## Robert Adrian

# Intelligent Machines

### Beyond Information

Most companies over a certain size tend to be schizoid, having two complementary identities: a physical identity composed of buildings, plant, employees etc., and a digitalised virtual identity in the form of networked computer data bases. In the virtual corporate world of networked computers, information, commands and money move at the speed of light, while back on the ground people and machines, even robotic machines, are still struggling with gravity and distance.

At the point of contact between the virtual company and its physical counterpart–between the data bases and the shop floor–increasingly sophisticated input/output interfaces control and manage the flow of information, products and services–and the return flow of data to the network–so that the flow can be measured and manipulated for computer-simulation of future corporate planning and development.

If the virtual company is well-designed and working properly, every detail about the company's physical and financial operations–the location of every truck, every employee, every document–will be available on-line in real time. Projections of future developments through simulations of the effects of changes in organisation, of currency fluctuation, of the introduction of new technologies, of marketing/public relations strategies can be played out with the help of various software programs. Managers at the appropriate decision-making level may still consult the network of databases for an overview of which ever element of company policy is to be reviewed but the automation of data updating and assessment proceedures means that managers increasingly act on machine-made decisions rather than themselves make decisions based on data supplied by the machines. Software is slowly replacing wetware in the corporate office tower.

These classic feedback loops, which in the case of a really large multinational corporation operate on a global scale, can be experienced in a microcosmic version every day at the supermarket where bar-code readers at the cash desk update the inventory and automatically transfer sales and stock data to the company headquarters. People still drive the trucks, stock the shelves and work the cash register but the store manager, like the shipping clerk who supplies her store, is merely a part of the computer-controlled data flow, her sphere of authority being strictly limited by the central computer. But the supermarket microcosm is also linked to the macrocosm of the national, if not global, economy. The latest development in the automation of consumption is the networking of financial institutions with retail outlets. The little card-readers appearing on checkout counters in supermarkets link the bar-code reader, the cash register and your personal bank account to the computer network of the supermarket chain and its connections to the global economy. In most parts of Europe the Giro banking system already makes it possible for the average person, at least theoretically, to live without touching actual cash for weeks at a time: The employer's computer transfers wages direct to the employee's bank account; standing orders in the bank's computer handle basic payments (rent, insurance, telephone, etc.) automatically; bank or credit cards handle direct purchases. Actual cash–like the intervention of human managers in corporate decision-making–is increasingly just a backup in case of emergencies.

Of course there is plenty of room for glitches in the implementation of this kind of management-automation. The sudden collapse of a computer system can–at least temporarily–completely cripple a company, as occured recently in Vienna when the main milk distribution firm automated and centralised its operations. Unfortunately the software had a few bugs and the system crashed repeatedly for the first week, leaving most of the city's shops without milk. However, regardless of the embarrassment and the costs (which ran into tens of millions of schillings), a return to the old reliable manpower methods was never a serious alternative. Digital automation technology is considered to be inevitable and irreversable–machines are simply perceived as being more reliable, more efficient and more profitable than people in spite of the social costs and periodic spectacular failures.

The savings in manpower and the increased speed of data transfer also have to be set off against the problems of security, always a serious matter for companies but much more complex in the environment of networked data flow. In the battle against hackers, computer crime and industrial espionage, a large part of research and development is being devoted to producing machines which can protect themselves against potentially damaging penetration. In order for such protection to be efficient the machine must be able to recognise increasingly sophisticated and resourceful intruders. That is it must be designed to be "aware" of its territorial borders and be able to decide who or what may cross them and have access to its memory and programs.

As in the case of the Vienna milk distributor's response to their software debacle, the corporate victim of a successful hacker attack does not consider a return to human-based data processing and transmission–the prevailing cultural bias in favour of computer automation prevents this–but to improved protective measures. This usually takes the form of isolating sensitive data from the communications networks (firewalls/intranets) and by developing and implementing software which is able to detect unauthorised activity. But the situation becomes more complex if the intrusion is not merely a hacking adventure but is connected to computer crime or industrial espionage because this kind of intrusion usually involves sophisticated professionals or, even worse, insiders–company employees or programmers.

It is at the interface of the virtual company and the physical company that the security loop-holes occur and, due to the cultural and ideological belief in the superiority of machines over people, the virtual company has priority–so the virtual company must be isolated from the human beings it was meant to serve. It must be taught to defend itself againt people–which means that the computer installation, and the entire corporate network (the virtual company), will be restructured in elaborate heirarchies of access that prevent–or minimise–unauthorised and/or criminal intrusion or abuse. The interesting, and largely unnoticed, effect of this bias in favour of the virtual company is that human workers, including managers, are increasingly perceived to be mere interfaces between different elements of the electronic networks. Inappropriate action by human agents may interfere with the proper working of the machines and machines are therefore being designed (or trained) to take over more managerial tasks. That is, they are to be provided with more decision-making ability–more autonomy.

It is easily foreseeable that, should this process of increased machine autonomy proceed at the same incredible pace as during the last 15 years, by the end of the first decade of the next millenium the virtual corporation, existing inside the global network, will have finally replaced the "real" corporation of offices and factories–and the human workers will be doing that which humans do best: Moving about in the world fetching and carrying for the machines. Not that this will make much difference to most of us–we have already become accustomed to the notion of the "service industries" as the main employers of the future.

In the very rough sketch above I have tried to point out some of the hidden elements in the relentless progress of the automation of "private" industry and commerce. However it is more normal to concentrate on the military and surveillance aspects because they are often in the public or governmental realm and therefore automatically the object of concern and critique. But perhaps a military example would be appropriate–and of course it has to do with the "Gulf War".

Virtual Reality is a product of the flight simulation systems designed for the U.S. Air Force. Zipped into a pneumatically dynamic suit, fitted with sensors and seated in a realistic cockpit connected to a powerful computer, pilots can be trained in simulated flight–and combat–situations without risking either themselves or their multi-million dollar aircraft. This flight training is so realistic that "trainer" hours are counted partly as actual flying time.

When the Gulf War came along the pilots were ready. The training systems were re-programmed to simulate the geography of Kuwait and Iraq and the pilots flew their "combat" missions in the simulators. Pilots are on record as saying that they could not really tell the difference between the training and the real thing once they had actually strapped themselves into the cockpit.

But the most telling element is the electronic command structure that actually controls the aircraft. An integrated surveillance system combining AWACS surveillance aircraft and geo-stationary satellites are connected to the on-board computers of the bombers. The mission and target is programmed into the computers and the pilots´ role is really to monitor the various systems and be available for take-off and landing or for emergency maneuvers should the plane be attacked or the systems fail. However most modern attack aircraft can hardly be flown without computers so a total system crash is, in most cases, an actual plane crash–a situation not dissimilar to the problem of milk distribution in Vienna when the virtual company broke down.

What we saw on television were images from monitors of the attack aircraft. Whether they were images seen by the pilots in actual or simulated attack is unimportant. The important thing is to notice that it is *unimportant*. In this sense Baudrillard was at least partly right when he said the Gulf War never happened. The war we experienced on TV didn't happen nor did the war the U.S. pilots saw on their monitors–but it really did happen to the people on the ground in Baghdad and to the Iraqi soldiers in the desert.

The U.S. government was able to demonstrate that, in a really serious war situation, an industrial army of men and machines on the ground is completely helpless against the integrated circuitry of a virtual army in the air. But it also demonstrated something else which is much more interesting: The real commander-in-chief is now the integrated command structure of computers networked in real time. Just as the pilot sits in his cockpit while his aircraft carries out the mission under the instruction of the computers, the generals wait in their command posts reading printouts and scanning monitors. Aside from periodic old-fashioned regional skirmishes, war has been automated. The virtual army has supplanted the real.