Georg Schöfbänker

From Cyberwar to INFOWAR
Computing and Telecommunications for "Real" and "Virtual" Warfare

The definition of the terms "war" and "computer," the difference between "real" and "virtual," and the meaning of "communication" seem to be generally well-known and highly plausible formulations in the language of everyday life. Nevertheless, this is not the case. A conceptual analysis including a clarification of the substance of the terms thus employed seems to be necessary. "Cyberwar," "infowar" and "netwar" are examples of a novel nomenclature that seemingly augur a paradigm shift from a general political and military concept of war, and which were developed during the early 1990s in the US at the RAND Corporation"s strategic proving grounds of the experimental apocalypse and its simultaneous prevention by means of countermeasures. These terms "cyberwar," "infowar" and "netwar" can still not be found in any dictionary or etymological encyclopedia. These are not only linguistic neologisms, but contextual and constructivist ones as well. As an initial approach, these terms can be translated as "cybernetic war," "informational war" and "warfare within computer networks."

"Real" "war" in the 19th and 20th centuries in the northern hemisphere of the globe was the continuation of power politics on the part of nation-states by means of armed conflicts between these nation-states in accordance with their imagined territorial, economic and imperial claims understood in a Clausewitzian sense. This is the standpoint of "political realism" in international relations. At the same time, warlike confrontations were a part of the process of subjugation and exploitation of the periphery of the world system, of the "South" and the "colonies" both by the industrialized-capitalist world as well as by the industrialized-communist one — a chapter of history that, to this day, has still not been completely documented and fully appraised.

It is said that "war" between nations of the developed world has become rather improbable nowadays. Nevertheless, extremely violent and bloody conflicts which have cost hundreds of thousands of human lives have not ceased in recent years. We need only think of the instances of genocide in Africa, or the conflicts in the states which came into being as a result of the disintegration of Yugoslavia and the Soviet Union. The casi belli have been described as "ethnic conflicts" or "new tribalism" between "warlords" or even as the "struggle between cultures." However, these seem to be rather inadequate intellectual attempts to describe and explain the factors lying at the root of the matter in these conflicts. In order to attain further insights, some other additional steps would be necessary. Nevertheless, murderous conflicts continue to occur, even if the precepts of international law and the vocabulary sanctioned by the international community of states have found new terminology to refer to them, and "war" in the classic sense may well have become a thing of the past, at least in the "rich North."

But the concept of war has still not changed in the logic of military planning. "Si vis pax, para bellum" — "If you desire peace, then prepare for war." This motto handed down from Antiquity continues to represent the viewpoint and the logic of military élites. The intellectual dilemmas resulting from it are sufficiently well-known: a military build-up and a perceived threat are followed by an arms race and a mirrored perception of threat. The changes which new information and communication technologies have engendered in the conceptualization and the logic of war are equally decisive and just as significant as those brought about by the development and introduction of nuclear weapons in the middle of this century.

C4I — standing for "Command, Control, Communication, Computer and Intelligence" — is a military abbreviation which succinctly sums up the consequences of the deployment of

conventional weapons on a "real battlefield" during wartime. This expression has to do with the "enhancement of effectiveness in battle"; what is meant thereby is the high-precision deployment of "intelligent munitions" which can independently seek their targets by means of electronic guidance systems. Although this concept of "cyberwar" was initially meant as a metaphor, what has emerged since its inception is an operative concept for missions carried out in a theater of war. The Gulf War conducted by the Allies against Iraq in 1991 serves as a case in point. "Cyberwar" is, at the same time, a collective designation for the experimental proving ground of the new individual soldiers comprising a fighting unit linked together by information technology and based upon communication with one another in real time. These soldiers wear computer-equipped battle dress and launch weapons which are guided to their targets by means of long-distance data transmission. "Cyberwar" is equated with the advantages of the blitzkrieg, with the possibility of achieving a "destructive advantage" by means of the long-distance data transmission and the deployment of computer-guided weapons. "At present, the US. Military has the international lead in the planning and preparation for cyberwar, both offensively as well as defensively… The US is the only country in the world which already has an arsenal available which makes cyberwar appear to be an attractive and feasible option," write RAND authors John Arquilla and David Ronfeldt.

"Infowar" ultimately goes far beyond the concept of guiding weapons to their targets. This term is also described as "strategic information warfare," meaning the deployment of all means and possibilities afforded by information and communication technologies for carrying out campaigns of sabotage and disinformation. These include the manipulation of banking and financial systems, telecommunications facilities, public administrative institutions and, of course, armed forces. If one accepts the hypothesis that modern life in the 20th century would no longer be possible without the use of computers and telecommunications equipment, then it is just a small additional step to assert the "vulnerability" of these systems to precisely targeted strikes and to regard this as a threat of the utmost significance. However, this threat, in the absence of other manifestations of endangerment, seems to have been partially invented or to have been played up in hysterical fashion. Nowadays, menacing images have already begun to assume extraterrestrial proportions — the possibility that an asteroid will collide with Earth in approximately 30 years — in order to thus make it appear to be advisable to go ahead with the development of the nuclear weapons which would be necessary to eliminate this threat in outer space — a concept which evokes memories of the "Star Wars" Project of the 1980s.

But we have still not yet encompassed the full extent of the implementation of computers for military purposes. The US is currently conducting the so-called "Stockpile Stewardship Program" for which the US Department of Energy commissioned IBM on February 3, 1998 to develop the world’s fastest supercomputers (100 teraflops). These will be put into operation by the US nuclear weapons development laboratory, and could possibly be used for the further development or even the new development of atomic weapons without having to conduct a full-scale nuclear weapons test which would be forbidden according to the provisions of the "Total Test Ban Treaty" now in effect. There are many such examples of the military roots of technological developments in the computer field. The ENIAC, one of the first primitive electronic processors, was developed to perform calculations in conjunction with the first thermonuclear weapons. The decentralization of the internet with which we are familiar today is based upon the requirements of the US military — they wished to have available decentralized communication facilities that would even be "capable of surviving" a nuclear strike against US territory. Which brings us back to our original point of departure — with respect to the development of computers capable of high-performance processing, as

well as the milestones in the emergence of the internet, we must certainly concur with Brecht's remark that war is the father of all things.

So ultimately, it is not at all amazing that cyberspace — that spatial domain of the modern information society that is completely unknown to many members of the political and military élites of this world — is generally perceived as a threat from which military attacks upon the information infrastructure might be expected. Whether this has more to do with science, with fiction, or with good public relations will be a key issue to be taken up at this year's Ars Electronica Festival.