Digital ways of forgetting. Smashing Computers and Newer Forms of Cyberclasm

Tjebbe van Tijen, Amsterdam, autumn 1998 *(with thanks to Ted Byfield, New York, for editing)*

The recent phenomena of "cyberclasm" started with radical student actions in North America against university and military administration facilities. One of the earliest examples was in 1969 at Sir George William University in Montreal where, during a conflict about racism on the campus, students stormed the computer center of the university, threw out thousands of punch cards from the windows and smashed the computer equipment.At that time computers were mostly stand alone machines with limited storage capacity and data was either stored in punch cards, that needed to be processed mechanically, or on reels of magnetic tape.

A year before a little book with the title *The Beast of Business: A Record of Computer Atrocities* was published in London, containing "a guerrilla warfare manual for striking back" at computers that, according to its author Harvey Matusow, were on their way to "grab power": "from now on it is them or us".[1] The whole book had a playful Luddite tone; the guerrilla actions it proposed were rather mild, for example, altering punch cards holes or demagnetizing computer-readable magnetic strips, in order to halt the advance of the computer in civil administration. Matusow mentions the military use of computers, but he seems not have understood their function very well, as becomes clear in his slogan: "It is the computers that want war." "It," of course, is the human beings who want and make war; the social network of political, military, industrialist, and scientific establishments - the "military-industrial complex" - that developed the first electronic computer during World War II. The computer's first function was to assist the calculation of ballistic trajectories of conventional weapons and, later, to aid in the development of the atomic bomb into the far stronger hydrogen bomb. The names of firms that originally specialized in mechanical office equipment - for example, IBM, Burroughs, Remington, and Underwood - can already be found at the military root of the computer pedigree in the forties and fifties: these companies were not just warmongers, their commercial interest also helped to transform the military computer into a civic instrument.

In the following decades the computer tree branched from gigantic machines - the ferocious "beasts" Matusow fought - into the familiar and helpful personal computer of our times. Matusow published his anti computer book in 1968, when the Vietnam War had been raging for four years - and the same year that saw a proposal to combine networks of military and civilian computers (ARPAnet) into a decentralized and flexible form of communication able to resist a nuclear strike. The growing importance of computers in warfare, now also for military logistics and wargames, had not yet been recognized by the radical movements of that time. Manuals for urban guerrillas of the late sixties and the beginning of the seventies do not mention computer facilities as a target; instead, they still emphasize on radio, television,

telephone switches, and electrical power facilities.[2] It was not until May 1972 that the first (publicly known) serious attack on a military computer center - the Heidelberg headquarters of the U.S. forces in Europe - was undertaken by the 'Kommando 15. Juli', a group related to the German Rote Armee Fraktion, to protest the escalation of bombings in Vietnam. Needless to say, this protest did not hinder the metamorphosis of the military ARPAnet into the civil network of networks called the internet. This development has, of course, created opportunities for new forms of 'cyberclasm' and guerrilla: no longer direct physical attacks on personnel and equipment but indirect attacks, using the computer system itself as a basis for disruptive and destructive activities.

Patrolling the Information Highway

It is an old tactical adage that each advantage carries with it a disadvantage. This holds true both for assailant and defender. Empires - the Chinese, Mongol, Roman, Napoleontic, and their modern heirs - can only grow on the basis of an efficient transport system of goods, armies, and information. Developed road systems with facilities for resting, refreshing, and maintaining vehicles were created to make such transport movements faster; but these roads, with their valuable traffic, also created new opportunities for robbers, bandits, and other highwaymen to ambush and take what they could not obtain otherwise. Expanding sea traffic showed a similar development, with pirates laying in wait to catch some of the rich cargo moving between colony and imperial motherland. Newer land and air traffic system continued this tradition of robbery and piracy: highwaymen evolved, became train robber, hijackers... All of these freebooters, over the centuries, hold one activity in common: "stealing something while in transit." The modern highwayman (or woman) roams the "information highway," lurking, waiting for the right moment to grab what is not intended for her or him.

The metaphor of the "information highway" can be related as well to other traditions associated with transit and travel, or, more precisely, stopovers - drinking, prostitution, and gambling, as well as authorities' constant fight to suppress such debauchery. It has become a truism that sex and, to a lesser extent, gambling have been very closely associated with the economic development of e internet, and efforts to suppress them have certainly been in the news. But this will never succeed: the moment one too-lusty site is closed down a new one pops up a farther down the road. Closing down the road itself would be the most effective measure, but, because modern society needs information traffic, it must learn to live with the unwanted side effects. Patrolling the net, by human and software agents, has made it possible to ban some of this unwanted information in some contexts, but there is an inherent danger in the principle that some authority will decide for individuals what to read, what to see and what not.[3] This is not entirely new, obviously: the Catholic Church's Index Librorum Prohibitorum (Index of Forbidden Books) was meant to prevent contamination of faith and corruption of morals dating to the end of the fifth century. It was regularly published from 1559 onward and only ceased publication in 1966. With the introduction of modern filtering software that stops what is not approved or, more radically, only let through what is approved, the old principle of worldwide censorship as practised by the church, has been re-introduced by "modern" governments and affiliated organizations at the end of the twentieth century on a larger scale than ever before.

Loyal Hackers and Spies

Information that isn't in transit isn't thereby safe, even when securely stored behind "firewalls." As in fairytales, however strong a fortification is made, in the end someone will be able to enter, often not by brute force but by deception. It is not surprising that, in the coming age of digital computers, mythological terms such as Trojan horse are still used for such cunning tactics whereby unsuspecting computer users allow hidden malicious information through the gates of their equipment, where it unexpectedly raises havoc and destroys valuable information.

One can go back in time two millennia plus three centuries to find this principle described in the oldest known text on tactics of war, Sun Tzu's Ping Fa ("The Art of War"). The beginning of this ancient Chinese text stresses that "all warfare is based on deception." Sun Tzu clearly distinguishes between direct and indirect ways of fighting and he favours the last form: "indirect methods will be needed in order to secure victory".[4] In 1995, the National Defence University at Fort McNair in Washington, D.C., has instituted a yearly award named after this Chinese war theoretician: *The Sun Tzu Art of War in Information Warfare Research Competition*.[5] Recent prize-winners include a group of researchers who thought up an imaginary scenario that could have taken place during the Balkan conflict in September 1998: a group of Serbian political activists intervene with the radio frequencies of a temporary airfield at the Bosnian-Croatian border where NATO troops are flown in during a flare-up of the conflict in Bosnia. The result is two military airplanes crashing. The Serbian cyberactivists, immediately after, inform the whole world press by email and put up a political statement on a website on a server in Amsterdam. CNN, Reuters, and others broadcast and publish the statement including the webpage address. Within twenty four hours the webpage has a million "hits," many from state intelligence organizations. Any computer used to access this website is infected by a Trojan horse program that the activists have embedded in the webpage, a program that starts to delete all files and hard disks after twenty-four hours. This exercise in military fiction is used as an explanatory introduction to what "information warfare" could be. The authors warn: "The US military could find it difficult to respond against a small and digitally networked enemy." They propose the establishment of "Digital Integrated Response Teams (DIRTs)" made up of "highly trained information warriors" from military and law enforcement agencies, to counter "information terrorism".[6] These state "information warriors" are supposed to work from "remote computers," using "anonymous response" tactics without open display of force, in order to avoid any public sympathy for political activists, fighting a possible "right cause" and being attacked by the state. In the past few years, incidents in which secret state information has been accessed by "intruders" have been played up in the press, but none seem to have posed an enduring security threat to any government to date.

At many levels of society is has become clear that the criminalization and persecution of computer hackers often misses the point: in most cases the sole aim of a hacker is to master computer and encoding systems, to explore how far or how deep one can go. Even most of the more political motivated hackers tend to have some basic loyalty to some national state. There are also, of course, cases in which of copyrighted and otherwise protected digital material have been infringed upon, but these incidents involve discrepant interpretation of and/or attitudes

toward what acceptable forms of ownership are; they differ from activities of organized crime or terrorist attacks against the functioning of the state. Several academic and military studies present a more differentiated or complex view on the "hacker scene"; some authors see hackers as a positive force in society that can be tapped as a resource to improve security systems.[7] This is, in essence, also an ancient tactic: one can read in the last chapter of Sun Tzu's Art of War that describes the use of spies: "The enemy's spies who have come to spy on us must be sought out, tempted with bribes, led away and comfortably housed. Thus they will become converted spies and available for our service."

A World Without Electricity

As the computerized informationization of all levels of society progresses, a feeling of vulnerability is growing. In early 1998 the Clinton administration issued a "White Paper on Critical Infrastructure protection" that describes what to do against "nations, groups or individuals" that "seek to harm us in non-traditional ways".[8] Others use catch phrases such as an "Electronic Pearl Harbor" or "cyberwar, blitzkrieg of the twenty-first century" to fire the imagination of the politicians and civil servants who decide about budgets for new research, new special task forces and new weapons. The reasoning is constant through human history: what the enemy can do to us, we should be able to do to the enemy.

Apart from the indirect methods and approaches of hackers, computer criminals, and their state counterparts, the "information warriors," a whole new arsenal for more direct forms of "information war" is being prepared: rumors of guns that fire "High Energy Radio Frequencies," hitting electronic circuits with an overload that will knock out any radio and television transmitter, telephone switch, computer network, aircraft or other transport system dependent on electronics; miniature "nanotechnological" robots that can physically alter or destroy electronic hardware; low-energy lasers that can damage optical sensors used in many modern vehicles and equipment; and, best of it all, the Electro-magnetic Pulse (EMP), originally discovered as a side effect of nuclear bombs, which disables all copper-wired electronic circuits, halting all electronic equipment and communication not specially shielded against this form of attack.[9] There are different plans for the usage of the EMP weapon: the "shock and awe" tactic whereby whole urban areas or battlefields will be blasted with such an energy that all electricity stops functioning, as well as the more "precise" targeting of single objects in a range of a few hundred meters. Modified cruise missiles for such confined operations exist already. It is difficult to imagine a world without electricity. One wonders what it would be like, to live without all those electric facilities and contraptions, to have lesser, but maybe deeper contacts, in a more tangible world.

Invisible Strings of Voltage

The basis of most electronic documents is recoding of human-readable text and graphics and machine readable sound and video. At all stages of production and reproduction, different layers of technology reside between the human organs of perception and digital documents. Recoding as such is not a new phenomena; it is recoding of language into written text that "permits us to create a record that many other people, far distant from us and from one another in time and space, can read".[10] The non electronic recoding of language, by hand with its

directly readable physical marks on a physical surface, have left us with only a limited number of documents from early ages; many did not even survive their own epoch. The shortage of good writing materials such as papyrus and parchment meant that reusable surfaces, such as wax tablets, were often favoured. Parchment was rare and expensive and for that reason often "recycled," reused as "palimpsest" by washing and scraping off the text it carried. The use of paper and the multiplication of writing by the printing press fundamentally changed this situation. The dispersal of multiple copies of a (printed) text led to the long-term preservation of that text.

Now digital documents are of another order: they are no longer tangible objects but "essentially an invisible string of stored electrical voltages"[11]. First it was scarcity of carriers for storing these electric currents (floppies, hard disks ,and the like) that led to the same practices as the recycling of wax tablet and parchment in antiquity: erase and reuse. Later the price of digital storage dropped dramatically, but this has introduced a problem of prodigality - the problem of managing large quantities of half-labeled and messy information, which often led to a similar outcome. As the fixity and multiplicity of the printed is more and more supplanted by the flexibility of multiplicitous digital document, we come to see that new media are posing problems when it comes to long-term preservation of content. Standards for computer hard- and software are in a constant flux, and backward-compatibility and long-term support seems not to generate enough profit to interest industry. Bankruptcy of a firm or defeat of a standard on the marketing battlefield can mean, in practical terms, the loss of massive amounts of information. Eternal transcoding of digital information from old to new standards will need to become a routine operation within bigger institutions, but such facilities are expensive and unreliable and, as such, all but unavailable to smaller institutions and much of the private sector.

This last sector of society was already underrepresented in archives and other deposits for historical studies; now, in the digital area, even fewer traces will remain of personal administration, letters, email, unpublished manuscripts, and the like. Going through the belongings of someone who died one might consider keeping some letters, notebooks or photographs, things we can read directly - but what to do with an outdated computer, a shoebox with unreadable floppies, mysterious-looking cartridges, and unlabeled CDs? Their fate is to rust, rot, or burn along with other refuse - or at best to be recycled somehow. In this sense we have seen a similar thing happening earlier this century when old cinematic film was recycled for their silver content.

Data Archaeology

Global and direct availability over the internet of a wide variety of electronic documents has led, on the one hand, to a speedup of information circulation and, on the other, to a loss of information. The life cycle of content made available over the internet is getting shorter and shorter. Thousands of web pages are "thrown away" each day for various reasons: storage costs, lack of space on computers, hard disk crashes and other digital disasters, information becomes outdated, unwanted, censored, neglected. Strangely enough, the information is often not directly lost but, rather, fades away slowly, like the light of a star that no longer exists but still can be seen in the sky. Information is duplicated on computers elsewhere in the form of mirror sites or caching proxies that temporary store often requested information to diminish long-distance

traffic over the internet. In the end, this duplicated information vanishes as well. Some see this as a positive aspect: why pile up the informational debris of each generation on the already towering heap? Others worry about the void of digital historical material we will leave for posterity.

Megalomaniac plans, with an imperialistic and totalitarian undertone, to periodically store "all information" available on the internet and associated networks in gigantic digital warehouses have been proposed; one example is Brewster Kahle's 1996 founding of the 'Internet Archive'.[12] It seems more logical that the old principle of "survival through dispersal" will have a longer-lasting effect on preservation and availability of digital documents from the past. ("Destruction, ruin, pillage and fire especially hit great amassments of books that according to the rule are situated in the centers of power. That's why what has remained [of the earlier period] in the end does not come from the big centres but from marginal places".[13] Even if a very small percentage of the electronic material on the global network of networks will be preserved, this will be of such a magnitude and diversity that special techniques of "digital palaeography," "data mining," and "information recovery" will be needed to dig up something that will make any sense to future generations. (One can imagine theories of extinct technologies...) Another approach is the simulation of the functioning of old hardware and software on new machines, be it military analogue computers of the fifties or one of the popular hobbyist computer types of the seventies and eighties. The real experience of the functioning and use of this equipment will be lost in this process, but is not most of what we think to experience from the past a simulation of a reality that never existed?

Lost in the Deafening Babble

The traditional containers of information (books, periodicals, gramophone records, audio CDs, film and video titles produced for the consumer market) fix information in such a way (cover design, title, colophon, credits, numbered series, publisher, place of publication, year, and so on) that we can easily deduce what they are about and have some understanding of the context in which they function(ed). It took more than four centuries for these standards to develop and come into common use. From this perspective, it is not surprising that the use of new standards for the description of networked electronic documents - a reality that exists hardly two decades - should be less stable. Consider the standards for storing data about data in an electronic document: some of this "metadata" is automatically generated when a document is created - for example, time, date, the hardware used and protocols needed to display or manipulate the document. Without this self-referential information the documents could not even be distributed and consulted. When it comes to description of content (author, title, subject, and so on), new standards do exist, but are little-known and rarely used.

This means that there is an immense amount of potentially valuable and interesting information on the internet that remains unnoticed and will be forgotten because its content is not properly described. Whatever powerful "search engines" are used, machine protocols can not sufficiently distinguish between meaningful and meaningless occurrences of search terms used. Most search results give so many "links" that one can not possibly follow all of them. In this way valuable information is "lost in the deafening babble of global electronic traffic".[14]

The Fragility of a Spider Web

There are people who think that such a comparison of new electronic information and communication systems with traditional media is not fruitful. Some of these people see a loosening of the bonds that bounded text, sound, and image to their respective media as, rather, a fusion of these elements into a new phenomenon, multimedia - something of a different order, where fixity and linearity are supplanted by a fluid, dynamic recombination of elements, which ultimately will abolish the notion of finite and finished works. This new form of human communication has one of its theoretical bases in literary and semiological theories developed three decades ago, which pointed to the relationships within a given text to a multitude of other texts and the possibility of a new kind of more personal and active reading. This theory of the possibility of different "readings" of text was also extended to the realm of imagery, as it became clear that computers offered new technical opportunities to interact with a corpus of many different linked texts fragments. Soon enough, these theoretical concepts were given a concrete form, 'hypertext'.[15] The first experiments were with interlinking, some say weaving, of different blocks of text and images in a virtual library made up of such lexias and icons, still residing on one computer, or a well-controlled internal network of computers.

With the advent of the internet, though, the concept of hypertext has been widened from linking materials on a "wide area network" to links made across networks and protocols. The growing enthusiasm for seemingly endless possibilities led some people to speak of the net as a global brain of interconnected and linked human resources. But these links are weak links: already, and even on the local level, it is very common to encounter an error such as "404: File not found." On a global level, this new digitally unified "brain" suffers from an even worse case of amnesia. One cannot escape the comparison with printed media here; it is like reading a book and suddenly missing a few pages or discovering that some of the footnotes have been torn out, or trying to read a newspaper after someone has cut a series of news clippings from it. The fascination with the internet is like the fascination with the beauty of a spider web dancing in the wind. It is based on the knowledge of its fragility - one unlucky instant will destroy all the work. This ephemeral aspect can of course also be seen in a positive way: enjoy the moment itself, do not leave too many traces, leave the others, the generations after you, some space to discover things for themselves. Ideally, a combination of the two elements might develop, whereby some examples of the constantly broken threads of the web will be collected and preserved, while the rest will be washed away by time.

As Simon Pockley has written in "Lest We Forget," "The digital era has been characterized by technological obsolescence and ephemeral standards, ironically threatening the usefulness of digital information. There is little firm ground upon which to build the institutional and private structures necessary for the effective preservation of this material. Nowhere are the challenges more difficult than those concerning the new networked medium of the World Wide Web. The vitality and flexibility of this medium mean that digital material is in a state of constant proliferation and mutation".[16]

This text belongs to a longer text on 'The Art of Forgetting', the complete version can be found in the 1996 Ars Electronica catalog Memesis: The Future of Evolution (Vienna: Springer Wien, 1996), 254ff.

Notes

1 H. Matusow, *The Beast of Business: A Record of Computer Atrocities* (London, Wolfe, 1968). In the late sixties, Matusow, an American expat, lived in London and circulated in its "cultural underground scene"; prior to that he worked in the U.S. as an FBI agent and was a paid witness in the McCarthy trials. See http://www.ibiblio.org/mal/MO/matusow/

2 For example, A. Bayo, "150 Questions for a Guerrilla" [1959/1965]; C. Marighella, "Minimanual of the Urban Guerrilla" [1969/1970]; E. Luttwak, "Coup d'Etat," 1968.

3 One such facility, Cyber Patrol Corporate, itemizes sites that contain "questionable" material: "Partial Nudity; Nudity; Sexual Acts/Text; Gross Depictions; Intolerance; Satanic or Cult; Drugs/Drug Culture; Militant/Extremist; Violence/Profanity; Questionable/ Illegal and Gambling; Sex Education and Alcohol and Tobacco." http://www.cyberpatrol.com/ There are several other censoring and spying software facilities like: CHECKNET Usage checker Free checking of your employees' Internet usage by SurfWatch; CYBERsitter, censoring software Block access to files or programs, by Solid Oak Software; GameWarden Monitor/control, control employee game playing and Net usage, by Wards Creek Software; Net Shepherd, censoring, filtering, rating system for parental control, by Net Shepherd; NetSnitch Informer, records all WWW URLs buts does not block anything, by NetSnitch; SurfWatch, censoring software, screens out the naughty bits/bytes; WebChaperone, parental control system, scans, evaluates - and blocks if content bad; WebReferee, Server utility, stop unauthorized references to your web content, by Maximized Software.

4 See http://www.promo.net/pg/_authors/tzu_sun.html#theartofwar.

5 The NDU offers the following welcome: "By making unprecedented amounts of information immediately available in easy-to-use forms at diminishing costs, the emerging information highway will certainly alter society, to say nothing of military conflict": see http://www.ndu.edu/.

6 M. G. Devost, B. K. Houghton, and N. A. Pollard [of Science Applications International Corporation] "Information Terrorism: Can You Trust Your Toaster?" [1996]

7 M. G. Devost writes, "The United States should utilize hackers, and give them recognition in exchange for the service they provide by finding security holes in computer systems"; see his "National Security In The Information Age," University of Vermont, 1995.

8 See http://www.uhuh.com.

9 For an overviews from a military point of view, see http://www.defence.gov.au.

10 P. Delany and G. P. Landow, "Managing the Digital Word," in *The Digital Word* (Cambridge, MIT, 1993) p. 6.

11 Pamela Samuelson, "Digital Media and the Changing Face of Intellectual Property Law," Ruthers Computer and Technology Law Journal 16 [1990], 334)

12 See http://www.archive.org;; recently his firm Alexa Internet donated a full "snapshot" of the web from early 1997 to the Library of Congress.

13 L. Canfora, *La Véritable histoire de la bibliothèque d'Alexandrie* (Desjonque, 1986).

14 Delany and Landow, 15.

15 See G. P. Landow, *Hyper Text* (Baltimore, Johns Hopkins, 1992).

16 See http://cool.conservation-us.org/.