SECURITY: A SOCIAL MODEL
By Jorge Luis Marzo

> "their lives, the very essence of their character, their abilities and their boldness, are nothing other than the expression of their faith in the security of their environment." [2]

I find myself wondering why the word security is so much in vogue these days. Has it always been so, and to such a degree? The advertising psychologists -who are always great essentialists, given the way they manage to persuade potential advertisers of the ease with which they can read the human soul, and thus pitch their client's product at people's insecurities- hold that the human being has seven natural desires, one of which is security.[3] But if we look at the other six, we see very clearly that the satisfaction of all seven is what creates the sensation of security: food and drink, comfort, sex, the welfare of our loved ones, social standing and longevity (health). In the light of this, what is being insinuated when security is included as a desire in its own right, as a discrete and autonomous subject, and on the same hierarchical footing as the other six?

In the communications media, which serve to confirm the certainty of the fact that the reality we see is unquestionably the one we live in, there are constant references to security; in line with tradition, political discourse and the discourse of the armed forces of the modern state continue to trade on the idea of security. Economic slogans, too, and of course the ad men, continue to exploit allusions to stability and strength. If we watch the news relating to food, to sex or to social prestige, we see that in the last few years the standard reference is without a doubt security, especially since the increase in food psychosis, the emergence of AIDS, or the precariousness of the job situation. But beyond all doubt it has been the generalized implantation of the new technologies in the West that has established a whole new panoply of definitions with respect to the role of security in our political, social and human relations. With technology, security has been given a new lease of life, in that those same technologies have imposed themselves as mechanisms of management that underpin and regulate the security of the whole of the existing social apparatus.

In practice -which is always what interests the publicists- the desire for security represents the need for a management of those mechanisms that ensure the satisfaction of the rest of our desires. And given that we are talking about a technical management of these mechanisms, security is perceived as a kind of administrative affair, a sort of department or agency which guarantees that all goes well. Thus, the desire for security would seem to correspond to the desire to enter inside the very fabric of the organs of social power, to ensure our acceptance in that fabric. The assumption of the value of security in these terms amounts in practice to consecrating it as a set of techniques with its own programme of formulas.

It seems almost inevitable that a world such as ours, subject to the supreme value of constant change and speed, requires a high degree of prediction as to what is

expected to happen; consoles that offer us the greatest possible number of variables in the face of more or less imminent problems. We have to be agile and ready to take a series of continually varying curves. Individuals, societies, corporations and systems in general need to adapt to such "sustained" change. Speed is not in the
habit of waiting, because basically it can't; it is not part of its nature. The machines that are geared to that speed serve us as tools, as points of contact with it. If speed seems "natural", as an extension of the human will itself, then it seems logical that the tools should also be legitimated "naturally", all the more so in view of their huge social and economic benefits.

Technology serves us for the future: it is our "life insurance". We need to make sure of what is already here in the present in order for that future to come to pass. We are forward-looking. The future, a kind of entity in its own right, already exists there in the distance and will inevitably come to occupy its place in its present, which oddly enough we can already see simulated in the crystal ball of our screens. The machine shows that there is a reality faster than the everyday. It serves as the vehicle that enables us to connect with subsequent realities, with the advantage of knowing them in the present. A mistake on our part would be fatal, catastrophic. That image we visualize on the screen would not take place. Or it would be different, another image, one we did not imagine or that seemed dispensable at the time, and then we would be in danger, since it was not predicted. Predictions save lives. The demiurge of the techniques of probability promises us that it will take place. Because it offers it to us even before it occurs. And that gives us a lot of
security, because it bestows meaning on the present and on our attitudes: we are not adrift in the void. Anticipating what might happen, we draw even closer to it, since we place the mechanisms of simulation and strategy in its service. There is no trick. You have to be ready for what is coming. Jesús Gil, in one of his menacing electoral videos, expressed it with perfect clarity: "Join up with what is on its way."[4] If we transfer this message to our perceptions of technology, we see the extent to which this model of thought has insinuated itself into the fibres of our being. Prediction and strategy are of tremendous value in the technological development of our culture. The slow but steady implantation of technology was justified by the need to face the probabilities, all the probabilities:

"Nowadays we find the rules of that prediction-science on all sides: in investment strategies on the Stock Exchange, in the decisions taken by some one playing a video-game, or in virtual reality, where we can simulate a building that has not yet been built. If science engages in a race to establish what may happen, then there is a great temptation to create a reality on the basis of what is to come. Science, by showing us that certain things are possible, demonstrably there in the glass of the eyepiece or the screen but not yet marketable, makes a radical break with the classical models of reality and of fiction and commits everything to a state of probabilities and simulation, of tests of nearness with regard to what is seen at the other end of the telescope. Those probabilities clearly end up affecting our own present, since in the framework of power we legislate existing reality with out eyes fixed on that day to come: legislation that is invariably

established institutionally and legitimates scientific mechanisms themselves on the basis of their capacity to survey and predict."[5]

In a culture of prediction in such tangible present-day strategy scenarios as the economy, defence, medicine, ecology and entertainment, security is a fully consolidated presence in the machines that provide us with supposed clues to what the future holds in store. In this way, the value of security is not confined simply to suppressing those factors that might spoil the fun for us here and now, but is hallowed as the real guarantor of our future, taking on in the process a mythical signification as that which affirms our very existence. The security of the future, at the present time, is the foundation of the security of our present.

A large part of the systems that maintain the order and functioning of most of the areas of our lives are highly technical and are directly linked to security: the management of our bank accounts and financial transactions, medical equipment, the co-ordination of policing, transport, the communications media, our domestic appliances, energy systems, etc.; they all operate thanks to the fact that their control systems are unified in a basically common technology (digital) which allows a unitary control and a wholly necessary interaction. It is significant that the most important invention of the Industrial Revolution in the 19th century was the universal screw, which made it possible to swap parts and adapt one machine to another. If we observe, as Friedrich Kittler has shown us[6] that new media are born out of the fusion and mutual adaptability of existing media, we come to see more clearly how the security factor (that is to say, the fluidity of the mechanisms of control) has become the key to the maintenance of the whole system.

Hence the fact, as we noted at the beginning, that the advertising psychologists consider security to be a fundamental desire in its own right, endowing it with specific characteristics of its own, over and above the fact that the other desires are defined by the security that comes from their fulfilment. This is not as silly as it might seem; it would reaffirm our reliance on a well-oiled system of pulleys that enables all the rest of the machinery to run smoothly.

The new technologies represent, if we cast an eye over their more evidently characteristic applications, a new, global and open model of human interaction. Many of us in the West can now enjoy almost unrestricted contact with one another, in the framework of a utilitarian utopia that some people are even trying to convert into a new and global civilizing mission. This state of affairs opens up new considerations than in what we understand by international relations, the public space and social connection, which if the truth be told, is not to the liking of many of the technologists, politicians and spokespersons of "the new society". And it is not to their liking because entering such arenas might potentially make a mockery of the idea that the technological process is determinist; in other words, that society changes as a result of technology, instead of technology being modelled on the basis of certain social and institutional developments and decisions.

In line with the expansion of the possibility of world-wide connection, with all that this implies in terms of openness, we have seen the parallel implantation of a

whole new language of security in an open and accessible world. Codes, keys, ciphers, encrypted messages, protocols and passwords exist side by side with a carefree, transparent and globalist discourse. The paradox is flagrantly apparent: tremendous possibilities for interaction and communication are being created, overcoming what were until not so long ago insurmountable barriers, but these are sustained by an equally massive and complex framework of security.

The political and institutional organization that came into being during the second part of the last century grounded many of its premisses in the idea of security and the maintenance of its various systems. The evident gradual decentralization of the mechanisms of control, especially in the last ten years, has not resulted in the disappearance of a unified power structure; rather it should be seen as an operation of self-protection on the part of that structure. Instead of having a single computer which handles everything, with the danger to the system this entails in the case of the computer breaking down, we now have a network of computers which ensure that the system will hold up if a few or even a lot of them go down. It is a kind of insurance against catastrophe for systems that are heavily dependent of a small number of control centres. We can observe this in a whole range of areas, and not only technical or technological ones, the most emblematic case here being the Internet; a system developed in the United States in the 60s in anticipation of the collapse of communications after a nuclear attack. The closest example in our social discourses is to be found in politics, with the privatization of the traditional public industries so that in the event of collapse the dead weight is distributed structurally. The privatization of society is not so much the product of ideological matters of party policy or a conservative or liberal dynamic as of the need for risk prevention inherent in a system such as capitalism, which is at the same time entering a phase of globalization and interdependence that may seriously affect the traditional homogeneity of security systems. If there is a sharing out of roles, the most important thing -as we are incessantly told- is that all of the new players accept the rules of the game with regard to security. We can see, for example, without going further afield, how European countries wishing to join the European Union are expected, before any other consideration, to adjust their economies not to the best possible forecasts, but to the security standards of the Union, so that their integration does not represent the slightest risk to the overall order of the European economy.

It is of tremendous interest to observe these processes with a view to understanding the new order of security in terms of this domino theory, according to which if one domino falls, all the others fall too. Curiously enough, these processes bear a very close resemblance to the traditional image of military intelligence and the information units of secret services or terrorist groups,[7] always so expert in the matter of passwords. In such societies, the constituent cells or elements are run on the basis of the tactic of knowing nothing about the other units, so that if one is infiltrated the framework as a whole can continue to operate with a few minor adjustments. This situation is clearly contradictory, in that it seems to distil images of secrecy and conspiracy but in a context of the expansion of communication. This latest paradox serves to indicate how far the former boundaries between institutional systems and decentralized systems have slowly but surely been dissolved. The set of keys that once served to open every

lock, in the possession of a small circle of individuals, has become an infinity of keys for opening and closing spaces that are like separate compartments in order to prevent infiltration and systemic problems. This is by no means to imply that those who were formerly in proud possession of this set of keys have lost them, but simply that they have delegated certain responsibilities so that accusations of nefarious activities cannot be directed at a single point. We have only to recall the cases of state terrorism in Spain during the last 25 years to see how these strategies of compartmentalization, which protect the system and the people at the top who make the decisions, are fully operational today.

Quarantines

Security, within the framework of self-protection, is largely defined by the image of prophylaxis. In the current dominant discourse on this issue, vaccine, antidote and prevention are the fundamental points of reference. Indeed, there is a certain irony in the fact that a vaccine is an anti-virus camouflage mechanism, or that prevention corresponds perfectly to the solutions generated by the domino theory. The AIDS crisis, for example, or the psychosis created by livestock epidemics have provided the culture medium for the justification of mass techniques of prophylaxis, isolation and quarantine.

The domino theory, as the basis of the security of the system, has assumed the proportions of a paradigm, the full extent of which it is hard to estimate. Today everything is subjected to prophylactic treatments: sexual relations, operations on the Stock Exchange (with the firebreak of prevention, euphemistically referred to as "preventive suspension of quotation") or the creation of the NASDAQ (separate from the traditional securities market on account of its exceptional volatility). Public "intervention" in high-risk companies, the massive extermination of livestock, the policy of dispersing terrorist prisoners in remote jails, the practice of "museifying" nature in natural parks, the legal isolation of immigrants and their segregation in urban ghettos, Western military operations officially described as "preventive" (such as those in Panama, Iraq, Somalia or Libya), the "security cordons" around suspect countries or zones, the very oath sworn by government ministers not to reveal the deliberations at Cabinet meetings so that no "outsider" can take advantage of confidential information, and so on. A long and easily enumerated list of etceteras that unfailingly refer to epidemiological policies quite
unashamedly applied to the social fabric. And it is surely not going too far to suggest that this is due precisely to the "naturalization" of the concept of security. A security that is thus equated with health, in the same way that danger is compared to a virus, to bacteria that have to be isolated to preserve the general good order of the organization. It is disheartening to think that Europe once fought to eradicate every trace of social biologism from its territory and that today this should be the dominant model, even if it is camouflaged as the panacea of global connectivity and global survival.

It is very common to see and hear terms such as area, zone or sector, not only in public administration and the entertainment media but increasingly in the more general domain of cultural production. In parallel with this, compartmentalization

reflects the growing social desire for a clearer picture of reality, through the cataloguing and easy identification of spaces. Generalities are out of favour because they do not correspond to personal experience, the basis of the present-day marketing of identity.

Keys and Access Protocols

In an ever more connected society, ever more dependent on its very connectivity as a paradigm of security, we often come across paradoxes that depict the sensational transformation in the functioning of our political and social relationships. One of these stems from the generalized introduction of the protocol as the mechanism regulating our accessibility and as the fundamental guarantor of our own security and that of the system.

With the advent of the Internet, certain formulas of identification and access originating in the military environment have gradually consolidated their presence in the civil field. Certainly the development of the Internet has evolved from the highly centralist concept of C+C (Command and Control) toward a network made up of a whole series of different networks which are independent of one another but linked by "compatible" languages. The notion of compatibility has thus been one of the principal arguments in the growth of the network and, in practice, an obsession of thinkers, engineers, industrialists, politicians and users of the Internet. In fact, the sustained expansion of the Internet since the early 90s is almost entirely due to the afore-mentioned search for protocols, for keys capable of linking with great security and with no loss of data a multitude of computer systems and languages, some of them very different from one another. Indeed, the very name Internet reflects the fact that it is conceived as a system "between networks". It was, then, a question of finding a standard that would serve as a common language.

The race to establish these standards began from the moment when the NSF (National Science Foundation), the American government agency responsible for the approval of scientific applications, unified various computation centres in 1985, but above all when it allowed the commercial use of the Internet in 1991.[8] Even before then research into programming languages had already largely prepared the ground,[9] but such research was geared above all to creating the best possible programme writing systems, rather than to facilitating common languages for use by different systems.The establishment of protocols, of universal languages making it possible to connect disparate sources, is a premiss that philosophers, scientists and humanists have eagerly pursued almost since the Baroque. Leibniz was the first to seek a symbolic system of communication that could adapt to any existing linguistic model. He called it Characteristica Universalis: "By means of this universal language, any information of whatever type may be systematically recorded in abstract symbols with which any problem of reasoning can be articulated and resolved."[10] In 1867, Melville Bell, the father of Alexander Graham Bell, one of the principal inventors of the telephone, developed Visible Speech, a universal alphabet capable of codifying various systems in a unitary form.[11] And in 1943, Noam Chomsky, then involved in

military research at the United States Navy's Psycho-Acoustic Laboratory at Harvard, proposed a Universal Grammar with the same purpose.[12]

Undoubtedly the search for those standards that would make different languages compatible raised the possibility of creating a fluid system of communication and interaction, but at the same time it opened up a Pandora's box, in that the use of a universal language could pose serious security problems, since anyone with the relevant symbolic code could without more ado enter inside a vast and often highly classified information network. Here we have the root of the paradox we noted above, a paradox that has come to be of central importance.

Protocols allow us to move around the network quickly and easily and with the assurance that the translations really work. "Protocol" comes from the Greek word *protokollon*, the name for the flyleaf glued to the frontispiece of a manuscript which contained the titles or brief summaries of the contents of the text. It therefore made it easier to find a particular topic and aided the comprehension of hard-to-read handwriting. Protocols are also traditionally the set of regulations and agreements that countries or institutions establish with one another for the purpose of "correcting" the differences of customs and diplomatic and cultural practices. It is a way of facilitating official relations and ensuring that there are no misunderstandings. In much the same way, a protocol in the present communications context is defined as a "set of procedures that serve to standardize a repetitive process" between computer systems.13 Of note among the protocols most familiar to the general public are those directly linked to the Internet and to the combined satellite telephone systems, such as the http or the wap.[14] All of these keys allow us to link up to a common network and convert the different systems into codes that all machines can read and interpret.

Now it seems clear that when the different systems were separate from one another, with no common protocols, the degree of security was much greater, since the frontiers between them were much harder to cross, although the price to be paid for this would be the lack of connectivity and a certain autarchy. At present, the situation is entirely the opposite: unification offers unlimited possibilities for the exchange and distribution of information, but the risks for the security of a system which uses protocols are perceived to be great. In other words, the establishment of common keys automatically leads to the generation of complex processes of encryption and encoding to ensure that the global dimension of networks does not bring about their destruction.

So what, then, is the role of the great mass of users in this whole process? Security, as an essential value of functional efficacy and survival in an integrated world, seems to confirm a hierarchic social dynamic that grants users the benefit of use but at the same time denies them access to the manipulation of the codes. It is curious to observe the sort of language that institutions and the communications media (an integral part of the structure of the network) direct at those groups which adopt attitudes and actions critical of the monopoly of the supposedly necessary management of security. In most news reports on cyberactivism, hackers and participants in open systems, the accusation is always the same: they are hotbeds of illegal activities and the principal sources of

computer viruses. The importance that the network's monopolistic corporations attach to these so-called "pernicious" activities is revealed by the fact that a considerable number of electronic pirates, some of whom have been convicted by the courts, have ended up being recruited by those same corporations to co-ordinate their security services, or have gone on to set up their own communications companies. This ought to give us some idea of the extent to which the terrorist or para-terrorist discourse has found a place in the very heart of contemporary capitalism, and all thanks to the central value that security has acquired in our social relations.

Camouflage

It is curious to say the least to observe how this analysis of the new articulation of the system through a conjunction of opposites (centripetal and fragmented movements) corresponds in many ways to another, very similar technique, of absolute relevance and also with a long tradition: camouflage. A long tradition, indeed, since it originates in the plant and animal kingdoms: a circumstance that provides a perfect basis of legitimation when it comes to applying these techniques culturally. The blurring of reality and simulation have always been good security strategies, good techniques for any individual which wants to survive.

The term camouflage, in the original French, means "to blind or veil". At the end of the 19th century, the American artist Abbott Thayer carried out a vast study of animals that has come to constitute an important tool in the development of modern camouflage. Thayer noted that the colour of many animals ranges from dark on their backs to almost white on their undersides. This gradation breaks up the surface of an object and makes it appear flat, without three-dimensional qualities. It seems no accident that art should have devoted so much attention to camouflage during the 20th century, given the symbiosis of certain Baroque traditions of illusion and the new technique of "montage" in photography and the cinema. In 1915 the French army created the first so-called "camouflage division", and many artists, designers and architects were enlisted to serve in such units, on both sides: Jacques Villon, Franz Marc, Arshile Gorky, Thomas Hart Benton, Grant Wood, László Moholy-Nagy and Oskar Schlemmer, among others.[15] We should bear in mind that many of these activities were intended to deceive not the soldiers in the front line but the aerial photographers in planes and observation balloons. To be precise, such "military-illusionist" experiments did serve to camouflage reality, but a mediatic reality. Their purpose was to mislead the "predictions" made by the enemy, their perception of reality, by means of scenographies of reality which would look real to the camera lens.

Reality is configured to the extent that we can contextualize it on our screens and give it a global meaning. In fact it has been the idea of montage that has governed that process of contextualization, in the same way that it has generated its opposite: falsification, the ultimate purpose of which has always been the protection and the security of "some one". The techniques of montage provided the necessary tools that allowed the photographic record of reality to be subjected to the manipulations of institutional "internal security" (we have only to

recall the great falsifications of history in the USSR). However, they also gave rise during the 20s and 30s to practices such as photomontage, which undermined the monolithic discourses of power, breaking down their strategies of camouflage. If we look at the digital production of illusion in the audio-visual interface in our own time, we find direct references to those processes of formal montage, in spite of the fact that the objectives are very different, in that today's digital illusions are in many cases designed to serve the interests of industry and symbolic homogenization. It is precisely this situation that has prompted many creative artists to position themselves in the slippery terrain of deception as a form of critical deconstruction of values -such as that of the reality and credibility of the visual record- and a response to the degree of false security implicit in these. We find contemporary instances of this kind of practice in the work of Joan Fontcuberta (I will never forget that when I read the book published by his Sputnik imprint I swallowed it eagerly, quite convinced it was true, and not seeing the trap until almost the end, to the delight of the artist).

In a culture of the audio-visual cut and paste, camouflage is the principal weapon of both defence and assault, as can be seen in the techniques of terrorism and psychological warfare,16 for example, which encourage the enemy to believe that the messages they are receiving are from their own side when in fact they are from ours.

Illusions

Nevertheless, the techniques of camouflage have assumed a great importance in the social fabric and in communications precisely on account of the capacity of the new digital information media to monitor, record and identify people. Given the massive presence of surveillance cameras in our daily lives, and the use of sophisticated monitoring technologies (credit cards, mobile phones, digital television, systems of fiscal and banking control, the Internet, etc.), our current perceptions hinge on the sensation that our identity is fully known at all times and in all places, and that it is extremely difficult to evade such control. Certainly we feel it is important that the on-line bookshop from which we buy books by credit card knows exactly who we are so that nobody can camouflage themselves as us and clear out our Visa account. On the other hand, it is no less true that these systems of identification also have a huge potential for those who want to put us on their commercial or police data bases.

At present, many of the arguments about the social advantages and disadvantages of the digital era are centred on the paradoxical contrast between a public life underpinned by the globalization of communications and marketing techniques aimed primarily at a mobile private individual, with inalienable rights in terms of personal privacy. On the Internet, for example, the security of the services we use is based on the key (the password) that protects our private domains and prevents any illegal use of these. The debate in the mass media about security on the Net is invariably defined by some scam by computer pirates whose ability to camouflage their identities or sources allows them to infiltrate any system they may have their eye on.

Security, then, is based on the fact that each of us has our own access code, which in addition legitimates us as fully enfranchised electronic citizens. But it does not end there, because at the same time we feel that the management of these passwords by the companies operating in the sector may seriously violate our right to privacy and personal security. So a lot of people exploit the contradictions within the system itself (between the secret and the lie) to create false identities when they want to access certain information, camouflaging themselves commercially or simply pretending to be some one they are not in chats and forums, in the same way that cyberthieves and cybercops carry out their operations. And this is a problem not only for the users, but for governments, too, as in the case of the dialectical opposition between the US and French governments, the former being openly committed to an exhaustive monitoring of the identity of Internet users, while the latter is in favour of a high degree of anonymity in electronic communications.

It seems clear that in a situation such as this, the idea of camouflage will present itself as an effective way of evading the empire of identity, in which the supreme value is security. And it is equally symptomatic that both that strategy and the very model adopted by the system derive from terrorist techniques and theories, which suggest that one of the best ways of planting a bomb in a police station is to disguise yourself as a policeman and simply walk into the building in a casual and inconspicuous manner. This warns us that the system -or rather, the series of integrated systems- will tend to assume military premisses when it comes to ensuring its own survival. Users and systems thus share the same techniques of defence in relation to the opposition. No doubt the result of all this is predictable: the system will continue to be governed by models of compartmentalization, of secrecy, of encoding and monitoring, while critical users will increasingly adopt techniques of camouflage and the blurring of their tracks.

In speaking of camouflage, we also need to consider the origin of the current media discourse on security, which is none other than the United States. It is astounding to witness the contradiction between America's massive consumption of the audio-visual imaginary and the country's total lack of critique of political and social conditions. The data could hardly be more overwhelming with regard to the concept of security that governs American society and American policy today. The United States has the world's highest proportion of prisoners in relation to size of population (1,700,000); it has the world's largest number of people under sentence of death (3,500); alongside Saudi Arabia, Syria and Iran it is the country that executes most prisoners. It is the only country in the Western world that systematically uses torture in its prisons. It is the only country in the Western world that rejects the creation of an international court for war crimes; it is the only country in the West that categorically opposes the application of the Kyoto Protocol on reducing emissions of pollutant gases (while itself producing one third of the world's total emissions). It is the only country in the world with the capability to shut down the rest of the world's satellite communications. It is the state whose police most often intercept private communications. It is the country that most often exercises its right of veto in the UN Security Council. It is the country that has carried out most direct military interventions in other

countries during the 20th century. It is the country with the highest level of illiteracy in the whole of the Western world. And so on, and so on.[17]

It is astonishing to see how policies of an evidently neofascist character are capable of camouflaging the truth, thanks above all to technology, the communications media and the economic impact of their globalization. Given the global economic impetus generated by the new technologies originally developed in the United States, the US has been able to create an immense political and moral protective shield as a way of consolidating its international leadership, constantly backed up by its military power. The concept of security in the United States is simply one of the army and the police, especially since the economic boom of the new technologies has led to the criminalizing of poverty to an extent perhaps inconceivable at any other time or in any other part of the world.

That pernicious influence of America's interpretation of "national security" has given international legitimation to the perception of the secret and the lie as forms of power, fully operative and widely accepted, politically, economically and socially. The United States is a fundamentalist and reactionary country in security terms, with an idea of security that swallows up everything else: the policy of policing the market. The language, attitudes and behaviour of the great majority of its media and industrial corporations are quasi-military, including threats, kidnapping (with the usual monopolistic practices), blackmail (forcing the governments of many countries to kow-tow to them in return for the siting of a factory on their territory) and even direct participation in military operations (AT&T, ITT, Westinghouse, General Electric, IBM, Coca-Cola, CNN, Monsanto, not to mention the science universities, many of them with juicy weapons contracts and military funding). And this kind of behaviour is no longer exclusive to the United States, but is increasingly in evidence in many other countries. A blind eye is turned to all of this on account of the immense economic benefits that companies and states are deriving from the new technologies and the huge media influence of the American communications industry, whose principal enterprise is the creation of global cultural symbols that reinforce and put a high polish on the ubiquitous camouflage screen that is being set up all over the world.

"Join up with what is on its way" is in fact the most consistent code of conduct in this state of affairs, because there is nothing more "secure" than joining in the train of those who hold the keys to the whole apparatus of security.

Interfaces, Reversibility, Responsibility

The use of technology has resulted in a curious situation of social and political transcendence: the machine sanctions social inefficiency. And indirectly, cultural and economic inefficiency, if we look at the poor countries of the world. It could even be said that our reliance on the technicians, when we don't understand how the machine works or when it breaks down, is like a punishment or a penalty in the form of high repair charges. Young people who do not possess computer skills are beginning to have real trouble finding a job; many girls have significantly less access to video games than boys, especially when the parents can only afford to buy one;[18] older people who are not familiar with using the new

technologies suffer a real "skills gap" between their own experience and the presence of and information associated with such machines in their daily lives.

This is not new. With the appearance of the capitalist machine, the technical specialization of workers led to social upheavals in the class structure; in the course of time these diminished, but never completely. According to many studies, workers were not especially mistrustful of the machines themselves but feared the potential danger they represented as instruments of class control,[19] because an understanding of the internal mechanism of the machine, over and above its mere operation, was the key to promotion within the hierarchy of work.

Nevertheless, the proliferation of interactive interfaces since the 80s has brought with it a significant change in the perception of the necessary security environment that these machines are supposed to create. Undoubtedly this is due to an application of interactivity that is increasingly simple in terms of its use but ever wider in its functions. The machine responds, in effect creating a familiar, personal, reliable relationship. Nor should we forget that computers demand a physically individualized interaction. We are almost always alone in front of the screen.[20] The bonds of trust and security which these interfaces have forged between user and machine are very strong, and without doubt condition a more global perception of the technological phenomenon.

The security of today's electronic user is based on reversibility: on the certainty that any error can be corrected. In the first commercial computer interfaces, developed by Xerox and Apple in the late 70s, the fundamental premise of the psychologists was that reversibility (Yes-No-Cancel) should not directly encourage the user's inefficiency or mistakes but broaden their spectrum of security in a pedagogical way, at the same time helping train them how to progress with the machine:

"You can encourage people to explore your application through the resource of forgiveness. Forgiveness means that actions on the computer are generally reversible. People need to feel that they can try things without damaging the system; you have to create safety nets so that people feel comfortable learning and using your product. Always warn people before beginning a task that could cause an irreparable loss of data. Alert boxes are a good way of cautioning users. However, when the options are presented clearly and the response is appropriate and prompt, learning how to use a program should be relatively error-free. Thismeans that frequent alert boxes are a good indication that there is something wrong with the design of the program."[21]

The user does not experience that constant Yes-No-Cancel as something annoying but accepts it as something fundamental, linked to the high degree of esteem with which he or she regards security. The appearance of interfaces of this kind socialized users in the new sphere of digital relationships, safeguarding susceptibilities and generating a confidence in the possibility of retracing the steps taken up to that point. This new attitude to the management of security, in the sense of placing the onus on individual responsibility in the general protection of the system, contrasts with the disappearance of public responsibility

for such protection. The gradual extinction (privatization) of government policies in our public spaces, in energy, in employment, in the management of aid and solidarity, etc., has pinned its colours to the banner of "active personal responsibility" in this deregulated new world trapped in the non-laws of the market.

One obvious example of this situation is our perception and use of the car. Speed is the fundamental value of our system of moral and cultural values. So important is it, that it is able to legitimate itself as the "ultimate" value of existence. However, it would seem logical that speed and security should go hand in hand in the interests of a properly functioning society. But this has not been so in the case of the car. We have agreed among ourselves that the value of speed ranks higher up the hierarchy than security.

Of all the machines with non-military purposes invented during the 20th century, the car is by a long way the one that has claimed most lives. In Spain, 120 people are killed in road accidents every week.[22] What other machine would be allowed to cause death to this extent? What would we think if mobile phones took the lives of ten people every week, or every month, or year, or if the use of lifts caused a similar volume of fatalities? As a result of fifty detected cases of mad cows and pigs with foot-and-mouth disease, the whole of Europe's livestock is suffering its own particular Auschwitz. However, in the case of the car, our societies have entered into a kind of contract with the mechanical world, a contract of security, even a form of constitution or Magna Carta. There have been traffic accidents since the very beginning of the history of the motor car, and no policy of restriction has ever been put into practice. The accident represents the public warning of the effects of user inefficiency in the handling of the machine (and of speed), and also the maximum penalty - death or permanent injury, a circumstance so definitive as to
have the status of law.

It is universally established that the responsibility for a traffic accident is always strictly individual. It is here that we have fixed the variable of security. The deaths of the passengers killed in buses or trains or aeroplanes has nothing to do with their possible social inefficiency in the use of machines. This is why such accidents receive greater public attention and news coverage. They arouse stronger feelings, because they are unjust. It is an undeserved tragedy for those people, even although a professional -the driver or pilot-may be to blame. Car accidents are morally justified precisely because the responsibility is individual. Personal freedom itself is the argument that underpins this moral model, and this is publicly manifested in the images used in car advertising. Individual liberty and speed remain thus wedded in the unconscious. And along the way we readily assimilate the huge toll of "collateral" deaths on roads the whole world over.[23]

The value of transport (as a manifest form of individual freedom), and by natural extension the value of speed, and the tremendous cost in human lives this entails, are so thoroughly woven into our lives that modern societies have been had to change the way death is presented and projected. The individual conquers

space, conquers time. His fate is his own responsibility, at the wheel. There is a lot at stake. And he needs somewhere to feel secure.

Refuges

If the development of capitalism from the mid 19th century can be defined by anything social, it is by having brought about an authentic revolution in the way people conceive of security in their private lives: it is what we call individuality. The home, as social representation of that new pursuit of privacy and security in the tough capitalist jungle, was defined in the England of 1880 as "the shining centre", the "refuge", the "ivory tower", the "fortified castle", the "sanctuary", the "oasis"; home, sweet home, in short.[24] As Manuel Delgado has written:

"In that new moral context, the public space became an inhospitable territory in which the human being was prey to every kind of moral and physical danger, and one in which the most absolute coldness held sway. On the other hand, private life, the source of meaning, had to be defended from any interference from outside, since such intrusion by the world would disactivate its qualities as a temple of both the spirit and nature. Closed off from the corruption of the society outside it, "true" humanity could survive in the domestic sphere: what had been the warm links of affect, the old pre-modern community, feelings, the truth, the sacred. We are faced here with the invention of the home, sweet home, that familiar model that the middle class made its own and that was to end up imposing itself slowly but surely on the rest of society."[25]

Today, the currency of the reading of privacy as the modern guarantor of security is still intact, underwritten by the propaganda issued by those intellectual, political and business circles engaged in marketing the new technologies. In spite of the numerous sociological reports of the last years which testify to the gradual disappearance of the traditional family structure,[26] such slogans are manifestly intended for domestic consumption in the bosom of a united family:

"The home is the nuclear institution of modern society. It embraces the smallest viable unit of social organization: the family. It is the place with which individuals can identify most closely and the one on which they can most depend as the symbolic expression of personal identity. It offers shelter and comfort, both physical and psychological."[27]

"The home has been transformed into a place rich in information and technical capacity. It is, at least potentially, a virtual centre of production. It contains an attractive range of appliances and instruments to occupy the time and the attention of nearly all the family. It offers privacy and security in an urban environment that reveals itself as increasingly dirty and dangerous."[28]

"With electronics, the home becomes at once a space of representation of public activity and a focus of social action."[29]

Capitalism, in the words of Georges Duby, "separates off a clearly defined space for that part of existence for which every language has some word equivalent to

"private", a zone of immunity into which we can retreat or take refuge. A place in which we can lay aside the weapons or the armour required in the public space, relax, feel at ease and rest without sheltering under the ostentatious shell we wear to protect ourselves in the outside world."[30] Philip Ariès pointed out a number of years ago that what triumphed with capitalism was not so much individualism as the family and the home, in that these were constituted as the real bastions of the modern idea of the private individual. The modern home was valued for the refuge it offered from the demands of public explanation. In a society governed by the requirement that every action performed in public be justified, the home guaranteed the security of an inviolable privacy, which also had the protection of law, when the state legally defined the private as a place in which government intrusion could legitimately be rejected.[31]

As early as 1890, lawyers -among them such influential figures as the Americans Warren and Brandeis- were drawing attention to the need to define the right to privacy as something conceptually different from other kinds of liberties. They argued that the "right to be alone" was "evident", and considered "sacred the precincts of private and domestic life."[32] This idea of a pleasant solitude in the domestic haven also reflected a new sensibility with regard to the subjective, the essential basis of capitalist identity. It was this hypersensitive subjectivity which "is instituted as a measure of value in order to exclude everything that might be offensive to the consciousness or a threat to physical security."[33]

If we apply the new theories of compartmentalization to the individual, there is no doubt that the notions of house, of home and of privacy are of fundamental importance. Privacy and the home have traditionally been understood in a defensive sense, in terms of the exclusion of others, of seclusion, of withdrawal.[34] Within the space of the bourgeois home, all the elements are constituted as a protectionist universe which confers the inestimable benefit of security. Walter Benjamin defined the birth of the bourgeois house as follows:

"Since the days of Louis-Philippe the bourgeoisie has endeavoured to compensate itself for the inconsequential nature of private life in the big city. It seeks such compensation within its four walls. For the makart style, the style of the end of the Second Empire, a dwelling becomes a kind of casing. This style views it as a kind of case for a person and embeds him in it together with all his appurtenances, tending his traces as nature tends dead fauna embedded in granite."[35]

The unstoppable advance of capitalism during the 19th century saw a great retreat into the middle-class home, occasioned by the fear of what was seen as the savagery of the new urban environment. Richard Sennett has extensively analysed this phenomenon, in which social encounters outside the home were replaced by the armchair in the living room at the centre of the house.[36]

The appearance of domestic appliances in the 1930s, initially in the United States, in turn gave rise to a further legitimation of the value of the home as secure refuge. More and more, the intersection between security and the moral danger of

an excessively changing society led large sections of society to centre privacy on domestic leisure:

"Together with the new sanitary facilities inside the home, the development of the washing machine reduced still further the need to go out of the house. The refrigerator reduced the frequency of trips to the shops, leading to the disappearance of the peddlers who had supplied households for so long. Leisure activities were increasingly centred on the home with the development of mass-produced gramophones, radios and televisions. In a rapid and changing world, the possibility of transferring leisure to the relative cultural and moral security of the home was welcomed by many Americans, especially the middle class."[37]

These are all old examples, but they show how capitalism created individual operatives who needed a base to return to, a place to unwind and stretch out, in a complex elastic movement. This to and fro between the jungle of the world and the home base has ended up creating a new scenario, with new functions and roles. The mobile technologies underline this situation. The security characteristic of the home is shifted to the exterior thanks to the connectivity of, for example, the mobile phone. And more and more the strategies of work and socialization characteristic of the outside world are being shifted to the home, as in the case of TV and the Internet.

The home and its extensions, the refuge of capitalist paradigms such as privacy, individuality, personality and identity, is being elevated more than ever to the condition of a paradise of comfort and security by the promise of social interactivity that the media (and now, too, their portability) project. People have a real lack of social contact, and the media promise to supply it instantaneously. If the bourgeoisie's fear of the street in the early days of capitalism led to the creation of domestic shells, today the panacea of technology promises a world of relationships that is subjected to an absolute prophylaxis: inside the home, we are safe from a whole series of dangers. With mobility, connectivity and protocols, we are provided with a magnificent hand-held umbilical cord, running straight to the womb of the home, rapidly identifiable, with our full address or mobile phone number. A Finnish cell phone manufacturer recently advertised its product as if it were a kind of Ariadne's thread that always leads to where we can be found. All we need is a code, a password, a protocol; in short, the key that gives us the security that we are not going to be left in isolation.

"Technology transforms everything it touches into a machine."[38] Nothing could be truer. When an issue such as security is based on technology, the former comes to depend entirely on the latter. It becomes a machine itself. And I cannot conceive of anything more predisposed to be converted into a machine than that which has to do with our welfare.

Notes

2. Joseph Conrad, *Una avanzada del progreso*, Alianza, Madrid, 1993, p. 11.
3. Melvin S. Hattwick, *How to Use Psychology for Better Advertising*, Prentice Hall Inc., 1964.

4. Jesús Gil y Gil, *La esperanza recobrada para muchos* [Hope recovered by many], electoral video for the Grupo Liberal Independiente, Marbella City Council, 1993.
5. See Jorge L. Marzo, "Cultura de registro", lecture delivered at the seminar *Culturas del archivo*, Fundació Antoni Tàpies, Barcelona, 2000.

-"Velocidad, ciencia y ficción", lecture delivered at the symposium *SciFi*: entre lo científico y lo fantástico, Festival Periferias, Huesca, 2000.

-"Consideraciones sobre la tele-depredación", 2000, at www.videoscopia.com

These texts can be accessed at www.soymenos.com
6. Cf. Friedrich A. Kittler, *Gramophone, Film, Typewriter*, Stanford University Press, 1999 (1st ed., Berlin, 1986).
7. Cf. Jorge L. Marzo, Herejías. *Una crítica de los mecanismos*, CAAM, Las Palmas de Gran Canaria, 1995. Available at www.soymenos.com
8. After years of network systems accessible only to the military and to universities with military contracts, the modern Internet gained the support of the NSF in 1985 when it set up the NSFNET, linking five supercomputing centres: the universities of Princeton, Pittsburgh, California at San Diego, Illinois at Urban-Champaign and Cornell in New York. This was soon followed by the development of regional networks. The US government decided to re-assign certain parts of the old ARPANET (Advanced Research Project Agency Network, the military research network) to the NSFNET. In 1991 the Internet was opened up to commercial uses and in 1995 the US government converted it into an independent industry.
At http://www.tcm.org/
9. Some of the best known are: FORTRAN, Formula Transition (1957); COBOL, Common Business Oriented Language (1959); ASCII, American Standard Code for Information Interchange (1963); BASIC (1964); SIMULATES (1965).
10. Leibniz, in Michael E. Hobart and Zachary S. Schiffman, *Information Ages. Literacy, Numeracy, and the Computer Revolution*, The Johns Hopkins University Press, Baltimore, 1998, p. 160.
11. Marshall McLuhan, *Understanding Media. The Extensions of Man*, The MIT Press, 1999, p. 268 (1st ed., Toronto, 1964).
12. Paul N. Edwards, *The Closed World. Computers and the Politics of Discourse in Cold War America*, The MIT press, 1996, p. 217.
13. José B. Terceiro, *Sociedad Digital. Del Homo Sapiens al Homo Digitalis*, Alianza, Madrid, 1996, p. 24.
14. HTTP, Hypertext Transmission Protocol; FTP, File Transfer Protocol; WAP, Wireless Application Protocol; PPP, Point to Point Protocol; TCP, Transmission Control Protocol; IP, Internet Protocol; UDP, User Datagram Protocol; RIP, Routing Information Protocol; HTML, Hypertext MarkUp Language.
15. Roy R. Behrens, http://www-mitpress.mit.edu/e-journals/Leonardo
16. On techniques of camouflage (or "black" propaganda) in psychological warfare, see: Jorge L. Marzo, *Ríndete. Octavillas y guerra psicológica en el siglo XX*, Centre de Cultura Contemporània de Barcelona, 1998
17. Amnesty International Report, 2000.
18. Karen Orr Vered, "Blue Group Boys Play Incredible Machine, Girls Play Hopscotch: Social Discourse and Gendered Play at the Computer", in Julian Sefton-Green (ed.), *Digital Diversions: Youth Culture in the Age of Multimedia*, University College London, London, 1998, pp. 43-61

See, too: Eric Hirsch, "Domestic Appropriations: Multiple Contexts and Relational Limits in the Home-making of Greater Londoners", in Nigel Rapport and Andrew Dawson (eds), *Migrants of Identity: Perceptions of Home in a World of Movement*, Oxford, 1998

19. See: Ursula Franklin, *The Real World of Technology*, CBC Massey Lectures Series, CBC Entreprises, Toronto, 1990, p. 62.

20. See: Veerle Van Rompaey & Keith Roe, "The Impact of Computer Technology on Family Life", in *The Impacts of Information and Communication Technologies on Social Realities*, Tripodos (extra 2000), Facultat de Ciències de la Comunicació Blanquerna, Barcelona, 2000, pp. 273-286

21. Apple Interface Manual, 1981. Created by Steven Jobs, Steve Wozniac, Jean Louis Gassé and John Sculley.

22. www.ine.es

23. In relation to technological progress and accidents that take their toll of human lives, cf. Paul Virilio, "Velocité et information", *Le Monde Diplomatique*, August 1995.

24. For a basic analysis of the birth and development of the notion of the home as the ultimate space of individual security, see:

-Patrice Flichy, *Una historia de la comunicación moderna. Espacio público y vida privada*, Gustavo Gili, Barcelona, 1993, p. 95 ff. (Paris, 1991).

-Walter Benjamin, "El Paris del Segundo Imperio en Baudelaire", *Poesía y Capitalismo*, Taurus, Madrid, 1972, 62 (1st ed., Paris, 1938).

-Stuart Shapiro, *Places and Spaces: The Historical Interaction of Technology, Home and Privacy*, Brunel University Press, Uxbridge, 1997.

-Krishan Kumar, "Home: The Promise and Predicament of Private Life at the End of the Twentieth Century", in Jeff Weintraub and Krishan Kumar (eds), *Public and Private in Thought and Practice*, The University of Chicago Press, 1997.

-Amitai Etzioni, *The Limits of Privacy*, Basic Books, New York, 1999.

-Richard Sennet, *El declive del hombre público*, Península, Barcelona, 1978 (New York, 1977).

25. Manuel Delgado, "Miradas impúdicas", Fundació "la Caixa", Barcelona, 2000.

26. Kumar, pp. 223-224.

27. The quote is from Peter Saunders, one of the principal advocates of the home-centred technological society. In Kumar, p. 206.

28. In Kumar, p. 206.

29. Javier Echeverría, *Cosmopolitas domésticos*, Anagrama, Barcelona, 1995, p. 62.

30. Georges Duby, "Preface"; Paul Veyne (ed.), *A History of Private Life*, Harvard University Press, 1987.

31. See David Lyon, *El ojo electrónico. El auge de la sociedad de la vigilancia*, Alianza, Madrid, 1995.

-"La máquina de la visión: ojos electrónicos en la ciudad", at www.videoscopia.com

32. Samuel Warren and Louis D. Brandeis, "The Right to Privacy", Harvard Law Review 4, 1890, pp. 289-320.

33. Enrique Ocaña, "Fotografía, guerra y dolor", in *Ernst Jünger: Guerra, técnica y fotografía*, Nicolás Sánchéz Durá (ed.), Universitat de València, 2000, p. 72 (1st ed., Berlín, 1930).

34. Altman, I., "The Environment and Social Behaviour", 1975, quoted in Paul

M. Insel and Henry Clay Lindgren, *Too Close for Comfort. The Psychology of Crowding*, Prentice Hall, New Jersey, 1978, p. 26.
35. Walter Benjamin, "El Paris del Segundo Imperio en Baudelaire*", Poesía y Capitalismo*, Taurus, Madrid, 1972, 62 (ed. orig, Paris, 1938).
36. Richard Sennett, *El declive del hombre público*, Península, Barcelona, 1978 (Nueva York, 1977)

-*Carne y piedra. El cuerpo y la ciudad en la civilización occidental*, Alianza, Madrid, 1997 (1st ed. New York, 1994).
37. Shapiro, p. 67.
38. Lewis Mumford, in Jacques Ellul, *The Technological Society*, Vintage, New York, 1964, 4 (1st ed., Paris, 1954).