Friedrich Kittler

On the History of the Theory of Information Warfare

Kai egeneto polemos en to ourano.
Apocalypse 12, 7

Of course, the nineties of this century weren't the first to discover that information counts in war. For ages now, three elementary lists, which probably differentiate warriors from merchants as well as from priests, have been in use. First, A tries to know what B knows without B knowing of A's knowledge. Second, A tries to communicate his knowledge to A' (subordinates or superiors or allies) without B knowing of the transmission, let alone of the transmitted data. The logic of this intersubjectivity itself suggests the existence of a third list: So his plans cannot be foiled by B, A would do well to split himself into A' and B' and, on the basis of his knowledge of B, calculate all possible moves of both sides. In other words, wars have implied espionage, communications technology and war games for a long time now. The only thing unheard of in Information Warfare is the fact that espionage, communications technology and war games all fall together in a global computer network.

The meaning of war game, in a prehistory whose technical models are infinitely inferior to the complexity of today's computers, can be explained with few words. In the age of Deep Blue, chess still prides itself on being the oldest toy with which the positions of two enemies on a battlefield could be geometrically simulated. There are grounds for the assumption that the great chess rules reform in the early modern age greatly increased freedom of movement for officers like bishops and rooks in order to better mirror the military innovations of the time. But the end of the cabinet wars coincides with the demise of chess board battles. The revolutionary theory of Clausewitz defined war as the clash of two subjects who could base their strategies solely upon calculations of probability, because they always had to take into consideration the unpredictable will of the opponent, the vagaries of the terrain and the uncertainties of communication. This theory, which had nothing but derision for the black and white squares of an ideally flat chess board, found its geographically adequate war game in the sand box, which Müffling introduced to the general staff in 1825. With the sand box, it was possible for the first time realistically to simulate the marching speed infantry or artillery could achieve in terrain of known gradient.

For a long time, espionage and communications could only dream of such physical reality. It lay in the nature of their considerably intersubjective structure that they applied more to subjects than to weapons, more to people than to machines. So the wars of the past cultivated exactly that which NATO, in its inimitable belief in acronyms, degraded to the term HUMINT (human intelligence). Spies, agents, scouts and secret couriers, since 1800 also military attachés in potentially hostile capitals–that was basically the traditional equipment of Information Warfare. Our word *angel* can be traced back to the Greek *angelos*, but *angelos* itself goes back to the Persian name of the mounted couriers who, in the name of their Great King, made up the first (and naturally military) postal service. War erupted in the sky, as the Apocalypse correctly states[1]–but that was the reason why the InfoWar stayed immaterial.

Technology or science (if one may even separate these two fields after Heidegger) were involved in only one aspect: the encryption of one's own messages and the decryption of the enemy's. Even today, a primitive alphabetic key is still named after the commander Caesar. But the military history of secret information still hides secrets, even after David Kahn's pioneering *Codebreakers*. Still unknown, for example, is the relationship between François

Vieta's invention of the algebraic notation of polynomials and his cryptanalytic work during the French religious wars. (After all, in both cases the goal is to assign letters and numbers to each other.)

But the information that was won or hidden this way was not yet a weapon itself. Therefore information technology in Old Europe decided the outcome of single battles, but not (as far as I know) wars. Things might have been different in other cultures, but European warriors at least were a fairly old-fashioned or traditional caste. A likely assumption is that the coupling of general staff and engineering education, which was institutionalized by the French Revolution through the founding of the …cole polytechnique in 1794, made information systems conceivable as weapon systems. In 1809 Napoleon decided the outcome of a whole campaign (against the Austrian empire, no less) by employing the then-revolutionary optical telegraphy[2]. For a time, the church towers of Linz, precursors to all Ars electronica as it were, served to transmit Napoleon's secret military codes…

So the campaign of 1809–to say it with Jacques Lacan–injected war with a function of urgency. The polite as well as suicidal waiting of the French Knights until the British enemy too was ready for the battle of Agincourt in 1415 came to an abrupt end. From optical to electrical telegraphy, from telegraphy over (at first strictly military) radio to satellite links, the history of war over the last two centuries has been pure dromology, according to Virilio's hypothesis. Not without reason are delay times ("delays") also called dead times in technical-military jargon. He who knows a few seconds too late is not punished by so-called life but by a hostile first strike.

By now it has become common knowledge what far-reaching consequences this war history has had upon civilian culture. (Perhaps still unknown is the fact that the self-proclaimed competence of mass media sociologists does not extend to these consequences.) Weapon systems made of wood or bronze, iron or Damascene steel eked out the exceptional existence of a warrior caste for thousands of years, while the weapon called telecommunications transformed cultures which were based on civilian (if not clerical) storage media like books and the printing press into information societies. Radio is just the military radio system of the First World War minus the talkback-capability, television just the civilian twin of the radar screens of the Second. Not to mention computer technology, whose cryptanalytical and therefore military background, in the case of Alan Turing, stopped being a British state secret in 1974, while the National Security Agency still seems to have declared a news blackout in the instance of Claude E. Shannon[3](*Communication Theory of Secrecy Systems*). The intelligence of computers, as Turing and Shannon developed them, arose not from the modeling of physical processes but from simulating enemy intelligence4. It is no wonder then that John von Neumann, as the designer of the computer architecture of the same name, transferred the war game back to the symbolic: The matrix algebra of games theory takes the place of Müffling's physical sand box.

In the English language, intelligence means not just brains, but also secret service, meaning knowledge of the enemy's knowledge. The good old C3I stood for command, control, communications, and intelligence, the current C4I also takes into account ñ as command, control, communication, computers, and intelligence ñ the modern-day hardware. It would be a worthwhile undertaking, albeit always threatened by the thirty-year waiting period on sensitive documents, to write a technology history as the gradual interlinking of COMINT, ELINT and games theory. COMINT or Communication Intelligence obviously originates from Bletchley Park's first computers, which could crack almost all code machines of the Wehrmacht's communication lines shortly before the end of the war. ELINT or Electronic

Intelligence probably derives from the early warning radar systems, which since the fifties not only re-programmed new computer generations from cryptanalysis to physics, but also brought the joystick and the computer monitor into the world.

The showplace of Electronic Warfare, paradigm of the late Cold War, was the imperceptible realm of physics, lying outside of human awareness. Electronic Warfare followed as a concept from the dictum of Admiral Moore, Joint Chief of Staffs, that victory in every future war would fall to that side which managed to gain superiority over the complete electromagnetic spectrum (from the ultra-low submarine communication frequencies to the interstellar gigahertz region). The second Gulf War made his adage come true. It is almost forgotten today that the first US bomber squads flew over the Iraqi border shortly before midnight, while the undeclared electronic warfare, which opened up the sky over Baghdad, had started in the early afternoon.

But Electronic Warfare, this dark side of the new media-compatible weapons systems, also has its disadvantage. Worldwide systems for early warning, reconnaissance, positioning and control of armies presuppose equally global computer networks. Only in the first planning phase did the forgotten ancestor of all our communicative raptures, ARPANET, connect the command bungalows, which were spread all over the United States, with select elite universities. The net already began its global proliferation with the fiber-optic cables which NATO laid in the Atlantic, in order to immediately feed the raw data from ELINT and COMINT back to their US head offices. An electronic duplicate of possible military campaigns which anticipates their topologies and operations in hardware and software tends to eliminate the difference between war and war game. Espionage and communications technology on the one hand, computer simulations on the other, all fall together in one and the same equipment.

The Pentagon has christened this new dispositive Information Warfare and has done everything possible in the last few years to redirect its still considerable funds, taking into account the end of the Cold War, from Electronic Warfare to Information Warfare. The reasons are plain to see. The Monroe Doctrine falls with the global networks and satellite links that have been established in the last thirty years. For eighty years, America was the sole continent that enjoyed the privilege of belonging to the Americans. (Only on Halloween 1938 and only in Orson Welles' magnificent radio drama, for one horrible day, did the states of New Jersey and New York undergo an invasion from Mars. These invaders already put into practice a Blitzkrieg and/or Information Warfare in that they did not attack armies, but only electrical networks, bridges and railway lines.[5]) The Internet, as the shadow which Electronic Warfare has cast upon the globe, disposes of any last vestige of "sanctuary", even if it is called God's own country.

Information Warfare can begin on any desk equipped with a PC. To copy a hostile CPU is easier, cheaper and therefore more likely to proliferate than copying a hostile phase radar. That is why, finally, the dealers and engineers (e.g. at Advanced Micro Devices) have learned from the warriors that knowledge only counts as knowledge of the enemy's knowledge (e.g. at Intel). Reverse engineering basically means to found one's own production techniques on espionage. This new intelligence will still present difficult questions, because it replaces the good old assumption of ignorance (among competitors, advertising customers and consumers).

But perhaps reverse engineering can also mean that subjects alias underlings–in marked difference to those of wood and bronze, iron and Damascene steel–have a chance again. If the

US Army can give up its old dream of having the best proprietary computer equipment possible and instead buy on the common market like the rest of the world, a form of equal opportunity weapons technology results; but this has historical consequences. According to the scenarios of Information Warfare, the monopoly on the use of force by nation-states sadly no longer exists. The end of Hobbes' civil wars has itself come to an end with mafias and cartels, NGOs and terror bands. When power systems coincide with operating systems and computer networks, they become susceptible on a level which is principally intelligible: the level of code.

Therefore the appeal to wage war according to the conditions and budgetary dreams of the newest arm of the service, an appeal as familiar as it is dull since the budgetization of the intelligence troops, is not the only thing to appear on the horizon of the Information Warfare. The figure of the artist-engineer reappears, after having been seemingly displaced by the founding of standing (meaning national) armies. Only art history still knows that the famed geniuses of the Renaissance did not just create paintings and buildings, but calculated fortresses and constructed war machines.[6] If the phantasm of all Information Warfare, to reduce war to software and its forms of death to operating system crashes, were to come true, lonesome hackers would take the place of the historic artist-engineers.

Not without reason does a famous InfoWar scenario of the RAND Corporation imagine the following scene: In the year 2002, the USA withdraws its military support for a collapsing Saudi-Arabian ruling house because Airbusses full of American tourists are dropping like flies from the sky over Chicago. The Airbus was the first civil plane that needed an on-board computer to remain in the air, just like its military predecessors. In the RAND Corporation's war game, Iranian mullahs, who have always thrown oily looks towards Saudi Arabia, have managed to bribe the Indian programmer of the Airbus software to hack his own program. A single artist-engineer of that un-incidental half continent, which once created the basis of all things digital with the invention of zero, suffices to strategically paralyze the last remaining super power with the transmission belt of the American media democracy.[7]

Such scenarios are not just based on the presumption that all powers on this earth will quake like God's own country, equally fearful of their inhabitants' dying media-effective kinds of death. They also stylize the writing of software into an artistic feat of an individual, who ceased to exist in the software forges a long time ago. It is therefore much to be feared, as in Alvin Toffler's ideology-laden *Cyberspace Manifesto*, that the free individual, with his power to lead the mind itself to victory over the materialism of the nineteenth and the military-industrial complexes of the twentieth century, will always remain a fig leaf.

When it comes to non-governmental organizations that might, step by step, dissolve the three-hundred-year old monopoly of the nation-states on the use of force, the strategists of information warfare, financed by the same nation-states, will not grow tired of naming environment-contaminated ecologists, peace-contaminated leftists and Islam-contaminated terror groups. What they fail to mention is the computer business itself–not as a mythical final frontier for hackers, but as a band of global companies, who are as imperialistic as they are warlike. This gang has already achieved the breaking of the state monopolies of mail, radio and telecommunications. Even the US Army has ceased to set high goals for the computer industry, such as Very High Speed Computing, but instead provides for its own needs, modest like the rest of the world, on the free market. So the gang has started to incorporate entertainment media and television companies into their chips and networks. When even Andy Grove's "War over the eye ball" will be won, there will hardly be any worthwhile opponents or unfriendly takeovers left–except for the nation-states themselves. Reading the

loud warnings of a loss of power of the nation-states in an alternate way may lead to the interpretation that computer warfare is best left to the computer industry itself. Bill Gates and Scott McNealy as condottieri of their private armies consisting of servers and clients, operating systems and proprietary networks …

All prognoses, however, no matter if they be sinister or neo-liberal, assume one thing: that the Universal Turing Machine is in fact and in theory the end of all history. Information Warfare simply means to fight over digital technology with digital technology. Physicists today assume that the Turing-Church Hypothesis in its most general (meaning physical) interpretation was a misapprehension, one that the information warriors are still laboring under: the one thing certain about nature, whatever this ancient term might imply, is that it is not a Turing Machine. From the fact that it exists we can assume that other programmable machines are possible. In this case world history will not have reached its inevitably digital end, and the Pax Americana, as far as it is still based on John von Neumann's combination of English computers, German rockets and American nuclear bombs, will have been an interlude. The war, started in the sky, will be continued in the heaven of Mathematics.

[1] and Luther weakly translates

[2] Cf. Rolf Oberliesen, *Information, Daten und Signale. Geschichte technischer Informationsverarbeitung*. Reinbek 1982, pp. 59—62.

[3] Cf. Claude E. Shannon, *Communication Theory of Secrecy Systems*. The Bell System Technical Journal, 28, 1949, pp. 656—715.

[4] Cf. Alan M. Turing, "Intelligent machinery." In: Bernhard Meltzer and Donald Michie (eds), *Machine Intelligence 5*., p. 14: "The field of cryptography will perhaps be the most rewarding. There is a remarkably close parallel between the problems of the physicist and those of the cryptographer. The system on which a message is enciphered corresponds to the laws of the universe, the intercepted messages to the evidence available, the keys for a day or a message to important constants which have to be determined. The correspondence is very close, but the subject matter of cryptography is very easily dealt with by discrete machinery, physics not so easily."

[5] Cf. Howard Koch/Orson Welles, "The War of the Worlds". In: Werner Faulstich (ed), *The War of the Worlds/Der Krieg der Welten. Vier Hörspiele*. Tübingen 1981, p. 23: "They seem to be making a conscious effort to avoid destruction of cities and countryside. However, they stop to uproot power lines, bridges, and railroad tracks. Their apparent objective is to crush resistance, paralyze communication, and disorganize human society." As parallel source cf. also Len Deighton, Blitzkrieg. Von Hitlers Triumphen bis zum Fall von Dünkirchen. 2. edn. München 1980, p. 225.

[6] Cf. Edgerton, Samuel Y., Jr., *The Heritage of Giotto's Geometry: art and science in the eve of the scientific revolution*. Ithaca (Cornell University Press) 1991.

[7] Cf. Roger C. Molander, Andrew S. Riddile, Peter A. Wilson (eds), *Strategic Information Warfare. A new face of war*. National Defense Research Institute, RAND Corporation. Santa Monica/Ca. 1996.