Information Warfare

Yael Yashar (ICT)
26/02/1997

ABSTRACT

Computer Warfare? Terrorists take control of the NewYork Stock Exchange? Terrorism over the Internet? Computer viruses in the arsenal of Hizballah ?
Sound implausible? Maybe. But such possibilities are currently being discussed by strategic analysts under the catch-all title, "Information Warfare". To date the defense establishment has yet to agree on the exact definition of the term “information warfare”. But on one thing everyone agrees, in the digital age, information, and its dissemination, has achieved the status of a vital strategic asset .

Infowar - Potential Weapons

If the response of the American defense establishment is any indication, strategic analysts are taking the possibilities of infowar seriously. Special committees in every branch of the U.S. armed forces are studying its potential, both as a defensive and an offensive weapon. The NSA (National Security Agency) is reportedly studying a rather imaginative arsenal of "info weapons". Among the possible offensive weapons are:

- Computer viruses, which could be fed into an enemy's computers either remotely or by "mercenary" technicians;
- Logic bombs, another type of virus which can lie dormant for years, until, upon receiving a particular signal, it would wake up and begin attacking the host system;
- "Chipping", a plan (originally proposed by the CIA, according to some sources) to slip booby-trapped computer chips into critical systems sold by foreign contractors to potentially hostile third parties (or recalcitrant allies?)
- Worms, whose purpose is to self-replicate ad infinitum, thus eating up a system's resources. An example is the infamous worm that crashed the entire internet network in 1994.
- Trojan horses, malevolent code inserted into legitimate programming in order to perform a disguised function.
- Back doors and trap doors, a mechanism built into a system by the designer, in order to give the manufacturer or others the ability to "sneak back into the system" at a later date by circumventing the need for access privileges.

A few other goodies in the arsenal of information warfare are devices for disrupting data flow or damaging entire systems, hardware and all. Among these - HERF (High Energy Radio frequency) guns, which focus a high power radio signal on target equipment, putting it out of action; and EMP (Electromagnetic Pulse) devices, which can be detonated in the vicinity of a target system. Such devices can destroy electronics and communications equipment over a wide area.

Trends - Information Warfare and Glass Houses

While all this seems to point to an increasing advantage of technologically advanced nations over those less advanced, there is a certain catch to this game. American strategists are very leery of the prospects of using the more malicious forms of information warfare, for the same reason that American policy forbids the assassination of foreign leaders. This policy rests on the principle, "Don't do to others what they can more easily do to you". The more technologically advanced a nation is, the more vulnerable it is itself to the techniques of information warfare. No nation is more dependent upon the information infrastructure (including the media) as the U.S. So it isn't surprising that American policy makers are quick to point out that infowar scenarios are being studied at present mostly with an eye toward defense rather than offense.

Added to this is the fact that it is primarily the civilian sectors that are most vulnerable, with consequences in both the military and the political sphere. Military infrastructure relies for the most part on civilian infrastructure. Nearly every aspect of the military industry, from basic research and development to paying personnel

depends on civilian information networks. Over 95 percent of military communications use the civilian network. Military bases, particularly the more sensitive ones, depend on the national electric power grid. Soldiers travel by means of the national bus cooperative. There is no way that the military can protect all of these networks from a focused infowar attack.

Trends in Warfare

In their book War and Antiwar, Heidi and Alvin Toffler divided human history into three distinct phases. The first phase, the Agrarian phase was called the First Wave; the Second Wave corresponded to the Industrial Revolution; while the present "age of information", characterized by the "digitalization" of society, was termed the Third Wave. To each of these ages, the Tofflers ascribed its own particular type of warfare.

During the Agrarian Age war was waged for control of purely local resources, and the warriors were either members of the parties in direct control of the disputed land or resources, or in the case of feudalism, conscripted tenants of same. Large standing armies were not feasible as a rule, due to lack of resources, and the exceptions to this rule (such as the Roman Legions) were assured military dominance

The Industrial Revolution brought with it a kind of "de-feudalization", which put society on a mass-driven footing. Resources and assets came to be controlled by larger sectors of the populace. This was true of war as much as any other industry. Warfare became an attack of society against society, with the involvement of millions of people, including civilians, on each side.

Our present age has been called the "Age of Technology", but a more apt name might be the "Information Age". Technology and information are interdependent, with advances in one entailing and dependent on, advances in the other. The increasing flow of information, the evolution of the global economy, and the creation of the internet are all factors in creating the modern global village. The main actors in our society are fast becoming international corporations, rather than nations. It is plain that the changes in human society as a whole will entail changes in the way we wage war as well. Among other trends, warfare is shifting more and more toward civilian targets. This is likely to be even more noticeable in future conflicts, in which information warfare will play a greater role.

Information Warfare in the Information Age

In war, both conventional and non-conventional, the priority of a target is dependent on its value to the other side. The same is true of terrorism, though targets are chosen more for psychological value than for military value. For this reason, any open conflict, communications facilities and supply lines have always been high priority targets. Today critical information, both on and off the battlefield, flows from place to place by means of digital technology. It is not surprising that information warfare is fast becoming a hot topic in military circles. With the increasing digitization of the battlefield it makes sense to find ways of protecting the computerized control of ones military apparatus while at the same time coming up with the means to disrupt that of the other side.

But information warfare, both defensive and offensive, is not confined to the battlefield. In fact, it is a matter of far more urgency to the citizen than to the soldier. It is more than likely that both the victims and the perpetrators of information warfare will be found in the civilian sphere. This is because it is in our civilian lives that we are most vulnerable to techniques of information warfare. It is to be expected that the military, concerned as it is with the continual need to protect its facilities and personnel from hostile action, will take all necessary precautions to guard its digital apparatus from outside interference. We need not be overly concerned over the penetrability of military computers; the military can take care of itself.

Unfortunately the same does not hold true for most civilian mission-critical computers. As mentioned above, the military itself depends on the civilian infrastructure, which is itself the achilles heel of our society. We have become overwhelmingly dependent on the digitized flow of information. Computers control our electric power supplies, run the national water system, control the air traffic into and out of the country, manage our bank accounts, and keep track of every aspect of our personal lives. All of these information systems are vulnerable, to one degree or another, to outside interference. In the past we have been fortunate in that the vulnerability of such systems has been less than the hacking talent of those who had most to gain by waging information war. This is something we mustn't count on in the future.

Information Warfare - the Perfect Terrorist Weapon

Terrorism is yet another example of how the focus of war has shifted toward civilian populations. The aim of terrorism is not to destroy the enemy's armed might, but to undermine his will to fight. The terrorist seeks to disrupt the daily life of his target nation by striking at the most vulnerable points in the society. Such vulnerable areas included transportation networks and public events, which insure good media coverage. By hitting the citizen just where he thinks he is safest, the terrorist causes the greatest confusion and loss of morale.

Today, with every aspect of our lives dependent on information networks, terrorists have a whole new field of action. And while the technology to operate and protect these networks is quite costly, the means required to attack them are relatively cheap. In the simplest case, one needs only a computer, a modem, and a willing hacker. According to Alvin Toffler, "It's the great equalizer. You don't have to be big and rich to apply the kind of judo you need in information warfare, That's why poor countries are going to go for this faster than technologically advanced countries."[1[

According to TIME Magazine, the Defense Science Board at the Pentagon warned that annoying hackers trying to crack the Pentagon's computers were not the only things the defense strategists have to worry about.

"This threat arises from terrorist groups or nation-states, and is far more subtle and difficult to counter than the more unstructured but growing problem caused by hackers. A large, structured attack with strategic intent against the U.S. could be prepared and exercised under the guise of unstructured 'hacker' activities. . . .there is no nationally coordinated capability to counter or even detect a structured threat"[2[

Can They Do It?

Needless to say, what applies to the U.S. applies as well to Israel. Moreover, we are far more likely to be the target of this new form of terrorism. Are terrorists currently capable of waging Infowar? In the past, there was no compelling reason for terrorists to be computer literate. This is changing fast. Today over 60 percent of University degrees in Computer Science are given to students from developing countries, the vast majority from Islamic countries. And even if terrorist organizations do have trouble supplying their own hackers, there are always mercenary hackers willing to do the job for the right price.

"During the Gulf War, according to Pentagon officials, a group of Dutch hackers offered to disrupt the U.S. military's deployment to the Middle East for $1 million. Saddam Hussein spurned the offer. The potential for disruption was great, says Steve Kent, a private computer security expert in Cambridge, Massachusetts, and a member of a Pentagon advisory panel on defensive information warfare. "In the Gulf War the military made extensive use of the Internet for its communications, and it would have suffered had the Iraqis decided to take it out.' "[3[

Consider also that the means to disrupt or destroy digital equipment are relatively inexpensive, easily smuggled from place to place, can be used from a distance, and are virtually untraceable. In short, the perfect terrorist weapon.

Psychological Warfare

The scenarios described above belong to a subset of information war, commonly called "Hacker warfare". However, the term infowar includes other ways of manipulating information, among them "Psychological Warfare". Psychological warfare is the attempt to warp the opponent's view of reality, to project a false view of things, or to influence his will to engage in hostile activities. It includes a variety of actions that can be divided up into categories according to their targets. Strategic analyst Martin Libicki proposes four categories: operations against troops, operations against opposing commanders, operations against the national will, and operations designed to impose a particular culture upon another nation. In an article for RAND, authors John Arquilla and David Ronfeld called this technique "Netwar"[4, [

"Netwar refers to information-related conflict at a grand level between nations or societies. It means trying to disrupt or damage what a target population knows or thinks it knows about itself and the world around it. A netwar may focus on public or elite opinion, or both. It may involve diplomacy, propaganda and psychological campaigns, political and cultural subversion, deception of or interference with local media, infiltration of computer networks and databases, and efforts to promote dissident or opposition movements across computer networks".

The Media as "Psycho-weapon"

This aspect of information warfare is nothing new. The attempt to influence the human element in a conflict is an old technique. Only the means have changed. Armies have always tried to make their forces seem stronger or weaker than they are, or to convince enemy soldiers that they have no escape but surrender. But to this component in the military arsenal has recently been added a relatively new technique, born of the technology of mass information transfer. Now psychological warfare includes the endeavor to influence the populace of an enemy country to oppose the

war effort, or to depose the reigning government. The means to this end reside in the mass media, and more recently in the internet.

Psychological warfare through the media has been used with success by the U.S. in the Gulf War of 1990-91. The Iraqis were led by media reports to believe that the air war was to be a short-term strike, followed by an immediate ground war, in which they felt themselves to have the advantage of numbers and territorial dominance. They were also kept busy along the Kuwaiti coasts, by means of disinformation pointing to an imminent American coastal offensive.

Another example of psychological warfare was chronicled in TIME Magazine [5];
"The Pentagon "launched a sophisticated psy-ops campaign aHaiti's military regime to restore depose President Jean-Bertrand Aristide. Using market-research surveys, the Army's 4th Psychological Operations Group divided Haiti's population into 20 target groups and bombarded them with hundreds of thousands of pro-Aristide leaflets appealing to their particular affinities. Before US intervention, the CIA made anonymous phone calls to Haitian soldiers, urging them to surrender, and sent ominous e-mail messages to some members of Haiti's oligarchy who had personal computers".

America has not always been on the winning side in psychological warfare. Democracies, by their very nature, are acutely sensitive to public opinion, making them vulnerable to manipulation through the media. American troops left Somalia after the loss of just nineteen American Rangers in a conflict with the forces of Somali leader Mohammed Aideed. That conflict reportedly cost Aideed about fifteen times that number, roughly a third of his forces. And yet it was the Americans who conceded defeat. Why? "photos of jeering Somalis dragging corpses of U.S. soldiers through the streets of Mogadishu transmitted by CNN to the United States ended by souring TV audiences at home in the U.S. on staying in Somalia. U.S. forces left, and Aideed, in essence, won the information war."[6]

New Weapons for Terrorism

CNN & Direct Broadcast

But although the media is a relatively new element in armed conflict, it is a weapon that terrorists have used from the outset. In fact terrorism has always been psychological warfare. Terrorists interact with an entire population through the media. Terrorism is analogous to a virus which transmits its "genetic message" through the legitimate means of information transferal of the society on which it preys, thus altering the society's perception of itself and the world around it. In essence, terrorism replaces society's view with its own, just as a virus replaces the host's genetic material with its own.

Global News Broadcasters, such as CNN bring events worldwide into private homes. Whether the events are real or choreographed specifically for public consumption is another question. In this age of Direct Broadcast Satellites no one needs a government's permission to speak directly to a country's people. The machinery for Direct Broadcast are well within the financial means of any well-funded terrorist group.

The Internet

To this already influential means of reaching the minds of the public terrorists now may add another option: the internet. Because the internet spans geographical, cultural, and economic boundaries, its potential for outreach is tremendous. And due to the way in which information searching is done, through the use of keywords, population targeting, and newsgroups, the message can be focused on particular elements of the population.

In a sense, the internet is becoming the prevailing means of information transferal. In the foreseeable future the internet will replace, or more accurately "swallow" the other forms of media. We will likely see a merging of Direct Broadcast Satellite TV merging with the net to target particular sectors of the population, a kind of "mega-newsgrouping". Thus the media will enter the age of "Me-TV."

This "newsgrouping" in the media offers a new capability to terrorists, no less than to the rest of the elements currently fighting for the attention of the public. Terrorists will be able to tailor their message to different sectors of the population, just as advertisers do.

What Can be Done About It?

In the U.S., where the threat is most immediately recognized debate is currently going on to decide what part government can and should play in protecting civilian networks. On the one hand the civilian networks are controlled by private interest groups, some of them internationally owned. Government regulation would seem to be interference or even repression. On the other hand, the vulnerability and ease of manipulation of some networks are weak links in modern society, and their exploitation by hostile elements threatens all elements of society, and not just the direct controllers of the networks. One solution is to require organizations with a dependence on sensitive information technology to fulfill certain security criteria before being issued a government license. In this field, Israel has already taken the first steps, with the "Computer Laws" of 1994.

However, it must be pointed out that although such measures can provide a minimum level of protection against tampering, there is no such thing as 100% security. What is more, the solutions are sure to lag behind the potential threat until the threat becomes reality. At present the cost of protection is higher than the cost of attack, and until an attack on a major system actually happens, organizations are unlikely to take security measures as seriously as they could, or should.

Summary

- Information technology is being developed by strategic planners both as an offensive battlefield weapon, and as a weapon for "logistics attack", as a means to disrupt the civilian infrastructure on which an enemy's military apparatus depends.
- Technology has already been used effectively by American forces in the Gulf War and in the conflict in Haiti.
- However, Information Warfare is a double-edged sword - those countries most capable of waging it are also the ones most vulnerable to it.

- The increasing dependence on sophisticated information systems brings with it an increased vulnerability to hostile elements, terrorists among them.
- Attacks on information technology are unsettling easy to carry out. The means are relatively inexpensive, easy to smuggle, virtually untraceable, and completely deniable. This, coupled with the fact that the civilian networks which are most attractive to terrorists are also the most vulnerable, makes infowar the perfect weapon in the terrorist arsenal.
- Currently, the security solutions lag far behind the potential threat. This situation is likely to continue until the threat becomes reality, forcing a reassessment of preventive measures.

Notes

.1 Toffler, quoted in TIME Magazine article, “Onward Cyber Soldiers”, August 21, 1995 Volume 146, No. 8

.2 Quoted in TIME Magazine article, “Onward Cyber Soldiers”, August 21, 1995 Volume 146, No. 8

.3 TIME Magazine article, “Onward Cyber Soldiers”, August 21, 1995 Volume 146, No. 8

.4 Arquilla and Ronfeldt, "Cyberwar is Coming!", article for RAND

.5 TIME Magazine article, “Onward Cyber Soldiers”, August 21, 1995 Volume 146, No. 8

.6 Libicki, Martin. “What is Information Warfare?”, article for the Institute for National Strategic Studies