National Security and Non Conventional Cyber Threats in North Africa

- The Moroccan Case-

Rezrazi, ElMostafa.
Ph.D (The University of Tokyo)
Professor of Security and Strategic Studies
Director of the Academic Program of Transregional
&Emerging Area Studies.

Introduction:

Computer technology represents an imperative constituent to national security, conceivably of supreme importance. Without computers, modern weapon store, and communications would be impossible. The future almost emerge to belong to so-called " smart" weapons, complex systems of command and control, telecommunications, satellites, electronic surveillance, and split-second information processing. Besides, the process of integrating advanced computers into weapons and command systems is speeding up at an exponential level.

What is often overlooked the threat to national security posed by networked computers, particularly through the Internet. During the period when the Internet was used almost exclusively by scientists, engineers, academics, and a handful of military personnel, the Internet was viewed by experts mainly as a benign and interesting research project, one with modest and limited application to national security objectives

Nevertheless, In recent years, the Internet has increasingly been regarded by national security officials as a emerging playing field for international conflict, a new medium in which national security will take on non conventional forms, and one in which the government agencies responsible for national security have a growing stake. The internet is emerging as a " critical national asset " that requires their attention and protection. This condition may signal a new era in the development of the Internet, equal in importance to its commercial potential. In fact, the commercial use of the Internet may be influenced by national security controversies as much as by consumer response to new Internet applications.

In this context, the Internet could emerge as a viable means for nations to attack one another. Nations capable of achieving such a status will be able to do so far more

cheaply than if they acquire vast arsenals of missiles and tanks. Therefore a relatively modest investment in the skills of a handful of network trespassers and hackers could become a substitute for immense investments in weaponry. It should thus be clear that that “ new terrain” of computer warfare or cyber-terrorism poses some serious and unfamiliar challenges to national security authorities.

A. A Changing Environment

All forms of warfare in the past have involved a threat to geographically specific assets by equally geographically specific threats- such as massed armies or ballistic missiles. One of the chief characteristics about computer attacks is their ambiguity in nearly every dimension: it is difficult to ascertain where the attack is coming from, who is behind it, what the motive is, whether it is the work of a determined enemy or merely a curious trespasser, etc. Penetrations can come from trespassers inside or outside the national territory, and at the outset is it is to determine whether attacks are benign or dangerous. This very ambiguity of significantly complicates decision-making in particularly , if a computer attack were to occur in the midst of some other crisis of national security. Many of the forms that fall under this type of warfare are grouped under the term “ cyber war”. But it is not ever clear what precisely this refers to. If it means an organized and coordinated attack on computer systems by another state government than the term “ Cyber-terrorism” my be more appropriate although such classification in turn calls for different responses than in typical war-type situations.

There is a lot of misinterpretation in the definition cyber-terrorism, the word consisting of familiar “ cyber” and less familiar “ terrorism”. An e-mail bomb maybe considered hacktivism by some and cyber-terrorism by others.

Cyber-terrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by sub national groups or clandestine agents.

the word cyber-terrorism has entered into the lexicon of IT security specialists and terrorist experts and mass media “professionals”. Cyber-terrorism

Under the above-mentioned definitions of cyber-terrorism, any telecommunications infrastructure attack, including site defacing and other computer pranks, constitutes terrorism.

Despite its relatively broad definition, many experts believe that cyber-terrorism has never been waged against the United States. Rather, the numerous hacking attacks over the post four years- including a 1998 web page set up by a supporter of the

Mexican Zapatistas rebel group, which led to attacks on the U.S. military from 1,500 locations in 50 different countries, only is seen as constitutes computer crime. Some highly ranked officers in Army Intelligence agree that the United States has not seen a cyber terrorist threat from terrorists using information warfare techniques.

The above-mentioned observations drive a clear line between cyber-terrorism, cyber-crime and Information war, and allow us to define cyber- terrorism as: Use of information technology and means by terrorist groups and agents.

Cyber-Terrorism

Cyber-terrorism is a development of terrorist capabilities provided by new technologies and networked organizations, which allows terrorists to conduct their operations with little or no physical risk to themselves. Cyber-terrorism is a new and somewhat unformulated concept, with debate as to whether it is a separate phenomenon, or just a facet of information warfare practiced by terrorists. Even for those that believe cyber-terrorism is a separate phenomenon; the boundaries often become blurred between information warfare, computer crime, online social activism, and cyber-terrorism.

To make an operational definition we suggest first the following terms to separate between cyber terrorism, Cyber Crime, cyber Attacks , information warfare and Netwar:

- Cyber terrorism – The use of the Net for terrorism: The use of the Internet and the computer networks will represent a major challenge in the near future. Such use but also as a means of communication between militants of terrorist organization and between various organizations[1].
- Cyber crime: The use of the Net for criminal actions.
- Cyber Attacks: Email bombs, viruses, intentional actions.
- Information Warfare: Formalized governmental warfare
- Netwar: Conducting warfare via Networks & the Net: netwar refers to an emerging mode of conflict and crime at societal levels, involving measures short of traditional war, in which the protagonists use network forms of organization and related doctrines, strategies, and technologies adjusted to the information age[2].

---

[1] Ely Karmon, Intelligence and the Challenge of Terrorism in the 21st Century

[2] John Arquilla, David Ronfeldt, Michele Zanini Networks, Netwar and Information Age Terrorism

In defining cyber terrorist activity, it is necessary to differentiate between action and motivation. There is no doubt that acts of hacking can have the international abuse of the information cyberspace must be a part of the terrorist campaign or an action.

Examples of cyber terrorist activity include the use of information technology to organize and carry out attacks, support groups activities and perception-management campaigns.

Thus, use of information technology and means by terrorist groups and agents constitute cyber- terrorism. Other activities, so richly glamorized by the media, should be defined as cyber crime.

Cyber Crime:

Cyber-crimes can be regarded as computer-mediated activities which are either illegal or considered illicit and which can be conducted through global electronic networks. The global connectivity of the internet, for example, makes it much easier for criminals to act beyond national boundaries to conduct their illegal affairs. It also makes it possible for existing organized crime to use more sophisticated techniques to support and develop networks for drugs trafficking, money laundering, illegal arm trafficking, smuggling and pornography, and the like. For hackers with the requisite computer skills, a large market exists for security and trade secrets which can be accessed and transmitted electronically. Furthermore, the numerous communication mechanism enables the production and worldwide dissemination of information and knowledge which could be potentially harmful, threatening or liable to incite violence.

Information War (IW):

The convergence of the technological and socio-political trends after the cold war area, suggests that cyber-terrorism may be the wave of the future.

Despite definitional disparities, the working definition used here is that information war is the action take to achieve information superiority by affecting: 1) adversarial information, 2) information-based processes, 3) information systems, 4) and computer-based networks while leveraging and defending one’s own information base. IW is also a deliberate and systematic attack on critical information activities which seek to exploit, modify, corrupt information or to deny service.

The important element to be emphasized is that of IW as attacks on information activities, not just information systems. The distinction between the two is important since the ultimate aim of an attack is to strike at the operational activities, or business processes, of an adversary. The information activities are what the target needs to carry out these business processes while the information systems are merely the physical and logical infrastructure that allow the information to be processed. Although these information systems are likely to be the immediate target of most IW, they are only the means, not the end.

Current concerns about the potential of IW has been fostered by the proliferation of information systems, in particular the convergence of computers and telecommunications that has deepened and broadened Information Infrastructures. These infrastructures are the focus of attention for Information Warriors. Infrastructures include the physical telecommunications and information processing systems, the software that runs cyberspace and the personnel that use and manage this infrastructure.

In any advanced nation it is common to define separate Defense Information Infrastructures and National Information Infrastructures. The latter is part of the Global Information Infrastructure. It is important to recognize however that in reality such discrete and well defined networks do not exist. Rather, Information Infrastructures are made up of myriad communications networks that interlink at many different levels and for which boundaries between civilian and military, national and international have little meaning.

B. IT techniques to use: Who, How and Why?

Following an explanation of the different terminology, one needs to look at what sectors are active in each of the categories. Here it is useful to distinguish between three classes of groups-hackers, criminals and politically motivated sub-state groups.

Hackers, or crackers as the computing fraternity prefers to call them, are in no way a homogenous group. Rather, the term refers to anyone with the technical skill to manipulate computer and telecommunication systems and in particular to subvert security mechanisms. As such, hackers provide the “ foot soldiers” for any sub-state groups interested in undertaking cyber-terrorist acts.

Hackers can usefully be divided into amateurs and professionals. The amateurs generally fit the conventional stereotype- youths with a fascination for the technical minutiae of computers and telecommunications systems. By definition, these hackers have led the way in the pioneering of digital attacks on information activities and, as

such have become a worldwide phenomenon.

Hacker attacks are however generally not intended to disrupt the information activities of the target but rather merely to explore information systems for the sake of curiosity. Even if the international aspect is not a predominant factor, it is still the case that amateur hackers have caused damage to the information activities of both governments and businesses. On the one hand, they have committed what are now defined as computer and telecommunications crimes. On the others, they have explored the propaganda applications of Information Technologies.

Professional hackers are different because of both their background and their motivation. Although some amateur hackers have crossed the line, the bulk of professional hackers have been nurtured by governments or businesses. Many, including former employees of the Eastern Bloc intelligence services, work on the open market and provide their services to sub-state groups. Clients include business intelligence firms engaged in industrial espionage as well as criminal organizations intent on outwitting police surveillance or on perpetrating electronic frauds.

Like their amateur counterparts, professional hackers have pioneered digital attacks on information activities.

Criminal groups, whether individuals confined to one city, or large, well-organized transnational groups, have exploited Cyber-terrorism. Secure and flexible communications are absolutely vital for them to conduct their activities and pursue their interests.

In the 1970s and 1980s, terrorists turned to hijackings and kidnappings to raise funds. With billions of dollars in electronic transit every day, cyberspace may provide a funding source that is both less risky and more profitable than conventional means of raising funds.

Examples of criminal sub-state group embracing new communication technologies was the Columbian drug cartels who established a sophisticated secure communications infrastructure, to protect their trading network. Others groups include hackers from different countries who may act in a very asymmetric strategy or just discontinued way.

Another case has emerged in the summer of 2006, when Authorities in Morocco and Turkey arrested two young people (F.E, 18, A. E, 21) thought responsible for a computer worm that infected networks at U.S[3]. companies and government agencies in

[3] This case is still in the court, so any information or accusation are based on just one source, so it is not at any level a confirmed criminal case. In that sense we are dealing with

august 2006. They are accused also for writing the Zotob and Mytob worms that caused computer outages at more than 100 US companies, including major media outlets like CNN, the New York Times and ABC News. . F.E is accused for writing the code that attacked computers that run Microsoft operating systems and A. E is for paying him for it. It's unclear that the two suspected persons they ever met, but they certainly knew each other via the Internet. According to Microsoft, the Zotob and Mytob worms "targeted a recently discovered flaw in the Plug and Play feature of Microsoft Corp.'s Windows 2000 operating system." Microsoft was aware of the threat and had a security update to protect against it. One only had to download the fix to protect their system from being hijacked by a remote user[4].
It is estimated that Microsoft's operating system has 90% of the world market. With that type of exposure, it is paramount that Microsoft provides for the tightest security. "The browser wars were never about security, the browser wars were about features.[5]"

Each new technical development in the Global Information Infrastructure meanwhile causes police forces to complain about the ingenuity of criminals- from the distribution of pirate software via Internet Relay Chat forums to the distribution of pedophile pornography by anonymous list serves on the Internet, and the use of money laundering techniques by various criminal organizations. For example Digital money can now be easily laundered through offshore banks, some of which may only exist in cyberspace.

The reality is more mundane, although the awareness of the technological opportunities is growing. In 1995, the Amsterdam police found themselves looked into an Information battle with hackers employed by a criminal organization. The hackers managed to cause serious disruption to the police investigation by hacking into their communication system, thereby gathering operational intelligence and disrupting their command and control net.

A number of documented cases have also emerged of criminals using hacking techniques to divert funds and extort money from companies.

Politically motivated sub-state groups is a term that covers the gamut from pressure groups in democracies using direct action tactics, through outlawed opposition movements in autocracies to organized paramilitary or terrorist organizations. Some of

---

the case in its general frame, and not concerned about who executed the operation.

[4] http://www.americanthinker.com/comments.php?comments_id=2953

[5] An interview with Microsoft's Steve Ballmer

these groups represent serious cyber-terrorism threats.

Like criminals, political radicals have a need for secure communications and for anonymous management of their funds. They also have a need for intelligence gathering and dissemination. Opposition movements in closed societies have seized on communication technologies to meet these needs. For instance, some exiled Islamic opposition movements based in Europe and the USA have set up World Wide Web(WWW) and E-Mail based information services that enable their informants in countries such Saudi Arabia, Iran and Pakistan, to transmit data which is then used for propaganda purposes.

Other cases include organizations like Sinn Fein, the Provisional Irish Republican Army's political wing, who have established Web sites where donations can be made on-line.

At this stage, there is little hard evidence on the use of the Internet as an intelligence tool by these groups, but they are becoming increasingly aware of the potential of the Internet as a source of Open Source Intelligence.

C- Beyond Hacking:

Terrorists are generally using the internet as Cyber Support to Terrorist Operations for planning, Recruitment, Research and Propaganda:

Planning

Terrorists use the cyber infrastructure to plan attacks, communicate with each other, and posture for future exploitation. Employing easy-to-use encryption programs that they can easily download from the Internet, terrorists are able to communicate in a secure environment. Using steganography, they hide instructions, plans and pictures for their attacks in pictures and posted comments in chat rooms. The images and instructions can only be opened using a "private key" or code known only to the recipients . Additionally, these encryption programs can scramble telephone conversations when the phones are plugged into a computer.

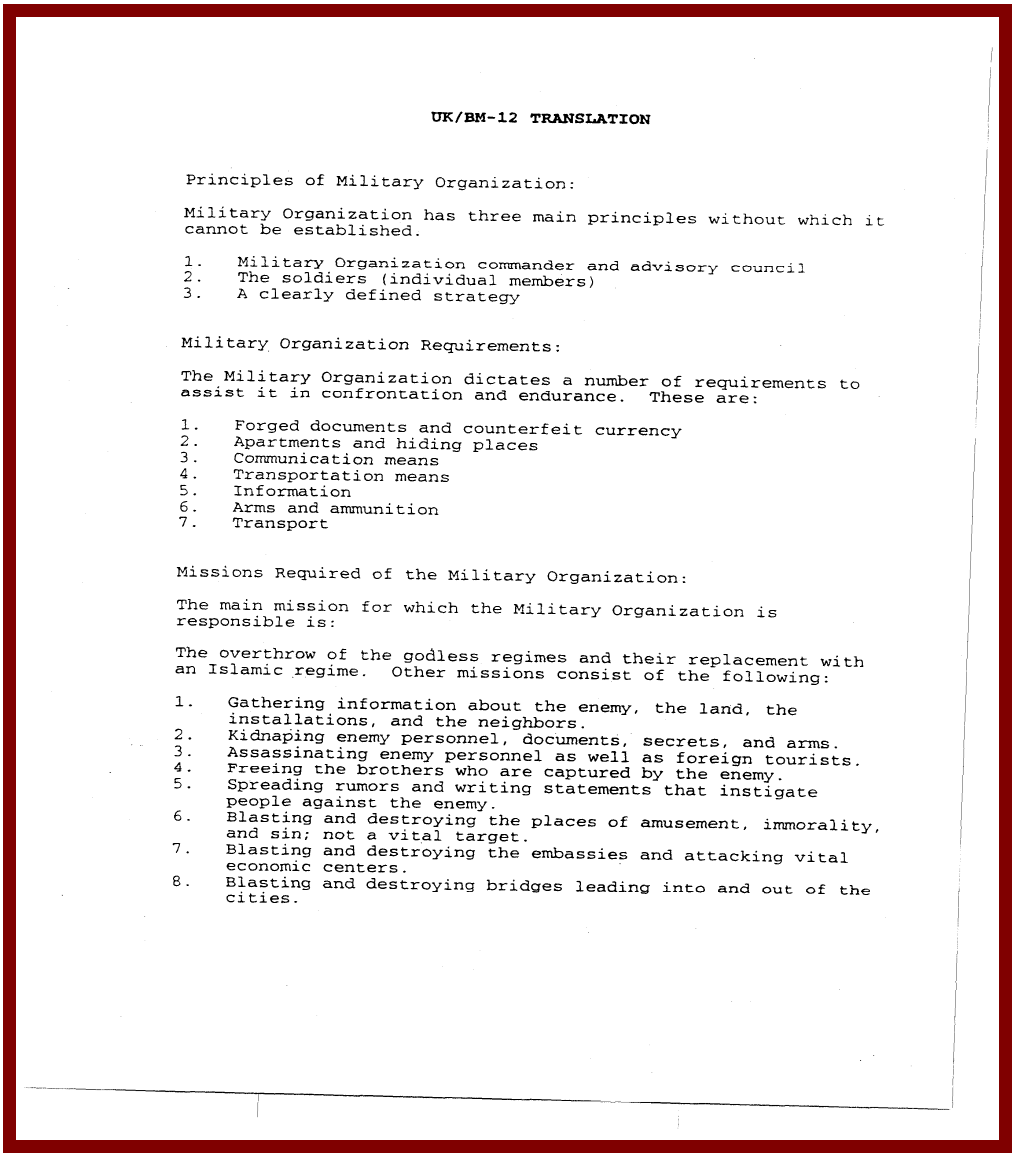
Recruitment

Recruitment is the life-blood of a terrorist organization and they use multiple methods to entice new members. In addition to traditional methods, such as written publications,

local prayer leaders, audio-video cassettes and CDs promoting their cause; terrorist groups also use their own websites to recruit new members. This is accomplished by providing their view of the history of their organization, its cause, and additional information to encourage potential members to join. Additionally, they often have hyperlinks to other material to encourage membership. They also use these sites to collect “donations” for their cause.

Research

Using the Internet, terrorists can tap into thousands of databases, libraries and newsgroups around the world to gather information on any subjects that they need to research. The information can be in the form of text, maps, satellite images, pictures or even video material. The use of search engines, such as Google, have made searching the Internet very easy and allows terrorists to obtain critical information located in the public domain using very simple resources. For example, by typing “Bombs” in the Google search engine, 2,870,000 references were found in 0.17 seconds. To narrow this list, typing “Bombs AND Homemade,” resulted in 47,200 references being found in 0.08 seconds. Although most of these are harmless references that may just refer to news articles, many provide detailed information on how to manufacture bombs.
To highlight the importance terrorists place on research over the Internet, an al Qaeda training manual recovered in Afghanistan states: “Using public sources openly and without resorting to illegal means, it is possible to gather at least 80% of information about the enemy.": (See a translated sample-page of the document)



UK/BM-12 TRANSLATION

Principles of Military Organization:

Military Organization has three main principles without which it cannot be established.

1. Military Organization commander and advisory council
2. The soldiers (individual members)
3. A clearly defined strategy

Military Organization Requirements:

The Military Organization dictates a number of requirements to assist it in confrontation and endurance. These are:

1. Forged documents and counterfeit currency
2. Apartments and hiding places
3. Communication means
4. Transportation means
5. Information
6. Arms and ammunition
7. Transport

Missions Required of the Military Organization:

The main mission for which the Military Organization is responsible is:

The overthrow of the godless regimes and their replacement with an Islamic regime. Other missions consist of the following:

1. Gathering information about the enemy, the land, the installations, and the neighbors.
2. Kidnaping enemy personnel, documents, secrets, and arms.
3. Assassinating enemy personnel as well as foreign tourists.
4. Freeing the brothers who are captured by the enemy.
5. Spreading rumors and writing statements that instigate people against the enemy.
6. Blasting and destroying the places of amusement, immorality, and sin; not a vital target.
7. Blasting and destroying the embassies and attacking vital economic centers.
8. Blasting and destroying bridges leading into and out of the cities.

Propaganda

Propaganda is a veritable terror group standard. Terrorist organizations depend on the backing of a broad base of support for both recruiting and funding. They use propaganda to discredit their enemy while making themselves look good. Earlier terrorist groups published newspapers and leaflets to spread their propaganda. Although this form of media is still widely used, terrorist groups are now using the Internet[6].

---

[6] Christopher C. Harmon, *Terrorism Today* (London: Frank Cass Publishers, 2000; reprint, Portland: Frank Cass Publishers, 2001), 55

الحق بالقافلة

بقلم: الدكتور عبد الله عزام

مقدمة الطبعة الأولى

الحمد لله رب العالمين والصلاة والسلام على أشرف المرسلين وبعد:

فهذه رسالة صغيرة كتبتها للذين يتحرقون للجهاد ويطمعون في الشهادة في سبيله، وهي من فصلين:

أولهما: مبررات الجهاد.

ثانيهما: والإسلاماه.

وختمتها بخلاصة وملاحظات.. نرجو الله أن ينفع بها وأن يصلحنا ويصلح بنا.. إنه سميع قريب مجيب.

وقد أملتها علي رغبة في الرد على كثير من الرسائل التي تصلني تستشيرني بالقدوم إلى أفغانستان:

فحي على جنات عدن فإنها منازلك الأولى وفيها المخيم

ولكننا سبى العدو فهل ترى نعود إلى أوطاننا ونسلم

العبد الفقير

عبد الله عزام

(71) شعبان (7041هـ)-(51) نيسان (7891م)

A book of Abdullah Azzam (the Godfather of Osama Ben Laden) published online by a group of al-Qaeda in Peshawar (in 2001) for Propaganda and Recruitment.

It is stillto say that the best publicized use of CYBER-TERRORISM by opposition groups has been propaganda. Many have established Web sites, Email, news services and fax broadcasts. The range of opposition groups using these technologies include groups from Iraq, Saudi Arabia, Northern Ireland, Mexico and the USA. Information techniques now supplement older methods such as radio, leafleting, distribution of audio and video cassettes and even newer ones such as satellite TV.

On occasions, pressure and political groups generate publicity by hacking Web pages of official bodies or economic and financial institutions. Further developments in the sophistication of such opposition activities are to be expected.

While violent opposition groups will continue to go after their traditional sets-politicians, members of the security forces, innocent civilians, the physical and

economic infrastructure of the state, the increasing importance of the Information Infrastructure means that they now have a new target set.

What type of targeted would depend on the particular aims of the group in question. A single issue protest group, such as anti-Israeli occupation protesters or human rights activists, may want to interfere with the information activities of individual contractors. An insurgent group may want to threaten the information activities of a company in order to extort funds. A guerilla force may seek to disrupt the information activities of the state's armed forces and their supporting logistical infrastructures. At the highest level, an insurgent or terrorist group may seek to carry out strategic Information Infrastructure Warfare. Such a campaign would involve the disruption of critical nodes of the National Information Infrastructure which would harm the national economy and national security.

D. The Black Scenario

The entertainment industry, in the form of films and novels, has popularized the notion of an electronic Black scenario in which sub-state groups manage to penetrate critical nodes of the National Information Infrastructure and Defense Information Infrastructure and are able to, variously, launch nuclear weapons, crash the telephone system, cause mayhem on the railways or in the air, or bring the financial sector to a catastrophic halt.

In order to target the National Information Infrastructure, however the sub-groups would have to transfer its intelligence skills onto a new terrain. In order to conduct such an analysis against either a portion of the National Information Infrastructure, say the communications infrastructure, or against the whole system, these groups would have to invest heavily in a lengthy and detailed nodal analysis process. This would include indentifying key nodes in the National Information Infrastructure, using a six step process:

1. indentify potential nodal targets,
2. classify them,
3. assess linkages between them,
4. determine the criticality of each node,
5. determine the vulnerability of each node and assign a priority to each target. Once accomplished,
6. a prioritized list of targets with the most critical and vulnerable ones highlighted. While much of the information could be gleaned openly, it would also require a

fair amount of covert intelligence gathering and a high degree of technical expertise.

At the same time, the lack of hardening of most of the National Information Infrastructure means that more traditional ways of attack such as subversion and physical violence could already accomplish a great amount of their objectives.

However, one of those group's problems in its attempts to disrupt the national infrastructure has been the inadequacy of its weapons, which have often failed to perform their designated function. These weaknesses may tempt the oriented groups to use digital attack methods against critical nodes. The aims of such software warfare could range from merely penetrating a system and monitoring activity to denying service by deleting data or shutting down an information system. Mounting such an attack would require three stages, once the critical nodes had been analyzed. First, access would have to be gained to the information system. This could be done by hacking from a remote site or by gaining access to the site through subversion or infiltration. Second, the network of the node would have to be mapped in detail. Third, an appropriate software weapon would have to be released.

The advantages of a digital attack over a physical attack are obvious. If it can be implemented from a remote site then the chance of detection is much smaller. The attack can be more flexible than a brute force physical attack and can be programmed to occur at a certain time or only if a logical condition is met. Furthermore, leverage can be much greater than for a physical attack. Placing bombs simultaneously takes at least one operative per location. Inserting a destructive virus or worm into hundreds of networked computers at dispersed sites my take only one operative on the other side of the world.

There are however, three key-drawbacks in terms of terrorist groups using digital offensive techniques. First, the technical expertise to hack into a site, plan an attack and design attack weapons is not easy to come by. Although the dedicated Internet surfer can easily download digital weapons and provide tips on hacking, the number of highly skilled hackers on the market is limited.

Second, the fact that these groups are extremely concerned with Operational Security makes them reluctant to allow outsiders close to its intelligence and planning functions. If planning an assault on the National Information Infrastructure, those groups' operators will be very wary about allowing a hired hacker to work closely with them. For fear of exposing their entire operation, this is , of course, not an insoluble problem, and there are already hints that the organization has dispatched trusted personnel on training course.

The third drawback is perhaps the most significant. Many senior officers in regular armed forces are notoriously reluctant to embrace the concept of CYBER-TERRORISM and to recognize the threat to their Command, Control, and Communications systems.

To conclude here, Sub-state groups have embraced the information revolution as has the rest of society. Going a stage further and attacking the National Information Infrastructure can certainly be an attractive option for sub-state groups, However, to inflict even a portion of the disruption that the doomsday mongers suggest would require a tremendous investment in IPB, not to mention actually implementing assault. More technology-savvy groups such as environmental protesters may in fact be the first to use offensive CYBER-TERRORISM techniques but they will have limited aims and not pose a national security threat. It is likely to be some time yet before professional cyber-terrorists become a significant CYBER-TERRORISM threat.

The main areas exposed to challenges by cyber-attacks are:

1- Computer Network Break-ins	Using software tools installed on a computer in a remote location, hackers can break into computer systems to steal date, plant viruses of Trojan horses, or work mischief of a less serious sort by changing user names or passwords.
2- Industrial Espionage	Corporations, like governments, spy on the enemy. Networked systems provide new opportunities for this, as hackers-for-hire retrieve information about product development and marketing strategies, rarely leaving behind any evidence of the theft. Not only is tracing the criminal labor-intensive, but convictions are hard to obtain when laws are not written with electronic threat in mind.
3- Software piracy	According to estimates by the U.S. Software and Information Industry Association, as much as US$7.5 billion of American software my be illegally copied and distributed annually worldwide. These copies work as well as the originals and sell for significantly less money. Piracy is relatively easy and only the largest rings of distributors are usually caught. Moreover, software pirates know that they are unlikely to serve hard jail time when prisons are overcrowded with people convicted of more serious crimes.
4- Pornography	Pornography could be seen here in two different angles:] Minor pornography which is one crime that is clearly illegal, both on and off the internet. While Crackdowns have resulted in the apprehension of sexual images of minors will continue to be available and accessible. Legally speaking, people who provide access to pornography involving minor face the same charges whether the images are digital or on a piece of photographic paper.
Mailing bombings	By instructing a computer to repeatedly send electronic mail to a specified person's email address, the cyber criminal can overwhelm the recipient's personal account

	and potentially shut down entire systems. This may at this stage not be illegal, but it is certainly disruptive.
Password sniffers	These are programs that monitor and record the name and password of network users as they log in, jeopardizing security at a site. Whoever installs the sniffer can then impersonate an unauthorized user and log in to access restricted documents. Laws are not yet set up to adequately prosecute a person for impersonating another person on-line, instead law designed to prevent unauthorized access to information may be more effective in apprehending hackers using sniffer programs. *The Wall Street Journal* suggests in recent reports that hackers may have been successful in gaining access to the passwords used by members of America Online, a service with around 4 million subscribers.
5- Spooting	Spooting is the act of disguising one computer to electronically " look" like another computer in order to gain access to a system that would normally be restricted. Legally, this can be handled in the same manner as password sniffers, although again, current legislation is proving to be insufficient.
6- Credit Fraud	The U.S. Secret Services believes that half of a billion US$ my be lost annually by consumers who have credit card and calling card numbers stolen from on-line databases. Security measures are improving, and traditional methods of law enforcement seem to be sufficient for prosecuting the thieves of such information

II. The implication for National Security

Having outlined the various facets of cyber-crime and cyber-terrorism, it should be cleat that a very real possibility exists that either domestic or foreign terrorist could in the next few years cause massive disruptions to information systems and networks. Attacks have already shut down Internet service providers across countries several times and there have been hundreds of thousands of attempted intrusions into military systems in recent years.

Further a successful attack could cause massive failure of such crucial elements as banking and the financial markets, transportation systems, the power grid or telecommunications network. While experts previously estimated that such a prospect was 10 years away, they are now revising their estimate to no more than a few years.

While the threat from cyber-crime or cyber-terrorist actively appears to increase exponentially private industry and government are at odds as to who should take the lead in managing cyber security. Whatever the case, counter Cyber-terrorism has to focus on eight vital areas, most of which are owned by the private sector: banking and financial services, telecommunications, electric power, oil and gas delivery, transportation, water, emergency services and government services.

In earlier forms of warfare, railroad junctions and communication systems were

bombed to confound the enemy's ability to transport equipment and transmit commands. Today, they can be rendered just as inoperable by a modern-equipped PC.

Information warfare (IW)can encompass everything from electronic jamming to psychological operations. The focus here is on the defense against the deliberate exploitation of information systems' inherent vulnerabilities in a manner that affects national security. The reality of information warfare is that all systems are vulnerable. As states grow more dependent on information systems, vulnerabilities will increase.

These weaknesses are compounded by the fact that military and civilian information systems are intimately linked. Before 11th September Railroads and airlines in most countries, for example, were controlled by relatively penetrable civilian systems, and much of the military's unclassified message traffic travels on the internet. In all types of cyber attacks in general and of Cyber War in particular, civilian information systems can be critical as military systems, and any effort to built a truly secure national information system will require close cooperation between business and government.

Cyber attacks requires a small capital investment to achieve tremendous results. The necessary computer equipment is easily obtained and is becoming less expensive every day. A team of computer mercenaries could be hired for less than the cost of one fighter aircraft. Information warfare can also be carried out remotely. A state or terrorist organization could easily disperse its operatives around the world making it difficult to pinpoint any attack and retaliate. The bottom line is that information warfare is cheap, effective and well within the reach of almost any state or well-endowed terrorist organization.

The vulnerabilities of military information systems are obviously an area of paramount concern. Most of the more than 250,000 attacks on U.S. military information systems each year fail, but a few successes can cause widespread damage. For example, in 1994, Air Force computer security experts discovered that their classified network at the Rome (New York) Laboratories had been breached. A subsequent investigation revealed that the hackers had gained complete access to all Rome Labs networks, and had breached other linked classified sites, like the South Korean Atomic Research Institute. This latter problem illustrates of the most serious problems of network security: once a hacker has found a valid ID and logon, he can transfer to other sites that might be better defended. The security of an information system is only as good as its weakest link.

Identifying the intruders was virtually impossible because they skillfully manipulated the phone system and ran their connection through multiple locations from New York to Latvia. While the intruders' computer code names – Datastream and Kuji –

were discovered, their identities remained secret until an informant revealed an e-mail conversation with a British hacker who bragged about his exploits in Rome Labs and left his phone number with the informant. A tap was put on the line and he was subsequently arrested. Datastream turned out to be a sixteen year-old armed with nothing more than a 486sx PC. Had he been a bit more mature, like his colleague Kuji who remains at large, he could have ended up doing devastating damage rather than just gaining access. If one teenager with fairly unsophisticated equipment can penetrate supposedly secure systems, consider the damage that ten or twenty equally skilled individuals could do in the employ of a rogue state or terrorist organization. The PC may thus become one of the most dangerous components in the terrorist's arsenal.

If military sites can be compromised, civilian networks are even easier to crack. Financial institutions are reluctant reveal information concerning systems intrusions for fear of sparking a panic, but such incidents appear to be relatively common. In 1994, for example, Citibank lost $ 400,000 to a group of Russian hackers, who were attempting to steal millions. A survey of computer security companies by the Senate Subcommittee on Investigations revealed that their corporate clients in the United States had lost $400 million last year alone. It is impossible to estimate the additional loses in comparative advantage due to computer industrial espionage.

To date, no clear government strategy for information security exists. A host of government agencies and informal public-private groups have been convened to discuss this problem, but actual results are minimal. In addition, efforts to comprehensively protect the entire information infrastructure faces the strong opposition from various sectors, including industry actors who are reluctant to encourage government intrusion. The present battle over encryption- which pits civil liberties advocates and law enforcement officials who hope to " tap" information networks- is another example. In today's rapidly changing technological environment, therefore the prospects for extensive government-industry cooperation remain limited.

The movement toward a plan to protect the National Information Infrastructure has yet to move past the theoretical stages. The information technology revolution spawned both tremendous promise and new threats. At the moment, however, the means of coping with the potential threat is barely in formation. While the recent attempts to secure the National Information Infrastructure appear to be a good start, they may ultimately prove to be a case of too little, too late.

III. Moroccan Strategic Capacities in IT and Cyber-space:

A- The Technical Capability and IT infrastructure in Morocco:

The Institute of Engineering El-Mohammadia in Rabat, was the first host site in Morocco to offer internet access in 1993, and offered a dial-up access through Paris (EUnet). Later this institute handled registration and technical support. By the sponsorship of PNUD, the ONPT established a leased line at 256K of speed of data transmission per second to the U.S. Offering full internet connectivity and started to sell Internet access directly to users or to small providers to resell to personal users or enterprises. In 1996, there were only six private companies authorized to provide Internet services including the representing of MCI Mail and the Morocco Trade & Development Services (MTDS).

In 1996, Internet users had to register for a personal identification from Ittisalat al-Maghrib (ONPT) which cost U.S.$33 per month, in addition to an annual $160 for IP account from the provider. Software for E-mail and Net almost cost about $300-400. The Set-up costs about $1.300-1.800 for companies and about $400-750 for individuals. For traffic charge users paid an average of 250-350 Dirhams.

At that time, the number of Internet users in Morocco was still very low, and did not surpass1000 personal users, and about 800 institutional users. But the phenomena of Internet Coffee-Shop absorbed many customers from those who are unable to cover the expenses of personal Internet setup.

From a social point of view, Personal Users were mainly those who are involved in International activities (research, business), or those attached to some inter-governmental responsibilities. This situation deals with three elements:

- The Net cost: to become a personal user requires : a computer, a modem, a telephone line, in addition to The daily, monthly, and annual cost of Internet access, setting, and dial-up.
- The lack of the basic knowledge on Computer using, setting, mainly in a developing country where problems related to frequency, cause many Net- cut or shut-off during uploading or downloading.
- The proxy system which reduce the marge of free access and free up-download actions

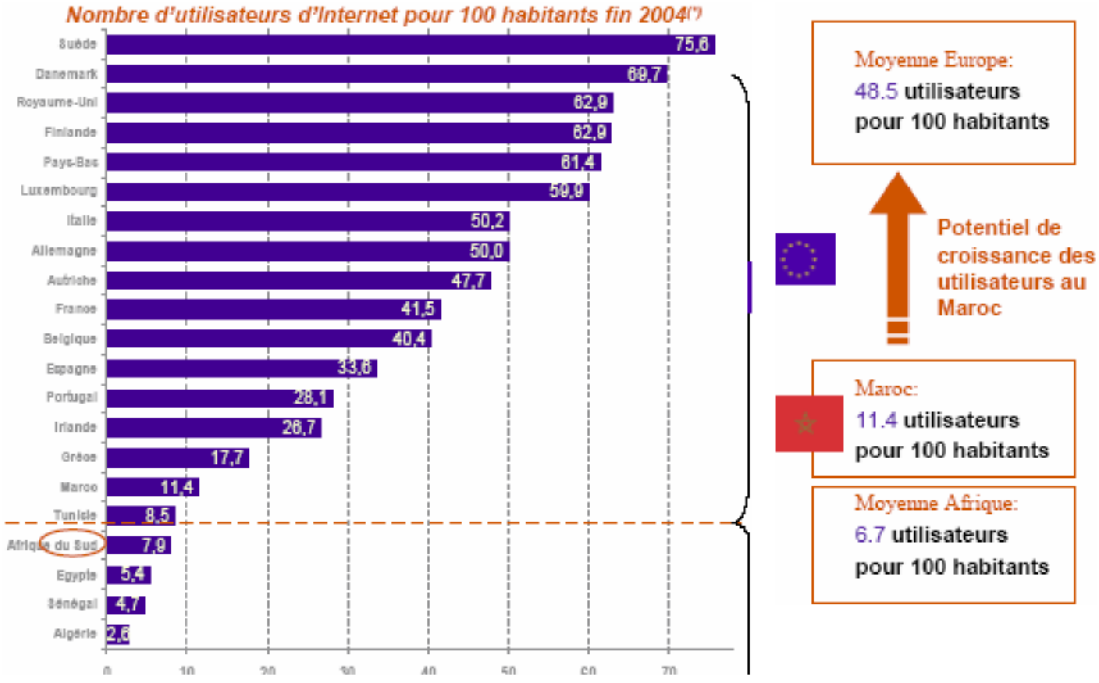
In 1996, MTDS had only 160 clients, however after two years later Ittisalat al-Maghrib succeeded to increase its customers after the decrease of the annual & the monthly cost.

Telephone services were either not available, or where available, the quality of the service was poor. The absence of basic telephone service restricts the availability of value added services such as the Internet. The Internet and basic e-mail services are only as good as the available telephone network.

Literacy is another element that made internet using a very prestigious field, that only a new category of educated people use.

Parmi les perspectives de développement de l'Internet au Maroc on peut citer les opportunités suivantes :

- by the new operators as Méditel and Morocco Connect did not lack activating the market of the Internet for individual users and to reinforce the competitiveness of Moroccan enterprises through the reduction of the costs, the improvement of the offers by package targeted to enterprises and the improvement of the quality of the services, were an additional assets to make Moroccan telecommunication market an attractive area.
- Internet in Morocco has strong growth potential insofar the number of users was has strong increasing between 2002 and 2004 , and jumped respectively from 700.000 to 3 millions. In spite of this development, some promising perspectives offer themselves since the Internet users doesn't pass 11,4% whereas the average of in Europe is of 48,5%.



Source UIT

The Human Capacity and Cyber-Community

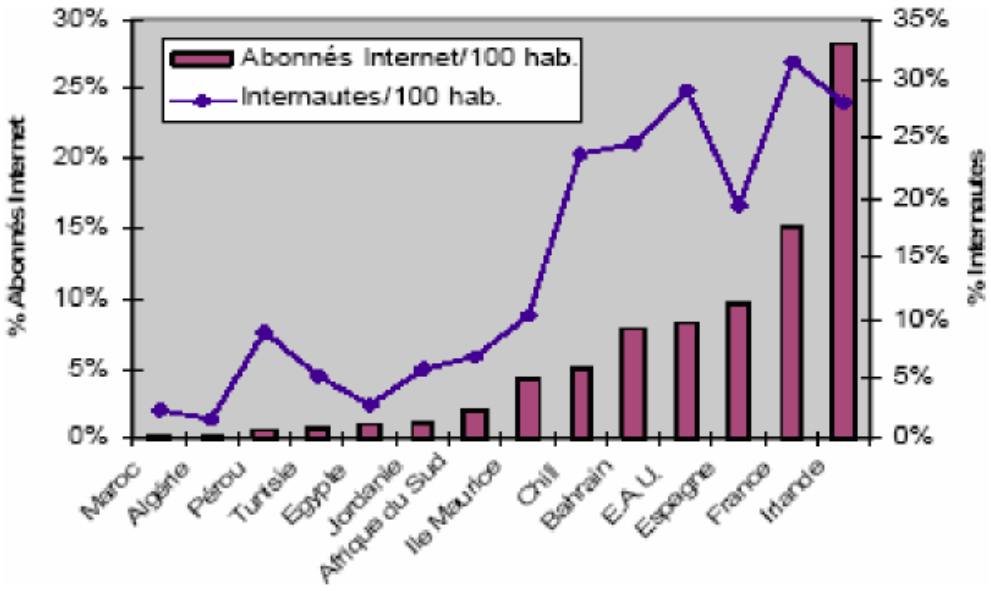
The level of Internet subscribers has experienced a clear progression between 2000 and 2005 by progressing from 37.000 subscribers to 206.452 to September end 2005 , which

is a yearly growth of 41,03%. This evolution is due to the advent of the ADSL that made evolve the Internet level between 2004 and 2005 to 128%.

Concerning enterprises, it is about 90% of the enterprises listed in the KOMPASS year Internet connection. One the other hand, among the concerned enterprises, 38% declared to have Web site and only 14% announced to resort to on line purchases. Concerning the uses of the Internet in enterprises, it concerns the B to B (business to business) rather than the e-trade.

Concerning households, the average of equipment of microcomputers is of 11%; the equivalent of some 600 000 units. This average is of 3% in electrified rural al areas. Otherwise, 64% of the Moroccan didn't ever have access to computer[7] .

Morocco is still far from its potential of Internet market development that is valued to about 500 000 subscribers..



Source : UIT/SITICOM (2002)

Internet Dimension in Morocco:

Strengths

- Presence of two innovating FSI in the market, and which are proposing the panoply of offering of access to Internet products, notably in term of method of access;

[7] Source based on ANRT estimation

- Availability of an infrastructure telecom relatively modern;
- Awareness of needs in national content, without which the market of the Internet would not be developed.
- non monopolization of the fix that would accelerate the competition in the market of the Internet while having some repercussions on the users: improvement of services and quality and reducing the cost of Internet products;[8]

Weaknesses

- Weak rate of equipments in fix telephone lines thus for PC there is a weakness in the spending power among consumers. This situation causes reducing the market potential thus ready to subscribe to Internet offers;
- lack of communication on the existing content, and especially with regard to the actions accomplished in the setting of the projects e-government.
- Strong rate of illiteracy especially in rural areas;
- lack of sensitization on the utility of the Internet, mainly in some critical sectors for the market development as education and economic enterprises.
- Weakness of content in Arabic language[9].

Risks

- Continuity of monopoly on fix services, with the same undesirable effects on the market, and more specifically on the FSI, either by their dependency upstream (transit international IP) or down-stream (Local Buckle) in front of opposite historical operator;
- Acceptance of fatalistic attitude on the weak evolution of the Internet under pretext that market potentiality development of the Internet doesn't exist;

• Increase of the digital divide at the national level with a majority of homes of strong incomes who are subscribers to the ADSL, and the others who are unable to host personal subscribing at home, and they are addressing to Cybercafés as only means of connection.

- growth in the quality of terrorism human resources capability, against a lack of a strong national security infrastructure; elements that may affect all projects related to the knowledge economy[10].

---

[8] Internet au Maroc: Etat des lieux et perspectives de développement. *Direction des Études et des Prévisions Financières, Ministere des finances et de la privatisation, Mars, 2006*

[9] Internet au Maroc: Etat des lieux et perspectives de développement

[10] Internet au Maroc: Etat des lieux et perspectives de développement.

Internet Dimensions in the Arab World:

Pervasiveness: After a late start, the Internet grew rapidly in the Arab world, where it has been accepted as an adjunct to other communications media that enable the international business that is the lifeblood of the cities. Almost four in every ten persons has an Internet account in the Arab United Emirates, and the penetration is likely to increase to more than 50 percent during 1999-2002.

Geographic Dispersion: The Internet is highly dispersed in the area. There are access nodes in every major political division, although the interface between Telecom and other providers is located in the major cities city. There are several emerging providers which are geographically dispersed although all are located in Rabat, Casablanca and some in northern cities.

Sector's Absorption: Take-up of the Internet has been concentrated in the commercial sector. Although most public sector agencies and companies are increasing in term of connection, the Internet has not permeated their daily operations to the extent that is common in the business community. Most of the country's universities have local area networks connected to the Internet: Primary and secondary education are currently not on-line. There is a little participation by the health sector in the Internet.

Organizational Infrastructure: with the increasing fairly robust physical infrastructure and wide customer base, there are still debates about the privatization of telecommunication services and its effect on information nation security, but alternatively that would increase competition and allow in certain valued-added services, so far no concrete plans have been announced yet.

Sophistication of Use: The level of application of the Internet increasing due to the high level of interest in and active use of the Internet. The " killer application " remains electronic mail, but both public and private organizations are becoming increasingly sophisticated at using the Web to promote local products and services and conduct research worldwide.

Censorhip:

When first opened, the internet service in Morocco, it was offered by a direct link to the Internet, but public concerns were soon voiced about radical groups, pornography and other inappropriate material. After may, the 16th , Moroccan authorities has increased the use of proxy server which was approved and implemented over the next years. Subsequently, installing remote proxy servers on leased lines, including the Cyber Cafes was initiated and expected to improve in the next Infra-server generations.

Next to the security dimension there are also other barriers against the advancement of IT use in Morocco. With the rapid expansion of the Internet services in the region, the discussion has reached up at times. Half of the concerns revolve around three specific are as: political, cultural as well as linguistic issues.

Political:

The political dimension, centers on propaganda that some countries, organized groups, or oriented figures launch their online messages. This could include a Hacks against the governing elite, disinformation related to vital issues of national security or the spread of radical political discourse in the hope of influencing young people and intellectuals and as a way to disrupt the stability of the country. Radical Islamic groups are at the top of the list in terms of making use of the web for such purposes.

Cultural:

In reference to the censorship of information on the internet, there appears no resolution in sight in this much publicized debate. The key issue revolves around the argument whether or not censorship is necessary to maintain a particular moral standard. Issues such the exposure of pornography is particular sensitive in a society that place religious values on providing a good and balanced environment of socialization

In addition there are at least five factors which account for the recent explosion of pronography via computer networks :

- Consumers enjoy considerable privacy on computer networks and can easily avoid the potential embarrassment in the public.
- Consumers have the ability to download selectively.
- Easy discrete storage of product on a computer enables consumers to conceal them from family members, friends or associates.
- The prevalence and fear of sexual transmitted disease has helped pornographers to successfully market what is named now in sociology

“ modern sex” and “ autoeroticism “ as sage and viable alternatives the danger of “ real sex”.

- New and highly advanced computer technologies are quickly being absorbed into the mainstream, permitting an every-expanding audience to gain access to digitized pornography available on the “ information superhighway”.

Linguistic:

English is the leading language on the Internet, with 192 million English speaking mass as of December 2000. The fact that the web in English dominated provides numerous differentiate for speakers of other language to access and use of information available on-line. For Arabic, there are additional technical obstacles in the terms of the arabization of the interfaces of Internet applications. In Morocco, the problem is more complicated since we are facing the problem under the international monopoly of English, and the regional and domestic monopoly of French

The Threat of Cyber-Attacks in Morocco and its regional environment:

Most of Arab Governments are recognizing the need to protect their information and critical infrastructures in light of the increased use and dependence on information technologies. In addition there is a realization that it is not sufficient to address only the local or national aspects of safeguarding information and critical infrastructures. Because attacks against the Internet typically do not require the attacker to be physically present in the site of the attack, the risk of being identified is significantly reduced. Besides the technological challenges this presents, the legal issues involved in pursuing and prosecuting intruders adds a layer of difficulty as they cross multiple geographical and legal boundaries. An effective solution can therefore only come in the form of regional and international cooperation.

Terrorism continues to appeal to its perpetrators for three principal reasons:

- It appeals as a weapon of the weak- a shadowy way- to wage war by attacking asymmetrically to harm and try to defeat an institutional body which is superior in size and structure. Terrorism has particular appeal to ethno-nationalists, racist militia, religious fundamentalists, and other minorities who can not match the military formations and firepower of their

“ oppressor”. The case of Hezbollah in Lebanon or Islamic Jihad and Hamas in Palestine vis-à-vis Israel, the provisional Irish Republican Army (IRA) vis –a vis Britain, are two models of such groups who were involved in using Cyber-terrorism as a way of fight.

- Terrorism enables a perpetrator to publicize and project his identity, and touch the nerves of powerful distant leaders. If mainstream revolutionary groups may view violence as a means of struggle such as the Palestine radical groups, then this kind of attraction to violence as an end in itself generates identity or damages the enemy’s identity. The GIA in Algeria is one model of such category. Al-Qa’ida has moved from the militia group to the category of those who believed in violence as a target itself.
- Terrorism is still seen as a way to achieve a new future order by willfully wrecking the present. The substance of the future vision may be only vaguely defined, but its moral worth is clear and appealing to the terrorist. This is manifest in the religious fervor of some radical groups such the Jama’a Islamiya in Egypt, as well as among millenarian and apocalyptic groups, like the Aum Shinrikyo in Japan. Their ultimate aim is wreak havoc and rend a system asunder so that something new may emerge from the cracks.

In terms of all these different categories, terrorists will continue moving from hierarchical toward information-age network design. Within groups, leadership will give way to flatter decentralized designs. Terrorists will likely gain new capabilities for lethal acts. Some terrorist groups are likely to move to a war paradigm that focus on attacking National or any other government’s military or civil infrastructures. But where terrorists suppose that “ information operations “ may be as useful as traditional commando-style operations for achieving their goals, systemic disruption may become as much as objective as target destruction. New difficulties in coping with the new terrorism will mount if terrorists move beyond isolated acts towards a new approach to doctrine and strategy that emphasizes campaigns on swarming. Terrorists are likely to increasingly use advanced IT for offensive and defensive purposes, as well as to support their organizational structures. Despite widespread speculation about terrorists using Cyber-space warfare techniques to take the Net down, they may often have stronger reasons for wanting to keep it up to spear their message and communicate with public operate between each other.

In the Arab world, Islamic groups such as Ansar as-Suna in Iraq or Qaeda network consist of groups organized in loosely interconnected, semi-independent calls

that have no single commanding hierarchy. Ansar as-Suna exemplifies the shift away from a hierarchically oriented movement based on " a great Leader". Netwar- as a frame of all types of cyber-terrorism- is consistent with patterns and trends in the Middle East, where the newer and more active groups appeal to be adopting decentralized, flexible network structures. The rise of networked arrangements in terrorist or radical groups in general is part of a wider move away from formally organized, state-sponsored groups to privately financed, loose networks of individuals.

In February 1998, the Pentagon detected several root-level intrusions into US Air Force and Navy computer networks. These intrusions, which appeared to be organized, rased fears that hackers were working for governments trying to disrupt the military's Internet-based communications and gain access to unclassified material on U.S plans and capabilities in the Gulf. As would later be found out, the intruders hid their tracks by routing their attack through computer systems in the United Arab Emirates. They accessed unclassified logistics, administration, and accounting systems that control US ability to manage and deploy military forces.

The attack took on a level of significance due to the fact that U.S. was involved in a stand off with Iraq because of Iraqi non compliance with UN inspection teams. Thus the precise timing of the attack raised concern that the intrusions were part of a larger cyber attack in conjunction with local tensions.

The disturbance was tracked to a building in Abu Dhabi, leading to the assumption that this was Saddam Hussein waging information warfare against U.S. in advance of some sort of military action. However as it turned out, the attack was launched by teenagers in Seattle, Washington[11].

To be sure, increased use of IT by the business community in Morocco as well as the potential for expose the present infrastructure to numerous challenges transnational attacks.

Under the requirement of Moroccan involvement in EUROMed partnership, Morocco has the obligation to be integrated into the wired world of information technology protecting computer systems against outside attack, either by commercial rivals, the simply curious or the electronic vandals who like to wreak havoc with commercial and government systems, becomes vital.

But it is not just big business and government that has to worry about hacker

---

[11] see: James Adames : "The Next World War, " in Computers are weapons in potential cyber attacks, by Susan Ellis/ published in http:www.fas.org/irp/news/ 1998/08/98082502__ ppo.html

attacks or cyber-terrorist attacks. Any Windows computer on the Internet can be affected by a cyber attack.

General Recommendations:

To protect the country from such non conventional threats, the governments is required to work on the following issues:

- A national framework for government –industry cooperation.
- An information and analysis warning center that would collect incidents of computer security breaches, broadcast the problem, and provide solutions to fix problem areas to industry and government agencies .
- Anonymous reporting methods- thus allowing companies to avoid public loss of confidence and minimizing threats of a competitor abusing the weaknesses.
- Enactment of legislation allowing private companies to conduct criminal, personal and psychological background checks – which some states now bar or limit- when hiring computer experts for sensitive positions.
- Promote a research project to research and coordinate these efforts.
- Create a Cyber-police that could deal with the specifies of cyber-cases either those related to crime or terrorist activity.