Gerfried Stocker
InfoWar

"Whenever I see a railroad, I look around for a republic."
Ralph Waldo Emerson

There is no sphere of civilian life in which the saying "war is the father of all things" has such unchallenged validity as it does in the field of digital information technology, whose chief protagonists, the computer and the Internet, are direct products of the military's technological wizardry. Nor is there a comparable example of a field's dynamic development having attained such tremendous independence to become–in a strategic alliance of military research, the entertainment industry and global financial markets–the actual driving force of civilization itself. Furthermore, this is a development that has transferred an enormous potential for the organization of surveillance and control from the military to the civilian sphere, the so-called consumer market.

Our understanding of war as the episodic outbreak of bilateral hostilities has undergone a change as a result of the incessant efforts to maintain a so-called balance of deterrence. This conception was projected onto the Cold War as a permanent simulation; war transformed itself into a logistic maneuver or, as Paul Virilio put it in 1983, into a "pure war." Nevertheless, the all-too-real wars pitting nation-states against each other, which have occurred in the wake of the fall of the Iron Curtain throughout Europe–wars which the West would have relegated so gladly to the dustbin of history–have resensitized and reminded us that the future of war will not erase its past.

From the development of military computing at Bletchley Park in England, where the cracking of the German encoding system decided World War II, to the Cold War's research labs at MIT, where the SAGE (Semi-Automatic Ground Environment) Project commissioned by the US Air Force produced the first network-linked computer system, to Ronald Reagan's SDI Starwars Program which, through its announced goals and purported successes alone, brought the Soviet Union economically to its knees–the scientific-technological network linking the military, research institutions and weapons manufacturers has endowed the concept of the power of knowledge with a new dimension in our century.

From the political role played by the gazettes and pamphlets during the French Revolution, to the acceleration of geopolitics by the electric telegraph prior to the First World War,[1] to the first political electioneering conducted via radio during the 1920 US presidential campaign, a highly conspicuous manifestation of modernism is evident in the parallels displayed by mass medial and military-industrial lines of development. This correspondence climaxes in the historic connection between the development of the atomic bomb and the computer, whereby the fateful synergy of destructive energy and information laid the foundation for the strategic power of information as a new type of weapon.

Notwithstanding the general absence of analyses pointing this out, it must be acknowledged that an enormous historical momentousness is to be attributed to the fall of the Iron Curtain, the 1991 Gulf War (or rather the medial fulfillment of its strategic objectives) and the development of the Internet from a military-scientific messaging system to the favorite technology of a fashionable new class of educated achievers in the US and, in the meantime, Europe as well (promoted by Al Gore and Newt Gingrich), in the wake of which fundamental changes have also occurred in the world of the military strategists. In June 1995, the first 16 infowar officers–warriors specially trained in defense against computer attacks, the

deployment of virtual reality in the planning of battles and maneuvers, and techniques to infiltrate enemy computer installations–graduated from the National Defense University in Washington.

Infowar as a concept going beyond conventional forms of warfare will, of course, continue to be treated as a viable military option; nevertheless, the forms that such warfare will take will be radically different from those with which we are familiar.

Information warfare will be waged without visible and definable fronts, and without geographically localizable hostilities, which will be replaced by duels fought everywhere simultaneously to decide the supremacy over information. War will not take on a martial form, because it will be invisible and intangible (unable to be grasped!) due to its fragmentation into numerous tiny entities and its widespread dispersal throughout all spheres of society. The dividing line between attack and defense will likewise become even fuzzier than has previously been the case during the nuclear era of the Cold War.

The politics of infowar is no longer a matter of victory or defeat. It will often be more advantageous simply not to lose and/or to prevent the other side from winning. It will even be increasingly important to prevent the complete annihilation of one's adversary who is, after all, one's business and trading partner–as, for example, in the case of India, which is a major player in the software business and whose low-paid but highly-qualified workforce develops software and processes data for airlines, banks and government institutions on a worldwide basis.

Non-government institutions–frequently transnational organizations and business conglomerates–will play a more important role than governments of nation-states. It will be increasingly difficult to ascertain which alliances exist, who supports whom, and who is threatening whom. Moreover, a wide array of minute, subtly penetrating activities have to be expected which would be indeterminable due to their heterogeneous appearance and multiple morphology, and would thus enable successful evasion of all UN resolutions, conventions of international law, and efforts to enforce global boycotts and bans–a substantial challenge for the world community of nations.

Project Infowar, however, not only speeds up the process of discreet interventions; this very same undertaking also inspires the hopes of arms merchants.

Where Do You Want to Fight Today …

The planning of "Force 21" (the army of the 21st century) with the 21CLW (21st Century Land Warrior) has provided new nourishment to the visions of post-human man/machines. These prototypes look as though they had just sprung from the monitor of a Computer Ball game, and are well within the tradition of 1950s sci-fi stories which suggested that contamination by mysterious forms of radioactivity could lead to the emergence of invincible mutants. (A hardly-coincidental analogy to the experiments to which the armies of East and West subjected their troops during the early phase of atomic testing.)

By means of "augmented reality" (editor's note: a technology enabling computer-aided amplification and enhancement of sensory perception and physical capabilities), the soldier is converted into a mobile command headquarters, whereby this conception has not yet brought about unanimity as to whether they should be self-directing or should rather function as remote-controlled fighting machines. They would by all means be equipped with body sensors

which, in the case of an injury, would provide commanders stationed at a safe distance from the theater of battle with precise information on the severity of their wounds and the risk-reward ratio of a potential rescue mission.

In the "war after next" (what sort can we expect in the meantime, one might ask with trepidation), this moral dilemma should well be resolved. There promises to be no more blood-drenched battlefields and no more tragic errors leading to soldiers who were "definitely at the wrong place at the wrong time"[2] being blown to bits by friendly fire. The solution promises to be not only one in which robot-soldiers have attained completely cybernetic form, but rather, to a much greater extent, the deployment of artificial intelligence–artificial live algorithms–on the triggering mechanisms of cannons and missiles which, despite all the euphoria about "smart and non-lethal weapons," will certainly not disappear from the repertory of military tacticians.

Non-lethal weapons–which, according to John B. Alexander, department head at Los Alamos, were thus named "because no other term made such a strong impression"–are among the most top-secret projects of US weapons research. Admiral William Owens, Vice Chairman of the Joint Chiefs of Staff calls them "America's gift to warfare."[3] These include blinding lasers; chemical and biological substances designed to make the enemy and/or his materiel unfit for battle before he is even aware of the fact that he is in a fight; electromagnetic bombs releasing high-energy doses of radiation which knock out all electronic devices within a wide radius and which exert an effect upon organic tissue like that of a gigantic microwave oven, whereby all life in the proximity of its detonation is simply grilled; or special microbes that can be bred to devour either electrical transmission lines or their insulating material.

"Commando Solo" is the name of an infoweapon which had already been presented by the Pentagon in 1995; it represents an additional promising field of information warfare: psychological warfare and propaganda (psyops). In a reversal of the function of spy planes and espionage satellites that attempt to gather information, the point here is the dissemination of false information and intentionally manipulated data. A $70 million aircraft with an 11-man crew and state-of-the-art electronic equipment is deployed to disrupt a country's entire radio and TV system and to broadcast its own transmissions on any desired frequency.

According to rumors, during the Gulf War there were those who toyed with the idea of creating a computerized image of Saddam Hussein with a glass of whiskey in one hand and a ham sandwich in the other, and broadcasting it on Iraqi TV–perhaps yet another indication of the connection between the entertainment industry and military technology. Nevertheless, it seems that following the end of the Cold War, Hollywood and the makers of Nintendo and Playstation have surpassed weapons researchers (above all in the areas of computer simulation and virtual reality) at the leading edge of information technology.

The informational automation of war by means of electronically-induced blindness and paralysis will not diminish the horror of socially sanctioned killing during the waging of war. The concept of "humane war" may perhaps "make a strong impression," but it certainly does not make a credible one.

Information and Business have no Front Line

In contrast to the military past (to which the Gulf War also belonged while it was being fought) when technology was deployed as a tool that enhanced weaponry's performance in battle, today's modern information infrastructure as the most essential pillar of transnational

economic systems is not only the highest-priority target of potential aggression, but has also become–due to the computer's inherent capability of automating intelligence and to be Medium and Message simultaneously–the weapon and the battlefield all in one.

Decisive strategic knowledge accumulates with ever-increasing speed, but it no longer does so only in the heads of top managers. Rather, it is implemented beyond the level of encyclopedic databanks, above all as algorithmic data processing and evaluation in computer systems linked by networks to autonomous decision-making structures. Consequently, the strategic objective is no longer destruction and elimination, but rather the acquisition and/or control of the knowledge of others, since destruction would no longer constitute a desirable option in light of the tightly interwoven character of global business. Even if, up to now, forgoing offensive infowar has been based upon the fear of a conventional counterstrike–for example, it is Russia's official position that an attack on its information infrastructure will provoke a thermonuclear response–it can nevertheless already be seen (in the case of the US, for instance) that industries whose international success is based to an overwhelming extent on the export of software (Microsoft and Hollywood, though also Coca-Cola and McDonalds, who actually export only software in the form of patented recipes and protected trademarks) would have absolutely no interest in the long-term destruction of elements of the global information infrastructure, to say nothing of the dependence of global financial markets upon the functioning of its networks. In this connection, it also becomes understandable that the most important basis for the normalization of relations between the US and China was not the implementation of international human rights standards, but rather the concession by China to put an end to its industrial software piracy.

Thus, infowar is not solely a matter for the military in cyberspace, but to a much greater extent a phenomenon inherent in our society whose driving forces are technologies that have been developed from out of a military context. Infowar is a question of the increasing emancipation of the civilian domain–"vote with your modem …"–a question of knowledge and perception of the world.

Infowar is thus an abbreviation standing for a way of dealing with power in a media society in which propaganda and the manipulation of perception have attained technological perfection, for "… the development of technical and electronic means to implement political control, particularly surveillance and identification technologies, the collection and storage of data, non-deadly weapons, technologies of imprisonment, execution and torture" as well as for the "trend toward increasing militarization of police technologies and the paramilitarization of military technologies, which is proceeding on a global basis in the direction of a convergence of technologies enabling political control."[4]

And whereas we civilians are only too familiar with the euphoric or apprehensive commentaries on the extent of these changes and innovations from our point of view in the civilian, or to put it more accurately, the consumer sector, it can be observed with astonishment as well as a bit of *Schadenfreude* how the military can no longer contain itself, at once speaking with pompous euphoria about its latest enhanced fighting capabilities and simultaneously scared to death by the nation's sudden vulnerability.

The international gangs of intelligence agencies and espionage organizations, sorcerers' apprentices from all branches of the military, secret services, research and business organizations seem to be afflicted by a collective nightmare that their mighty surveillance networks could fall into the hands of the foe. Since the enemy has disappeared since the fall

of the Soviet Union and the economic opening of China, a new one must be reinvented, of course. And what serves this purpose better than the Internet?

Centralize Strategically, but Decentralize Tactically.

The Arpanet, conceived as a guarantee for the invulnerability of military command-and-control functions in the case of an atomic attack, has transformed itself by means of its public, civilian use as the Internet into the very opposite of its original intention: a veritable military nightmare. Even if the early visions and hopes of a democratic Global Village have proved to be illusory, a new category of "public" and a new dimension of "civilian" are making their presence felt.

The actual danger of hacker attacks and cyberterrorists in the US does not lie in highly-improbable large-scale acts of destruction or sabotage, but rather in the effects of a small number of spectacular attacks on the American media public with the resulting consequences on the decision-making latitude of American politics.

What is the actual background of the potential threats being conjured up? Is there a real danger that a few hackers in the employ of the good old enemies of the US–is it any wonder that the list of countries to which US military experts attribute the greatest potential for cyber-destruction is headed by Libya?–could plunge the country into public chaos, or is this just meant to stir up public opinion? This latter conjecture immediately suggests itself in light of the boldly simplistic allusions to American history during World War II, whereby the threat is referred to as an "electronic Pearl Harbor" and the research and development offensive being promoted is termed the "Manhattan Cyber Project."[5]

The hysteria surrounding the images conjured up of these new enemies could have a variety of motives. First, the race to secure a portion of the funding being doled out by Congress from the research and defense budgets is in full swing, pitting the lobbies of the conventional arms industry against those of the increasingly powerful computer and software sector. In comparison to the good old days of the Cold War and to the sums that continue to be devoured by conventional weapons technology, direct investment in the development of cyberwar and netwar is infinitesimally minute. During the last few years in the US, more than 50% of the construction costs of weapons systems has indeed gone into electronic components, but this primarily has to do with conventional weapons whose efficiency is enhanced by equipping them with electronic systems. Thus, the cost of producing one Stealth bomber gets run up to $1 billion; in comparison, a budget of $500 million was recently approved for the development of a new supercomputer (IBM’s successor to Deeper Blue) to be designed to perform atomic weapons simulations.

Second, authorities have learned the lesson from their failed attempts to impose state control and regulatory measures upon digital communications networks (Clipperchip, CDA). It will take a massive shift in public opinion to make it possible to introduce a "key escrow" system for all citizens–or "digital dog tags" as the staunch opponents of this state-controlled cryptography system refer to it.

The enormous economic potential of the Internet, and the knowledge that the hegemony of the US economy and, consequently, that of American culture as well, can be assured over the long term only by means of predominance in the Internet, have shifted this medium into the center of economic, political, and military interest. Since information has become the most important resource fueling economic growth, and software increasingly yields more

substantial profits than hardware, the Internet has become the primary arena of global competition and, for this reason, there is a pressing need for intervention to establish order. Once adequate security and order are in place, the major investors will follow the pioneers of the digital gold rush and occupy their respective territories.

Recent history provides a model for this strategy. In the 1950s, as the highly profitable export potential of the US film industry–with Hollywood as the first gigantic American software producer–began to emerge, as film's enormous public influence became clear, and its potential with respect to a claim to cultural hegemony started to unfold, the evils of Communism were advanced as a justification to begin methodically cleaning house, primarily in the intellectual milieu surrounding Hollywood. This form of persecution doubtlessly had an adverse effect upon the artistic development of Hollywood, but this was what made the medium of film–indeed, no longer new but, as an international economic factor, newly-emerging–financially interesting for big business. Regardless of the *Weltanschauung* with which one evaluates this development, or whether one regards it as cultural imperialism or as an essential contribution to a global culture, the winners are easy to identify.

Just as clear is the analogy to the efforts to project a new public enemy in the form of "Libyan-financed cyber-terrorists" and hackers as criminal outlaws, in order to sanction drastic measures to control and regulate the Internet and thus to restrict the rights of private individuals in digital space.

It is by no means surprising that measures to introduce public key encryption are also being planned within the EU in order to finally get digital commerce rolling there. Because one thing is certain: there is not going to be any big money made in the Internet without a comprehensible system of identification available to buyers and sellers. In virtual space as well, the concept of property is linked to the concept of the identifyability of the property's owner.

Such efforts still encounter resistance at present. The American conception of civil rights for the citizenry of virtual spaces has a powerful advocate in the form of associations like the Electronic Frontier Foundation. On the part of business, massive resistance has formed primarily outside of the US in opposition to the implementation of encoding systems which can be broken at any time–for example, by US government agencies.

The Innocent have Nothing to Fear

The consciousness of this issue inherent to Information Society on the part of politicians as well as the general public in Europe is not highly pronounced and is emerging rather late in the game. Up to this point, the process of working out concepts for the regulation of the Internet has been left up to industry experts and government security officials. It was not until a few months ago that we got our first taste of the effects this will have on the civil realm of our society and on the private sphere of its citizens in the form of media reports about the storage and evaluation of cellular phone companies' logfiles as well as the long-awaited public confirmation of the existence of the Echelon System. (cf.)

Since as early as 1991, European security officials have been working–more or less secretly and in collaboration with expert advisors from the FBI and the US Drug Enforcement Administration–on the surveillance of existing and future data and communication networks. The generally agreed-upon procedures were set down in a "Memorandum of Understanding concerning the lawful interception of telecommunications," ENFOPOL 112, 10037/95.[6]

For example, this memorandum discusses the network link-up of security agency databanks that are currently being set up throughout Europe, whereby the central intention is "… not necessarily the proof of a perpetrator's guilt in the commission of some particular felony, but rather provisions for the prosecution of future felonies, and thus criminal prosecution in the broadest sense (anticipated criminal prosecution)…"

Behind the scenes of this initiative is the view that the liberalization of the telecommunications market will make current control and surveillance practices ineffective or impossible. It is thus regarded as absolutely essential that wiretapping methods and techniques be constitutionally and legally established, and that private telecommunications providers be obligated to adapt their systems to make them compatible with state bugging practices. This means, among other things, the installation of word scanners and permanent, dedicated access lines to also enable remote surveillance. Wherever this is being carried out (including Austria) the financing of the corresponding infrastructure is the responsibility of the telecommunications provider, with the costs then passed on in the form of user charges …

In countries that refuse to accept these conditions, surveillance can still be carried out against an individual's will, since wiretapping technology comes preinstalled by the manufacturers of communications systems. For instance, ISDN technology makes it possible to activate any telephone by remote control and to thus transform it into a bug without the user being aware of this.[7]

The British research institute Statewatch reports on agreements between EU member states regarding the legal preconditions for global wiretapping.[8]

This report points out that not only basic telephone data and information about incoming and outgoing calls and their content are to be recorded, but also data on the movements of the telephone subscriber–even if no calls have been made. "… neither the bugging target not any other person is to be informed that modifications have been made to any communications systems in order to allow the wiretapping assignment to be carried out […] and that absolute secrecy is to be maintained as to who is being listened in on by whom, as well as the techniques and methods that are being employed." (Source: Statewatch Institute, "Memorandum of Understanding concerning the lawful interception of telecommunications," Enfopol 112, 10037/95, Limite, Brussels, 25.11.95)

According to Statewatch, this memorandum was signed on November 23, 1995 by representatives (the respective secretaries of the interior and attorneys general) of all 15 EU member states–including those of Austria!

The report goes on to summarize the fundamental legal situation with respect to surveillance in each individual member state: Germany, Austria, Denmark, Luxembourg, Spain and Portugal can implement surveillance simply by modifying their legal codes, whereas Belgium, France, Great Britain, Ireland, Greece, Norway and Sweden either require new laws or a combination of the two methods to make it possible.

In the individual countries, discussions are already underway which bring out what a "tremendous advantage" the police would have if "they could place individuals under surveillance once they were even suspected of criminal activities." The report refers explicitly to Austria, where investigative proceedings are initiated as soon as a request to conduct a bugging operation is filed. (Source: "Report on the national laws regarding the questionnaires on phone tapping," Enfopol 15, 4354/2/95 REV2, Restricted, 13.11.95)[9]

Some Numbers Beat No Numbers Anytime

Of course, surveillance and spying on communications is nothing new, and is closely connected with technical progress in the field of communications.

… In 1786 a secret instruction by Kaiser Joseph II hinted to the governors of the Austrian crown lands that it would be useful to the state if the operation of the so-called small posts and their post office boxes were "played into the hands of such persons whose righteous and loyal character the police is certain of." […] As early as 1759 the head of the Paris controlling Office promoted the institution of the Paris Petite Poste with the argument that it gave the police for the first time "a means by which the addresses of all people could be found out that have been looked for in vain in the great Mail, because they only correspond within Paris".[10]

Whereas state security agencies and military intelligence have been making the effort ever since then to find out what the other side knows and to prevent them from doing the same in return, the concept of espionage and counter-espionage did not begin to emerge in industry and business until World War II and the postwar return to the world of commerce by experts from the field of military intelligence. (Heavy industry in the 19th century was hardly conscious of the strategic importance of information about what the competition knew.)

The acquisition by business managers of techniques used by army commanders and intelligence operatives has militarized management to a certain extent, and has thus introduced into the field of information technology the concept of "reverse engineering" as the industrial correlate of military spying on the enemy.

A particular variant of "reverse engineering" became an element of the Cold War when the USSR and, above all, Bulgaria began to produce knock-offs of computer chips obtained in the West. Entire universities were set up to train a host of scientists and technicians, whose job was to dismantle and analyze PCs that had been smuggled in from the US, and to use the knowledge gained thereby for a computer industry of their own–with considerable success, as has come to be known since then. In China until not all that long ago, software piracy organized by the People's Liberation Army functioned as a primary supplier.

The term "competitive intelligence" has since come to assume a place in the standard vocabulary of advanced business strategy. The US consulting firm with the highly indicative name "WarRoom Research," which makes its intelligence services–that is, "corporate espionage" as well as "counter-espionage"–available to private firms, military and political institutions, major banks and insurance companies, as well as the telecommunications industry and high-tech research institutes, and which is considered to be the initiator of the so-called "Manhattan Cyber Project,"[11] performed a study in 1996 in cooperation with the US Senate on the security of information systems among Fortune 1000 companies, in which they investigated a large number of successful attacks in a wide variety of sectors. There were relatively high financial damages associated with each of these incidents; the intruders came from outside as well as inside the company; competitors were frequently behind them. The overwhelming majority of these attacks were never made public and charges were rarely pressed, due to an understandable fear of the resulting damage to the company's public image and the loss of public trust. And–as is probably typical for the US–the motive given for this sort of reaction was very often a fundamental mistrust of "governmental investigations."[12]

Is It a War Crime to crash another Country's Stock Market?

In the sense of the concept propagated by Paul Virilio referring to the shift from exo- to endo-colonialism, the military has ascertained the identity of the new enemies of Information Society as, above all, those domestic foes among the country's own citizenry. They are identified as hackers and cyberguerilleros who constitute a threat to national security and could compliantly serve the interests of enemy nations.

Indeed, it is not so much the fear of intrusion into military computer installations, although published statistics document an enormous level of vulnerability in this area as well. (The word is that over 1,000 hacker attacks are carried out each day against Pentagon processors, whereby only about 50 of them are noticed and/or reported. As a rule, the hardest part of hacking is to just get past the first computer in a system; once inside the firewall, almost all computers regard the intruder as a legitimate user.) It is, above all, the numerous computer networks–inadequately secured, running on relatively unstable operating systems–of local government agencies, private firms, banks and insurance companies, electric and gas companies, etc. that have become causes for concern on the part of nations that have long been dependent on such computer systems.

According to the essential conception of infowar, it actually represents the culmination of a trend in the conduct of warfare during this century: namely, aiming it at civilian targets, from the bombings of London, Dresden, and Hiroshima to the ethnic cleansings in Bosnia. Disrupting civilian air traffic control, erasing the databanks of insurance companies and banks, devastating the currency of an enemy nation–all of these missions can be accomplished in a clean and bloodless fashion by means of computer. Each of them, however, constitutes a violent attack aimed at the civilian populace, and has the most terrible consequences.

The Bush administration repeatedly considered the option of destroying the computer infrastructure of the Iraqi financial authorities, but it was purportedly the CIA who came out against this plan. In August 1995, Time Magazine quoted a former high-ranking CIA employee: "Every time screwing around with financial systems has been discussed as a covert action, people have walked away from it … Messing with a country's money represents a fundamental attack. No CIA director has ever recommended it."

That the players in the global finance business are not so over-scrupulous (or at least pretend to be) has been shown most recently by the events surrounding the crisis in Asia triggered by the speculation directed against the Malaysian currency. In its wake, the entire region was forced into the position of a dependency of the International Monetary Fund and its plans to reorder the regions economic systems and practices. A textbook example of infowar.

"Software code–more than law–defines the true parameters of freedom in cyberspace, the question of what the architecture of cyberspace should be is not a neutral question. We need to think about it in political terms." Lawrence Lessing, special master in the antitrust case of US vs. Microsoft

[1] "As large as the battlefields may be, there is nothing of them that meets the eye. […] No Napoleon […] takes up a position upon a promontory […] The field commander is stationed further to the rear […] in a house with a spacious den, where telegraph, radio, telephone and signaling devices have been installed. From there, the modern Alexander telephones in his rousing words […], there he receives his situation reports […]." Count Alfred von Schlieffen, 1909 cited by R. Genth, J. Hoppe, "*Telephon! Der Draht, an dem wir hängen,"* Berlin 1986, p. 60.

[2] US general in a TV statement regarding an incident during the Gulf War in which a US Army truck was blown up by friendly fire.

[3] Time Magazine, August 21, 1995, Vol. 146, No. 8

[4] "An Appraisal of Technologies of Political Control," Scientific and Technological Options Assessment / STOA, Working Document (Consultation version), PE 166 499, Luxembourg, January 6, 1998

[5] http://www.warroomresearch.com

[6] http://www.poptel.org.uk/statewatch

[7] The message switching system used on digital exchanges like System X in the UK supports an Integrated Services Digital Network (ISDN) Protocol. This allows digital devices, e.g. fax, to share the system with existing lines. The ISDN subset is defined in their documents as Signalling CCITT1-series interface for ISDN access. What is not widely known is that built in to the international CCITT protocol is the ability to take phones 'off hook' and listen into conversations occurring near the phone, without the user being aware that it is happening. This effectively means that a national dial up telephone tapping capacity is built into these systems from the start. (System X has been exported to Russia and China)–"An Appraisal of Technologies of Political Control," Scientific and Technological Options Assessment / STOA, Working Document (Consultation version), PE 166 499, Luxembourg, January 6, 1998

[8] Memorandum of Understanding concerning the lawful interception of telecommunications, ENFOPOL 112, 10037/95.–http://www.poptel.org.uk/statewatch/

[9] cited in: Edmund E. Lindau, pressetext.austria, February 22, 1998

[10] cited in: Bernhardt Siegert, Online S 131, 132

[11] http://www.warroomreseach.com/mcp/

[12] http://www.warroomreseach.com/WRR/SurveysStudies/1996ISS_Survey_SummaryResults.htm