

Friedrich Kittler

Infowar. Notes On The Theory History

Kai egeneto polemos en to ourano.
Apokalypse 12, 7

Naturally, the nineties of this century weren't the first ones to discover that information counts in war. For ages now, two 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.

But it lay in the nature of this intersubjective structure that it 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 fervent 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, if any. (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 École 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. 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 and suicidal waiting of the French Knights until the British enemy too was ready for the battle of Azincourt 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 an existence in 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; to say nothing of computer technology, whose cryptanalytical and therefore military background, in the case of Alan Turing, stopped being a British state secret in 1974, while there still seems to be a news blackout in the instance of Claude E. Shannon (Communication Theory of Secrecy Systems).

In the English language, intelligence means not just brains, but also secret service, meaning knowledge of the enemy's knowledge. The good old C3 I stood for command, control, communications, and intelligence, the current C4 I also takes into account — as command, control, communication, computers, and intelligence — the modern-day hardware. In any case, weapons and knowledge systems, material and immaterial armament coincide in the Information War. Heaven, where John once saw war break out, seems to have become the strategic present. The showplace of Electronic Warfare, paradigm of the late Cold War, was the imperceptible realm of physics, lying outside of human awareness; 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 us with 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 or 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. [2] 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. The war in Heaven would truly break out.

[1] and Luther weakly translates

[2] 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.