Ute Bernhardt

The Empire Strikes Back

Information Warfare is concerned with the disturbance and the destruction of information technology (IT) systems in conflict situations. The aim is to create damage in civil and military systems in order to achieve one's own military or political purposes. The prospect of risk is nothing new. Years ago it had been discussed how the use of IT systems as the basis of ever greater parts of our economic and social system constituted a new quality of social vulnerability.

> This new quality leads the concept of conventional warring ad absurdum: Disturbing effects on information and control technical systems cannot be excluded in the eventuality of a war, and are, on the contrary, probable. They cripple an industrial society and can lead to its breakdown within a short period of time (…) they mean the destruction of our industrial society, whether there is a victory, or defeat.[1]

When the military speak of Cyberwar or communication guerillas toy with their disruptive power sometimes little more than a fashionable attitude lies behind it. Sometimes, however, it conceals the beginning of new conflicts. In the study which has meanwhile already become a classic, the authors John Arquilla and David Ronfeldt include human rights' and environmental groups amongst the possible conflict parties in a netwar.[2] In the meantime the picture of cyber-terrorists who lead to the breakdown of national economies has developed from this. In this process hackers mutate to terrorists who are just as dangerous as the terrorists in the independence movements in the 60s to Moscow's satellites and a world revolution which never took place.

The deadly seriousness of the matter can all too easily be forgotten. Anybody who thinks that information warfare is bloodless is naive. To shut out the results of such a conflict is even worse. The vulnerability of the IT based society is an old theme for critical computer specialists. The military now want to deliberately and systematically exploit this vulnerability through information warfare and to make it a means of conflict settlement. IT system programmers can only shake their heads and ask whether they really know what they are doing. After all, we are happy when our systems function reasonably stably–they are unstable enough without any outside intervention.

I do not wish to examine the military significance of information warfare here, but to discuss its effects on information technology and its use.[3]

The vulnerability of the information society receives scant consideration in the civil context. The year 2000 will demonstrate this in many computer systems. If translated into the military context, furious activity takes place. What has apparently not been understood is the significance of seeing IT systems themselves as a means to superiority, to destruction. What does it mean for the information society and its infrastructure to become a theatre of war? What are the results of such militarisation–can a civilian information society continue to exist? And: How can the risks of IT systems be exploited and simultaneously eliminated for one's own side?

Civil Defence Exercise 2000

Would it really be so bad if the information society experienced a blackout due to computer failure? Alright, we couldn't access the internet, but we should be able to cope with that. Yet without a computer we could neither use the telephone, nor get very far by train, car or plane.

Neither banks nor cashpoints would be able to pay out cash. We wouldn't be able to use it anyway, because the computer cash tills wouldn't be working. The medical profession would have to do without most of their equipment. Absolutely nothing would work because the computer crash would also cause an electrical power blackout. We will just have to wait and see how well atomic power stations are prepared for such situations.

All of this could result from information warfare. We are going to experience at first hand the implications of information warfare for the infrastructure of a computer-dependent society at the turn of the century. The year 2000 will bring us a very special kind of civil defence exercise. For the basis for information warfare is not just the attack on military infrastructure, but the attack on the much more important, but significantly less well-protected civil infrastructures. Information warfare, just like the street and rail networks, makes no distinction between civil and military infrastructures. Information warfare takes place not only in the internet, but also in the telecommunications net. When we have managed the transition into the year 2000, politicians and the military should sit down and have another good think about the possible consequences, should they seriously consider information warfare as a possible option for conflict settlement. My concern is therefore the absurdity of trying to increase the vulnerability of our society through information technology and simultaneously still test means–not to systematically reduce this vulnerability, but to use security loopholes as war weapons.

A New Deterrent

In times past it was not a display of courage, even by members of the military, to run around a gunpowder chamber with a burning fuse in the hand. The fuse has today been replaced by other forms of self-destruction. During the past few decades the atomic bomb has been the symbol of this progress. It seriously cast doubt on the continued existence of humankind. Luckily the self-deterrent effect was strong enough to prevent anybody lighting the fuse and using this weapon. But nowadays deterrence is no longer confined to nuclear weapons. The USA see information warfare as a suitable successor: the nuncial deterrent replaces the nuclear deterrent. To this end foreign military observers are given ample opportunity to study the manouevres of fully digitalized US troops. The present state of development is being compared with the early phase of the nuclear deterrent.[4] As a result the nuclear umbrella as a basis for alliances is being replaced:

> Just as nuclear dominance was the key to coalition leadership in the old era, information dominance will be the key in the information age.[5]

To think here on the scale of having access to satellite pictures is to fall way too short of the mark. Information warfare is based on the use of the technological edge in information technology. If every weakness of a computer system was general knowledge, that nice advantage in knowledge would be lost, just as it would if everyone had the knowledge of how to protect oneself from such attacks. Information warfare is therefore based on the loopholes in IT security and the well-protected knowledge about them. If there were computer systems which had no security loopholes, information warfare would be powerless. In this way for as long as American businesses maintain their lead in the IT sector, and, above all, as long as their lead in know-how is adequate, information warfare is of real significance, at least for the USA.

This has bitter consequences for the civilian information society. As the fighting grounds for the clash, the security of civil IT systems will be measured primarily by strategic and tactical standards. Some of the ensuing mechanisms can be illustrated by example of cryptography.

Information Technology as a War Weapon

The concept "Cryptocontroversy" is the term used for the bitter debate about the unlimited use of coding methods. Private persons and industry want to protect the confidentiality of their data from spying during transference. Secret services are creating horror scenarios in the case of their no longer being able to do precisely this. Crypto procedures are today what other IT security techniques will become: war weapons for information warfare. They can still be freely used nationally in most countries, however, for decades they have been classed as war weapons when exported.[6] Not only in the Federal Republic of Germany is it the same crime to export plutonium and other mass destructive weapons and crypto-software.

If the security of data constitutes as serious a crime as the construction of atomic bombs, this should be a clear warning for the career of information warfare. Yet crypto-procedures do not only secure data and their confidentiality. They are the basis for digital authentification and reliability and other concepts. Just as the atomic bomb re-defined the military significance of some countries, so the control of coding procedures is changing the political map. The exporters of coding systems have, according to military experts, the "strategic control" over the protected communication of their customers with sales of systems to neutral countries.[7]

The unleashing of cryptography as a science, the fruits of which we are now harvesting, was a tale of obstructions and intimidation by people representing military interests. In the 80s it almost looked as if the Pentagon was going to declare the whole branch of science as being "born secret". Only the resolute, at times desperate, resistance of the scientific community was able to prevent this.[8] Even pressure from various governments–including the German Federal Republic, despite its denials,[9]–on the international standardisation organisation, ISO, to refrain from the standardisation of crypto-systems had little effect. The ISO had, it is true, forbidden those involved the standardisation of crypto-algorithms as a result of their technical committees, but this did nothing to stop the dissemination of a cryptoprogramme like Pretty Good Privacy (PGP); in fact, it promoted it. The USA is now pressurizing the ISO for standardisation in order to be able to counter the quasi-standard. With cryptography the civil world opened a key technology of IT security for itself. Whether the same will be possible with the abundance of individual techniques for the security of IT systems is less clear.

Distrust

Cryptography also offers a wealth of examples for the growing distrust, born of the clash between civil and military interests, of government promoted security standards. The key length of the Data Encryption Standard (DES), which was declared the standard in 1997, had been criticized for being too short when it was developed.[10] DES was laid down for the coding of US bank transactions in 1984.[11] In the 70s a method based on one-way mathematical functions, the so-called knapsack procedure, came to rival the asymmetrical RSA procedure. Only after extensive developments did the vulnerability of this procedure due to flaws become known. Only then did NSA admit that it had known about these flaws for a long time.[12] One thing is certain: if the knapsack procedure had replaced the RSA procedure, NSA would have had far less worries. A short while ago the news that even well-protected chip cards could divulge their secret crypto-code with the appropriate treatment and a differential fault analysis caused a great stir. But yet again the government crypto experts stated officially that the danger was purely theoretical and that it had not been proven.[13]

It is obvious that such behaviour gives rise to growing distrust in the truth content of statements from official institutions if these institutions are either secret services or have developed from secret service connections like the Federal Ministry for Security in Information Technology.[14] The only institutions with enough experience to make an independent assessment of the quality of security systems are therefore the very same ones who should find ways to gain military benefits from security loopholes.

Security loopholes in connection with cryptographic procedures are, however, only the tip of the iceberg. Most of the time it remains unclear what background led to specific security holes, but the distrust of the security of IT products from other countries is in the meantime so deeply seated, even within the government, that German Federal Republic offices warn of using certain systems from the USA.[15]

There, by contrast, people are industriously cataloguing which security loopholes are available for attacks on IT systems. The Joint Command and Control Warfare Center of the US forces keeps a collection of all available data on weapons and C^{3}I systems of a potential opponent and their weak spots. These data are processed and made available to information warriors in the so-called Constant Web databank on a network which covers 67 countries.[16]

When the Military become Hackers

The military who penetrate federal authority computers do not just demonstrate the latters' vulnerability. At the same time they are working on job creation measures for themselves. For who could be in a better position to protect the security of the national IT infrastructure than those very people who wish to make this infrastructure a war zone? In this way information warriors misuse the original hacker ethics of spying on others to draw the victims' attention to the security loopholes found.

What those affected have understood as a modern form of protection money blackmail, information warriors use on whole nations–their own first of all. After the military had to accept a certain increase in IT security for some time, the active encouragement of information warfare as a systematic increase in IT insecurity allows them to repress non-military solution concepts: The Empire Strikes Back. In contrast to occasional hackers and professional IT advisors, information warfare is actually concerned not with the systematic reduction of vulnerability, but with its selective use. As the example cryptography shows, the military represents an insecurity factor, not a security factor. Their interests stand in sharp contrast to those of civilian society.

But when there are security concepts, their applicability for civilian areas is often not really appropriate. Alternatives, for example, to the outdated authenticization via password are biometrical procedures for definite identification. Finger or hand prints, iris scans or thermo scans of the vascular system of the facial blood vessels are used as definite biometrical characteristics to protect entry to all kinds of sensitive systems. Plans are also known of military research projects in which the usefulness of GPS-measured places of issue, and even implanted identification chips as an entry check, are also being considered. The soldier's implanted dog tag thus becomes a multifunction device. In the end we have the complete transparence of activities in the internet. All of these procedures could perhaps be carried out in military scenarios. However, they have the serious drawback that in the civil context they can only be deemed constitutional with great difficulty.

This gives rise to the question of whether we really only have the alternative between a completely militarized information society or much too little IT security. Do we really only have the choice between the pointless renunciation of IT for critical security purposes and the classification of IT security in military categories?

Alternative Civil Concepts to Information Warfare

What we need is to reduce the vulnerability of the information society, independently of information warfare. Alongside an early assessment of the risks, an improvement in IT security can best contribute to this. The first IT security criteria from the Pentagon, the Orange Book, have been made only slightly less military for the Common Criteria. From the civilian standpoint the definition and evaluation of IT security has thus hardly ever been developed. If the reliability, the security and the availability of the infrastructure of the information society depend on security measures, then we cannot seriously leave their definition and assessment to the military or to secret services. The real question is therefore about the civilian demands for evaluation criteria and their significance in everyday life.

The conclusion of the debate on information warfare can only be the consistent politicization and civilianisation of IT security. IT security should be placed in civilian hands and developed according to civilian demands instead of it continuing to be regarded under military aspects. We do not need the military to highlight where the vulnerability of the information society lies. As mentioned at the beginning, even before the coining of the concept "information warfare" there was a lively debate both about the results of a lack in security and about security loopholes. Why should hackers first have to become soldiers in order that these security loopholes be taken seriously?

The security and the protection of a vulnerable information society are better off in the hands of civilian institutions. It was NGOs and professional organisations which called attention to the explosive nature of this theme in the past 20 years. They will also have to be involved in this debate in the future instead of leaving the security of the information society to government institutions which have a dubious reputation and military interests. Instead of seeing the exposure of security loopholes as a risk, the very opposite should be the case. Information exchanges should be built up to support the system administrators affected. The exposure of standards and security features protects us from nasty surprises. To regard NGOs such as human rights' groups or network activists as enemies in a net war is to go in the wrong direction. With their work in the past few years they offer the best guarantee for developing the information society along democratic and civil principles and reducing its vulnerability in the interests of the general public. If such activities are not supported and such groups are not included, security will not increase, but at best protection against improper use. Information warfare therefore forces us to decide whether this should be the aim of a civilian information society or not.

[1] Ralf Klischewski, Arno Rolf: "Informationstechnische Vernetzung und Kriegsunfähigkeit in hochentwickelten Industriestaaten" in Ute Bernhardt, Ingo Ruhmann (Ed.): *Ein sauberer Tod. Informatik und Krieg*, pp.268-282, p.282, Marburg 1991

[2] John Arquilla, David Ronfeldt: "Cyberwar is coming!" in *Comparative Strategy*, No.2, 1993, pp. 141-165, p.147

[3] cf. Ute Bernhardt; Ingo Ruhmann: "Der digitale Feldherrnhügel. Military Systems: Informationstechnik für Führung und Kontrolle" in: *Wissenschaft und Frieden*, Vol.1/97, Dossier No.24, pp.1-16

[4] "Information Dominance Edges Toward New Conflict Frontier" in: *Signal*, Aug. 1994, pp.37-40, p.39

[5] J.S. Nye, Jr.; W.A. Owens: "America's Information Edge" in *Foreign Affairs*, March/April 1996, pp.20-36, p.27

[6] The USA regulates the export embargo of efficient cryptosystems in the International Traffic in Arms Regulation (ITAR), the Federal Republic of Germany in the Export List Part 1 C, Paragraph 5 Part 2 in keeping with foreign trade regulations. In all western countries coding secret services like NSA or BSI assess and so authorize exports; cf. the Federal Republic's answer to Dr. Manuel Kiper's query "Sicherheit der Informationstechnik und Kryptierung", Drs. 13/4105, qu. 6

[7] Mike Witt: "Tactical Communications" in: *Military Technology*, No.5, 1991, pp.19-25, p.22

[8] cf. Ingo Ruhmann: *Politik der Chiffren* in *FlfF-Kommunikation* 3/96, pp.45-49

[9] cf. the Federal Republic's answer to Dr. Manuel Kiper's query *Sicherheit der Informationstechnik und Kryptierung*, Drs. 13/4105, question 11

[10] Whitfield Diffie, Martin Hellman: "A Critique of the Proposed Data Encryption Standard" in: *Communications of the ACM*, March 1976, pp.164-165

[11] Edith Myers: "Speaking in Codes" in *Datamation*, Dec. 1, 1984, pp.40-45

[12] Adi Shamir and Len Adleman (the "S" and "A" of the acronym RSA) demonstrated two different procedures for breaking the knapsack code at the Crypto '82 conference in mid 1982. cf. David Kahn: "The Crypto '82 Conference" in: *Cryptologia*, Jan.1983, pp.1-5. Shortly after this the NSA chief at that time, Inman, stated that the flaw had been detected, but that no warning had been given about using it, in Gina Kolata: "NSA Knew of Flaw in "Knapsack" Code" in: *Science*, 24.12.1982., p.1290

[13] cf. the Federal Republic's answer to Dr. Manuel Kiper's query "Lage der IT Sicherheit in Deutschland", Drs. 13/7753

[14] Ute Bernhardt; Ingo Ruhmann: "Der militärische Maßstab der Computersicherheit–Das Bundesamt für Sicherheit in der Informationstechnik" in: title as above, (Ed.): *Ein sauberer Tod*, see above, pp.252-267

[15] cf. the Federal Republic's answer to Dr. Manuel Kiper's query "Sicherheit der Informationstechnik und Kryptierung", Drs. 13/4105, question 10

[16] "Information's Dominance Edges Toward New Conflict Frontier", see above, p.38ff.