

Preparing the Instantaneous Battlespace: A Cultural Examination of Network-Centric Warfare

ABSTRACT

The aftermath of the Cold War signalled a revision in the global position of the United States and a new emphasis on the country's status as a military superpower. Liberated from the stand-off between rivals that existed with the Soviet Union, the United States military has been able to greatly expand its scope of operational theories and aspire toward global dominance, using such programs as the Air Force's Global Reach, Global Strike, The Navy's Aegis Program and the Department of Defense, Joint Vision 20/20 Full Spectrum Dominance. Each of these examples suggests the expansion of the battlefield to well beyond what had been understood as the limits of military ambition. By exploiting the strategic capabilities of information based technologies, military thinking has been reoriented in a number of fundamental ways, all of which are associated with the doctrinal conceptualization of the Revolution in Military Affairs and the development of Network-Centric Warfare. Despite a change in presidential administrations, the tendency to globalize the battlespace prevails.

RÉSUMÉ

Préparer instantanément l'espace de guerre : examen culturel de la guerre en réseau

La période suivant la fin de la Guerre froide a suscité une révision du positionnement mondial des États-Unis et a placé l'accent sur le statut de superpuissance militaire du pays. Sorties de l'impasse qu'était la confrontation avec l'Union soviétique, les forces armées américaines ont pu étendre largement l'envergure de leurs théories opérationnelles et aspirer à la domination mondiale, au moyen de programmes tels que les Global Reach et Global Strike de l'Air Force, le système Aegis de la Navy et le « Spectre de la domination totale » du programme Joint Vision 2020 du Ministère de la Défense. Chacun de ces exemples suggère l'expansion du champ de bataille bien au-delà de ce que l'on tenait autrefois pour les limites de l'ambition militaire. En exploitant les capacités stratégiques des technologies de l'information, la pensée militaire s'est réorientée vers un certain nombre de fondamentaux, tous associés à la conceptualisation doctrinale de la révolution dans

les Affaires militaires et le développement d'un réseau guerrier centralisé. Malgré le changement d'administration présidentielle, la tendance à la mondialisation du champ de bataille se maintient.

ix

Network-Centric Warfare (NCW) is a military doctrine developed by the United States Department of Defense and designed to mobilize information into a competitive fighting advantage through the networking of operations and forces. NCW is an attempt to adapt to the rapid changes associated with information systems and the globalization of the economy, against the operational challenges of all-volunteer forces. Globalization and technological transformation have led to a greater need for interoperability on the part of military. The idea of networking is comprehensive throughout the planning and implementation of the doctrine. Melding human action and military capability, NCW signifies the integration of human systems and technical capacity into a networked, joint command structure. This total integration of forces has been theorized to encompass an expanded theatre of operations designed for globally scaled missions in order to achieve global dominance, both militarily and through the use of information systems. The transition is associated with new partnerships with other military and with the private sector. The paradigm relies on contract arrangements to carry out the majority of operations, including the management of troops, design of weapons systems, formulation of strategy and procurement of supplies and support arrangements. Network-Centric warfare represents the most seismic change to the U.S. military since the Department of Defense was established in 1947.

The evolution of Network-Centric warfare emerged from the confluence of three historical trajectories: the rapid technological change associated with the globalization of communications and technology, which has led to a greater emphasis on networking; the rise of militarism as an ideology following the Cold War, which reorganized the military along the lines of joint operations with tightened control at the top; and, finally, the increasing privatization of government functions. The paradigmatic foundation of NCW borrows from corporate economic restructuring as a model, particularly the managerial theory of "just-in-time" (JIT), production designed for rationalizing systems and increasing communication through networks of labour, technologies and transport. In military terms, and using an integrative approach, JIT networking seeks to produce responsive firepower and massed effects in real-time operation. The concept of massed effects borrows from the language of complexity theory to suggest that effects will be overwhelming and multiply in a self-organizing fashion.

The concept of interoperability comes into play as a means for achieving total informational awareness through the integration of military systems and manpower into the global command structure. The paradigm, in some sense, presents a double-edged paradox in that the magnification capabilities of NCW global risk scenarios produce a quest for an unachievable level of perceptual awareness. Nonetheless, the impetus behind this organizational logic requires the creation of a total global security environment. Toward this end, the goal of NCW is to establish a “predictive culture” throughout all service branches, agencies, organizations and personnel and among allies and private contractors. The human and technological elements of NCW are merged into a networked membrane outfitted with acute sensory capabilities. The key for NCW operators is to maintain an integrated network that enables precise and instantaneous reaction. NCW assumes a level of sensitivity resting within each weapon system, information system and human actor. Within this calculation, there is a collapsing of geographic distance. The instantaneous response expected from network-centric operations requires total knowledge not only to defeat an “unprepared adversary, but also to the defeat of a world as a field” (Virilio 1986: 133). Underlying this is an ecology of responsiveness emulating the command-driven logic of an integrated computer network.

The research informing this paper is derived from a range of intersecting literature that links the role of technological transformation with economic restructuring and the rise of various networked social formations (Castells 1996; DeLanda 1991; Harvey 2006; Hirst and Zietlin 1989; Wallerstein 2009). The research also incorporates defence literature, including formative work (Arquilla and Ronfeldt 1996, 1998; Cebrowski and Gartska 1998; Shultz 1991; VanCreveld 1991) and a wealth of recent military literature on technological and economic transformation (Berkowitz 2003; Cares 2006; Mitchell 2009; Safranski 2008). In addition, the article incorporates an emerging body of cultural theory focused on new forms of conflict (Armitage 2006; Berkowitz 2003; Blackmore 2005; Singer 2003; Turse 2008; Virilio 1986, 1991, 2009). Such literature is enhanced by a small body of anthropological research dedicated to examining military transformation in the current era (Grey 1997; Keenan 2009; Gutmann and Lutz 2010). The majority of anthropological material, however, is focused on the use of ethnographic knowledge in intelligence operations (Gonzalez 2009; Miyoshi 2007). This paper attempts to examine wholesale conceptual changes in the military from a cultural, as well as anthropological, perspective. It is part of a larger, ongoing ethnographic study on the social effects of military privatization. The work is intended to render a more contextualized picture of the economic and technical transitions associated with the rise of networked forms of warfare, and to supply a historical context for envisioning the virtual simulation of battle in the context of the globalization of warfare.

This article first examines the conceptual history of the Network-Centric Warfare paradigm and identifies the communicative features that have informed its evolution. It also interrogates NCW as a general framework concerned with the nature of conflict, conceived as global in scope and reliant upon simulated information. Second, it will identify the discursive features of NCW based on the conceptualization of global threats in terms of intrinsic qualities (stereotypical signatures of cultural difference, i.e., radical Islam). The discursive features include the development of an aesthetic of soldiering suitable for establishing conditions favourable to U.S. interests. These conditions are predicated on the continuous assessment of threats and instantaneous global response.

Finally, changes in military strategy associated with network-centrism are predicated on the concept of the network as a weapon, with all of the assumed cultural, geographic and temporal features built into the operation of the system. Therefore, the paper poses questions related to the transformation of military strategy and the potential dislocations between the ideals of the Network-Centric paradigm and the reality of an evolving doctrine of warfare that has no identifiable cultural, geographic or temporal boundaries.

Historical Background

The term Network-Centric Warfare is usually credited to Vice Admiral Cebrowski and John J. Garstka in their 1998 article entitled “Network-Centric Warfare: Its Origin and Future.” Preceding this publication, Admiral William A. Owens produced an article for the Institute of National Security Studies, entitled “The Emerging System of Systems,” which described a constellation of firepower combined with manpower to produce “dominant battle-space knowledge” including the use of sensors, precision weapons and command and control systems with “enhanced situational awareness, rapid target assessment and distributed weapons management” (Owens 1996). Owens’s paper became one of the conceptual templates for the Joint Vision 2010 plan issued by the Joint Chiefs of Staff, introducing concepts such as, “Dominant Maneuver,” “Precision Engagement,” “Focused Logistics” and “Full Spectrum Dominance.” The article aimed to theorize a range of missions, from peacekeeping to full-scale warfare that uses technology to achieve massed effects through information superiority” (Mitchell 2006: 5). A number of publications underscored the growing interest in information regarding conflict scenarios, including “The Rise of Netwar” by Arquilla and Ronfeldt (1998); “Understanding Information Warfare” by Alberts et al. (2001); and “Power to the Edge: Command and Control in the Information Age” by Alberts and Hayes (2003). The foundational ideas, however, have been mostly attributed to the writings of Vice Admiral Arthur Cebrowski and John Gartska.

The emergence of Network-Centric Warfare corresponded with the broader transformations attributed to the globalization of economy and culture, popularized by the work of futurist critics Alvin and Heidi Toffler, who coined the phrase “The way we make wealth is the way we make war” (1993). Such transformations have also been theorized in terms of “Postmodern War” (Grey 1997). Changes in military doctrine have been predicated on the accelerated role of communication technologies in military planning and the “co-evolution of economics, information technology and business processes and organizations” (Kellner 2003: 3). Manuel Castells conceptualizes these changes in terms of the “network society,” emphasizing the broader social and economic transformations brought about by communication technologies and the connection between technological changes in the military and business (1996). NCW borrows from the fields of organizational behaviour, economics, anthropology, biology and sociology, and makes use of the popular understanding of chaos and complexity theory. The conceptual ideas of NCW are often encapsulated in the language of management studies, and use social networking as a framework to better understand the effects of technology, strategy, organization, performance and personnel effectiveness in combat (Edison 2006). NCW signifies a reconceptualization of the concept of warfare associated with technological change and the cultural traits necessary for the mastery of the military environment through coordinated information, training and weapons systems.

The early stages of NCW emerged from U.S. Department of Defense planning after the Second World War, derived from new computational capabilities of computer networks coupled with the development of advanced weapons and detection systems (Mitchell 2006; Castells 1996; DeLanda 1991). This transformation involved political, economic and cultural changes associated with globalization, and the spectacular technological development of the postwar period. Many changes were instigated within the military, including developments with imaging, the Internet, microprocessing and complex systems research. These innovations were accomplished through government, military and university research partnerships (Castells 1996; DeLanda 1991).

The Second World War saw the rapid technological development of imaging, radar, communications and targeting weapons systems. The U.S. strategy during the Cold War focused on containment; conflicts were usually carried out through proxy rather than direct opposition. Massive retaliation was almost unthinkable under the threat of mutually assured destruction; granted, the military has to develop flexible responses involving diplomacy and the use of surveillance and information systems to achieve defence objectives. The Cold War witnessed a period of deepening technological development, against the incipient realization of the coming nature of conflicts that foreshadowed the fall of the Soviet Union.

During the Vietnam War, the United States military faced a number of operational and manpower challenges. The Vietnam War was fought with a demoralized, draftee army. Given the unpopularity of the war, it was unlikely that the decade-long conflict would have continued without a conscripted military (Bradford and Brown 2008). The Vietnam War also combined unclear military objectives, vacillating between low intensity skirmishes to large-scale aerial and ground bombardment. After the engagement in Vietnam, strategic planners began reformulating objectives for military engagement with a focus on technological capabilities and an all-volunteer force.

When the Vietnam War ended, the U.S. was left with a smaller force based on voluntary service, and a reduced defence budget. The abolishment of military conscription represented a preliminary step toward greater reliance on contract arrangements and the privatization of military service. This normalization of conflict was consistent with other late-capitalist reorganizations, such as the reconceptualization of the soldier's body and its performance in terms of labour expectations. Like similar flexible labour regimes, the emphasis switched from a dedicated workforce to one of increasing adaptability and greater force delivery (Hirst and Zeitlin 1989). The military's version of economic rationalization became synonymous with the new military criterion of synchronization.

Throughout the 1970s and 80s, the U.S. Navy and Air Force developed informational warfare strategies with an increasing focus on both deterrent and low-intensity conflict. Much of the emphasis remained an outgrowth from the heyday of Soviet/U.S. posturing. This tendency formed the paradigmatic foundation for thinking about conflict following the collapse of the Berlin Wall. Yet the rapid advancement of technical means also enlarged spheres of interest through the use of optical tools, including the Star Wars Strategic Defense Initiative, computer-directed command-and-control systems, precision-guided munitions and stealth and satellite imaging. These played a role in the development of the NCW concept. The increased influence of operational theories of warfare also grew out of the attempt to learn from the Vietnam conflict, which was seen as a failure of coordination among service branches and called for the implementation of unified operational objectives (Thom 2000).

When the Cold War came to an end, the situation created a large void in the security environment. Global threats became less predictable, more variable and empowered in new ways. Moreover, the conventional responses to conflict were at their weakest. As former Soviet countries demobilized, a large influx of decommissioned soldiers entered the global labour pool. At the same time, a flood of cheap weapons were discharged from the former communist nations. The end of the Cold War re-instigated regional and civil conflicts that had previously been contained (Singer 2003). Postcolonial states dependent on patronage during the

height of U.S./Soviet tensions began dissolving as a result of internal political pressures.

Since the end of the Cold War, the incidence of civil war has increased spectacularly, while global growth in the number of conflict zones has doubled (Kaldor 1999; Singer 2003; van Crevelde 1991). At the same time, the aftermath of the Cold War signalled a revision in the global position of the United States, placing a new emphasis on the country's status as the remaining military superpower. No longer constrained by the stalemate between rivals that existed with the Soviet Union, the U.S. military was able to expand its scope of operational theories and aspire toward global regimes of dominance, using programs such as the Air Force's Global Reach, Global Strike, the Navy's Aegis Program and the Department of Defense Joint Vision 20/20 Full Spectrum Dominance.

This reorientation reflected the expansion of the battlefield to beyond what had been understood as the limits of military ambition (Mitchell 2006). By exploiting the strategic capabilities of information-based technologies, military thinking was reoriented in relation to the doctrinal conceptualization of both the Revolution in Military Affairs (RMA) and the development of Network-Centric Warfare. The technological features of weapons programs and the increasingly global reach of such technologies underscores the ability to render, geo-strategically, an enlargement of military awareness, planning and intervention strategies on a global scale. It has also enabled the U.S. to engage other militaries in order to leverage its own security needs through joint planning, training, missions and the sharing of technology.

Revolution in Military Affairs

The Revolution in Military Affairs is a futuristic theory about the coming nature of warfare derived from technical and organizational recommendations for the restructuring of U.S. forces and their allies. The RMA theory rests on transformations in communications, information and space technologies. Often referred to as "The transformation," it involves a move toward total systems integration and is accompanied by other totalizing efforts such as the Office of Total Information Awareness and Total Situational Awareness programs.

The earliest RMA research was done by Marshal Nikolai Ogarkov and his colleagues for the Soviet Armed Forces during the 1970s and 80s (Metz and Kievit 1995). U.S. interest in the topic was initiated by Andrew Marshall, head of the internal Pentagon think tank The Office of Net Assessment (Trilling 2002). Support for the doctrine grew within political circles associated with the 1992 Defense Planning Guidance Initiative and the 1997 Project for a New American Century, involving former Vice President Dick Cheney, Paul Wolfowitz and Donald Rumsfeld, as well as a core group of pro-defence conservatives (Trilling

2002). The idea was disseminated to other nations also exploring the RMA's transformative effects on organization and technology. Canadian interest in the RMA began in the late 1990s, fuelled in part by an eagerness to maximize the nation's military capabilities. Commitment to the RMA, however, was also stimulated by a desire to avoid the geopolitical marginalization associated with non-adoption of the doctrine (Sloan 2002).

In the U.S., the RMA was greatly facilitated by the passage of the U.S. *Goldwater Nichols Act* in 1986, which initiated a sweeping transformation of the U.S. military. The Act entailed a streamlining of the military chain-of-command, consolidating control with the President and the Secretary of Defense. The *Goldwater-Nichols Act* initiated changes with both the chain-of-command and the interaction of the services, unifying these services under a Unified Combatant Command. The Commander-in-Chief of the Army underwent a name change to Combatant Commander (CCDR), enacted in 2002 by Rumsfelt, who reasoned that the title "Commander-in-Chief" should be reserved solely for the U.S. president. Under the new organization, CCDR designations were transformed to emphasize joint commands, missions and training. New personnel requirements for officers mandated joint duty and joint professional development instruction, while completion of joint ventures became a requirement for eligibility for promotion. Moreover, the overall orientation of the branches shifted from mission-driven commands to those focused on a geographic region within a global theatre of operations (Lederman 1999).

The new commands, finalized by 2007, have been broken into their regional responsibilities and functional duties, designated into ten geographic areas: U.S. Africa Command, U.S. Central Command, U.S. European Command, U.S. Pacific Command, U.S. Northern Command and U.S. Southern Command. The four functional duty commands include: U.S. Joint Forces Command, U.S. Special Operations Command, U.S. Strategic Command and U.S. Transportation Command. Each command is led by a four-star general or admiral chosen by the Secretary of Defense and the President, and confirmed by Congress. Strategic partnership in NORTHCOM includes Canada and Mexico, while USSOUTHCOM is building partnership capacity with Countries in the Caribbean, as well as in Central and South America. Thus, the development of partnerships corresponds to strategic interests in the geographically designated region.

The reorganized chain-of-command runs from the President to Secretary of Defense to the combatant commanders of the Unified Combatant Commands. Under the *Goldwater-Nichols Act*, the Service Chiefs have been delegated a secondary role in the conduct of war, and their duties have been relegated to organizing, training and equipping soldiers. Service chiefs no longer exercise operational control over their forces. Of all the service branches, the Army has

undergone disproportionate effects from the reorganization, losing its traditional control over the Central Asian, European and Southern theatres. In addition, the RMA represented a de-emphasis on provisioning for regular soldiers and a reallocation of resources to joint commands and special operations (Lederman 1986).

Validation for the RMA was fuelled in part by what was regarded as the dramatic asymmetrical victory by the U.S. in the 1991 Gulf War. U.S. dominance was evident in the use of satellite technologies, precision-guided weapons and communications systems. The swift success in the first Gulf War provided confirmation of the RMA's success, allowing U.S. commander Army General Norman Schwarzkopf to exercise full control over all service branches without having to consult with their respective commanders. The media coverage also made him a television star (Bourne 1999; Khalilzad, White and Marshall 1999).

The 1986 *Goldwater-Nichols Act* allowed for shared resources, eliminating some of the competition between branches for resources and equipment. It had a disciplining effect on the individual services by removing a good portion of operational authority over the respective branches. It also decreased disagreement within the command structure and created the context for service branches to share smart weapons, stealth and drone technologies, while increasing the move toward the interoperability of communications between services, thus stimulating the development of a joint doctrine. Without the restructuring in the Act, the integration of branches and restructuring and implementation of doctrinal changes would not have transpired. The *Goldwater-Nichols Act* was the most important step for realizing the goals of the RMA and for the implementation of Network-Centric Warfare.

The effect of changes to overall structure cannot be overstated. If the traditional organization of the military is pyramidal (i.e., hierarchical), then the new shape might be characterized as a standing arrow. The *Goldwater-Nichols Act* transferred an unprecedented amount of control to the Chairman of the Joint Chiefs of Staff, who holds almost as much authority as the Secretary of Defense. As the Secretary determines the appointment of the Joint Chiefs, this reinforces the tendency to appoint commanders of similar mind, thereby increasing the tendency of the two positions to ideologically converge and decreasing the diversity of opinions available. In turn, this further solidifies presidential authority over military matters, and reinforces authority at the top by creating a command structure that mirrors the doctrinal position of the President.

The self-reinforcing tendency is further solidified by consolidating the middle and upper command into a joint structure answerable immediately to the Secretary of Defense. Troops are broken into a two-class system made up of regulars, who disproportionately inhabit the bottom, and elite forces who are granted a great

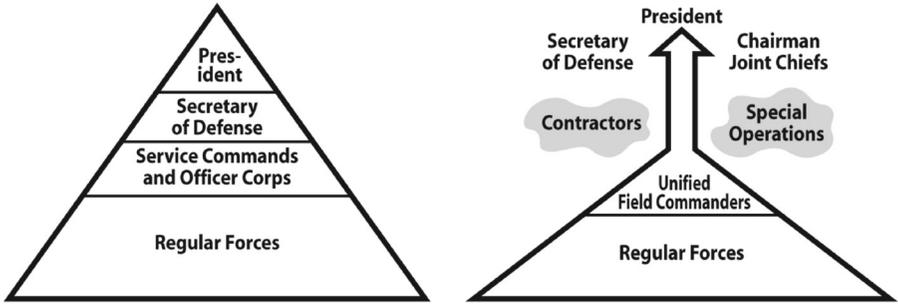


Fig. 1
Integrated Command Chain Specified by the Goldwater- Nichols Department of Defense Reorganization Act of 1986.

deal of operational and tactical autonomy. The *Act* set the stage for the private sector's greater involvement in warfare. Elite forces are now able to blend together in a grey universe of special operations, soldiers for hire, clandestine operatives and contract companies that characterize the field of conflict.

The *Goldwater-Nichols Act* has spelled the end of the public monopoly on the military with a shift toward private militarism (2003: 8). A wide spectrum of military and security functions that used to be exclusively under the public domain are now open to contractors. This has increased new supplies and demands in the global military market, many of which have been filled by for-profit military companies. This shift was facilitated by the philosophy of privatization dominating government discourse in the latter half of 20th century. Moreover, the failure of command economies in the former Soviet Union tended to further validate market driven approaches (Castells 1996; Harvey 2005; Singer 2003). By the 1990s, whenever governments on the left and right of the political spectrum addressed budget issues, they tended to fall back on the private sector. During the Clinton presidency, *The National Performance Review* stipulated the privatization of previously untouched areas of government, such as schools and prisons (Singer 2003). Privatization has since become the guiding principle of leading global financial institutions, such as the World Bank, the International Monetary Fund and the World Trade Organization. While the RMA was responsible for the move toward restructuring the military, it was the accelerated political drive toward privatization that provided the foremost catalyst for the growth of the global, for-profit defence industry.

Total System Integration

Network-Centric Warfare is predicated on the centrality of networks as a way of conceptualizing the organizational challenges of new technologies. It relies on joint operations between services, contractors and partnerships with other

militaries. The doctrine is articulated in the strong managerial language of just-in-time production. Simulations also play a critical role in how sensors, technologies and individual soldiers are reconceptualized as interchangeable parts of a system of systems. The new doctrine dramatizes the move from strategic warfare based on standing armies to a brand of pre-emptive warfare based on developing an informational ecology throughout the military. The goal is to establish a “predictive culture” (Phister, Busch and Plonisch 1996; Virilio 2009) able to penetrate all service branches, agencies, contractors, organizations and personnel in a process enabling instantaneous and precise reaction.

The culture of predictive surveillance differs from the concept of “comprehensive insurance” that dominated the intelligence-gathering of the last century and was focused on amassing information for national defence. The ambition of predictive surveillance is to secure supremacy on all fronts, from the globalization of geopolitical relations to the militarization of circumterrestrial space. “Defenscive” and “Offensive” lose their meaning in the face of a genuine world security force made up of transnational, networked military partnerships organized around deterrence, or what Paul Virilio terms the “pure offensive” of global power (Virilio and Lotringer 1983: 41-47). While NCW supporters may refer to the transformation in the military as revolutionary, the concept of total deterrence has a politically reactionary quality that aims to logistically extend geo-presence into resource-rich networks using information as a panoptical weapon.

Like the distributed functions of a computer network, the objective is to attain “massed effects” from an economy of force by instantaneously moving technology and manpower where they are needed (Murdock 2002). The doctrinal precedents follow a progressive logic. NCW is to be achieved through a team effort aimed at the integration and synchronization of capabilities in the different service branches, based on the observation that a networked force improves information sharing, which in turn allows for the collaboration necessary to enhance the quality of information and achieve a shared situational awareness. Increased situational awareness enables the synchronization of capabilities, meant to increase the effectiveness of operations (Cebrowski and Gartska 1998).

The premise underlying the NCW concept is that military operations will increasingly capitalize on the advantages of information technology. Assuming that transformations in the economy and business are the actual driving forces in a new era of war, the military must shift from stationary operations to networked operations. This shift entails envisioning the military as part of a continuously adapting ecosystem. The model self-consciously mimics

the dynamics of growth and competition that have emerged in the modern economy. The new dynamics of competition are based on increasing returns on investment, competition within and between ecosystems, and

competition based on time. Information technology (IT) is central to each of these. (Cebrowski and Garska 1998: 3)

The NCW model displays much of the promotional language common in business marketing, with its emphasis on competition, capitalization and the rationalization of personnel.

NCW employs the language of “just-in-time” corporate restructuring when referencing “Network-Centric Retailing” (Cebrowski and Garska 1998: 3). The model uses Walmart as an example of an outperforming company able to achieve competitiveness by shifting to Network-Centric operations. Walmart is credited with translating information superiority into a competitive advantage by establishing an operational architecture of sensors, scanners and a transaction grid exhibiting a high level of awareness “within its retail ecosystem” of ninety million transactions per week (4). This information is shared with suppliers in real-time to control their production and distribution and to manage supply chains. Cebrowski and Garska note that when Walmart sells a lightbulb, a signal goes to General Electric telling them to make a new one. This degree of synchronization is purported to meet seasonal needs and market preferences in real-time. The Walmart model of synchronization operates to create local awareness within each store day by day, letting neighbourhood stores identify new opportunities, re-price items based on competition, or prominently display items with higher volume to increase sales (1998).

The NCW appropriation of just-in-time management language paints a compelling picture of synchronicity. It moves from viewing partners as independent to conceiving of them as part of the military’s own continuously adapting ecosystem, able to increase speed and profits from the automated command and control systems implemented on a transactional grid. NCW entails a major conceptual leap from seeing other militaries as competitors to envisioning them as an extension of U.S. force projection. Theoretically, the shift to NCW involves a transition away from drawn-out conflicts to faster, effective war fighting characterized by the speed of command and synchronization. Running throughout the paradigm is the metaphor of the computer with its push-button execution of command. The level of control attributed to NCW allows them to “lock out” enemy strategy and “lock in” success, permitting forces to develop the “speed of command.” The wording implies disseminating the orders from above almost immediately to the units and individuals on the battlefield, while reducing the friction derived from a commander’s lack of access to direct knowledge of battlefield. In principle, NCW enables forces to organize from the bottom up, mirroring the self-synchronizing capability present in both computers and ecosystems to “meet the commander’s intent” (Cebrowski and Garska 1998: 3)

At the heart of the change are the technologies, referred to as “force multipliers” (1998). The change involves a move away from slow, heavy, dedicated equipment

to light, rapid, flexible and smart weapons systems that can be networked into the larger system and thereby increase their effects. Weapons like exoskeletons, computerized helmets and eyepieces have been designed to augment a soldier's capabilities (Jordan 2007; Shachtman 2009). Such weapons share similarities with the smart technologies designed for the consumer market to facilitate networking and technology integration. However, military technologies differ in that the self-organizing capabilities have been enhanced for automated response. Technologies have been designed to be autonomous, such as unmanned aerial vehicles for strategic intelligence, reconnaissance and reaction. The arsenal includes weaponized imagery technologies augmented by satellite and aircraft surveillance, synthetic aperture radar, electro-optical cameras and infrared and other sensors. Video teleconferencing has augmented the development of a Common Operating Picture. Technologies in development include minesweepers, smart bombs, predator drones, nano-robotics and microscopic weapons with viral engines—all of which enhance the overall predictive culture of networked operations (Kellner 2007). Scale is a factor in the miniaturization of weapons that are light and transportable and have flexible uses. Another class of weapons merit descriptives such as “intelligent” and “brilliant,” underscoring their ability to think for themselves. These carry built-in communication relays to add to the overall networking capabilities.

The technologies are networked in such a way as to become smaller or larger depending on the military objectives. Virilio calls this altered experience the “logistics of perception” based on the use of optical substitution in battle. The disruption of time and space is a dimension of postmodern warfare, evident not only in the televised spectacle that simultaneously brings images closer even as they are sanitized of conflict, but also in the disappearance of the topographical features of war (Virilio and Lotringer 1983: 49). Conflict, in this sense, becomes a war of images, an infowar in which the disparity between the image of battle and actual battle falls subject to the enhancements and distortions of sensory disturbance. Accordingly, perceptual substitution reduces sight to the function of “a sighting device,” a form of vision without looking that “registers the waning of reality” (Armitage 2000).

Synthetic Architecture

The disciplinary circuits of control within a network emanate from both its decentralized structure and its unseen surveillance capabilities (Foucault 1985; Galloway and Thacker 2007). The dispersed nature of networks allow for a hyper vigilance, deploying decentralization as a means to re-centralize control. The impulse corresponds to Hardt and Negri's idea of biopower, harnessing the non-human aspects of networks (emergent systems, atoms, rhizomes and swarm dynamics) for the purpose of linking biology with the informatics of

Common Operating Picture of Network-centric battlefield

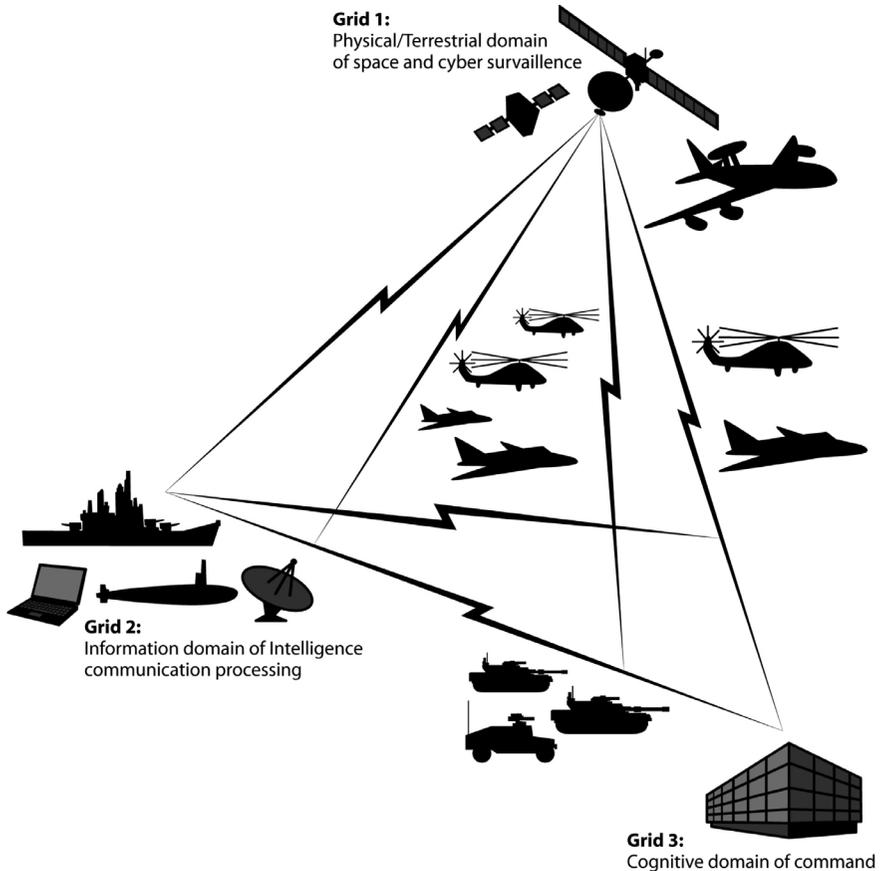


Fig. 2
The three domains of the network-centric battlespace.

control (2001). According to Gilles Deleuze, the signature of a control society is its dispersal and self-organizing capacity, its ability to transmute, mold and constantly change from one instant to the next (2002). Theoretically, this level of adaptability allows for the continuous monitoring and control of an environment remotely.

The doctrine of network-centrism starts with three premises of how the environment is sensed. The battlespace environment is sensed in terms of the physical domain, where events occur and are perceived by individuals and sensors. The data from the physical domain is then transferred to the information domain. Once received and processed, that information becomes part of the cognitive domain, where it is analyzed and acted upon. The three domains replicate the

“observe, orient, decide, act loop” feedback cycle first identified by Colonel John Boyd of the U.S. Air Force (Luddy 2005).

An underlying assumption guiding the conceptualization of a networked military is that the modern environment is too complex to be understood by any one individual, organization or service branch. Information technologies permit the rapid sharing of data, to such an extent that “edge entities,” those at the frontlines, should be able to pull information from repositories rather than relying on centralized headquarters to anticipate information needs and to “push” data to them (Alberts and Hayes 2003). The premise underlying NCW is that the more information that is available, the better. Edge entities have the most direct access to battle knowledge. Thus, the idea is to empower the edges by shortening the links of data transferred directly to the command, where the decision-making actually occurs. In this conceptualization, “edges” are assumed to be small units on the frontline, representing the individual, highly trained special operations soldiers in direct contact with the enemy. The impulse remains to brake the interceding links between command and the edges, so as to allow the command post to have direct contact with the most expert soldiers.

Cebrowski and Gartska argue that as a first step toward accomplishing this networked ecology, the network environment should be conceived of as a grid referencing the Global Information Grid (GIG). The authors recognize the advantages of a robust network topology on the battlefield, advocating the empowerment of the edges as an effective response to the kind of strategic environments present in the network age, including asymmetrical and urban warfare scenarios. Network-centrism is the cornerstone of the new Office of Force Transformation as mandated by the Secretary of Defense (Luddy 2005). The GIG serves as the intelligence backbone of the Department of Defense, as well as an evolving perceptual system, enhancing the visualization process through sensors, registers and data-absorption tools to produce an emergent picture of the global conflict environment.

The Global Information Grid serves as the technical framework to facilitate network-centric operations. It is an all-encompassing system governing all communication aspects of the Department of Defense. Advanced weapons, sensors and command and control systems are linked to the grid, actualizing the “system of systems” that is integral to the military’s massive integration effort originally specified by Albert and Hayes (2001). The grid architecture comprises a range of information acquisition tools including sensors, radar, radio frequency, infrared receptors, low light and optical devices, acoustical detectors and human operators. Another level of the grid incorporates communication satellites, data transmission, microwave relays and computers and command centres. The information grid transmits all of the sensory information, intelligence and orders in real-time, efficiently connecting logistics to control operations. The transaction

grid utilizes the sensor and information grids to guide weapons to targets. Other weapons are considered “brilliant” since they contain auxiliary sensors able to attack autonomously by responding to self-initiated data streams (Murdock 2002).

More than a decade ago, the Pentagon began referencing the technical framework to facilitate Network-Centric operations through the Department of Defense Architecture Framework (DoDAF). The framework is the master platform for organizing both the system architecture and the enterprise architecture into an integrated network. It acts as a mechanism for visualizing and understanding the complexity of the NCW paradigm using graphics and textual references, and sets the protocols for interaction with the Global Information Grid. It also identifies the goals for interoperability. It is the interface for both military personnel and corporate contractors (Singer 2003). The system uses the acronyms of military-speak combined with the marketing language of global business.

The DoDAF evolved from two directives: the Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) and Technical Architecture Framework (TAFIM) programs. These two programs were initiated by the 1996 U.S. *Clinger-Cohen Act*, designed to improve the government’s management of information resources. The DoDAF went into operation in 2003 as a visualization device for providing a common operating picture that integrates information across the spectrum of missions, organizations, joint operations and multinational arrangements. It sets the rules and relationships and identifies a set of products for enhancing the entire system. The architecture includes families of systems, systems of systems and NCW systems. The framework acts as a shared interactive repository organized into Levels of Information System Interoperability.

The larger DoDAF framework is articulated in terms of products. The inventory offers a set of products used by defence customers and military and business personnel. These are all integrated into an architectural system containing portals and links meant to aid in visualizing the operational environment and complexity of human and technological relationships that make interoperability possible. The DoDAF framework is meant to interact with other systems, including the NATO Architecture Framework, the U.K. Ministry of Defense Architecture and the multinational IDEAS group comprised of Australia, Canada, the U.K. and the U.S. The DoDAF virtualizes the shared operating picture and demonstrates the available work products. A number of militaries have been developing NCW protocols, such as Australia and Sweden (Luddy 2005), but other countries have experienced difficulty overcoming the costs associated with the technology and installation. Countries unable to implement their own NCW technical architecture have opted for niche roles or secondary positions in the service of the overall Network-centric operations (Luddy 2005: 17; Mitchell 2009).

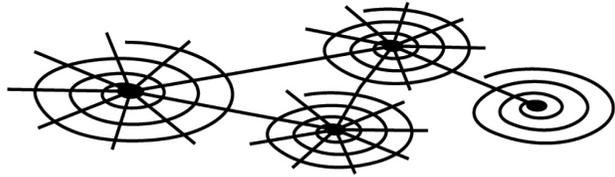
Countries wanting to participate in joint operations need to upgrade their capabilities in order to interface with the DoDAF architecture. The Canadian military exercises its coalition task force responsibilities in conjunction with NORTHCOM, the U.S. Departments of Homeland Security and Homeland Defense. This involves increasing integration within the country's own military, government and civil agencies, including Canada Command. For the most part, the Canadian military has been able to integrate its capabilities effectively with the U.S. Joint Command structure, although challenges have arisen with communications and the willingness of the U.S. Command to share information freely.

It has been noted that Canadian officers benefit from the training and expertise obtained on joint missions (Mitchell 2009). For many nations, however, this task has been difficult. To be considered for joint operations, an individual country must demonstrate its interoperability capabilities. Performance is evaluated in a simulated operational environment that provides the context from which to assess the DoDAF/C4ISR solutions. Countries must improve their command to meet the specifications of conventional and irregular warfare, demonstrate real-time voice and text translation and implement multinational joint staff coordination and information sharing. Countries must also demonstrate planning for psychological operations, computer network operations and electronic recovery missions. Each partner is expected to comply with the functional interoperability of forces, by integrating its communication and weapons systems while utilizing C4ISR military and business tools. Countries wishing to engage in joint operations must maintain integration with both the relevant business and military partnerships (Frank 2009).

In 2005, the U.S. *National Defense Authorization Act* set up the Business Transformation Agency (BTA), responsible for the enterprise architecture of the DoDAF. The *Act* gave to the business community the authority to determine priorities in the development and installation of the architecture for the DoDAF. The main focal areas for the BTA include investment management and the alignment of services, systems and solutions in support of the objectives of interoperable business solutions for the DoDAF. Two principle areas of enhancement include visualization enhancements and end-to-end enhancements that improve the business flows of the network architecture. The BTA has been granted authorization to define the business capabilities needed to achieve the priorities and to define the combinations of enterprise systems and initiatives needed to realize defence capabilities.

The development of the DoDAF exemplifies a significant shift in the values and priorities governing military planning. Private companies have been given a leading role in developing the architecture that defence capabilities depend on. The rationalization of defence functions has led to a dependence on the

Fig. 3
Sampling of network
mapping based on social
connectivity.



- **Visualization** involves auto-identification, matching social network links with categoric signatures of identification.
- **Recursive functions** amplify and multiply risks to include connections circumstantially attached through association.
- **Feedback Loops** reinforce the identification of risks through iteration of network tracking.

private sector to stay abreast of cutting-edge technical development. Though the military has been unable to compete for personnel with the private sector, the underlying philosophy of NCW nevertheless depends on the operational concept of “information dominance” (Singer 2003: 64). The Department of Defense relies on private contracts for the training of personnel, troubleshooting and repair of equipment, and programming of military matters. Often the companies that engineer high-tech weapons are the only ones who can maintain them. As the U.S. military becomes more reliant on the profit-seeking sectors to achieve its objectives, such companies will become more integral to determining the conflict spectrum, from designing the weapons to providing technical support advice in the field. This is leading to a greater civilianization of warfare, which stands in marked contrast to the traditional form of warfare as violence between powerful states for political purposes (Singer 2003: 64; von Clausewitz 1997).

The synthetic battlespace precludes civilian involvement in the representation of threats. The use of simulation by the military is not new; war games have been employed since the Second World War. However, recently developed simulation capabilities have included a level of automation and integration that permits almost immediate results, as the technology doing the simulating necessitates less human input (Krebs 2002). In the virtual simulation of warfare there is a higher propensity for false proof, however, because the representation of threats remains formulated from a synthetic automation of data that cycles through a feedback loop that rests on itself for verification.

Many network mapping simulations operate in a radial fashion, emanating from a central point to encompass an increasing number of connections through snowball sampling. Studies in complexity modelling demonstrate that a characteristic feature of a network is its ability to expand continuously, incorporating wider areas into its conceptual framework. This is particularly true of social network modelling, where the mapping of connections eventually achieves a level of density that approximates the “six degrees of separation” problem, in which everyone is

connected to everyone else on the planet by six or fewer acquaintances (Milgram 1967; Newman 2003; Watts 1999). In network modelling, threats lose much of their specificity as they are scripted together into a universal risk schematic. Individuals are networked together through their associative connections on a network grid, whether or not those connections exist in the real world. Amounting to a “guilty by virtual association” approach, the model may be less effective in identifying terrorists than in expanding the categories of definitions that qualify as pre-terrorist, since the sensory capability of computer-automated networking leads to a level of hyper-vigilance that exponentially widens what gets included as “threatening.”

These new dangers are identified as unconventional threats, while the protagonists are drawn from the low-intensity spectrum of warfare (van Creveldt 1991). In the absence of clear enemy definitions, fighting becomes focused on possible threats. These are portrayed as multiplying and driven by different logics other than statecraft; for instance, criminal behaviour and drug conflicts in Colombia, or the control over the diamond and coltan mines in the Congo. The largest force propelling such conflicts is money. The protagonists have also changed to include terrorists, forced child recruits, and soldierless forces such as pirates and looters. Key to the conceptualization of risk is the process of visualization. The visualization determines the threats and what kinds of actions and manpower are needed for intervention. At the far end of the risk scenario, the shaping of threats has broadened to include a number of unconventional actors, such as nongovernmental activists rechristened as “militant activists,” or civilians abducted from conflict regions who are re-termed enemy combatants (Arquilla and Ronfeldt 1996, 1997). In many cases, the visualization of such groups bears the stereotypical signature of cultural difference (i.e., tribal, radical, militant). Such identifications contain sweeping categorical assumptions about the intent and nature of the threats posed.

The globalization of conflict has meant that supposed terrorists operate within the multicultural environments of countries like the United States and Canada. In the case of the 2001 attack on the World Trade Center, the hijackers dressed in Western clothes and were virtually indistinguishable from the millions of Muslims living in the country. Tracking the full range of networking tools may thus be ineffective in preventing future attacks (Downey and Murdock 2003).

The aim of developing techniques for classifying and managing groups sorted by levels of danger replaces individual suspicion with categorical suspicion. The presumption of guilt implied in such a task implicates whole groups of people, while the burden remains on the individual to demonstrate their innocence against a field of presumed guilt. The networked systems of surveillance now under development obtain information from every available source. Such a level of acquisitiveness dismantles the protective shield between the military and the

civil domain traditionally relied upon to uphold civil liberties, and protects against unwarranted search, seizure and detention. The entire project elevates defence objectives across the whole of civilian life and marks the shift toward a fully globalized militarized culture (Downey and Murdock 2003: 79).

Conclusion

The road from prediction to pre-emption is a short one. One of the greatest ironies of the Network-Centric paradigm is that the concept has been formulated at a time when the United States has reached the apex of military might. The U.S. is the undisputed leader in defence spending and advanced weapons development. The country's technical superiority has inspired a philosophy of insecurity that permeates the whole of military culture and that theorized a spectrum of conflict out of a multitude of small threats that, when combined in a synthetic architecture, amount to a cumulative threat portrayed as omnipresent and ongoing.

The history of postwar technology has included the development of perceptual technologies from motion detectors to satellite monitoring systems, which have in turn enabled a global perspective to emerge. This picture has been realized through the optical and sensing capabilities of networked systems. The transition entails the emergence of a world-view, both through the data and sensing streams, but also a world-view as in a conceptual template for thinking about military strategy. In the completion of NCW capabilities, complex registers have been combined with the architecture of networked systems to produce a universally coherent image of danger in a globalized world. Through its technical and strategic dominance, the United States has been able to convince its allies to adopt and implement the NCW vision as a new cooperative strategy of planetary warfare.

The NCW paradigm is heavily reliant on simulation technologies involving the projection of risks and the automated reaction to those risks. The intelligence and implementation functions have been built into the synthetic architecture of the GIG and the DoDAF network, a military network engineered as a co-project between the Department of Defense and private contractors. In another sense, the concept of Network-Centric Warfare is a simulation in itself; a conceptual product concerned with the virtual rendition of threats, predictions and the art of soldiering. The architecture is not independent of physical reality but rather interacts with the spatial and temporal frameworks of lived life. The objects and data received through the medium of the sensors produce an emergent picture, while the registering and representation of that reality is relegated to an integrated machine. Thus, the task of the DoDAF is not to represent real dangers, but to collapse the distinction between the real and the copy (Baudrillard 1981). The simulative framework of the NCW is associated with non-places; that is, the normalized experience of virtual space without attachment to definitive time

or place (Auge 1995). In this representation, there is a mismatch between the construction of problems and their solution.

The discourse of threat inherent to NCW is virtualized apart from the intrinsic or extrinsic dangers that may exist. Threat becomes the guiding force behind the logic of automated command. The detection of threats is obtained through all of the sensory relays within the networked conflict spectrum. The automation compresses the steps between retrieving information, discerning threat and eliminating threat. The idea depends on the synchronization of all forces and capabilities into a common operating picture. Synchronization purportedly “enables the kill chain” (Phister, Busch and Plonische 1996). Yet while information superiority may translate into a faster reaction, such responsiveness does not always translate into a desired outcome (Luddy 2005). Automated information loops have led to an increase in civilian deaths and incidences of firing on allies (Drew 2009; King 2008; Thompson 2008). This problem is exacerbated by the failure of allies of even the most technologically advanced countries to keep up with the technical requirements of NCW. Thus, the goal of global integration is undercut by the inability to reliably communicate with other militaries.

The assumption underlying my focus on information in the NCW paradigm is that advances in technology will supply more information to operators at various levels in the “sensor to shooter chain,” leading to the elimination of uncertainty (Bolia, Vidulich and Nelson 2006). This understanding suggests that uncertainty is an obstacle that can be overcome by adding more information. Still, no amount of data can compensate for poor intelligence, nor can it alter uncertainty. War is all about the nature of chance. Chance multiplies the uncertainty of all circumstances and interferes with the course of events (von Clausewitz in Bolia, Vidulich and Nelson 2006: 4). Contemporary studies of complexity regard uncertainty as an inherent property of the physical world. Thus, more information does not equal less uncertainty but tends to multiply the opportunities for error.

Since the early days of air power, military leaders have promoted one version or another of “massed effects” intended to strike an enemy’s position and lead to a swift, bloodless victory (Douhet in Barnett 1999: 36-39). The concept of massed effects is similar to the historical doctrines of the *blitzkrieg*, cluster bombing and today’s “shock-and-awe” strategy. The reference to massed effects represents a resurrection of counterinsurgency doctrine, with its proposition about warfare as a long, open-ended affair. In this sense, massed effects find new life in Cebrowski and Gartska’s “lock out” strategy (1998). The core of the idea, however, remains predicated on the notion that “punishment equals control” (Barnett 1999: 36-39). According to Barnett, the collateral damage from such operations remains very high and comes seriously close to the definition of war crimes. The greater technological capability of information-age weaponry increases the potential for civilian casualties. Massed effects become a way to deliver an enormous amount

of irreversible damage and increase the potential of escalating conflict. The NCW ideal of information dominance is too complicated to control from a remote position. As such, “massed effects” is merely an antiseptic term for weapons of mass destruction (36-39).

In a technical paper for the Air Force Research Laboratory entitled “Unintended Consequences of the Network-Centric Decision Making Model,” Bolia, Vidulich and Nelson argue that the automation of the command chain has the potential for accidental consequences (2006). The issue stems from the need to avert the problems associated with information overload, resulting in the automation of much of the processing that might otherwise be relegated to human actors. Automation may vary from simple calculation, tracking entities and data fusion, to more involved, automated decision support relying on a spectrum of fully autonomous combat vehicles and weapons systems.

Decision-making in the military functions as a chain. Traditional military theory distinguishes between three levels of war decision-making: strategic, operational and tactical. Authority is conferred on the basis of rank and varies according to expertise. Consequences from decisions thus differ in magnitude based on that authority. One of the problems of NCW is that it makes quality information available on all levels of the command chain. Decision-making authority is decreased to lower levels, which theoretically expedites the execution of time-sensitive targeting. This is a concept referred to in network-centric parlance as “power to the edge” (Alberts and Hayes 2003: 1).

A fundamental challenge to NCW decision making is this devaluation of the command chain (Bolia, Vidulich and Nelson 2006). This may not mean much from a civilian standpoint, yet the hierarchy of the command chain is what discourages decision-making at inappropriate levels. Changes in the decision-making chain generate uncertainty as to the rules of engagement during war. The situation allows commanders to retain their authority while distributing accountability. In the event of a poor or illegal operation, there is an increased tendency to pass responsibility on to the lowest levels.

Without clear rules of engagement, two predictable outcomes result. First, there is an increase in civilian casualties, stemming from confusion about what counts as a legitimate target. Second, problems with accountability are exacerbated by a command structure in which decentralized units are granted a wide amount of autonomy and informational decisions are devolved to lower levels. Ultimate authority is concentrated at the top of the command chain, which is nonetheless insulated from the consequences. The basic structure multiplies the potential for so-called “isolated incidents”—unintended casualties resulting from misinformation or an improper response to information. Thus, the standing arrow configuration of Network-Centric operations allows lower-level soldiers to hazard the brunt of responsibility. The situation is complicated by the presence of contractors who,

by their designation as civilian support, are exempt from prosecution. Ceding control of the automation of warfare to the private sector increases the risks of unintended consequences.

The wholesale adoption of the Network-Centric paradigm is largely an outcome of the move away from state-centric warfare and toward pre-emptive war with a heavy reliance on simulated information. Yet the distinction between the real and unreal is misleading in this sense, since all effects of warfare are devastatingly material. Network-centric warfare ultimately ends in human-centric casualties (Barnett 1999; Bolia, Vidulich and Nelson 2006). The doctrine provides insulation from the immediate results of automation, though it does not resolve mounting questions about its limitations.

Note

Many thanks to Manuel King for considerable help with the illustrations for this article, to Brian Murphy for excellent consultation, to the reviewer for insightful comments, and to the editors for their patience and assistance.

References

- Alberts Donald and Richard Hayes. 2003. *Power to the Edge: Command and Control in the Information Age*. Santa Monica Command and Control Research Program.
- Alberts, Gartska, Richard E. Hayes and David Signori. 2001. *Understanding Information Warfare*. http://www.dodccrp.org/html4/books_downloads.html. Accessed 29 March 2007.
- Armitage, John. 2000. Beyond Postmodernism? Paul Virilio's Hypermodern Cultural Theory. *CTheory* Nov. 15. <http://www.ctheory.net/articles.aspx?id=133>. Accessed 13 February 2010.
- . 2006. The Elite War on Utopia. *TOPIA* 15: 69-90.
- Arquilla, J. and Ronfeldt. 1996. *The Advent of Netwar*. Santa Monica: RAND MR-789-OSD
- Arquilla, John and David Ronfeldt, eds. 1997. *In Athena's Camp*. Santa Monica: RAND.
- Arquilla, John, David Ronfeldt and Graham and Mellisa Fuller. 1998. *The Zapatista Social Netwar in Mexico*. RAND Abstracts Document No: MR-994-A.
- Auge, Marc. 1995. *Non-Place: Introduction to an Anthropology of Supermodernity*. New York: Verso.
- Barnett, Thomas. 1999. *The Seven Deadly Sins of Network-Centric Warfare*. U.S. Naval Institute. <http://thomaspmbarnett.com/published/7d.htm>. Accessed 13 May 2006.
- Baudrillard, Jean. 1981. *Simulacra and Simulation*. Trans. Shelia Glaser. Ann Arbor: University of Michigan Press.
- Berkowitz, Bruce. 2003. *The New Face of War*. New York: Simon and Schuster.
- Bolia, Robert, Michael Vidulich and Todd Nelson. 2006. Unintended Consequences of the Network-centric Decision-making Model: Considering the Human Operator. Paper of the Airforce Research Laboratory. Wright-Patterson Airforce Base, OK. http://docs.google.com/viewer?a=v&q=cache:ER6aHwKt_ZUJ:www.dodccrp.org/events/2006_CCRTS/html/papers/054.pdf+Bolia,+Vidulich+and+Nelson,+2006&chl=en&gl=us&sig=AHIEtbSl8MtHW0tkQ2NFEKA7fu9yVhBDg. Accessed 28 June 2008.

- Bourne, Christopher. 1999. Unintended Consequences of the *Goldwater-Nichols Act*. *JFQ* (Spring 1998): 99-108.
- Blackmore, Tim. 2005. *War X*. Toronto: University of Toronto Press.
- Bradford, Zeb and Frederic Brown. 2008. *America's Army: A Model for Interagency Effectiveness*. Westport, CT: Praeger Security International.
- Business Transformation Agency of the Department of Defense. http://www.bta.mil/products/BEA/html_files/dodaf.html
- Cares, Jeffrey. 2006. *Distributed Networked Operations: The Foundations of Network-Centric Warfare*. New York: Universe.
- Castells, Manuel. 1996. *The Rise of the Network Society*. New York: Blackwell.
- Cebrowski, Arthur and John Gartska. 1998. *Network-Centric Warfare Its Origin and Future*. In *Naval Institute Proceedings*. <http://all.net/books/iw/iwarstuff/www.usni.org/Proceedings/Articles98/PROcebwski.htm>. Accessed 7 August 2003.
- Coalition Warrior Interoperability Demonstration (WID) 2009. Defense Information Systems Agency Office of Procurement Directorate, Location DITCO-NCR Solicitation Number: CWID2009 (revised) Primary Point of Contact: Edward Shannon Frank, Contract Specialist. <https://www.fbo.gov/indexs=opportunity&mode=form&ctab=core&id=9ad750134a13843b77bcdcf27ebb3e0d&cview=0&ccck=1&au=&ck=>. Accessed 20 September 2009.
- De Landa, Manuel. 1991. *War in the Age of Intelligent Machines*. New York: Zone Books.
- Downey, John and Graham Murdock. 2003. The Globalization of Guerrilla Warfare. In *War and the Media*, edited by Daya Kishan Thussu and Des Freeman, 70-86. London: Sage.
- Drew, Christopher. 2009. Human Rights Group Says 29 Civilians Killed by Israeli Air Attacks in Gaza. *New York Times*, 30 June, A14.
- Deleuze, Gilles. 2002. Postscript on Control Societies. In *CTRL Space: Rhetorics of Surveillance from Bentham to Big Brother*, edited by Thomas Levin, Ursula Frohne and Peter Weibel, 318-21. Cambridge, MA: MIT Press.
- Edison, Thomas. 2006. Social Networking Analysis: One of the First Steps in Network-Centric Operations. *Defense Acquisition Review Journal*. <http://www.dau.mil/search/gsaresults.aspx?k=+pubs|arq||2005arq||2005arq-40||Edison.pdf>. Accessed 14 December 2007.
- Foucault, Michel. 1985. *Discipline and Punish: The Birth of the Prison*. New York: Vintage.
- Frank, Edward Shannon. 2009. Coalition Warrior Interoperability Demonstration, (CWID). Solicitation # CWID2009. Defense Information Systems Agency Office of Procurement Directorate DITO-NCR. <http://www.fbo.gov/index?tab=core&=opportunity&mode=form&id=gad750134>. Accessed 2 May 2009.
- Galloway, Alexander and Eugene Thacker. 2007. *Exploit*. Minneapolis: University of Minnesota Press.
- Gonzalez, Roberto, 2009. *American Counterinsurgency: Human Science and the Human Terrain*. Chicago, IL: Prickly Paradigm Press.
- Gray, Christopher. 1997. *Postmodern War*. New York: Guilford Press.
- Grey, Christopher Hables. 1997. *Postmodern War: The New Politics of Conflict*. New York: Guilford Press.
- Gutmann, Matthew and Catherine Lutz. 2010. *Breaking Ranks: Iraq Veterans Speak Out against the War*. Berkeley, CA: University of California Press.

- Hardt, Michael and Antonio Negri. 2001. *Empire*. Cambridge, MA: Harvard University Press.
- Harvey, David. 2005. *A Brief History of Neoliberalism*. New York: Oxford University Press.
- Hirst, Paul and Jonathan Zeitlin. 1989. *Reversing Industrial Decline, Industrial Structure and Policy in Britain and Her Competitors*. Oxford: Berg Publishers.
- Jordan, Kenneth. 2007. The Consolidation of Networks for Outsourcing. Case Studies in National Security Transformation Paper #12 prepared for the Center for Teaching and National Security Policy.
- Kellner, Mark. 2007. Networking the Air Force Defense News. <http://integrator.hanscom.af.mil/2007/May/05242007>. Accessed 3 December 2009.
- Khalilzad, Zalmay, John White and Andrew Marshall. 1999. *Strategic Appraisal: The Changing Role of Information in Warfare*. Santa Monica, CA: Rand Corporation.
- Kaldor, Mary. 1999. *New and Old Wars: Organized Violence in a Global Era*. Cambridge, MA: Polity Press.
- Keenan, Jeremy. 2009. *The Dark Sahara: America's War on Terror in Africa*. New York: Pluto Press.
- Kellner, Douglas. 2003. *The Politics and Costs of Postmodern War in the Age of Bush II*. <http://www.gseis.ucla.edu/faculty/kellner/essays/politicscostspostmodernwar.pdf>. Accessed 8 August 2009.
- King, Laura. 2008. Coalition Friendly Fire Kills Nine Afghan Soldiers. *LA Times*, 23, October. <http://articles.latimes.com/2008/oct/23/world/fg-afghan23>. Accessed 20 September 2009.
- Krebs, Valdis. 2002. Mapping Networks of Terrorist Cells. *Connections* 24(3): 43-52.
- Lederman, Gordon. 1999. *Reorganizing the Joint Chiefs of Staff: The Goldwater-Nichols Act of 1986*. http://books.google.com/books?id=ANmsazlpQ10C&pg+PR10&dq=reorganizing+the+joint+chiefs+of+staff+gordon+lederman&source=bl&ots=8fdnRhUqVt&sig=Ej054ecKoQIWzwNsA-dM8cqboFA&hl=en&ei=iCR7Spv7MYj8MfOV5PoC&sa=X&oi=book_result&ct=result&resnum=1#v=onepage&q=&f=false. Accessed 2 July 2009.
- Luddy, John. 2005. The Challenge and Promise of Network-Centric Warfare. *Lexington Institute*. <http://www.lexingtoninstitute.org/docs>. Accessed 5 April 2006.
- Metz and Kievit. 1995. *Strategy and the Revolution in Military Affairs: From Theory to Policy*. <http://www.au.af.mil/au/awc/awcgate/ssi/stratma/pdf>. Accessed 31 July 2007.
- Milgram, Stanley. 1967. The Small World Problem. *Psychology Today* 2:60-67.
- Mitchell, Paul. 2006. *Freedom and Control in Military Networks*. Singapore: Institute of Strategic Studies.
- . 2009. *Network-Centric and Coalition Operations: The New Military Operating System*. London: Routledge.
- Miyoshi, Jager. 2007. *On the Uses of Cultural Knowledge*. Strategic Studies Institute, U.S. Army War College. <http://www.StrategicStudiesInstitute.army.mil/>. Accessed 3 December 2009.
- Murdock, Paul. 2002. Principles of War on the Network-Centric Battlefield: Mass and Economy of Force. *Parameters* 32: 86-95.
- Newman, Mark. 2003. The Structure and Function of Complex Networks. *SLAM Review* 45(2003): 167-256.

- Owens, Admiral William A. 1996. The Emerging System of Systems. *Strategic Forum* 63. Institute for National Strategic Studies.
- Phister, Paul, Timothy Busch and Igor Plonisch. 1996. *Joint Synthetic Battlespace: Cornerstone for Predictive Battlespace Awareness*. Air Force Research Laboratory Information Directorate. Rome, NY. http://www.dodccrp.org/events/8th_ICCRTS/pdf/005.pdf. Accessed 19 June 2008.
- Safranski, Mark. 2008. *The John Boyd Roundtable: Debating Science, Strategy, and War*. Ann Arbor: Nimble Books.
- Shachtman, Noah, 2009. The Army's New Land Warrior Gear: Why Soldiers Don't Like It. *Popular Mechanics*. <http://www.popularmechanics.com/technology/military/4215715>. Accessed 11 April, 2010.
- Singer, Peter W. 2003. *Corporate Warriors*. New York: Cornell University Press.
- Shultz, R. 1991. The Low Intensity Conflict Environment of the 1990s. *The Annals of the American Academy of Political and Social Science* 517:120-34.
- Sloan, Elinor. 2002. *The Revolution in Military Affairs*. Montreal: McGill-Queen's University Press.
- Thom, William. 2000. Africa's Security Issues through 2010. *Military Review (Dept. of the Army Professional Bulletin* 100-99-5/6 80(4). <http://www.cgsc.army.mil/milrey/english/JulAug00/thom.htm>. Accessed 19 August 2009.
- Thompson, Mark. 2008. Afghan Civilian Deaths: A Rising Toll. *Times Online*, 4 September. <http://www.time.com/time/magazine/article/0,9171,1838778,00.html>. Accessed 20 September 2009.
- Toffler, Alvin and Heidi. 1993. *War and Anti-War*. Boston: Little and Brown.
- Trilling, Roger. 2002. Why the War Works. *Village Voice*, 13-19 November. www.village-voice.com/issues/0246/trilling.php. Accessed 4 January 2003.
- Turse, Nick. 2008. *The Complex*. New York: Metropolitan Books.
- Van Creveld, M. 1991. *The Transformation of War*. New York: Free Press.
- Virilio, Paul. 1986. *Speed and Politics*, translated by Mark Polizzotti. New York: Semiotext(e).
- . 1988. *The Vision Machine*. Bloomington and London: Indiana University Press.
- . 1991. *The Aesthetics of Disappearance*. New York: Semiotext(e).
- . 2000. *The Information Bomb*. New York: Semiotext(e).
- . 2008. *Negative Horizon: An Essay in Dromoscopy*, translated by Michael Degener. New York: Continuum Books.
- . 2009. *War and Cinema: The Logistics of Perception*. New York: Verso.
- Virilio, Paul and Sylvere Lotringer. 1983. *Pure War*. Trans. Mark Polizzotti. New York: Semiotext.
- von Clausewitz, Carl. 1997. *On War*. Hertfordshire, U.K.: Wordsworth Classics.
- Wallerstein, I. 2009. *The United States Confronts the World*. New York: Paradigm.
- Watts, Duncan. 1999. Networks, Dynamics and the Small World Phenomenon. *AJS* 105(2): 493-527.