Michael Geyer

Elektronische Todesarten/Electronic Ways of Death

The idea of a historic rupture, once limited to esoteric French theorists of the postmodern and their US American acolytes in academia, has become something of a bottom line in war-talk and war-thought. Information Warfare is the catch-phrase which articulates this sentiment of historic discontinuity and, occasionally, of an outright millennial sense of a new beginning. Information Warfare is gaining status as the utopia of the 21st century–and lest there be any doubt, information warfare is conceived as utopia rather than dystopia in the mind of its prophets.

The belief in the efficacy of new informational technologies of violence–in short Information Warfare or IW–is outrunning by far the pragmatics of their development and deployment. But information warfare has become a discursive and institutional reality. While much of IW remains controversial, it is conceived as being radically different from the way US American collective memory remembers and the US military fights wars. It is characterized as a "military revolution" or even more emphatically a remaking of the nature of war.

Assessments of the effects of this new kind of warfare differ dramatically. When Paul Virilio says that "all military technologies reduce the world to nothing," he thinks of information warfare as a means of total subjugation in a long tradition of thinking imperial homogenization of the world.[1] Others coolly answer that "open skies," self-destruct chips in weapons sold to third parties, and a massive dose of televised propaganda, plus a few assorted weapons from super-secret labs, will actually ascertain peace and eventually make war a non-lethal affair.[2] Where Virilio's evokes the imminent dissolution of historically formed bodies and polities into nothingness, the Tofflers see a global future for (American) individualism and life in peace and prosperity. Where the former sees the desertification of the planet, the latter feel that "[at] the highest level … military, economic and informational power [will] reduce the violence so often associated with change on the world stage."[3] They promise a revolution without terror–an American revolution.

The idea of a profound transformation of warfare is compelling. Nonetheless, efforts to dress up this change as a millennial transformation, presumably ushering in a new thousand year rule of information-power, are mostly funny, if one considers them as slapstick, more Charlie Chaplin than Adolf Hitler (The Great Dictator). If it is true, as Arquilla and Ronfeld argue, that Athena is the goddess of information-warfare, that her warfare is theorized by Sunzi and practiced by the Mongols, and if it is further true that the latter engaged just "in some initial rape and pillage" but otherwise settled comfortably into hands-off rule, it might as well be true, as the Tofflers suggest, that George Washington belongs into the same time/space as Conan the Barbarian.[4] It would be intriguing to contemplate this longing for myth and the recourse to allegory in an otherwise pretty hard-nosed military intelligentsia. But in effect these myth-histories just obfuscate the key issue when it comes to understanding warfare. What kind of violence, if any, does information exert? This means to ask how and what Information Warfare actually threatens to kill.

Athena turns out to be the right goddess for the information age. She was known as the Grey-Eyed, the Destroyer of Cities and Goddess of Spoil. She is a brain-child with a lethal attitude, and so is information warfare.

The American Revolution in Warfare

There is overwhelming agreement within the US civil-military establishment that the rules of military engagement will change profoundly. The military establishment–without inside knowledge it is difficult to pinpoint the main agents–has put a premium on advancing a process of technological innovation and, more haltingly, of organizational transformation. This process also entails the reshaping of military policy with tremendous implications for the way the United States conceives of and plans to use force. The bottom line of occasionally quite outrageous comments about goddesses (Arquilla) and "waves" of human development (Toffler) is that the US American military is in the process of reinventing itself.

Despite a great deal of institutional resistance, the readiness to engage in an all-encompassing reimagination of what the military does and what war might become is as striking as it is overwhelming. In part, the military intelligentsia's myth-making is an indication of the general readiness, even eagerness, to throw out history–warfare practices which have guided the military over the past century into the present. To be sure, there is tremendous infighting. But the spirit of innovation in key military and civilian institutions (and the budget to back up respective decisions) has few precedents in past military experience. If anything, it is comparable to the technological enthusiasm of the progressive era. But the latter was a civil enthusiasm and this is distinctly a military one.

The key term for these initiatives is Information Warfare. IW has developed from a series of more or less workable systems programs associated with electronic Command and Control (C2W) on the battlefield and, in the wider sense, of an electronically integrated battlespace. It has turned into the promise of a master-plan and master-doctrine–a "system of systems"–for the future use of force. IW is emerging, neither as weapons (systems) nor as pure C2W, but as doctrine and organization for US American war in the future. It is a revolution of how to think war that is hailed as "the American revolution in military affairs."[5]

The rapidity of development is best demonstrated in two snapshots. Insiders use the March 8, 1993 Chairman of the Joint Chiefs of Staff Memorandum of Policy 30 (MOP 30) as a starting point. This memorandum articulates the Gulf War experience and defines Information Warfare as Command and Control Warfare: "C2W is the military strategy that implements information warfare on the battlefield and integrates physical destruction. Its objective is to decapitate the enemy's command structure from its body of combat forces." Even in the narrow confines of "the electronic battlefield" this is a most reticent reading of the Gulf War experience, since it reasserts long-standing operational doctrine–what Liddell Hart and others had once called "indirect strategy." The difference is that electronically integrated command of one's own forces and the control and, possibly, disruption of enemy "information" have replaced physical "mobility" as the means to achieve the end.

The other snapshot comes from the January 1996 Chairman of the Joint Chiefs of Staff Instruction 3210.01.

> Information Warfare (IW). Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems, and computer-based networks.

This is not just a much more expansive definition of what IW does; rather, it suggests a new understanding of war. War moves from the electronic battlefield into the information sphere which is conceived as a separate and fifth domain of warfare in addition to land, water, air, and space. This kind of warfare entails, in its more sober definitions, spoofing and confusing sensors (intelligence-based warfare); degrading and corrupting communications (electronic warfare); corrupting and turning processors against themselves (hacker warfare); disabling command centers (electronic warfare); as well as discouraging, pacifying, and confusing opposing forces and decision makers (psychological operations).[6] Especially this latter task of IW is less well entrenched in the military, although it has made considerable in-roads. It is, however, the darling of a new generation of defense intellectuals, mostly tied to the military institutions of higher learning.

Their signature is the synergy of technological radicalism and utopianism, focused on knowledge and information. Who knows what Foucault might have made of them, but in IW "knowledge, more than ever before, is power."[7] The subtle difference is that when they say this, they mean it. Control of information generates the power to kill. This is a revolution in military affairs.

War Fighting

The more knowledge/power-oriented members of the military intelligentsia have come to downplay the use of physical violence, but IW has dramatically increased the ability to deliver lethal force. Although the American military establishment is very reluctant to commit force, there is nothing in IW that would hedge against the actual use of violence, once force is committed. Whatever else IW may promise, it delivers battle-ready compellance on an unprecedented scale.

IW had its breakthrough in the context of the theoretical and practical elaboration of the "electronic battlefield." The latter was mostly developed for NATO contingencies in Central Europe. I had its brief heyday during the Gulf War. It is now ancient history, because the understanding of what constitutes battle has changed. For one, this electronically guided violence is emerging in a new interservice synergy of destruction that runs the gamut from subnational (low-intensity) warfare to regional state/power conflagrations to major wars. For another, the territory of battle is transformed into an electronic battlespace. IW facilitates the flexible use of force with physical geography being an ever smaller factor.[8]

Key elements of electronic warfare are (1) the rapid force "flow" along a global positioning grid. While the net of global information is permanent, actual force is assembled according to the input from close-up surveillance platforms. Force is put on the ground in the form of (2) mixed Combat Groups of variable size, determined by the task environment. The Pentagon rather thinks of brigades, whereas the military intelligentsia imagines the equivalent of Wehrmacht *Jagdkommandos*. Their foremost mission is to act as sensors and relays for an array of remote weapons systems.

The effect of IW is above all that very small groups of soldiers on the ground can (threaten to) kill very large numbers of people without ever coming into direct contact with them. Much has been made of precision guided weapons which seem to suggest a reduction of violence. But the ability to deliver violence and the sheer lethality of it is the true advance that comes with information guidance. A further effect is that information diminishes communication. Information-based knowledge displaces and disrupts interaction. The enemy is a computer-generated construct, excluded from interconnectivity. Never mind the growing role of policing and peace-keeping which work on the basis of dialogue/interconnectivity in order to achieve the simplest things. The IW scenario knows only information that is generated from within. This system is self-enclosed–and such systems tend to be exceedingly violent.

If it were up to IW theory, (3) mission command of individual combat groups would be radically decentralized. Units would proceed largely independent of a hierarchical command structures with an extraordinary freedom of action. However, (4) (mission-)control of military action is, at the same time, more centralized due to the availability "total" electronic surveillance. Empowerment (mission-command) on the one hand and disempowerment (mission control) on the other go hand in hand. The effect is a much expanded battlespace with discontinuous, local actions being centrally coordinated over extended territory. With the disappearance of continuous front-lines, overwhelming violence is instantiated with elemental force only to disappear, commando-style, with the conclusion of action.

The real-time "top-sight" of the command central is crucial for the ability to lift the Clausewitzian "fog of war" from the battlefield. But quite apart from the fact that the fog of battle is replaced by electronic smog, top-sight generates the conditions, not for a differentiated and calibrated uses of force, but for what Count Schlieffen once called the *Gesamtschlacht*.[9] Much like Schlieffen IW war-fighting theory knows few options short of either annihilation or unconditional surrender. Once force is committed, there is only destruction or subjugation–or failure of mission.

Epistemic Warfare

The military-academic intelligentsia is moving in the opposite direction from the military establishment. They think of IW as a means of compellance short of physical violence. Non-lethal compellance is the much-quoted "acme of skill."[10] Disruption and disorientation are the military intelligentsia's key to "strategic information warfare" or "cyberwar."[11]

The simplest version is still closely tied to Command and Control Warfare, but makes information a weapon in its own right. If one were capable of lifting the "fog of war" from one's own side (say with the help of perfect "topsight") and, at the same time, of fogging in the enemy's view of the battlefield, this would be of extraordinary advantage. If one were further able to corrupt the signals between elements of the enemy's armed forces and between headquarters ("the leadership") and units, one could cause havoc. Decision-making would be thoroughly thwarted. Hierarchical systems would lose their coordination, acephalous groups their bonds. Some of these C2W initiatives are more far-fetched than others, but, altogether, current electronic systems facilitate the transition from passive "intelligence" to active Information Operations (IO).

Information Operations do not, for the most part, account for the fact that information carries meaning and that meaning is generated in knowledge and belief "systems." What if one were to target these systems, rather than the bits and bytes of information? This can be done by attacking the infrastructure of information in a deep infiltration that cracks through network protectors and imposes one's own information templates upon the enemy's in an act of perfect mimicry. If one can worm oneself into the mind of the enemy by gaining control over their circuit-boards, it may become possible to effect decisions which otherwise would not be taken. The effect is that the enemy is guided into "decisions (and actions) that consistently mismatch and fail to support the intentions or aims of the adversary leader." Ideally this means that deception might lead "human decision-makers to choose to assent to US policies" and, moreover, "to assent of their own free will." This sounds far-fetched, but "a successful information warfare campaign interposes a false reality on the human target."[12]

But the true "acme of skill" consists in corrupting or destroying the knowledge and belief architecture; that is, the collective memory as a repository of meaning and individual sense-security as the source of identity. This scenario takes its starting point from the notion that human knowledge and belief form a complex architecture which can be understood and mapped in an imitation of electronic life-forms. Once a knowledge architecture is known, it can be degraded–and brought to collapse. Thirty seconds of a video-clip of a dead American soldier dragged behind a jeep was enough to end the military operation in Somalia.

Since knowledge and belief-systems generate meaning and identity, an awareness of self, this awareness and its attending sense-security can be attacked–or so it is argued. The effect would be utter disorientation, a loss of (a sense of) reality. In contrast to decision-making loops, knowledge architectures are collective properties, if not of entire nations, of groups or associations. The corruption of such architectures, should it be possible, is thus an attack on society at large. In fact, it is an attack on society in lieu of physically fighting combatants.

This is cyberwar in its pure, if futuristic form. It attacks and corrupts not simply information, but the collective net of knowledge and sensory perception that makes human association possible. In the view of at least one author this kind of warfare "maybe no less wrongful than to force another into starvation or cannibalism."[13]

This is war that does not kill people, but their sensory habitat. It is celebrated as non-lethal warfare that ends physical violence. But in fact it is an act of devastation–scorching the mind–directed at non-combatants. It may be fiction or fantasy, but it is post-modern genocide.

Changing States of War

Efforts to redefine U.S. National Security have been under way for quite some time. Most recently they have been associated with the proliferation of small wars and the threat of ethnic and religious terrorism which Samuel Huntington has elevated to the level of a "clash of civilizations."[14] The Tofflers have their own reading of civilization wars. They suggest that future wars will be fought between those who are rich (and members of the information wave) and those who are not (agricultural and industrial producers).[15] Yet others have pointed to threats that emanate from transnational criminal organizations, terrorist groups, weapons proliferations and computer hackers.[16] The particular nature of this threat consist in the ability of these diverse groups to use the global information infrastructure and its capabilities to undermine the security of the people, the territory, and the way of life of the United States. They thus constitute a "clear and present danger" which is a *casus belli*, whether war is declared or not.[17]

The latter is of some import. For there is a great deal of loose talk about threat, war and crimes, as if they were the same. They are not. It is one thing to be an (accused) criminal and it is a very different thing to be an enemy alien (or however one would call an information soldier). It is one thing to rob a bank (even if by electronic means in a big way) and it is another one to threaten the sovereignty of the United States. You might be put to death in either case, but in one instance you have at least technically a right to trial. In the other you do not. Hence, if hackers are declared "a clear and present danger," there is some reason for concern.[18] If there were a *casus belli*, hackers might well be able to outwit the system. But in the end, they'd be dead–and if John Arquilla had his way, there would be more efficient ways to achieve that end.[19]

The acute problem is that "netwars" are no longer mind games of the military intelligentsia. While they are still sold as the new order of things revealed, they have been incorporated into Presidential policy. It is difficult to say what is stranger: the fact that this policy exists in the first place or that it is not recognized as such in a good part of the IW debate. In any case, the lengthy White House Document "A National Security Strategy of Engagement and

Enlargement" (February 1996) identifies, in addition to a number of more conventional security concerns, a new "transnational" class of "problems which once seemed quite distant."

While "environmental degradation, natural resource depletion, rapid population growth and refugee flows" are mentioned in passing, the "new challenges … of the information and technology age" are elaborated more extensively. The speedy circulation of information, money and ideas facilitates "the violence of terrorism, organized crime and drug trafficking." Arms trafficking might be added to the trias. But the key point here is that "non-state, as well as state, forces" are identified as dangers. Equally important, the Presidential document asserts that "clear distinctions between threats to our nation's security from beyond our borders and the challenges to our security from within our borders are being blurred." "[F]orces can now try to threaten our security from within our borders."

The consequences of this Presidential statement are far-reaching. First, if the "Report of the Defense Science Board Task Force on Information Warfare–Defense (IW-D)" suggest that non-state actors can be a "clear and present danger," it asserts (and in this reflects the realities of the drug-war) that elements of internetted society have become subject states of war. They are aggressors. If caught, they are, de jure, prisoners of war. Second, if the presidential text about the permeability of boundaries has any meaning at all, a state of war may also come about between the United States of America and some of its citizens. This is a breathtaking turn, although the Presidential document, in contrast to some of the IW literature, is careful not to declare war on its citizens. But it creates a grey zone in which distinctions become blurred and where the protection of being an American citizen is wearing thin.

Third, while the "circle of the 'we'" is becoming narrower, American sovereignty stretches further than ever.[20] If, as the Presidential document asserts, "problems which start beyond our border can now much more easily become problems within our borders" this demands and legitimates "American leadership and engagement in the world." The latter no longer means the occupation of territory, not even the stationing of troops all around the world. But it calls for global presence along the sinews of communication and, as its prerequisite, the control of crucial nodes. The Joint Chiefs of Staff speak of "US global responsibilities [which] require global capabilities, despite a regional focus in implementing the strategy."[21] This quest for globality entails "enlarging the community of secure, free market and democratic nations" in real world politics. In cyberspace, it amounts to the Americanization of the fifth domain.

Sovereignty and Constitutionality

The control of cyberspace is a tall order and, some would say, an impossible one. The "info-sphere" has many and diverse proprietors and is tolerating a great number of squatters and nomads. Yet, control of this domain is what "information dominance" as the key concept of an IW grand strategy means. Information dominance, it should be noted, is not a permanent occupation. Rather it is the ability to preempt any and all other proprietors in the information-sphere in case of war (war itself now covering a different spectrum).[22]

Sovereign is the one who controls the exception. Carl Schmitt declared this to be the foundation of sovereign power.[23] IW Strategy aims at the control of the exception in cyberspace. It is not interested at all in constitution-building. The IW debate makes the United States of America the new global sovereign in order to ascertain protection against the vulnerabilities of the information age.

"The project of establishing order leads human beings right into an endless progression of violence," says one observer who should know.[24]

[1] Virilio, Paul. 1994. Cyberwar, God and Television. *ctheory*, 21 October.

[2] Toffler, Alvin and Heidi. 1993. *War and Antiwar: Making Sense of Today's Global Chaos*. New York: Warner Books.

[3] Toffler, p.3.

[4] The former are contentions of Arquilla, John, and David Ronfeldt. 1997. Cyberwar is Coming! In *In Athena's Camp: Preparing for Conflict in the Information Age*, edited by J. Arquilla and D. Ronfeldt. Santa Monica: RAND. The latter is the popular "three wave" theory of the Tofflers which divides the human past into an agricultural, industrial, and informational age.

[5] Owens, William A. 1996. Foreword. In *The Information Revolution and National Security: Dimensions and Directions*, edited by S. J. D. Schwartzstein. Washington, D.C.: The Center for Strategic and International Studies, p. XI.

[6] Lipicki, Martin. 1997. *Information Dominance*. Available from http://www.ndu.edu/ndu/inss/strforum/forum132.html.

[7] Nye, Joseph P., and William A. Owens. 1996. America's Information Edge. *Foreign Affairs* 75 (March/April):20-36.

[8] Cooper, Jeffrey R. 1996. Another View of Information Warfare: Conflict in the Information Age. In *The Information Revolution and National Security: Dimensions and Directions*, edited by S. J. D. Schwartzstein. Washington, D.C.: The Center for Strategic and International Studies.

[9] Cooper, Jeffrey R. 1997. Another View of the Revolution in Military Affairs. In *In Athena's Camp: Preparing for Conflict in the Information Age*, edited by J. Arquilla and D. Ronfeldt. Santa Monica: RAND.

[10] Szafranski, Richard. 1994. Neocortical Warfare? The Acme of Skill. *Military Review* (November):41-55.

[11] Stein, George, and Richard Szafranski. 1996. *US Information Warfare*. Alexandria, VA: Jane's Information Group.

[12] Szafranski, Richard. 1995. A Theory of Information Warfare: Preparing for 2020. *Airpower Journal* (Spring):56-65.

[13] Ibid., p.64.

[14] Huntington, Samuel P. 1996. *The Clash of Civilizations and the Remaking of World Order*. New York: Simon & Schuster.

[15] Toffler, *War and Antiwar.*

[16] Arquilla, John, and David Ronfeldt. 1996. *The Advent of Netwar*. RAND.

[17] Andrews, Duane. 1996. *Report of the Defense Science Board Task Force on Information Warfare-Defense (IW-D)*. Washington, D.C.: Office of the Undersecretary of Defense for Acquisition & Technology.

[18] Ibid., p. 2-17. Hackers are list as "good" "threat" as opposed to aggressors which are "bad" "threat."

[19] Arquilla & Ronfeldt, *Netwar.*

[20] Hollinger, David A. 1993. How Wide the Circle of the "We"? American Intellectuals and the Problem of the Ethnos since World War II. *American Historical Review* 98 (2):317-337.

[21] Chairman Joint Chiefs of Staff. 1995. *National Military Strategy of the United States of America 1995: A Strategy of Flexible and Selective Engagement*. Washington, D.C.: U.S. Government Printing Office.

[22] Molander, Roger C., Andrew S. Riddile, and Peter A. Wilson. 1996. *Strategic Information Warfare: A New Face of War [Abstract]*. Available from http://www.rand.org/publications/MR/MR661/MR661.html.

[23] Schmitt, Carl. 1996. *The Concept of the Political*. Translated by George Schwab. Chicago and London: university of Chicago Press.

[24] Sofsky, Wolfgang: *Traktat über die Gewalt*, Frankfurt/Main, S. Fischer 1996, 16