limitation on secrecy and knowledge is reached when many similar products are circulating performing similar services; at that point, they argue, it makes more sense to open up research in order that products and services can be improved through information sharing.
[86] Richard Hunter, *World Without Secrets: Business, Crime, and Privacy in the Age of Ubiquitous Computing*, (New York: John Wiley and Sons, 2002), p. 97.
[87] Quoted in Williamson Murray, "Contingency and Fragility of the German RMA", *The Dynamics of Military Revolution, 1300-2050*, (Cambridge: Cambridge University Press, 2001), MacGregor Knox & Williamson Murray (ed.s), p. 159.

commissioned officers.[88] The goal of *auftragstaktic,* as von Seekt saw it, was "a soldier who, in character, capability, and knowledge, is self-reliant, self-confident, dedicated, and *joyful* in taking responsibility as a man and as a military leader."[89] In many ways, von Seekt's observations capture the essence of both the Open Source Movement and Hinamen's "culture of innovation."

It is also possible to overstress the role that freedom plays in the foundations of the Internet. Just as creativity and initiative in military endeavours have had an important role to play, so too does control and restraint feature strongly in the architecture of the Internet. Control through information is central to the notion of cybernetics, and as Burnett and Marshall discuss, modern computer technology is a concatenation of cybernetic processes simplifying complex series of events. Yet the power that is generated by these steering systems comes at a cost of constraint within the confines of its very design parameters. As they elaborate, "the computer user must conform to some of the rules of the computer and Web as technologies."[90] Similarly, literature on the Orwellian nature of databases and the centralized control of information also point to more totalitarian outcomes than the anarchic Internet myth.

The necessary point here is not that the GIG will be unable to innovate because civilian web users will always have far greater power to manipulate and exploit information within the anarchical confines of the Internet. The dialectic of innovation and control will play itself out in both civil and military domains of the network environment in unpredictable fashions. Rather it is necessary to point out that even in the most liberal of national security networks, the role that information assurance will play guarantees that coalition interoperability will be subject to an extraordinarily high degree of control. If unrestricted trust is difficult to establish in a

---

[88] Robert Leonhard, *The Art of Maneuver: Maneuver Warfare Theory and AirLand Battle*, (Novato Ca: Presidio Press, 1991), pp. 50-51.
[89] Murray (2001), pp.160-161. Emphasis added.
[90] Burnett & Marshall (2003), pp. 27-28. A classic example of this problem is the misinterpretation of sensor data by CIC operators in the USS Vincennes, portrayed by the system as a F-14 when in fact, the contact was a civilian airliner. The misidentification was caused when an Iranian F-14 was taxiing at Bandar-Abbas airport at the same moment Iran Air Flight 655, causing IFF systems to confuse the two aircraft as one and the same thing. See, Marita Turpin, Niek du Plooy, "Decision-making Biases and Information Systems", *Decision Support in an Uncertain and Complex World: The IFIP TC8/WG8.3 International Conference*, accessed at http://vishnu.sims.monash.edu.au:16080/dss2004/proceedings/pdf/77_Turpin_Plooy.pdf, April 9, 2006. Similar issues can occur with respect to trust and digital identies.

purely national setting, then its achievement in a combined military network is most unlikely, even between the closest of allies.

As elaborated earlier, networks enhance power through their scalability, survivability, and flexibility. The ability for actors to take advantage of these features, however, critically depends on "the pattern of power present in the configuration of the network".[91] As Arthur Cebrowski famously observed, if "you are not on the net… you are not in a position to derive power from the information age."[92] But just as not everyone on the planet is able to access the Internet, not all military forces are able to interoperate with larger powers. In many studies, such outcomes have been largely portrayed in terms of inadequate capital investment in communication and information sharing technologies, or a failure of US technological developments to facilitate high levels of allied interoperability. This mirrors the observation that those who have not participated in the information developments of the last decade have simply failed to incorporate "previous social forms into the new dominant logic" of the information age. Castells, criticizes that such a focus on the emerging "digital divide" misses the point that fragmentation is a "structural feature of the network society."

> This is because the reconfiguring capacity inscribed in the process of networking allows the programs governing every network to search for valuable additions everywhere and to incorporate them, while bypassing and excluding those territories, activities, and people that have little or no value for the performance of the tasks assigned to the network.[93]

Exclusionary practices in networks result in a differentiation in terms of labour, distinguishing between those who are sources of innovation, those who simply carry out instructions, and those who are irrelevant as either workers or consumers.[94] The role that coalition partners will play in shaping the larger network and the goals towards which it will work will not necessarily be determined by technical capability or ability to interoperate. While plug and play interoperability will undoubtedly be important for those that do participate, who are allowed within the larger confines of

[91] Castells (2004), p. 12.
[92] Peter Howard, "The USN's Designer of Concepts," *Jane's Defence Weekly,* 3 October 2001.
[93] Castells (2004), p. 23.
[94] *Ibid,* p. 29.

the network, and the role that they play therein will be determined by traditional national interests and in this matter, issues of operational control, and thus control of the interpretation of information on the network will be central. By nature of the fact that in most operations, US forces will establish and control the majority of the network, US forces will play roles both as innovators and doers. Questions must be posed as to whether coalition partners can also play roles as innovators within a network, or whether they will be relegated to less powerful roles, drones in other words. The term "flags around the table" heard frequently in the context of coalition operations, neatly captures the reality of partners as irrelevant players. Cast in terms of the impact of this structural feature on military cooperation, networks pose a looming challenge for an age of coalitions.

IDSS Working Paper Series

1. Vietnam-China Relations Since The End of The Cold War (1998)
   Ang Cheng Guan

2. Multilateral Security Cooperation in the Asia-Pacific Region: Prospects and Possibilities (1999)
   Desmond Ball

3. Reordering Asia: "Cooperative Security" or Concert of Powers? (1999)
   Amitav Acharya

4. The South China Sea Dispute re-visited (1999)
   Ang Cheng Guan

5. Continuity and Change In Malaysian Politics: Assessing the Buildup to the 1999-2000 General Elections (1999)
   Joseph Liow Chin Yong

6. 'Humanitarian Intervention in Kosovo' as Justified, Executed and Mediated by NATO: Strategic Lessons for Singapore (2000)
   Kumar Ramakrishna

7. Taiwan's Future: Mongolia or Tibet? (2001)
   Chien-peng (C.P.) Chung

8. Asia-Pacific Diplomac*ies:* Reading Discontinuity in Late-Modern Diplomatic Practice (2001)
   Tan See Seng

9. Framing "South Asia": Whose Imagined Region? (2001)
   Sinderpal Singh

10. Explaining Indonesia's Relations with Singapore During the New Order Period: The Case of Regime Maintenance and Foreign Policy (2001)
    Terence Lee Chek Liang

11. Human Security: Discourse, Statecraft, Emancipation (2001)
    Tan See Seng

12. Globalization and its Implications for Southeast Asian Security: A Vietnamese Perspective (2001)
    Nguyen Phuong Binh

13. Framework for Autonomy in Southeast Asia's Plural Societies (2001)
    Miriam Coronel Ferrer

14. Burma: Protracted Conflict, Governance and Non-Traditional Security Issues (2001)
    Ananda Rajah

15. Natural Resources Management and Environmental Security in Southeast Asia: Case Study of Clean Water Supplies in Singapore (2001)
Kog Yue Choong

16. Crisis and Transformation: ASEAN in the New Era (2001)
Etel Solingen

17. Human Security: East Versus West? (2001)
Amitav Acharya

18. Asian Developing Countries and the Next Round of WTO Negotiations (2001)
Barry Desker

19. Multilateralism, Neo-liberalism and Security in Asia: The Role of the Asia Pacific Economic Co-operation Forum (2001)
Ian Taylor

20. Humanitarian Intervention and Peacekeeping as Issues for Asia-Pacific Security (2001)
Derek McDougall

21. Comprehensive Security: The South Asian Case (2002)
S.D. Muni

22. The Evolution of China's Maritime Combat Doctrines and Models: 1949-2001 (2002)
You Ji

23. The Concept of Security Before and After September 11 (2002)
a. The Contested Concept of Security
Steve Smith
b. Security and Security Studies After September 11: Some Preliminary Reflections
Amitav Acharya

24. Democratisation In South Korea And Taiwan: The Effect Of Social Division On Inter-Korean and Cross-Strait Relations (2002)
Chien-peng (C.P.) Chung

25. Understanding Financial Globalisation (2002)
Andrew Walter

26. 911, American Praetorian Unilateralism and the Impact on State-Society Relations in Southeast Asia (2002)
Kumar Ramakrishna

27. Great Power Politics in Contemporary East Asia: Negotiating Multipolarity or Hegemony? (2002)
Tan See Seng

28. What Fear Hath Wrought: Missile Hysteria and The Writing of "America" (2002)
Tan See Seng

29. International Responses to Terrorism: The Limits and Possibilities of Legal Control of Terrorism by Regional Arrangement with Particular Reference to ASEAN (2002)
Ong Yen Nee

30. Reconceptualizing the PLA Navy in Post – Mao China: Functions, Warfare, Arms, and Organization (2002)
Nan Li

31. Attempting Developmental Regionalism Through AFTA: The Domestics Politics – Domestic Capital Nexus (2002)
Helen E S Nesadurai

32. 11 September and China: Opportunities, Challenges, and Warfighting (2002)
Nan Li

33. Islam and Society in Southeast Asia after September 11 (2002)
Barry Desker

34. Hegemonic Constraints: The Implications of September 11 For American Power (2002)
Evelyn Goh

35. Not Yet All Aboard…But Already All At Sea Over Container Security Initiative (2002)
Irvin Lim

36. Financial Liberalization and Prudential Regulation in East Asia: Still Perverse? (2002)
Andrew Walter

37. Indonesia and The Washington Consensus (2002)
Premjith Sadasivan

38. The Political Economy of FDI Location: Why Don't Political Checks and Balances and Treaty Constraints Matter? (2002)
Andrew Walter

39. The Securitization of Transnational Crime in ASEAN (2002)
Ralf Emmers

40. Liquidity Support and The Financial Crisis: The Indonesian Experience (2002)
J Soedradjad Djiwandono

41. A UK Perspective on Defence Equipment Acquisition (2003)
David Kirkpatrick

42. Regionalisation of Peace in Asia: Experiences and Prospects of ASEAN, ARF and UN Partnership (2003)
Mely C. Anthony

43. The WTO In 2003: Structural Shifts, State-Of-Play And Prospects For The Doha Round (2003)
Razeen Sally

44. Seeking Security In The Dragon's Shadow: China and Southeast Asia In The Emerging Asian Order (2003)
Amitav Acharya

45. Deconstructing Political Islam In Malaysia: UMNO'S Response To PAS' Religio-Political Dialectic (2003)
Joseph Liow

46. The War On Terror And The Future of Indonesian Democracy (2003)
Tatik S. Hafidz

47. Examining The Role of Foreign Assistance in Security Sector Reforms: The Indonesian Case (2003)
Eduardo Lachica

48. Sovereignty and The Politics of Identity in International Relations (2003)
Adrian Kuah

49. Deconstructing Jihad; Southeast Asia Contexts (2003)
Patricia Martinez

50. The Correlates of Nationalism in Beijing Public Opinion (2003)
Alastair Iain Johnston

51. In Search of Suitable Positions' in the Asia Pacific: Negotiating the US-China Relationship and Regional Security (2003)
Evelyn Goh

52. American Unilaterism, Foreign Economic Policy and the 'Securitisation' of Globalisation (2003)
Richard Higgott

53. Fireball on the Water: Naval Force Protection-Projection, Coast Guarding, Customs Border Security & Multilateral Cooperation in Rolling Back the Global Waves of Terror from the Sea (2003)
Irvin Lim

54. Revisiting Responses To Power Preponderance: Going Beyond The Balancing-Bandwagoning Dichotomy (2003)
Chong Ja Ian

55. Pre-emption and Prevention: An Ethical and Legal Critique of the Bush Doctrine and Anticipatory Use of Force In Defence of the State (2003)
Malcolm Brailey

56. The Indo-Chinese Enlargement of ASEAN: Implications for Regional Economic Integration (2003)
Helen E S Nesadurai

57. The Advent of a New Way of War: Theory and Practice of Effects Based Operation (2003)
Joshua Ho

58. Critical Mass: Weighing in on Force Transformation & Speed Kills Post-Operation Iraqi Freedom (2004)
Irvin Lim

59. Force Modernisation Trends in Southeast Asia (2004)
Andrew Tan

60. Testing Alternative Responses to Power Preponderance: Buffering, Binding, Bonding and Beleaguering in the Real World (2004)
Chong Ja Ian

61. Outlook on the Indonesian Parliamentary Election 2004 (2004)
Irman G. Lanti

62. Globalization and Non-Traditional Security Issues: A Study of Human and Drug Trafficking in East Asia (2004)
Ralf Emmers

63. Outlook for Malaysia's 11th General Election (2004)
Joseph Liow

64. Not *Many* Jobs Take a Whole Army: Special Operations Forces and The Revolution in Military Affairs. (2004)
Malcolm Brailey

65. Technological Globalisation and Regional Security in East Asia (2004)
J.D. Kenneth Boutin

66. UAVs/UCAVS – Missions, Challenges, and Strategic Implications for Small and Medium Powers (2004)
Manjeet Singh Pardesi

67. Singapore's Reaction to Rising China: Deep Engagement and Strategic Adjustment (2004)
Evelyn Goh

68. The Shifting Of Maritime Power And The Implications For Maritime Security In East Asia (2004)
Joshua Ho

69. China In The Mekong River Basin: The Regional Security Implications of Resource Development On The Lancang Jiang (2004)
Evelyn Goh

70. Examining the Defence Industrialization-Economic Growth Relationship: The Case of Singapore (2004)
Adrian Kuah and Bernard Loo

71. "Constructing" The Jemaah Islamiyah Terrorist: A Preliminary Inquiry (2004)
Kumar Ramakrishna

72. Malaysia and The United States: Rejecting Dominance, Embracing Engagement (2004)
Helen E S Nesadurai

73. The Indonesian Military as a Professional Organization: Criteria and Ramifications for Reform (2005)
John Bradford

74. Martime Terrorism in Southeast Asia: A Risk Assessment (2005)
Catherine Zara Raymond

75. Southeast Asian Maritime Security In The Age Of Terror: Threats, Opportunity, And Charting The Course Forward (2005)
John Bradford

76. Deducing India's Grand Strategy of Regional Hegemony from Historical and Conceptual Perspectives (2005)
Manjeet Singh Pardesi

77. Towards Better Peace Processes: A Comparative Study of Attempts to Broker Peace with MNLF and GAM (2005)
S P Harish

78. Multilateralism, Sovereignty and Normative Change in World Politics (2005)
Amitav Acharya

79. The State and Religious Institutions in Muslim Societies (2005)
Riaz Hassan

80. On Being Religious: Patterns of Religious Commitment in Muslim Societies (2005)
Riaz Hassan

81. The Security of Regional Sea Lanes (2005)
Joshua Ho

82. Civil-Military Relationship and Reform in the Defence Industry (2005)
Arthur S Ding

83. How Bargaining Alters Outcomes: Bilateral Trade Negotiations and Bargaining Strategies (2005)
Deborah Elms

84. Great Powers and Southeast Asian Regional Security Strategies: Omni-enmeshment, Balancing and Hierarchical Order (2005)
Evelyn Goh

85. Global Jihad, Sectarianism and The Madrassahs in Pakistan (2005)
Ali Riaz

86. Autobiography, Politics and Ideology in Sayyid Qutb's Reading of the Qur'an (2005)
Umej Bhatia

87. Maritime Disputes in the South China Sea: Strategic and Diplomatic Status Quo (2005)
Ralf Emmers

88. China's Political Commissars and Commanders: Trends & Dynamics (2005)
Srikanth Kondapalli

89. Piracy in Southeast Asia New Trends, Issues and Responses (2005)
Catherine Zara Raymond

90. Geopolitics, Grand Strategy and the Bush Doctrine (2005)
Simon Dalby

91. Local Elections and Democracy in Indonesia: The Case of the Riau Archipelago (2005)
Nankyung Choi

92. The Impact of RMA on Conventional Deterrence: A Theoretical Analysis (2005)
Manjeet Singh Pardesi

93 Africa and the Challenge of Globalisation (2005)
Jeffrey Herbst

94 The East Asian Experience: The Poverty of 'Picking Winners (2005)
Barry Desker and Deborah Elms

95 Bandung And The Political Economy Of North-South Relations: (2005)
Sowing The Seeds For Revisioning International Society
Helen E S Nesadurai

96 Re-conceptualising the Military-Industrial Complex: A General Systems Theory Approach (2005)
Adrian Kuah

97 Food Security and the Threat From Within: Rice Policy Reforms in the Philippines (2006)
Bruce Tolentino

98 Non-Traditional Security Issues: Securitisation of Transnational Crime in Asia (2006)
James Laki

99 Securitizing/Desecuritizing the Filipinos' 'Outward Migration Issue'in the Philippines' Relations with Other Asian Governments (2006)
José N. Franco, Jr.

100 Securitization Of Illegal Migration of Bangladeshis To India (2006)
Josy Joseph

101 Environmental Management and Conflict in Southeast Asia – Land Reclamation and its Political Impact (2006)
Kog Yue-Choong

102 Securitizing border-crossing: The case of marginalized stateless minorities in the Thai-Burma Borderlands (2006)
Mika Toyota

103 The Incidence of Corruption in India: Is the Neglect of Governance Endangering Human Security in South Asia? (2006)
Shabnam Mallick and Rajarshi Sen

104 The LTTE's Online Network and its Implications for Regional Security (2006)
Shyam Tekwani

105 The Korean War June-October 1950: Inchon and Stalin In The "Trigger Vs Justification" Debate (2006)
Tan Kwoh Jack

106 International Regime Building in Southeast Asia: ASEAN Cooperation against the Illicit Trafficking and Abuse of Drugs (2006)
Ralf Emmers

107 Changing Conflict Identities: The case of the Southern Thailand Discord (2006)
S P Harish

108 Myanmar and the Argument for Engagement: *A Clash of Contending Moralities?* (2006)
Christopher B Roberts

109 TEMPORAL DOMINANCE (2006)
Military Transformation and the Time Dimension of Strategy
Edwin Seah

110 Globalization and Military-Industrial Transformation in South Asia: An Historical Perspective (2006)
Emrys Chew

111 UNCLOS and its Limitations as the Foundation for a Regional Maritime Security Regime (2006)
Sam Bateman

112 Freedom and Control Networks in Military Environments (2006)
Paul T Mitchell