

Computer terrorism: What are the risks ?

Patrick Galley

May 30, 1996

English translation July 1, 1998 by Arif M. Janmohamed

Project : Science, Technology and Society

Swiss Federal Institute of Technology

Introduction

Our society relies more and more upon computers. No matter where you are or what you do, you are likely to deal, either directly or indirectly with computer. When you pay with your credit card, book a seat on an aircraft, deposit money in your bank account and even when you simply make a phone call, it is a computer which, finally, deals with you.

From time to time, the press reveals to the public that computer hackers broke into such or such system, stole hundreds of credit cards numbers and can now consult and modify the contents of your bank account or visit the computers of the army. It has also taught us that computer viruses jump from computer to computer waiting for the opportune moment to destroy the contents of our hard disks.

What would happen, if an organization or a government united these isolated hacker's skills to take a large scale action against a State? Authors such as Winn Schwartau in his novel *Terminal Compromised* have exploited this assumption.

Is such scenario possible or is this merely the speculation of science fiction authors.

This is the question that I will try to answer in this document. I will only concentrate on strongly industrialized countries, particularly the United States in which the computer infrastructures are well developed.

Method

First of all, I will speak briefly about terrorism and the terrorists, in order to determine if their motivations and usual methods would allow them to use computer as new weapon (or as a new target) and to thus obtain results similar to the use of bombs, kidnappings or assassinations.

Then, I will touch upon the topic of computer criminality to show what motivated people can do with computers that do not belong to them.

I will discuss the vulnerability of certain significant information processing systems, about breakdowns or sabotages.

I will talk about "Information Warfare", one of the US Army's new preferred subjects, in order to see at which point the risk of such a conflict worries them.

Finally, I will synthesize all of these elements and will attempt to determine if there is or if there is not a risk of computer terrorism.

Chapter 1: Terrorism

Definitions

The term "terrorism" appears for the first time in 1798 when the philosopher Emmanuel Kant uses it, strangely, to describe a pessimistic view of the destiny of humanity. The same year, one finds the term in a supplement to the large Dictionary of the French Academy; it evokes excesses of revolutionary Terror then and thus does not have the meaning that we accord to it today. We refer, generally, to the action of clandestine movements which target the government of a country with an aim of radically reversing its political and social command: it is not only the State which is aimed, but the entire social system

Let us look at some other definitions:

"Terrorism: The systematic use of terror especially as a means of coercion"

"Terrorism: Set of acts of violence made by an organization to create a climate of insecurity or to reverse the established government. "

(...) The terrorism be thus primarily a strategy intended to unbalance a country or a regime, use the subversion and the violence on a medium or a institution in crisis to contribute with disorder, the day before of a revolution or a war of conquest carried out by a foreign power(...)"

It is advisable to add to these definitions, the use of terrorism as a means of pressure. In the case of international terrorism, the attacks are generally used to create pressure on a government by means of public opinion, in order to obtain something precise such as the release of a prisoner or stopping the export of weapons to a certain country.

Forms of terrorism

Terrorism can take various forms. Luigi Bonanate proposes following classification:

First of all, it is necessary to distinguish internal *terrorism* and international *terrorism*. Internal terrorism includes at the same time the terrorism of State (terror) and revolutionary *terrorism*, according to whether it is a question of reinforcing or of destroying the State. The State can apply *the reign of terror* or use *the terrorism of State*, as when one shows it to support destabilizing terrorist actions with an aim of reinforcing the central authority. The State can be finally at the origin of aggressive forms of *terrorism*, when, for example, during the war, it ordered massive bombardments to frighten the enemy

(bombardment of Dresden, February 7-15, 1945) or to definitively discourage it (atomic bombardment of Hiroshima and Nagasaki, August 6, and 9 1945).

There are also various types of international *terrorism*. Initially, comes independence or separatist *terrorism*, which are movements that wish to overcome a colonial domination or to constitute an independent State or even sometimes to link itself to another State than that to which they belong. By nature, independence *terrorism* is always international, because it carries its strikes beyond the borders of the concerned territory. this is the case of Palestinian terrorism. On the other hand, one can find a *colonialist* terrorism that aims to preserve the sovereignty of a State on a colony.

To supplement this picture, it is advisable to evoke an ultimate form of recourse to terror on a planetary scale, even if it comes out of the specific problems of terrorism: it is about " the balance of terror ". This formula summarizes the policy led by the United States and the Soviet Union (until the dissolution of the latter), in order to freeze the international order resulting from the Second World war, via the threat of a total nuclear destruction.

In 1937, after the attack against the king of Yugoslavia and the French minister Louis Barthou in October 1934 in the city of Marseilles (France), the LON (League Of Nations) drew up a International Convention which was signed in Geneva on November 16 1937 by twenty-five countries (except Italy and the United States). This convention defined overall the terrorist acts as " criminal facts directed against a State and of which the goal or nature is to cause terror towards determined personalities, groups of people or the population " (article 2). The signatories of the text thus drew up the detailed list of the various forms of terrorism:

- Facts intentionally directed against the life, the physical integrity, health or freedom of:
- heads of States, people who exert the prerogatives of head of State, their hereditary or designated successors;
- husband or wife of the above peoples;
- invested people of functions or public offices when the above-mentioned fact was made because of the functions or the responsibilities which these people exert.
- The fact of destroying or of intentionally damaging public goods or goods intended for a public use, which belong to another State signatory or which belong to the State.
- The fact of intentionally endangering human lives in order to create a common danger.
- The attempt to commit offences envisaged by the preceding provisions of this article.
- The fact of manufacturing, of getting, of holding or of providing weapons, ammunition, explosive products or harmful substances for the execution, in any country, of an infringement envisaged by this article

Evolution of international terrorism

The tenth annual International Conference on Criminal Justice Issue, joined together, among other things, at the end of July 1995, current and old members of the FBI, the American State and the Defense Departments, Argentinean and Israeli anti-terrorists experts.

It was learnt from this conference, that in the future, the use of weapons causing much more civilian victims is very probable. According to Peter Probst (DoD), the ethnic or religious terrorist groups will

not be reticent to cause a great number of victims, whereas the old political terrorist groups hesitated to do it, fearing to lose the possibility of population support. Moreover, the attack with toxic gas, in Japan, broke the taboo of using chemical weapons

Chapter 3: Vulnerability of systems

Introduction

This chapter is intended to quote some incidents which happened in significant systems such as the telephone company or an airport. They were not criminal acts, but only "normal" incident.

Examples

Breakdown of the AT&T long-distance network

January 15, 1990, following a software update of telephone switches, the long-distance network of AT&T was down during 9 hours resulting in 60' 000 people completely unable to use telephone and 70 million blocked calls(million others passed without problems). The problem started from a switch in Manhattan and was spread across the country in less than ten minutes

A cut cable paralyses an airport

October 15, 1990, a grower of trees in the suburbs of Chicago damaged a significant telephone cable, depriving 150' 000 people of telephones. ATMs of some banks were paralyzed. All flights to the international airport O' Hare were delayed because the control tower lost contact with the principal FAA air control center for the Chicago area

Telephone breakdown: Three paralyzed airports

September 17, 1991, the power to a group of telephone switches of the area of New York is cut and the spare batteries do not engage. Moreover, the two people in charge of monitoring the system were following a course on the procedures in the event of breakdown that day! As a result, three airports were closed: Kennedy, Guardia and Newark. 500 flights were cancelled, 500 others delayed.

Chapter 4: Information Warfare

General

Information Warfare ⁶ is the hot topic of many world wide armies especially in the United States. It is a large field, grouping together several concepts ⁷ such as electronic warfare, psychological warfare, information and hacker warfare (hacker war). Dr. John Algiers proposes the following definition.

Actions taken to achieve information superiority by affecting adversary information, information based processes, and information systems, while defending ones own information, information based processes and information systems.

Winn Schwartau proposes following classification:

Class 1: Personal Information Warfare

This class includes attacks against individual privacy. This includes the disclosure of information stored in an unspecified data base. We currently do not have any control over our own data stored all over the place such as credit card history, banking accounts, medical files, criminal records, etc. In summary, we should remember the following points:

- Hundreds of data bases contain a digital image of our life.
- Available Information is not necessarily accurate.
- It is almost impossible to correct erroneous information.

Class 2: Corporate Information Warfare

Concretely, today, this class corresponds to competition between companies which clash in a war without pity. Industrial espionage is one of the possible activities, but misinformation is a very effective means to get rid of a competitor. Presently, it is very easy to launch rumors with a world range, using Internet. Moreover, it is well-known that the more a fact is contradicted, the more public opinion believes it.

Class 3: Global Information Warfare

This type of conflict is aimed at industries, the whole of the economic forces, the whole of a country. In this class, it is necessary to multiply the power of classes 1 and 2 by a great factor. With ridiculous investments with respect to those authorized in the case of " traditional " weapons, it is possible for a terrorist group or a country to bring a great economic power to its knees. The advantage for the attacker, if it is included in the category of developing countries, is that it will not be as sensitive to reprisals of comparable nature. Moreover, it would be very difficult for an industrialized democratic country to answer an attack of this kind by armed reprisals, without hurting public opinion

Diverging opinions

Certain authors think that the first information war was the Gulf War. The allied coalition led by the United States had total control of information on the battle field (satellites, AWACS, JSTARS, etc), whereas Iraq had been, from the war's first moments, deprived of its principal communication infrastructures.

Others, on the other hand, find that the means employed during the conflict came from not only the "industrial wave" (use of massive bombing) but also of the "information wave" (dropping of " intelligent " bombs on communication centers). For them, this war was not "pure" a war of information.

Security of military computers

Paradoxically, it was only after the Gulf War that the United States became aware of its vulnerability. By request of the Pentagon, DISA brought together a team of hackers, gave them access to the Internet, and asked them to break into the most DoD computers possible. They took control of 88 % of the 8900 computers which they attacked and only 4 % of the attacks were announced to the various persons in charge of the computers! While combining these results with 350 detected intrusions coming from unidentified hackers, they concluded that 300' 000 DoD computer intrusions took place in 1994!

The military computers, which are connected on Internet, generally do not contain confidential information and do not carry out vital tasks. However, these computers are nevertheless in charge of logistics, accounting, and personnel management, which can appear sensitive. At the time of the Gulf War the United States used the Internet to transmit logistics information, sometimes even without encryption. Personnel information can be used with an aim of determining potential targets for blackmail or corruption in order to obtain access to confidential information. A group of Dutch hackers would have proposed to Saddam Hussein to disturb the communications of the army over Internet for a million dollars. He would have declined the offer.

Dependence of the army with respect to civil infrastructures

As we saw before, the army has well protected computers for its critical activities. However, American military bases (it must also be the case in other countries) depend upon civil infrastructures particularly for power supply and the communications. Nearly 95 % of the American army's communications use the normal telephone network. Transport of troops by rail or by plane is also done under the control of the civilian infrastructure!

Simulations

In order to determine the problem of information warfare, the American Defense Department asked the company RAND to lead strategic exercises of simulations on this subject. Six exercises took place between January and June 1995. The participants were highly placed persons in charge of national security as well as industrialists from the communication sector. One of the situations was the following:

February 2000.

The crisis: A Middle East state decides the time is ripe for a power grab in the Persian Gulf and directs its threat to an oil-rich neighbor that the United States is pledged to protect. Determined not to repeat Saddam Hussein's mistake, the aggressors elect not to challenge America in a head-on military confrontation. Instead they prepare a more insidious assault. In the United States and abroad among U.S. allies, a pattern of computer mayhem begins to emerge in a cascading sequence of events. Actually,

the war has already begun but no one in the United States yet realizes it; keyboard mice, logic bombs and computer viruses don't make much noise.

The attack: A three-hour power blackout in a Middle Eastern city has no reasonable explanation, computer-controlled telephone systems in the United States "crash" or are paralyzed for hours, misrouted freight and passenger trains collide, killing and injuring many passengers; malfunctions of computerized flow-control mechanisms trigger oil refinery explosions and fires . . . electronic "sniffers" sabotage the global financial system by disrupting international fund-transfer networks, causing stocks to plunge on the New York and London exchanges. In America, local automatic teller machines begin randomly crediting or debiting thousands of dollars to customers' accounts; as news spreads across the country, people panic and rush to make withdrawals. Television stations in the Middle East lose control of their programming and a misinformation campaign of unknown orchestration sows widespread confusion. Computerized dial-in attacks paralyze the phone systems at bases where U.S. troops are scheduled to begin deployment; various groups flood the Internet calling for massive rallies to protest U.S. war preparations; computers at U.S. military bases around the world are stricken--slowing down, disconnecting, crashing; more ominous, some of the military's most sophisticated computer-controlled weapon systems are exhibiting flickering screens and other signs of electronic malaise.

From there, the participants in the exercise had 50 minutes to find what to make...

The principal conclusions drawn from these exercises were:

- ***Everyone can attack you.***
- ***You cannot know what is real.***
- ***It is difficult to know that you are under attack.***

Not all the soldiers believe in this kind of disaster scenario. For Martin Libicki, teacher at the National Defense University, it is excessive to extrapolate a threat to national security starting from facts which until now were only electronic versions of a "joyride in a stolen car"!

Various techniques

The goal of this section is to highlight certain techniques usable at the time of an information warfare of which the general public is surely unaware.

Chipping

Chipping is the hardware version of a [Trojan horse](#). That consists in adding a function, without the knowledge of the purchaser, in an electronic component of a weapon (or other hardware), so that if one day this weapon were to be used against the country of the manufacturer, it can be neutralized at a distance.

Bombs EMP-T

Since the beginning of the atomic era, soldiers undertook to protect their electronic systems from electromagnetic radiations, which would be produced during a nuclear explosion. Without adequate protective measures, it is possible to destroy the electronic systems of a country by exploding an atomic bomb at a high altitude.

Since years, non-lethal weapons are developed, charged to neutralize the enemy electronic systems. According to Winn Schwartau, EMP-T bombs (Electro-Magnetic Pulse Transformer) can be built for a few hundreds dollars, and are able to erase information stored on a magnetic medium around 200 meter.

Van Eck Radiations

Until now, I have primarily treated cases of hacking which have taken place because the target computer was connected to the external world, by a computer network or by telephone. If I told you that your personal computer, without an external connection to the world and on which you are writing a confidential report can reveal your secret to a person who is only one hundred meter from your office, without your knowledge, you would say that it science fiction.

You are wrong! It is possible. Your computer screen emits radiations, even with the strictest standards (civil), and it is possible, with the adequate equipment, to reconstitute the contents of your remote screen. This technique was employed by the FBI during the monitoring of Aldrich Ames, a KGB agent found within the CIA.

The term used by the American army to describe this technology is TEMPEST monitoring. Equipment protected from this type of listening is known as TEMPEST certified. The standard defining the details, such as the quantity of emitted radiations authorized, in order to avoid any detection is classified. In the United States, it seems that the use of the TEMPEST monitoring is possible by the government without court authorization, whereas it is illegal, for a private individual or a private company, to protect himself!

Frank Jones, who works in a company producing equipment in the field, amongst other things, of computer security, coarsely explains how they have designed such detection equipment in order to their customers' computers. Once developed, they successfully tested their hardware, on targets such as banks, police stations, banknote distributors, television sets and offices.

If the design of such equipment is within the range of a team of engineers, then it is extremely probable that bad guys can also procure such equipment without problem to devote themselves to criminal activities.

Chapter 5: Computer Terrorism

Introduction

Until now, I have tried to give a rather broad outline of our vulnerability with regards to computers, and I hope that I have convinced you that we are sitting on a bomb. It is time, now, to determine if a terrorist organization could use computer either as arms, or as targets, with an aim of continuing its fight, usually carried out by bombings or removals.

In January 1995, a conference was held in Montreal on information warfare, that brought together Canadian, American and European soldiers, as well as representatives of the FBI and Canadian Service of Information and Security. One of the topics of discussion was the attack of New York's World Trade Center, in February 1993. This attack, which at first seems to have nothing to do with the conference's subject, can be regarded as one of the first acts of computer terrorism. There were less material damages than "virtual" ones. Thousands of firms were unable to connect their computers to the rest of the world for many days. According to studies, this situation generated losses evaluated at more than 700 million dollars, during the first week!

Definition

Let's define, the concept of "computer terrorism". Since this subject is not treated as such in literature, I propose two definitions:

Computer terrorism is the act of destroying or of corrupting computer systems with an aim of destabilizing a country or of applying pressure on a government.

Computer terrorism is the act of doing something intended to destabilize a country or to apply pressure on a government by using methods classified in the category of computer crimes.

It is possible to carry out three types of actions against an information system, a physical, syntactic or semantic attack.

- **The physical attack** consists of damaging equipment in a " traditional " way, bomb, fire, etc.
- **The syntactic attack** consists of modifying the logic of the system in order to introduce delays or to make the system unpredictable. An attack by means of a virus or of a Trojan horse is included in this category.
- **The semantic attack** is more perfidious. It exploits the confidence that the users have in their system. It consist of modifying information that is entering or exiting the system, without the users' knowledge, in order to induce errors.

Reflections

After having listed a large number of weaknesses in information processing systems, and to having shown how easily it is possible to introduce chaos even from remote location, it is interesting to wonder **why have terrorist computer attack not yet occurred?**

If we look at the last wave of terrorist attacks in France (1995), carried out by Islamite Algerian of the GIA (Armed Islamic Group) an answer may be that these groups rejecting the westernization of their country, reject consequently associated technology, and are thus not able to effectuate computer terrorism. Moreover, and I believe that it is the principal reason, disproportion of the means to implement computer terrorism results in the fact that terrorist groups remain confined to traditional method.

Means to implementation

According to the theory of the class 3 information warfare, this type of conflict requires much less human and financial resources than a conflict with "traditional" weapons. This is the case because the cost of modern conflicts are very expensive, but, if we look at the absolute value of the investment for terrorism, the result/cost ratio is strongly against computer terrorism, compared to "traditional" terrorism.

If we take the case of a tiny terrorist group, it is able, with a small amount of financial and logistical support, to carry out some home-made bombs and to create panic across a country. In the case of the attack to the administrative building of Oklahoma City, in April 1995, the home-made bomb made of fertilizers, caused the death of nearly 100 persons, was apparently the act of a single terrorist! In these two cases, with the same investment, it would have been impossible for them to produce the same psychological effect with computer attacks.

Computer terrorism must be seen as an act similar to an act of war. It needs to be effective to establish a **long-term strategy** and to have control of very large number of factors. Hacking of computer systems (many different) in a perfectly synchronized way, as well as the infiltration of agents in various companies with an aim of inserting Trojan horses or back doors, is a long-term job.

Field of application

This kind of terrorism does not lend itself to reprisals following a precise event such as arrests or the assassination of a movement leader, except if the possibility had been envisaged a long time in advance. The ideal framework for the use of such weapons is the prelude to a war, a kind of "electronic Pearl Harbor". It is currently one of the main fears of the people in charge of American defense. As the United States has a strong interventionist policy (cops of the world), a country deciding to attack its neighbor (ally of the USA) would have an interest to initially conduct a computer attack against the USA, before dealing with its genuine target. As a plan of invasion is not hastily established, it is conceivable to include a plan in order to first neutralize any response coming from the interventionist country such as the USA or France.

Conclusion

As we are now at the end of this document, it is time to answer the question that I asked at the beginning: "Computer Terrorism: What are the risks? "

After having made this broad study, my opinion is that from the point of view of terrorist threats that Western countries have already encountered, there will not be a change to computer terrorism in the near future. On the other hand, movements such as the American militia, or the drug cartels who have embraced new technologies and who are thus completely immersed in the information society, are more likely to carry out an offensive in Cyberspace.

From the military point of view, I am of the opinion that a scenario of the type of those used in simulation by the American army is very plausible. It would be suicidal for any dictator such as Saddam

Hussein at the present time to conceive a major offensive without benefiting of the advantages from the principal Achilles' heel of the Western civilization: information systems.

At present, information warfare worries the Western governments and they are taking measures in order to avoid being an easy target. However, the task to be achieved is colossal. to just secure military systems one will already need years and millions of dollars, without even touching civilian infrastructures.

It is impossible to know at the moment when you read these lines, if a computer attack is preparing or if it already started. Who knows if universally widespread software like Microsoft Windows or Netscape Navigator are not Trojan horses?