Information technology breeds new age terrorism

Amita Aziz

Follow this and additional works at: https://repository.rit.edu/theses

Recommended Citation

This Thesis is brought to you for free and open access by the RIT Libraries. For more information, please contact repository@rit.edu.
Information Technology Breeds New age Terrorism

By

Amita Aziz

Thesis submitted in partial fulfillment of the requirements for the degree of Master of Science in Information Technology

Rochester Institute of Technology

B. Thomas Golisano College of Computing and Information Sciences

September 2002
I, Amita Aziz, hereby grant permission to the Wallace Library of the Rochester Institute of Technology to reproduce my thesis in whole or in part. Any reproduction must not be for commercial use or profit.

Date: 8/30/02  Signature of Author: __________________________
Student Name: Amita Aziz

Project Title: Information Technology Breeds New Age Terrorism

Thesis Committee

Name           | Signature | Date
---             | ---       | ---
Prof. Rayno Niemi |           | 9/3/2002
Chair

Prof. Rudy Pugliese |           | 9/5/2002
Committee Member

Prof. Alec Berenbaum |           | 9/6/2002
Committee Member
ABSTRACT ................................................................. 1

INTRODUCTION ............................................................ 2

TERRORISM .................................................................. 6

Definitions ..................................................................... 6
There are several other definitions available and some are as follows: ........................................ 6
Forms of terrorism............................................................. 7
Evolution of International terrorism........................................ 8
Past terrorist attacks as enlisted by the United States Embassy on October 8th, 2001........... 8

INFORMATION AGE TERRORISM .................................... 30

INFORMATION WARFARE ............................................... 32

Attractions of Information Warfare......................................... 33
Information Warfare proves Advantageous to Terrorism........................................... 38

CYBER TERRORISM ......................................................... 40

Definitions ..................................................................... 40
Advantages of Cyber terrorism.................................................. 41
Levels of cyber terror capability............................................... 43
Cyber Attacks that have occurred in the past.................................. 43
Al-Qaeda organizations Cyber Capabilities.................................. 45
Cyber Attacks during Gulf War................................................ 46

NETWORKED TERRORISM ............................................... 49

Netwar ............................................................................ 50
Communications................................................................... 54
Connectivity........................................................................ 56
Propaganda......................................................................... 57
Sample of the websites belonging to the terrorist groups:...................................................... 60

INFORMATION TECHNOLOGY TOOLS USED BY TERRORISTS ............................................. 61

Encryption ........................................................................ 61
PGP ................................................................................. 62
E-Mail Bombs ..................................................................... 64
Flight Simulator................................................................. 67
History of Flight Simulator.................................................... 68
Steganography..................................................................... 70

INFORMATION TECHNOLOGY TO COUNTER TERRORISM .............................................. 73

New IT for detection, prevention, remediation, and attribution of attacks................................. 74
Technologies to Address Future Passenger Screening Requirements ........................................ 79
Research required for effective deployment of Information Technology ........................................ 82
Information and Network Security................................................ 83
IT and C4I for Emergency Response........................................... 85

THE IMPACT OF C4I IN THE PAST ........................................ 92

PLANNING FOR THE FUTURE ............................................ 94

PRIVACY AND CONFIDENTIALITY ........................................ 96
Abstract

This thesis examines the impact information technologies have had on the age-old phenomenon of terrorism. It looks at how terrorism has evolved into what has come to be known as information terrorism over this Information Era.

Information revolution has introduced a new paradigm called Information Warfare for conflict among nations based upon attacking information infrastructures. The political attractions and deterrents to using these new information warfare methods are discussed at great length.

The information age is affecting not only the types of targets and weapons terrorist choose, but also the ways in which such groups operate and structure their organizations. This paper will discuss how several of the dangerous terrorist organizations today are using information technology -- such as computers, software, telecommunication devices, and the Internet -- to better organize and coordinate dispersed activities. Like the large numbers of private corporations that have embraced IT to operate more efficiently and with greater flexibility, terrorists are harnessing the power of IT to enable new operational doctrines and forms of organization.

The final chapters offer prescriptions and solutions for integrating information technology into the framework of the United States' grand strategy to decrease the security threat and facilitate international cooperation in this area.
Introduction

A decade ago or so ago, terrorism was a rather distinct entity on the spectrum of conflict, with its own unique attributes. Today it seems increasingly connected with broader trends in irregular warfare, especially as waged by non-state actors.

Today's main threat to many states, including specifically the United States, no longer comes from other states. Instead it comes from small groups and other organizations, which are not states.

Terrorist experts have been warning that the phenomenon of terrorism is growing worse (Arquilla & Ronfeldt, 1997). Terrorism is not a fixed phenomenon, its perpetrators adapt it to suit their times and situations. What changes is the conduct of terrorism – the operational characteristics built around the motivations and rationales? In this age of Information revolution, the use of information technology (IT) has become more appealing to these groups.

In the aftermath of the September 11, 2001 carnage in the United States, it is now widely reported that the terrorists used high-tech tools to plan and consummate their reprehensible attacks. The irony of it all is that the high-tech tools they used are the very same tools we use to enhance our lives. Yes, they used common tools such as mobile phones, e-mail, the Internet.

Our transition into the Information Age has come with a series of threats to our nation’s security. The new technological developments that have occurred during the last two decades have shifted the conception of national security to a great extent. Today nations face the danger of a physical damage but also having their information infrastructures destroyed, altered, or incapacitated by the new genre of offensive technologies. Hence there is the need to incorporate these vulnerabilities while designing the military strategy. This thesis will discuss the different information technology tools that are being used by terrorist organizations today and the need for
us to examine the level of threat posed by new technology and how it has affected the entire world's political scenario. This thesis provides a brief introduction to terrorism and how it has evolved over the years and then moves onto the ways in which information technologies have been utilized today by these terrorist groups to threaten the national security of different countries. The paper also discusses how information technology can be deployed in an effective manner to assist in countering terrorism (Devost, 2001).

There is a great need for extensive research in this area. The work done in the political science field to examine security issues related to information technology has been minimal. David Ronfeldt reports in his RAND article that with few exceptions, policy makers and analysts are just beginning to discern how government and politics may ultimately be affected by the information revolution (Arquilla & Ronfeldt, 1997)

As a result, this thesis draws from a wide range of material that has been taken from the information technology as well as the political science field and puts it all together reveal national security vulnerabilities posed by the very same technologies we depend on a daily basis.

This paper discusses in detail how the transition into the Information Era proves to be advantageous for terrorist organizations by posing as both a tool as well as a target for their attacks.

It has been reported that, within hours of the attacks on the World Trade Center and the Pentagon, U.S. intelligence was able to pick up phone calls made to the mobile phones of suspected terrorists linked to Osama bin Laden. Callers were congratulating the terrorists for the successful consummation of their dastardly attacks.

The terrorists reportedly used the Internet as well. They used the free and easy-to-use e-mail personal accounts on Yahoo and Hotmail. It has also been found that terrorists conduct their meetings in the chat rooms available on Yahoo and Hotmail (Yam, 2001).
The terrorists reportedly practiced their aeronautical skills by flying into the virtual World Trade Center towers using Microsoft's Flight Simulator software. The terrorists trained by practicing on these computer-powered flight simulators that allowed them to experience flying a 767 commercial airplane over the Manhattan skyline (Yam, 2001).

Arquilla and Ronfeldt state that Information Revolution is reshaping the spectrum of terrorism across the world. First, the Information Revolution is favoring and strengthening network forms of organization, often giving them an advantage over hierarchical forms. The rise of network forms means that power is migrating to non-state actors who are able to organize into sprawling multi-organizational networks more readily than can traditional, hierarchical, state actors. Non state actor’s networks are thought to be more flexible and responsive than hierarchies in reacting to outside developments. Second, as the information revolution deepens, conflicts will increasingly depend on information matters. More than ever before, conflicts will revolve around “knowledge” and the use of soft power. Adversaries will emphasize “information operations” and “perception management” – that is, media-oriented measures that aim to attract rather than coerce and that affect how secure a society, a military or other actor feels about its knowledge.

IT offers new opportunities to terrorists. A terrorist organization can reap low-risk, highly visible payoffs by attacking information systems. As technology becomes more cost effective to terrorists – that is availability and potential for disruptive effects rise while its financial and other costs go down – terrorists are becoming more technologically oriented in tactics and strategies.

Indeed, we are dazzled with breathless prophecies of social progress through breakthrough technologies. The flipside is that with these breakthroughs, we shall also experience technological change.

Today, we find ourselves in a deadly duel with the technological juggernaut, whose powers ironically threaten to annihilate those who created it.
And so, in the aftermath of the September 11, 2001 carnage, we need to ask ourselves: Have we become a people unable to comprehend the technology we invent?
Terrorism

Definitions
As cited by Patrick Galley in his article on “Computer Terrorism: What are the risks?”, term "terrorism" was used by the philosopher Emmanuel Kant for the first time in 1798, to describe a pessimistic view of the destiny of humanity (Galley, 1996). The same year, it was found in one finds the term in a supplement to the large Dictionary of the French Academy. However terrorism then did not mean what it accords for today. The FBI defines ,

“Terrorism is the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives. (Terrorism Research Center,2000)”

There are several other definitions available and some are as follows:

"Terrorism: The systematic use of terror especially as a means of coercion" (Terrorism Research Center,2000)

“Terrorism is the unlawful use or threat of violence against persons or property to further political or social objectives. It is usually intended to intimidate or coerce a government, individuals or groups, or to modify their behavior or politics.” as defined by the Vice-President’s Task Force in 1986. (Terrorism Research Center,2000)

The systematic use of violence to create a general climate of fear in a population and thereby to bring about a particular political objective. Terrorism has been practiced by political organizations with both rightist and leftist objectives, by nationalistic and religious groups, by revolutionaries, and even by state institutions such as armies, intelligence (Britannica.com).

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**

There are various forms of terrorism. Luigi Bonanate as cited by Galley (Galley, 1996) distinguished internal *terrorism* and international *terrorism*.

Internal terrorism: Terrorism of state (terror) and revolutionary terrorism comes under this form. Here terrorism is an act of reinforcing or of destroying the state. The State can use the terrorism of State to destabilize terrorist or extremist actions with an aim of reinforcing the central authority. The State can be an originator of terror during a war when it orders air strikes in order to frighten its enemy or to definitively discourage it as it took place during the Second World War at Hiroshima.

International Terrorism: Firstly, comes independence or separatist *terrorism*, which are movements that are carried out to fight against a colonial domination or for an independent State or sometimes to link itself to another State than that to which they belong. Bonanate says, by nature, independence *terrorism* is always international, because it carries its acts beyond the borders of the concerned territory as is the case with Palestinian terrorism. On the other hand, *colonialist* terrorism is observed aim at the preservation of the sovereignty of a State on a colony.

The LON (League Of Nations) soon after the attack against the king of Yugoslavia and the French minister Louis Barthou drew up an International Convention, which was signed in Geneva on November 16 1937, by twenty-five countries (except Italy and the United States). This convention defined 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" . The signatories of the text thus drew up the detailed list of the various forms of terrorism (Galley, 1996):

- 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 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 (Cryan, 2001).

Evolution of International terrorism

In July 1995, the tenth annual International Conference on Criminal Justice Issue (Hoffman, 1999), brought to attention with the help of experts that there is high probability of the use of Weapons of Mass Destruction in the future. It was also reported, the ethnic or religious terrorist groups will not hesitate to use such weapons that would cause a great number of victims, whereas the fearing of popular support would keep old terrorist groups from using such weapons. It was seen from the attack with toxic gas, in Japan, the taboo of using chemical weapons was broken.

Past terrorist attacks as enlisted by the United States Embassy on October 8th, 2001
First U.S. Aircraft Hijacked, May 1, 1961: Puerto Rican born Antuilo Ramírez Ortiz forced at gunpoint a National Airlines plane to fly to Havana, Cuba, where he was given asylum (terrorism.com).

Ambassador to Guatemala Assassinated, August 28, 1968: U.S. Ambassador to Guatemala John Gordon Mein was murdered by a rebel faction when gunmen forced his official car off the road in Guatemala City and raked the vehicle with gunfire.

Ambassador to Japan Attacked, July 30, 1969: U.S. Ambassador to Japan A.H. Meyer was attacked by a knife-wielding Japanese citizen.

Ambassador to Brazil Kidnapped, September 3, 1969: U.S. Ambassador to Brazil Charles Burke Elbrick was kidnapped by the Marxist revolutionary group MR-8.

U.S. Agency for International Development Adviser Kidnapped, July 31, 1970: In Montevideo, Uruguay, the Tupamaros terrorist group kidnapped USAID Police adviser Dan Mitrione; his body was found on August 10.

"Bloody Friday," July 21, 1972: An Irish Republican Army (IRA) bomb attacks killed 11 people and injured 130 in Belfast, Northern Ireland. Ten days later, three IRA car bomb attacks in the village of Claudy left six dead.

Munich Olympic Massacre, September 5, 1972: Eight Palestinian "Black September" terrorists seized 11 Israeli athletes in the Olympic Village in Munich, West Germany. In a bungled rescue attempt by West German authorities, nine of the hostages and five terrorists were killed.

Ambassador to Sudan Assassinated, March 2, 1973: U.S. Ambassador to Sudan Cleo A. Noel and other diplomats were assassinated at the Saudi Arabian Embassy in Khartoum by members of the Black September organization.
Consul General in Mexico Kidnapped, May 4, 1973: U.S. Consul General in Guadalajara Terrence Leonhardy was kidnapped by members of the People's Revolutionary Armed Forces.

Domestic Terrorism, January 27-29, 1975: Puerto Rican nationalists bombed a Wall Street bar, killing four and injuring 60; 2 days later, the Weather Underground claims responsibility for an explosion in a bathroom at the U.S. Department of State in Washington.

Entebbe Hostage Crisis, June 27, 1976: Members of the Baader-Meinhof Group and the Popular Front for the Liberation of Palestine (PFLP) seized an Air France airliner and its 258 passengers. They forced the plane to land in Uganda, where on July 3 Israeli commandos successfully rescued the passengers.

Assassination of Former Chilean Diplomat, September 21, 1976: In Washington, exiled Chilean Foreign Minister Orlando Letelier was killed by a car bomb.

Kidnapping of Italian Prime Minister, March 16, 1978: Premier Aldo Moro was seized by the Red Brigade and assassinated 55 days later.

Iran Hostage Crisis, November 4, 1979: After President Carter agreed to admit the Shah of Iran into the U.S., Iranian radicals seized the U.S. Embassy in Tehran and took 66 American diplomats hostage. Thirteen hostages were soon released, but the remaining 53 were held until their release on January 20, 1981.

Grand Mosque Seizure, November 20, 1979: 200 Islamic terrorists seized the Grand Mosque in Mecca, Saudi Arabia, taking hundreds of pilgrims hostage. Saudi and French security forces retook the shrine after an intense battle in which some 250 people were killed and 600 wounded.

Assassination of Egyptian President, October 6, 1981: Soldiers who were secretly members of the Takfir Wal-Hajira sect attacked and killed Egyptian President Anwar Sadat during a troop review.

Murder of Missionaries, December 4, 1981: Three American nuns and one lay missionary were found murdered outside San Salvador, El Salvador. They were believed to have been assassinated by a right-wing death squad.

Assassination of Lebanese Prime Minister, September 14, 1982: Premier Bashir Gemayel was assassinated by a car bomb parked outside his party's Beirut headquarters.

Colombian Hostage-taking, April 8, 1983: A U.S. citizen was seized by the Revolutionary Armed Forces of Colombia (FARC) and held for ransom.

Bombing of U.S. Embassy in Beirut, April 18, 1983: Sixty-three people, including the CIA's Middle East director, were killed, and 120 were injured in a 400-pound suicide truck-bomb attack on the U.S. Embassy in Beirut, Lebanon. The Islamic Jihad claimed responsibility.

Naval Officer Assassinated in El Salvador, May 25, 1983: A U.S. Navy officer was assassinated by the Farabundo Marti National Liberation Front.

North Korean Hit Squad, October 9, 1983: North Korean agents blew up a delegation from South Korea in Rangoon, Burma, killing 21 persons and injuring 48.

Bombing of Marine Barracks, Beirut, October 23, 1983: Simultaneous suicide truck-bomb attacks were made on American and French compounds in Beirut, Lebanon. A 12,000-pound bomb destroyed the U.S. compound, killing 242 Americans, while 58 French troops were killed when a 400-pound device destroyed a French base. Islamic Jihad claimed responsibility.

Naval Officer Assassinated in Greece, November 15, 1983: A U.S. Navy officer was shot by the November 17 terrorist group in Athens, Greece, while his car was stopped at a traffic light.
Kidnapping of Embassy Official, March 16, 1984: The Islamic Jihad kidnapped and later murdered Political Officer William Buckley in Beirut, Lebanon. Other U.S. citizens not connected to the U.S. Government were seized over a succeeding 2-year period.

Hizballah Restaurant Bombing, April 12, 1984: Eighteen U.S. servicemen were killed, and 83 people were injured in a bomb attack on a restaurant near a U.S. Air Force Base in Torrejon, Spain. Responsibility was claimed by Hizballah.

Golden Temple Seizure, June 5, 1984: Sikh terrorists seized the Golden Temple in Amritsar, India. One hundred people died when Indian security forces retook the Sikh holy shrine.

Assassination of Prime Minister Gandhi, October 31, 1984: The Indian premier was shot to death by members of her security force.

Kidnapping of U.S. Officials in Mexico, February 7, 1985: Under the orders of narcotrafficker Rafael Cero Quintero, Drug Enforcement Administration agent Enrique Camarena Salazar and his pilot were kidnapped, tortured, and executed.

TWA Hijacking, June 14, 1985: A Trans-World Airlines flight was hijacked en route to Rome from Athens by two Lebanese Hizballah terrorists and forced to fly to Beirut. The eight crew members and 145 passengers were held for 17 days, during which one American hostage, a U.S. Navy sailor, was murdered. After being flown twice to Algiers, the aircraft was returned to Beirut after Israel released 435 Lebanese and Palestinian prisoners.

Air India Bombing, June 23, 1985: A bomb destroyed an Air India Boeing 747 over the Atlantic, killing all 329 people aboard. Both Sikh and Kashmiri terrorists were blamed for the attack. Two cargo handlers were killed at Tokyo airport, Japan, when another Sikh bomb exploded in an Air Canada aircraft enroute to India.
Soviet Diplomats Kidnapped, September 30, 1985: In Beirut, Lebanon, Sunni terrorists kidnapped four Soviet diplomats. One was killed, but three were later released.

Achille Lauro Hijacking, October 7, 1985: Four Palestinian Liberation Front terrorists seized the Italian cruise liner in the eastern Mediterranean Sea, taking more than 700 hostages. One U.S. passenger was murdered before the Egyptian Government offered the terrorists safe haven in return for the hostages' freedom.

Egyptian Airliner Hijacking, November 23, 1985: An Egypt Air airplane bound from Athens to Malta and carrying several U.S. citizens was hijacked by the Abu Nidal Group.


Berlin Discoteque Bombing, April 5, 1986: Two U.S. soldiers were killed, and 79 American servicemen were injured in a Libyan bomb attack on a nightclub in West Berlin, West Germany. In retaliation, U.S. military jets bombed targets in and around Tripoli and Benghazi.

Kimpo Airport Bombing, September 14, 1986: North Korean agents detonated an explosive device at Seoul's Kimpo Airport, killing five persons and injuring 29 others.

Bus Attack, April 24, 1987: Sixteen U.S. servicemen riding in a Greek Air Force bus near Athens were injured in an apparent bombing attack, carried out by the revolutionary organization known as 17 November.


Kidnapping of William Higgins, February 17, 1988: U.S. Marine Corps Lt. Col. W. Higgins was kidnapped and murdered by the Iranian-backed Hizballah group while serving with the United Nations Truce Supervisory Organization (UNTSO) in southern Lebanon.

Naples USO Attack, April 14, 1988: The Organization of Jihad Brigades exploded a car bomb outside a USO Club in Naples, Italy, killing one U.S. sailor.

Attack on U.S. Diplomat in Greece, June 28, 1988: The Defense Attaché of the U.S. Embassy in Greece was killed when a car bomb was detonated outside his home in Athens.

Pan Am 103 Bombing, December 21, 1988: Pan American Airlines Flight 103 was blown up over Lockerbie, Scotland, by a bomb believed to have been placed on the aircraft in Frankfurt, West Germany, by Libyan terrorists. All 259 people on board were killed.

Assassination of U.S. Army Officer, April 21, 1989: The New People's Army (NPA) assassinated Col. James Rowe in Manila. The NPA also assassinated two U.S. government defense contractors in September.


Kidnapping of U.S. Businessmen in the Philippines, January 17-21, 1992: A senior official of the corporation Philippine Geothermal was kidnapped in Manila by the Red Scorpion Group, and two U.S. businessmen were seized independently by the National Liberation Army and by Revolutionary Armed Forces of Colombia (FARC).

Bombing of the Israeli Embassy in Argentina, March 17, 1992: Hizballah claimed responsibility for a blast that leveled the Israeli Embassy in Buenos Aires, Argentina, causing the deaths of 29 and wounding 242.


World Trade Center Bombing, February 26, 1993: The World Trade Center in New York City was badly damaged when a car bomb planted by Islamic terrorists explodes in an underground garage. The bomb left six people dead and 1,000 injured. The men carrying out the attack were followers of Omar Abd al-Rahman, an Egyptian cleric who preached in the New York City area.

Attempted Assassination of President Bush by Iraqi Agents, April 14, 1993: The Iraqi intelligence service attempted to assassinate former U.S. President George Bush during a visit to Kuwait. In retaliation, the U.S. launched a cruise missile attack 2 months later on the Iraqi capital Baghdad.


Air France Hijacking, December 24, 1994: Members of the Armed Islamic Group seized an Air France Flight to Algeria. The four terrorists were killed during a rescue effort.


Tokyo Subway Station Attack, March 20, 1995: Twelve persons were killed, and 5,700 were injured in a Sarin nerve gas attack on a crowded subway station in the center of Tokyo, Japan. A similar attack occurred nearly simultaneously in the Yokohama subway system. The Aum Shinrikyu cult was blamed for the attacks.

Bombing of the Federal Building in Oklahoma City, April 19, 1995: Right-wing extremists Timothy McVeigh and Terry Nichols destroyed the Federal Building in Oklahoma City with a massive truck bomb that killed 166 and injured hundreds more in what was up to then the largest terrorist attack on American soil.

Kashmiri Hostage-taking, July 4, 1995: In India, six foreigners, including two U.S. citizens, were taken hostage by Al-Faran, a Kashmiri separatist group. One non-U.S. hostage was later found beheaded.

Jerusalem Bus Attack, August 21, 1995: Hamas claimed responsibility for the detonation of a bomb that killed six and injured over 100 persons, including several U.S. citizens.

Attack on U.S. Embassy in Moscow, September 13, 1995: A rocket-propelled grenade was fired through the window of the U.S. Embassy in Moscow, ostensibly in retaliation for U.S. strikes on Serb positions in Bosnia.

Saudi Military Installation Attack, November 13, 1995: The Islamic Movement of Change planted a bomb in a Riyadh military compound that killed one U.S. citizen, several foreign national employees of the U.S. Government, and more than 40 others.
Egyptian Embassy Attack, November 19, 1995: A suicide bomber drove a vehicle into the Egyptian Embassy compound in Islamabad, Pakistan, killing at least 16 and injuring 60 persons. Three militant Islamic groups claimed responsibility.

Papuan Hostage Abduction, January 8, 1996: In Indonesia, 200 Free Papua Movement (OPM) guerrillas abducted 26 individuals in the Lorenta nature preserve, Irian Jaya Province. Indonesian Special Forces members rescued the remaining nine hostages on May 15.

Kidnapping in Colombia, January 19, 1996: Revolutionary Armed Forces of Colombia (FARC) guerrillas kidnapped a U.S. citizen and demanded a $1 million ransom. The hostage was released on May 22.

Tamil Tigers Attack, January 31, 1996: Members of the Liberation Tigers of Tamil Eelam (LTTE) rammed an explosives-laden truck into the Central Bank in the heart of downtown Colombo, Sri Lanka, killing 90 civilians and injuring more than 1,400 others, including two U.S. citizens.

IRA Bombing, February 9, 1996: An Irish Republican Army (IRA) bomb detonated in London, killing two persons and wounding more than 100 others, including two U.S. citizens.

Athens Embassy Attack, February 15, 1996: Unidentified assailants fired a rocket at the U.S. embassy compound in Athens, causing minor damage to three diplomatic vehicles and some surrounding buildings. Circumstances of the attack suggested it was an operation carried out by the 17 November group.

ELN Kidnapping, February 16, 1996: Six alleged National Liberation Army (ELN) guerrillas kidnapped a U.S. citizen in Colombia. After 9 months, the hostage was released.
Hamas Bus Attack, February 26, 1996: In Jerusalem, a suicide bomber blew up a bus, killing 26 persons, including three U.S. citizens, and injuring some 80 persons, including three other US citizens.

Dizengoff Center Bombing, March 4, 1996: Hamas and the Palestine Islamic Jihad (PIJ) both claimed responsibility for a bombing outside of Tel Aviv's largest shopping mall that killed 20 persons and injured 75 others, including two U.S. citizens.

West Bank Attack, May 13, 1996: Arab gunmen opened fire on a bus and a group of Yeshiva students near the Bet El settlement, killing a dual U.S.-Israeli citizen and wounding three Israelis.

No one claimed responsibility for the attack, but Hamas was suspected.

USAID Worker Abduction, May 31, 1996: A gang of former Contra guerrillas kidnapped a U.S. employee of the Agency for International Development (USAID) who was assisting with election preparations in rural northern Nicaragua. She was released unharmed the next day after members of the international commission overseeing the preparations intervened.

Zekharya Attack, June 9, 1996: Unidentified gunmen opened fire on a car near Zekharya, killing a dual U.S./Israeli citizen and an Israeli. The Popular Front for the Liberation of Palestine (PFLP) is suspected.

Manchester Truck Bombing, June 15, 1996: An IRA truck bomb detonated at a Manchester shopping center, wounding 206 persons, including two German tourists, and caused extensive property damage.

Khobar Towers Bombing, June 25, 1996: A fuel truck carrying a bomb exploded outside the U.S. military's Khobar Towers housing facility in Dhahran, killing 19 U.S. military personnel and wounding 515 persons, including 240 U.S. personnel. Several groups claimed responsibility for the attack.
ETA Bombing, July 20, 1996: A bomb exploded at Tarragona International Airport in Reus, Spain, wounding 35 persons, including British and Irish tourists. The Basque Fatherland and Liberty (ETA) organization was suspected.

Bombing of Archbishop of Oran, August 1, 1996: A bomb exploded at the home of the French Archbishop of Oran, killing him and his chauffeur. The attack occurred after the Archbishop's meeting with the French Foreign Minister. The Algerian Armed Islamic Group (GIA) is suspected.

Sudanese Rebel Kidnapping, August 17, 1996: Sudan People's Liberation Army (SPLA) rebels kidnapped six missionaries in Mapourdit, including a U.S. citizen, an Italian, three Australians, and a Sudanese. The SPLA released the hostages 11 days later.

PUK Kidnapping, September 13, 1996: In Iraq, Patriotic Union of Kurdistan (PUK) militants kidnapped four French workers for Pharmaciens Sans Frontieres, a Canadian United Nations High Commissioner for Refugees (UNHCR) official, and two Iraqis.

Assassination of South Korean Consul, October 1, 1996: In Vladivostok, Russia, assailants attacked and killed a South Korean consul near his home. No one claimed responsibility, but South Korean authorities believed that the attack was carried out by professionals and that the assailants were North Koreans. North Korean officials denied the country's involvement in the attack.

Red Cross Worker Kidnappings, November 1, 1996: In Sudan, a breakaway group from the Sudanese People's Liberation Army (SPLA) kidnapped three International Committee of the Red Cross (ICRC) workers, including a U.S. citizen, an Australian, and a Kenyan. On December 9, the rebels released the hostages in exchange for ICRC supplies and a health survey for their camp.
Paris Subway Explosion, December 3, 1996: A bomb exploded aboard a Paris subway train as it arrived at the Port Royal station, killing two French nationals, a Moroccan, and a Canadian, and injuring 86 persons. Among those injured were one U.S. citizen and a Canadian. No one claimed responsibility for the attack, but Algerian extremists are suspected.

Abduction of US. Citizen by FARC, December 11, 1996: Five armed men claiming to be members of the Revolutionary Armed Forces of Colombia (FARC) kidnapped and later killed a U.S. geologist at a methane gas exploration site in La Guajira Department.

Tupac Amaru Seizure of Diplomats, December 17, 1996: Twenty-three members of the Tupac Amaru Revolutionary Movement (MRTA) took several hundred people hostage at a party given at the Japanese Ambassador's residence in Lima, Peru. Among the hostages were several U.S. officials, foreign ambassadors and other diplomats, Peruvian Government officials, and Japanese businessmen. The group demanded the release of all MRTA members in prison and safe passage for them and the hostage takers. The terrorists released most of the hostages in December but held 81 Peruvians and Japanese citizens for several months.

Egyptian Letter Bombs, January 2-13, 1997: A series of letter bombs with Alexandria, Egypt, postmarks were discovered at Al-Hayat newspaper bureaus in Washington, New York City, London, and Riyadh, Saudi Arabia. Three similar devices, also postmarked in Egypt, were found at a prison facility in Leavenworth, Kansas. Bomb disposal experts defused all the devices, but one detonated at the Al-Hayat office in London, injuring two security guards and causing minor damage.

Tajik Hostage Abductions, February 4-17, 1997: Near Komsomolabad, Tajikistan, a paramilitary group led by Bakhrom Sodirov abducted four United Nations military observers. The victims included two Swiss, one Austrian, one Ukrainian, and their Tajik interpreter. The kidnappers demanded safe passage for their supporters from Afghanistan to Tajikistan. In four separate
incidents occurring between Dushanbe and Garm, Bakhrom Sodirov and his group kidnapped two
International Committee for the Red Cross members, four Russian journalists and their Tajik
driver, four UNHCR members, and the Tajik Security Minister, Saidamir Zukhurov.

Venezuelan Abduction, February 14, 1997: Six armed Colombian guerrillas kidnapped a U.S. oil
engineer and his Venezuelan pilot in Apure, Venezuela. The kidnappers released the Venezuelan
pilot on February 22. According to authorities, the FARC is responsible for the kidnapping.

Empire State Building Sniper Attack, February 23, 1997: A Palestinian gunman opened fire on
tourists at an observation deck atop the Empire State Building in New York City, killing a Danish
national and wounding visitors from the United States, Argentina, Switzerland, and France before
turning the gun on himself. A handwritten note carried

by the gunman claimed this was a punishment attack against the "enemies of Palestine."

ELN Kidnapping, February 24, 1997: National Liberation Army (ELN) guerrillas kidnapped a
U.S. citizen employed by a Las Vegas gold corporation who was scouting a gold mining
operation in Colombia. The ELN demanded a ransom of $2.5 million.

FARC Kidnapping, March 7, 1997: FARC guerrillas kidnapped a U.S. mining employee and his
Colombian colleague who were searching for gold in Colombia. On November 16, the rebels
released the two hostages after receiving a $50,000 ransom.

Hotel Nacional Bombing, July 12, 1997: A bomb exploded at the Hotel Nacional in Havana,
injuring three persons and causing minor damage. A previously unknown group calling itself the
Military Liberation Union claimed responsibility.

Israeli Shopping Mall Bombing, September 4, 1997: Three suicide bombers of Hamas detonated
bombs in the Ben Yehuda shopping mall in Jerusalem, killing eight persons, including the
bombers, and wounding nearly 200 others. A dual U.S./Israeli citizen was among the dead, and seven U.S. citizens were wounded.

OAS Abductions, October 23, 1997: In Colombia, ELN rebels kidnapped two foreign members of the Organization of American States (OAS) and a Colombian human rights official at a roadblock. The ELN claimed that the kidnapping was intended "to show the international community that the elections in Colombia are a farce."

Yemeni Kidnappings, October 30, 1997: Al-Sha'if tribesmen kidnapped a U.S. businessman near Sanaa. The tribesmen sought the release of two fellow tribesmen who were arrested on smuggling charges and several public works projects they claim the government promised them. They released the hostage on November 27.

Murder of U.S. Businessmen in Pakistan, November 12, 1997: Two unidentified gunmen shot to death four U.S. auditors from Union Texas Petroleum Corporation and their Pakistani driver after they drove away from the Sheraton Hotel in Karachi. The Islami Inqilabi Council, or Islamic Revolutionary Council, claimed responsibility in a call to the U.S. Consulate in Karachi. In a letter to Pakistani newspapers, the Aimal Khufia Action Committee also claimed responsibility.

Tourist Killings in Egypt, November 17, 1997: Al-Gama'at al-Islamiyya (IG) gunmen shot and killed 58 tourists and four Egyptians and wounded 26 others at the Hatshepsut Temple in the Valley of the Kings near Luxor. Thirty-four Swiss, eight Japanese, five Germans, four Britons, one French, one Colombian, a dual Bulgarian/British citizen, and four unidentified persons were among the dead. Twelve Swiss, two Japanese, two Germans, one French, and nine Egyptians were among the wounded.

UN Observer Abductions, February 19, 1998: Armed supporters of late Georgian President Zviad Gamsakhurdia abducted four UN military observers from Sweden, Uruguay, and the Czech Republic.
FARC Abduction, March 21-23, 1998: FARC rebels kidnapped a U.S. citizen in Sabaneta, Colombia. FARC members also killed three persons, wounded 14, and kidnapped at least 27 others at a roadblock near Bogota. Four U.S. citizens and one Italian were among those kidnapped, as well as the acting president of the National Electoral Council (CNE) and his wife.

Somali Hostage-takings, April 15, 1998: Somali militiamen abducted nine Red Cross and Red Crescent workers at an airstrip north of Mogadishu. The hostages included a U.S. citizen, a German, a Belgian, a French, a Norwegian, two Swiss, and one Somali. The gunmen were members of a sub clan loyal to Ali Mahdi Mohammed, who controlled the northern section of the capital.

IRA Bombing, Banbridge, August 1, 1998: A 500-pound car bomb planted by the Real IRA exploded outside a shoe store in Banbridge, North Ireland, injuring 35 persons and damaging at least 200 homes.


IRA Bombing, Omagh, August 15, 1998: A 500-pound car bomb planted by the Real IRA exploded outside a local courthouse in the central shopping district of Omagh, Northern Ireland, killing 29 persons and injuring over 330.
Colombian Pipeline Bombing, October 18, 1998: A National Liberation Army (ELN) planted bomb exploded on the Ocensa pipeline in Antioquia Department, killing approximately 71 persons and injuring at least 100 others. The pipeline is jointly owned by the Colombia State Oil Company Ecopetrol and a consortium, including U.S., French, British, and Canadian companies.

Armed Kidnapping in Colombia, November 15, 1998: Armed assailants followed a U.S. businessman and his family home in Cundinamarca Department and kidnapped his 11-year-old son after stealing money, jewelry, one automobile, and two cell phones. The kidnappers demanded $1 million in ransom. On January 21, 1999, the kidnappers released the boy.

Angolan Aircraft Downing, January 2, 1999: A UN plane carrying one U.S. citizen, four Angolans, two Philippine nationals, and one Namibian was shot down, according to a UN official. No deaths or injuries were reported. Angolan authorities blamed the attack on National Union for the Total Independence of Angola (UNITA) rebels. UNITA officials denied shooting down the plane.

Ugandan Rebel Attack, February 14, 1999: A pipe bomb exploded inside a bar, killing five persons and injuring 35 others. One Ethiopian and four Ugandan nationals died in the blast, and one U.S. citizen working for USAID, two Swiss nationals, one Pakistani, one Ethiopian, and 27 Ugandans were injured. Ugandan authorities blamed the attack on the Allied Democratic Forces (ADF).

Greek Embassy Seizure, February 16, 1999: Kurdish protesters stormed and occupied the Greek Embassy in Vienna, taking the Greek Ambassador and six other people as hostage. Several hours later the protesters released the hostages and left the embassy. The attack followed the Turkish Government's announcement of the successful capture of the
Kurdistan Workers' Party (PKK) leader Abdullah Ocalan. Kurds also occupied Kenyan, Israeli, and other Greek diplomatic facilities in France, Holland, Switzerland, Britain, and Germany over the following days.

FARC Kidnappings, February 25, 1999: FARC kidnapped three U.S. citizens working for the Hawaii-based Pacific Cultural Conservancy International. On March 4, the bodies of the three victims were found in Venezuela.

Hutu Abductions, March 1, 1999: 150 armed Hutu rebels attacked three tourist camps in Uganda, killed four Ugandans, and abducted three U.S. citizens, six Britons, three New Zealanders, two Danish citizens, one Australian, and one Canadian national. Two of the U.S. citizens and six of the other hostages were subsequently killed by their abductors.

ELN Hostage-taking, March 23, 1999: Armed guerrillas kidnapped a U.S. citizen in Boyaca, Colombia. The National Liberation Army (ELN) claimed responsibility and demanded $400,000 ransom. On July 20, ELN rebels released the hostage unharmed following a ransom payment of $48,000.

ELN Hostage-taking, May 30, 1999: In Cali, Colombia, armed ELN militants attacked a church in the neighborhood of Ciudad Jardin, kidnapping 160 persons, including six U.S. citizens and one French national. The rebels released approximately 80 persons, including three U.S. citizens, later that day.

Shell Platform Bombing, June 27, 1999: In Port Harcourt, Nigeria, armed youths stormed a Shell oil platform, kidnapping one U.S. citizen, one Nigerian national, and one Australian citizen, and causing undetermined damage. A group calling itself "Enough is Enough in the Niger River" claimed responsibility. Further seizures of oil facilities followed.
AFRC Kidnappings, August 4, 1999: An Armed Forces Revolutionary Council (AFRC) faction kidnapped 33 UN representatives near Occra Hills, Sierra Leone. The hostages included one U.S. citizen, five British soldiers, one Canadian citizen, one representative from Ghana, one military officer from Russia, one officer from Kyrgyzstan, one officer from Zambia, one officer from Malaysia, a local Bishop, two UN officials, two local journalists, and 16 Sierra Leonean nationals.

Burmese Embassy Seizure, October 1, 1999: Burmese dissidents seized the Burmese Embassy in Bangkok, Thailand, taking 89 persons hostage, including one U.S. citizen.

PLA Kidnapping, December 23, 1999: Colombian People's Liberation Army (PLA) forces kidnapped a U.S. citizen in an unsuccessful ransoming effort.

Indian Airlines Airbus Hijacking, December 24, 1999: Five militants hijacked a flight bound from Kathmandu to New Delhi carrying 189 people. The plane and its passengers were released unharmed on December 31.

Car bombing in Spain, January 27, 2000: Police officials reported unidentified individuals set fire to a Citroen car dealership in Iturreta, causing extensive damage to the building and destroying 12 vehicles. The attack bore the hallmark of the Basque Fatherland and Liberty (ETA).

RUF Attacks on UN Mission Personnel, May 1, 2000: On May 1 in Makeni, Sierra Leone, Revolutionary United Front (RUF) militants kidnapped at least 20 members of the United Nations Assistance Mission in Sierra Leone (UNAMSIL) and surrounded and opened fire on a UNAMSIL facility, according to press reports. The militants killed five UN soldiers in the attack. RUF militants kidnapped 300 UNAMSIL peacekeepers throughout the country, according to press reports. On May 15 in Foya, Liberia, the kidnappers released 139 hostages.
On May 28 2000, on the Liberia and Sierra Leone border, armed militants released unharmed the last of the UN peacekeepers. In Freetown, according to press reports, armed militants ambushed two military vehicles carrying four journalists.

A Spaniard and one U.S. citizen were killed in a May 25 2000 car bombing in Freetown for which the RUF was probably responsible. Suspected RUF rebels also kidnapped 21 Indian UN peacekeepers in Freetown on June 6 2000. Additional attacks by RUF on foreign personnel followed.


ELN Kidnapping, June 27, 2000: In Bogota, Colombia, ELN militants kidnapped a 5-year-old U.S. citizen and his Colombian mother, demanding an undisclosed ransom.

Kidnappings in Kyrgyzstan, August 12, 2000: In the Kara-Su Valley, the Islamic Movement of Uzbekistan took four U.S. citizens hostage. The Americans escaped on August 12.

Church Bombing in Tajikistan, October 1, 2000: Unidentified militants detonated two bombs in a Christian church in Dushanbe, killing seven persons and injuring 70 others. The church was founded by a Korean-born U.S. citizen, and most of those killed and wounded were Korean. No one claimed responsibility.

Helicopter Hijacking, October 12, 2000: In Sucumbios Province, Ecuador, a group of armed kidnappers led by former members of defunct Colombian terrorist organization the Popular Liberation Army (EPL), took hostage 10 employees of Spanish energy consortium REPSOL. Those kidnapped included five U.S. citizens, one Argentine, one Chilean, one New Zealander, and two French pilots who escaped 4 days later. On
January 30, 2001, the kidnappers murdered American hostage Ronald Sander. The remaining hostages were released on February 23 following the payment of $13 million in ransom by the oil companies.

Attack on U.S.S. Cole, October 12, 2000: In Aden, Yemen, a small dingy carrying explosives rammed the destroyer U.S.S. Cole, killing 17 sailors and injuring 39 others. Supporters of Osama Bin Laden were suspected.

Manila Bombing, December 30, 2000: A bomb exploded in a plaza across the street from the U.S. embassy in Manila, injuring nine persons. The Moro Islamic Liberation Front was likely responsible.

Srinagar Airport Attack, January 17, 2001: In India, six members of the Lashkar-e-Tayyba militant group were killed when they attempted to seize a local airport.


ETA Bombing, March 9, 2001: Two policemen were killed by the explosion of a car bomb in Hernani, Spain.

Bus Stop Bombing, April 22, 2001: A member of Hamas detonated a bomb he was carrying near a bus stop in Kfar Siva, Israel, killing one person and injuring 60.

Tel-Aviv Nightclub Bombing, June 1, 2001: Hamas claimed responsibility for the bombing of a popular Israeli nightclub that caused over 140 casualties.

Hamas Restaurant Bombing, August 9, 2001: A Hamas-planted bomb detonated in a Jerusalem pizza restaurant, killing 15 people and wounding more than 90.
Terrorist Attacks on U.S. Homeland, September 11, 2001: Two hijacked airliners crashed into the twin towers of the World Trade Center. Soon thereafter, the Pentagon was struck by a third hijacked plane. A fourth hijacked plane, suspected to be bound for a high-profile target in Washington, crashed into a field in southern Pennsylvania. More than 5,000 U.S. citizens and other nationals were killed as a result of these acts. President Bush and Cabinet officials indicated that Osama Bin Laden was the prime suspect and that they considered the United States in a state of war with international terrorism. In the aftermath of the attacks, the United States formed the Global Coalition Against Terrorism.
Information Age Terrorism

The world as a whole has made a transition to a new age. Alvin Toffler describes this transition as the Third Wave, in his 1980 book of the same title. According to Toffler, the pattern of societal development follows a series of waves and says that each period spans a lesser time than the previous one. Toffler writes (Toffler, 1980):

"Until now the human race has undergone two great waves of change, each one largely obliterating earlier cultures or civilizations and replacing them with ways of life inconceivable to those who came before. The First Wave of change - the agricultural revolution - took thousands of years to play it out. The Second Wave - the rise of industrial civilization - took a mere three hundred years. Today, history is even more accelerative, and it is likely that the Third Wave will sweep across history and complete itself in a few decades".

Toffler made these predictions over fifteen years ago, and there can be seen a close relation between the societal revolution he describes and today's Information Revolution.

In a Third Wave society, there are two general methods in which terrorist might employ an attack:

i) When information technology is a target.

ii) When information technology is the tool of a larger operation.

The first method implies a terrorist would target an information system for sabotage, either, electronic or physical, thus destroying or disrupting the information system itself and any information infrastructure (e.g., power, communications, etc.) dependant upon the targeted technology. The second method implies a terrorist would manipulate and exploit an information
system, altering or stealing data, or forcing the system to perform a function for which it was not meant (such as spoofing air traffic control).
Information Warfare

Devost in his article on "National Security in the Information Age", says, "Information warfare is about destroying information, reducing information flows, reducing the reliability of information content, and denying access to services". As cited by Devost, author and security expert Winn Schwartau writes (Denning,

"Information warfare is waged against industries, political spheres of influence, global economic forces, or even against entire countries. It is the use of technology against technology; it is about secrets and the theft of secrets; it is about turning information against its owners; it is about denying an enemy the ability to use both his technology and his information".

Research reveals that past historical patterns reveal that there is no doubt that information warfare is the warfare of the future. As Toffler reports, it has been observed that warfare always followed the course of development in society. Science has always had a great impact on war. Agrarian society saw the development of the crossbow. As our scientific expedition advanced, so did the weapons societies we used. The Industrial Revolution saw the birth of in formidable weapons such as tanks and aeroplanes. Increased understanding led to the thought of using atomic and nuclear fusion to create devastating bombs. Today, the new technologies brought by the Information Revolution lets us cause even more damage at the comfort of our own homes. As we move, or have already moved, into the Third Wave or Information Age our weapons have also naturally followed this course of transition.

The concept of information warfare, is not as new as we think it to be. The use of information warfare can be traced back to 1912, when the British cable ship Telconia hauled up and cut the five cables that was a major link of communication for Germany to the outside world. It can be learned how well the British recognized the strategic significance of communications
(information transfer) during wartime and utilized their capabilities to hinder Germany's ability to communicate. It can also be seen that when the United States intercepted and decrypted Japanese communications intelligence during wartime operations and diplomatic negotiations, the United States was actually waging information warfare recognizing the importance of information transfer.

However the importance of information in the industrial societies was not as high as it is today in the information driven societies. Information then was just one of the valuable assets. More importance and attention was given to the protection of industrial base. However, today's Information age are driven solely based on information flow. As Devost states, this means that information warfare poses a greater threat to national security in the Information Age than it did in the Industrial Age. The advantages of information warfare may make it the most preferred mode of conflict in the Information Age. General Gordon Sullivan and Colonel James Dubik state that "To succeed against an industrial state generally requires the destruction not only of its army, but also of the military infrastructure, resources and manufacturing base of the total war-making capability. Achieving victory against an information-based state will entail destroying that country's armed forces, as well as destroying its war-making capability (which may well include industrial and information-related targets) and its information systems."(Sullivan & Dubik, 1994)

**Attractions of Information Warfare**

There are many political and strategic attractions to state-sponsored information warfare.

**Low Cost**

The relatively low cost and high return on your investment with information warfare techniques when compared to conventional warfare makes it most attractive. Steele's and Schwartau's (Schwartau, 1994:) estimated the cost to reduce the United States to information rubble are
incredibly cheap when compared to the cost of conventional military weapons. This poses a great advantage to Third World nations and offers them the same basic capability to inflict the level of damage on information infrastructures as Second and First World nations.

**Timely and Not Location Specific**

Information warfare is timely and it is not location specific. Information warfare can be waged just by a single hit on the keyboard. It is waged without a warning. Denning says that, he constant anticipation of it causes a sense of paranoia. A single overseas call that cannot be picked up by our radar can cause more monetary damage than a dozen planes carrying conventional bombs. The World Trade Center is a perfect example of how drastic the effects a damage to the information infrastructure can be. It was reported that the damage to the flow of information, estimated at over $1 billion (Yurcik, 1994). This proved to be more costly than the structural damage inflicted on the building. Viruses can be imported into the United States through information networks, telephone lines, or on simple floppy disks which do not attract the attention of U.S. Customs Inspectors.

Though a well planned attack on the information structure takes a long time to be developed, it just takes a moment to. A great deal of investigation would be required to uncover the plan of such an attack. A low level information attack can be planned and orchestrated outside the boundaries of a victim nation. It makes it easier for nations who have easy access to U.S. visa to carry out an attack that would require to breach international boundaires. However, the September 11th attack proves, a nation's boundaries are capable of being breached by anyone with malicious intent.

**Anonymity**

Anonymity is one of the plus points of communication in the Information Age. Information warfare offers this advantage to a great extent which makes it an attractive tool to terrorists who can keep
their identity hidden. As Denning states, an anonymous attack creates two problems. Not only has a state's national security been breached, but there is no one to hold accountable for the attack.

This also causes a havoc as the government would not know who to target when citizens demand retribution. The government has no target. People would start blaming the government and this would result in a political instability in the country and sometimes may also lead to the collapse of the government.

Though computers are need in our lives on a daily basis, people seem to have lost their trust in them. As cited by Denning, Winn Schwartau calls these conflicting feelings "binary schizophrenia." When used anonymously, information warfare plays on feelings of binary schizophrenia causing insecurity and chaos. In this regard, anonymous information warfare is comparable to the German blitzkrieg of World War II. It makes an impact on the citizenry as well the government. Targets can be strategically selected to generate the maximum amount of chaos and insecurity possible.

**Minimal Loss of Human Life**

There is minimal loss of human lives within the target nation in an information war. This makes information warfare techniques politically attractive to State sponsored terrorism as there is no obligation on waging a war that would cause least harm to lives. Jeff Legro states three reasons for states to restrain from using certain weapons or means of warfare(Legro, 1994)

i) popular opinion vilifies certain weapons

ii) leaders believe use of such weapons would damage their domestic and international political support

iii) states fear retaliatory attacks.
As the level of human casualties and structural damage is relatively low compared to a regular warfare there is no reason for the public to vilify the use of such a weapon. In fact, populations would not be even aware of such an attack being waged against them until it is too late. Even, not many people understand the methodology of such an attack. Therefore it is highly unlikely that information warfare will be considered an inhuman way to pursue diplomacy by other means.

There is little reason to believe that using information warfare will be politically damaging to the country that wages such an attack. And another point to be noted is the anonymity offered by Information warfare assures that the identity of the aggressor will be well kept till the aggressor wishes to disclose it.

An anonymous strike is very unlikely to be followed by a retaliatory attack. Hence fear of retaliation or escalation will act as a deterrent to using information warfare. Alliances can be formed strategically and nations can choose to remain neutral.

Legro gives examples to demonstrate that military culture is a strong factor in determining when alternative or taboo forms of warfare will be used. Being a relatively new concept it is doubtful as to how well it has been understood to be incorporated in the military culture. However, reports indicate that area of information warfare has been receiving a great deal of attention and increased funding lately. This indicates that the military culture views information warfare as a reasonable and perhaps preferable form of warfare in the future. It has been reported that three branches of the United States Armed Services have publicly admitted to concentrating on information warfare concerns (Legro, 1994). The Aerospace Daily reports that "Major advances in information technologies are spurring the U.S. Air Force to mainstream information warfare into its operations by incorporating information warfare into its doctrine. (USAF, 1995)" With Legro's thesis in mind, perhaps the military culture will accelerate the use of information warfare as a method of conflict resolution. The use of information warfare techniques by the Allied forces
in the Gulf War indicate that the military culture has already accepted information warfare as a supplement to conventional military tactics (Mann, 1995).

**First Strike Advantage**

There is a huge first strike advantage in information warfare, but this is only if the aggressor aims at unlimited destruction and chooses to remain anonymous to prevent retaliatory attacks. As stated by Devost, "there is a high correlation between the extent to which a nation damages its enemy's information capabilities and their ability to respond using purely information warfare techniques. A nation can execute this first strike anonymously if it so desires, thus delaying retaliation indefinitely" (Devost, 1995).

Countries exercising the highest restraint to information warfare is likely to face a security dilemma because of the first strike advantage of information warfare. It is possible that the first strike advantage prevents the victim nation from even responding as the damage caused is so tremendous. It can be understood that the most strategic advantage of waging a first strike is that the aggressor nation is always prepared for a response. Devost states that in an anarchic international system, conflicts might escalate quickly into information warfare in an effort to generate a strategic advantage over one's adversary. If conventional conflict is inevitable, then whoever destroys their adversary's information systems first, gains a strategic advantage in battle.

**Offensive Nature of Information Warfare**

As information technology and computers are vulnerable by nature, there is always a high level of difficulty and increased cost in taking defensive measures against the information systems. The improvement of defense against an information war also involves a security dilemma as decreasing one's vulnerability to information warfare simultaneously increases the attraction of using information warfare offensively. Devost feels that in order to neutralize the security
Terrorism dilemma presented by defensive postures, states may share defensive technologies to ensure that a defensive equilibrium is maintained. This offers two advantages:

i) balance of power can be maintained among states;

ii) and reduced threat from rogue and terrorist states (Molander, Riddle & Wilson, 1996).

**Information Warfare proves Advantageous to Terrorism**

The anonymity and the ability to wage war against countries with strong military operations makes it an attractive tool for terrorists. When waged anonymously or by non-state entities, all of the advantages of information warfare are present but the deterrents are not. Terrorist groups care least about economic interdependence or political support therefore, the only significant deterrent vanishes. There is no question of retaliation as when carried out anonymously there is no target to retaliate. In some cases lack of technical expertise acts as a major deterrent. However, offensive information warfare weapons are easily built using open source material. One of the most important deterrent for terrorists in waging an information warfare is the lack of policy regarding this area. Terrorists are likely to feel that bloody bombs can create more havoc and chaos than waging an information warfare. However, this deterrent will gradually neutralize as the military operations are slowly recognizing the importance of its information systems, and as terrorists are beginning to realize the extent economic damage that can be inflicted.

Legro gives three constraints that might have adverse influence on terrorists that might keep them from restraining from pursuing information warfare.

i) No popular opinion to vilify the use of certain weapons or means of warfare within a terrorist organization.
ii) Leaders of these groups or states may use these weapons to gain domestic support, and may have little apprehension about loosing international political support since such support is usually negligible in the first place.

iii) Terrorist organizations usually seek retaliation, rather than fear it, because retaliation focuses attention on their organization and their cause (Legro, 1994).

Terrorists may recognize that the benefits from this far exceeds the costs in utilizing a non-anonymous information warfare. It can be understood that as the knowledge of information warfare spreads, the number and locality of the threats will increase as well. Mr. Schwartau (Schwartau, 1994) speaks of cyber-civil disobedience in his book which may gradually take the form of information terrorism. As cited by Devost, anarchists have talked about creating information anarchy should the commercialization of the net continue. This would again be information terrorism in a very limited sense.

Information warfare is best averted by concentrating a major portion of resources to research on building defensive military information systems. Information terrorism can also be prevented by making cost a major deterrent in using this means of warfare(ict.org).
Cyberterrorism

Definitions

The term “cyberterrorism”, was coined by Barry Collin, a senior research fellow at the Institute for Security and Intelligence in California, in the 80’s.

According to Collins, "cyberterrorism" refers to the convergence of cyberspace and terrorism. Mark Pollitt, special agent for the FBI, defines cyberterrorism as,” 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. Politically motivated attacks that cause serious harm, such as severe economic hardship or sustained loss of power or water, might also be characterized as cyberterrorism. (Krasavin, 2000)

The National Infrastructure Protection Center (NIPC) under Director Ronald Dick, a key figure in the government’s infrastructure protection scheme, defines cyberterrorism:

“a criminal act perpetrated through computers resulting in violence, death and/or destruction, and creating terror for the purpose of coercing a government to change its policies”. (Dick, 2001)

According to Denning, to qualify as cyberterrorism, an act must fulfill two criteria:

i) a political motivation and

ii) a destructive result.

Cyber or computer attacks usually satisfy only one: the motivation. It is by far too difficult to cause a massive destruction using computers. Phone lines being cut can be annoying and sometimes cause some insecurity issues, however that need not be destructive. As can be seen from the past, the most often cited cyberterrorist threat—shutting down the Internet—can
also be just a major inconvenience than a mass destruction. Even most experts believe it's the former. According to Denning very few malicious uses of technology qualify under Dick's definition of cyberterrorism.

There have been few if any computer network attacks that meet the criteria for cyber terrorism. The closes thing to closest thing to cyber terrorism that has occurred so far is the 1998 e-mail bombing by the Internet Black Tigers against the SRI Lankan embassies. However, the damage caused by the flood of e-mail (Schwartz, 1995), for example, seems to be pale when compared to the 240 deaths caused by the physical bombings of the U.S. embassies in Nairobi and Dar es Salaam in August of the same year.

**Advantages of Cyber terrorism**

As told by Avi Rubin, an AT&T Labs security expert, during his chat with the CNN, Cyber attacks could even become a force to reckon with in politics, at least if some communities follow through on plans to allow voting over the Internet. All that a malicious agent would have to do is launch a mild attack that would slow down a vote-processing server enough to prevent a few percent of the ballots from getting through in a few districts. "It's the easiest type of attack one could possibly launch, and it could be enough to disrupt an election," says Rubin.

Louis J. Freeh, Director of FBI in his Congressional Statement 2000 on Cyber Crime (Freeh, 2000) stated, "The prospect of information warfare by foreign militaries against our critical infrastructures is perhaps the greatest potential cyber threat to our national security. We know that several foreign nations are developing information warfare doctrine, programs, and capabilities against the United States or other nations. Knowing that they cannot match our military might with conventional or kinetic weapons, nations see cyber attacks on our critical infrastructures or military operations as a way to hit what they perceive as America's Achilles heel – our growing dependence on information technology in government and commercial operations". He also
mentions that, "Two Chinese military officers recently published a book that called for the use of unconventional measures, including the propagation of computer viruses, to counterbalance the military power of the United States. And a Russian official has also commented that an attack on a national infrastructure could, by virtue of its catastrophic consequences, completely overlap with the use of [weapons] of mass destruction."

There has been little concrete evidence to prove that terrorists are preparing to use the Internet as a venue for inflicting a massive destruction. However, in February 1998, Clark Staten, executive director of the Emergency Response & Research Institute in Chicago, testified that "members of some Islamic extremist organizations have been attempting to develop a hacker network to support their computer activities and even engage in offensive information warfare attacks in the future." (Staten, 1998) The very same year, The Detroit News, reported that Khalid Ibrahim, a member of the militant Indian separatist group Harkat-ul-Ansar, had tried to buy military software from hackers who had stolen it from U.S. Department of Defense computers they had hacked. Harkat-ul-Ansar, declared war on the United States attack on a suspected terrorist training camp in Afghanistan run by Osama bin Laden, which was reported to have killed nine of their members. Ibrahim’s attempt was caught when an 18-year-old hacker identifying himself as Chameleon attempted to cash a $1,000 check from the suspected terrorist. Chameleon denied all these charges, but it is likely that Ibrahim may have obtained it or other sensitive information from one of the many other hackers he approached.

Terrorists might use cracking for more than destroying data. According to Denning, an attack on the information systems causes a major distraction thus giving room for carrying out a physical attack. As stated by Ronefeldt, if a determined group wanted to bring New York to its knees, what better way than to combine a physical bombing campaign with simultaneous IT attacks on the power grid, hospitals, emergency services and the media? (Ronefeldt, 1992)
In August 1999, the Center for the Study of Terrorism and Irregular Warfare at the Naval Postgraduate School in Monterey, California, issued a report titled "Cyberterror: Prospects and Implications.(Denning, 2000)". The study was done to evaluate the demand side of terrorism. They assessed the prospects of terrorist organizations pursuing cyberterrorism. They concluded that the barrier to entry for anything beyond annoying hacks is quite high, and that terrorists generally lack the wherewithal and human capital needed to mount a meaningful operation. Cyberterrorism, as they argued, was a thing of the future, although it might be pursued as an ancillary tool.

**Levels of cyber terror capability**

The Monterey group defined three levels of cyberterror capability.

**Simple-Unstructured:** The capability to conduct basic hacks against individual systems using tools created by someone else. The organization possesses little target analysis, command and control, or learning capability.

**Advanced-Structured:** The capability to conduct more sophisticated attacks against multiple systems or networks and possibly, to modify or create basic hacking tools. The organization possesses an elementary target analysis, command and control, and learning capability.

**Complex-Coordinated:** The capability for coordinated attacks capable of causing mass-disruption against integrated, heterogeneous defenses (including cryptography). Ability to create sophisticated hacking tools. Highly capable target analysis, command and control, and organization learning capability (Devost, 1995)

**Cyber Attacks that have occurred in the past**

As listed by Dorothry Denning in her article on “Cyberterrorism”.

In 1996, a computer hacker allegedly associated with the White Supremacist movement temporarily disabled a Massachusetts ISP and damaged part of the ISP's record keeping system. The ISP had attempted to stop the hacker from sending out worldwide racist messages under the ISP's name. The hacker signed off with the threat, "you have yet to see true electronic terrorism. This is a promise." (Denning, 2000)

In 1998, Spanish protestors bombarded the Institute for Global Communications (IGC) with thousands of bogus e-mail messages. E-mail was tied up and undeliverable to the ISP's users, and support lines were tied up with people who couldn't get their mail (Ronefeldt, 1992). The protestors also spammed IGC staff and member accounts, clogged their Web page with bogus credit card orders, and threatened to employ the same tactics against organizations using IGC services. They demanded that IGC stop hosting the web site for the Euskal Herria Journal, a New York-based publication supporting Basque independence. Protestors said IGC supported terrorism because a section on the Web pages contained materials on the terrorist group ETA, which claimed responsibility for assassinations of Spanish political and security officials, and attacks on military installations. IGC finally relented and pulled the site because of the "mail bombings."

In 1998, ethnic Tamil guerrillas swamped Sri Lankan embassies with 800 e-mails a day over a two-week period. The messages read "We are the Internet Black Tigers and we're doing this to disrupt your communications." Intelligence authorities characterized it as the first known attack by terrorists against a country's computer systems.

During the Kosovo conflict in 1999, NATO computers were blasted with e-mail bombs and hit with denial-of-service attacks by hacktivists protesting the NATO bombings. In addition, businesses, public organizations, and academic institutes received highly politicized virus-laden e-mails from a range of Eastern European countries, according to reports. Web defacements were
also common. After the Chinese Embassy was accidentally bombed in Belgrade, Chinese hacktivists posted messages such as "We won't stop attacking until the war stops!" on U.S. government Web sites (Denning, 2000).

Since December 1997, the Electronic Disturbance Theater (EDT) has been conducting Web sit-ins against various sites in support of the Mexican Zapatistas. At a designated time, thousands of protestors point their browsers to a target site using software that floods the target with rapid and repeated download requests. EDT's software has also been used by animal rights groups against organizations said to abuse animals. Electro hippies, another group of hacktivists, conducted Web sit-ins against the WTO when they met in Seattle in late 1999. These sit-ins all require mass participation to have much effect, and thus are more suited to use by activists than by terrorists (Lal, 2002).

Another example is India and Pakistan engaging in a cyber protest caused by national and ethnic differences (Waalia, 2001). After a cease-fire in the Kashmir Valley hackers took it upon themselves to continue the hostilities. In 2000, pro-Pakistani hackers defaced more than 500 Indian web sites. Conversely, only one known Pakistani site was hacked by the Indians. This illustrates a large difference in technical, hacking abilities or the willingness to use the skills to strike at an adversary. In this event the apparent level of sophistication on both sides is relatively low. Web site defacements are the leading form of this protest. The group G-Force Pakistan was the most active group claiming involvement in the events.

**Al-Qaeda organizations Cyber Capabilities**

There has been very little evidence that points to the Al-Qaeda launching cyber attacks against critical infrastructure. Inspite of its highly sophisticated logistical and organizational capability, to date, has launched only physical attacks that have been clearly "low-tech. There has been
significant, reports, stating that Bin Laden and his Al-Qaeda organization use computer and telecommunication technology to a great extent on a daily basis. (Gellman, 2002)

In the wake of the September 11th attacks, Osama Bin Laden reportedly gave a statement to Hamid Mir (editor of the Ausaf newspaper) indicating that:

“hundreds of young men had pledged to him that they were ready to die and that hundreds of Muslim scientists were with him and who would use their knowledge in chemistry, biology and (sic) ranging from computers to electronics against the infidel. He said they had no atom bombs and missiles but the passion for jihad was more important than those weapons.”

This statement clearly suggests that the most wanted terrorist of the 21st century, Osama Bin Laden, is threatening to use cyberterrorism against the West. Bin Laden’s has financial resources, which would enable him or his organization to purchase the equipment and expertise required for a cyber attack and mount such an attack in very short order. Though there has been no report of an attack directly associated with the Al-Qaeda organization, there has been a cycle of attacks coming from hackers sympathetic to the cause of Islamic extremists.

Not surprisingly, foreign intelligence has adapted to using cyber tools as part of their espionage tradecraft. Ever as far back as 1986, before the worldwide surge in the Internet use, the KGB employed West German hackers to access Department of Defense systems in the well-known “Cuckoo’s Egg” case. It should not surprise to anyone that foreign intelligence services increasingly view computer intrusions as a useful tool for acquiring sensitive U.S. government and private sector information (Freeh, 2000).

**Cyber Attacks during Gulf War**

The United States vulnerability to an attack on its computer systems was demonstrated by attacks on Department of Defense computer systems during the Gulf War. The Testimony before a
Senate committee confirmed that (Mann, 1994), computer hackers from the Netherlands penetrated thirty-four Department of Defense computer sites during April and May of 1991. Some of the highlights from the report are as follows:

Many of the sites gave the hackers access to unclassified, sensitive information on topics such as:

(i) military personnel--personnel performance reports, travel information, and personal reductions

(ii) logistics - descriptions of the type and quantity of equipment being moved; and

(iii) weapons system development data.

Although the information is unclassified, it can be highly sensitive, particularly during times of international conflict. For example, information from at least one system, which was successfully penetrated at several sites, directly supported Operation Desert Storm/Shield. In addition, according to one DOD official, personnel information can be used to target employees who may be willing to sell classified information.

U.S. soldiers put their lives on the line to fight a war for a country that cannot even protect the sensitive information related to their activities, let alone personal data that could be used against their families. What is most distressing about the report is its conclusion that the hackers exploited known security holes to gain access to a majority of these systems. The United States government knew that these security holes were there, yet it did nothing to fix them. The report also indicates that the hackers "modified and copied military information," and that many of the sites were warned of their vulnerability but failed to realize the implications. The report ends with a warning of things to come: "Without the proper resources and attention, these weaknesses will continue to exist and be exploited, thus undermining the integrity and confidentiality of government information."
Dutch hackers are known to be one of the most respected hacking groups in the world.

Fortunately the Dutch exploits were for only educational purposes (U.S.D.O.D, 1991). Their attacks have been low level, open and recorded by video. They made sure that their explorations were noticed and hence created a user account named 'Vice President Quayle'. If only one of the Dutch hackers had an alliance with the Iraqi armed force or had a malicious intent the damage that could have been inflicted on the Allied operations in the Gulf is unimaginable.
Networked Terrorism

What has been emerging in the business world is now becoming apparent in the organizational structures of the newer and more active terrorist groups, which appear to be adopting decentralized, flexible network structures. The rise of networked arrangements in terrorist organizations is part of a wider move away from formally organized, state-sponsored groups to privately financed, loose networks of individuals and subgroups that may have strategic guidance but that, nonetheless, enjoy tactical independence (Arquilla & Ronfeldt, 1997).

For example, in the Greater Middle East, terrorist organizations have diverse origins, ideologies, and organizational structures but can be categorized roughly into traditional and new-generation groups. Traditional groups date to the late 1960s and early 1970s, and the majority were (and some still are) formally or informally linked to the Palestine Liberation Organization (PLO). Typically, they are also relatively bureaucratic and maintain a nationalist or Marxist agenda. These groups have utilized autonomous cells as part of their organizational structure, but the operation of such cells is guided by a hierarchy through clear reporting relationships and virtually little horizontal coordination.

In contrast, the newer and less hierarchical groups (such as Hamas; the Palestinian Islamic Jihad; Hizbollah; Algeria’s Armed Islamic Group; the Egyptian Islamic Group; and Osama bin Laden’s terrorist network, al-Qaeda) have become the most active organizations. In these loosely organized groups with religious or ideological motives, operatives are part of a network that relies less on bureaucratic fiat and more on shared values and horizontal coordination mechanisms to accomplish its goals (Arquilla & Ronfeldt, 1997).
The new and more active generation of Middle Eastern groups has operated both inside and outside the region. For instance, in Israel and the occupied territories, Hamas and to a lesser extent the Palestinian Islamic Jihad have demonstrated their strength over the last five years with a series of suicide bombings that have killed more than 100 people. In Egypt, the Islamic Group (also known as al-Gama’a al-Islamiya) carried out a 1997 attack at Luxor, killing 58 tourists and four Egyptians. Another string of terrorist attacks (and foiled attempts) has focused attention on a loosely organized group of “Arab Afghans”—radical Islamic fighters from several North African and Middle Eastern countries who have forged ties while resisting the Soviet occupation of Afghanistan. One of the leaders and founders of the Arab Afghan movement is Osama bin Laden, a Saudi entrepreneur based in Afghanistan (Gambill, 2000).

To varying degrees, these groups share the principles of the net-worked organization—relative flatness, decentralization and delegation of decision making authority, and loose lateral ties among dispersed groups and individuals. Hamas, for example, is loosely structured with some elements working clandestinely and others working openly through mosques and social service institutions to recruit members, raise money, organize activities, and distribute propaganda. According Arquilla and Ronfeldt in their RAND report, which was the result of a year long project sponsored by the air force deputy chief of staff for air and space operations, these developments indicate the emergence of a new form of terrorism known as “netwar”. According to the report, Netwar is quickly changing the way terrorist groups operate and communicate so it requires government agencies to develop new defensive strategies (Arquilla & Ronfeldt, 1997).

**Netwar**

This term 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 attuned to the information age. The ability of terrorist
groups to capitalize on modern technology is now a requisite for developing in the underlying basis for effective and robust activity. In previous decades, terrorist groups were initially constrained because accumulation of sizable resources was inevitably linked to sufficient manpower and the ability to keep growth activities clandestine. The recent introduction of information technology has not lessened the need to accumulate similar resources but has had major implications for how they are accrued.

Terrorist groups are relying increasingly on the advanced communications and networks technologies to revolutionalize the way they organize and carry out attacks, according to Arquilla and Ronefeldt’s report. In this sense terrorist groups are simply exploiting modern tools to accomplish the same goals they sought in the past. The difference between conventional terrorist tactics and those involving computers can be found in three key points:

i) Ease of operation

ii) Developing potential

iii) Increased anonymity

None of these activities are easily detected or readily countered and this enables terrorist groups that take advantage of the information technology to create viable support structures to further their tactical and strategic goals. These are accomplished through

i) Political propaganda

ii) Recruitment

iii) Financing

iv) Intra and inter group communication

v) Information/intelligence gathering

vii) Stealth/anonymity in the routine activity and tactical operations
According to Ronald L Dick, Director of National Infrastructure Protection center of the FBI (Dick, 2001), in his congressional statement on issue of intrusions into government computer Networks in 2001, "Terrorist groups are increasingly using new information technology and use Internet to formulate plans, raise funds, spread propaganda and to communicate securely. Director of Central Intelligence George Tenet, in his statement on the world wide threat in 2000, testified that the terrorists groups including Hizbollah, HAMAS, the Abu Nidal organization and Bin Laden’s Al-Qaeda organization are using computerized files, e-mail ad encryption to support operations" Ronal L. Dick, quoted as an example where convicted terrorist Ramzi Yousuf, the master mind of the World Trade Center bombing, stored detailed plans to destroy United States airliners on encrypted files on his lap top computers. Ronald. L. Dick stated, "whole we have not seen these groups employ cyber tools as a weapon to use against critical infrastructure, their reliance information technology and acquisition of computer expertise are clear warning signs. More over we have seen other terrorist groups such as Internet Black Tigers (who are affiliated with Tamil Tigers); engage in attacks on foreign government web site and e-mail servers. During the riots on the west bank in the fall of 2000, Israeli government sites were subjected to e-mail flooding and "ping "attacks. The attacks allegedly originated with Islamic elements trying to inundate the systems with e-mail messages. As one can see from these examples overseas, "cyber terrorism"......meaning the use of cyber tools to shutdown critical national infrastructure such as energy, transportation or government operations for the purpose of coercing or intimidating a government or civilian population------ is thus a very real threat".

It has been observed by Arquilla and Ronefeldt that most modern adversaries of nation states in the spectrum of low-intensity conflicts, such as guerilla insurgents, drug smuggling cartels, as well as racial and tribal gangs are all well organized networks even though their leadership may be quite hierarchical. This could be one of the reasons why military and police institutions often
face difficulty in engaging in low intensity conflict. They are not configured to combat such groups. This implies that it requires a network is needed to counter another network. (Arquilla and Ronefeldt, 1997). The future may belongs to whoever masters the network

Arquilla and Ronfeldt describe how transnational terrorists use flexible network designs that may have multiple leaders. They suggest that transnational terrorist groups are increasingly building transnational networks as “force multipliers” and using all manners of old and new technologies to do so. The shift is from absolute hierarchies, to hydra-headed networks, which are less easy to decapitate than once they have been. Arquilla and Ronfeldt say Netwar has been modeled by trends that have been reshaping big global institutions for years. One is the growing influence of ‘non-state actors’-corporations, activist groups and other non-governmental organizations and networks. A second trend is the flattening of hierarchies, both racial and managerial and their replacement with more fluid and horizontal organizational forms. A third factor is the explosive growth of computer and telecommunications networking. When these trends take on military mien, the result is this:” The world’s most virulent aggressors are not armies whose order of battle is tidy ziggurat of corps, divisions and brigades but amorphous networks of terror and crime groups like Osama bin Laden’s Al-Qaeda and it affiliates, the Irish Republican Army, and Columbian narco-trafficking cartels.”

Richard. E. Hayes, president of Evidence based research a company that advises the military on issue like command and control and information warfare, says, “Al Qaeda and its cousins are designed to exploit all the advantages of networking robustness, speed, flexibility that business has discovered. Communications is multi-directional. Command is shared. People are multi-skilled. Trust is high”.
The FBI investigation into Hamas activity in the US indicates part of Hamas' command and control was located in Tampa, Florida. This is now believed to have moved to London. In London it publishes Filistine Al Muslima and also has some of its fund raising infrastructure. Another good example of network form of organizations among terrorist groups is the Algerian Armed Islamist Group (GIA). The GIA appears to have had a command and control center in Britain for a few years untouche by British authorities (Whine, 1998).

To realize its potential an inter-connected network, requires a capacity for constant, dense information and communication flows, more so than do other forms of organizations (e.g. Hierarchies). This capacity is afforded by the latest information and communications technologies-cellular phones, fax machines, electronic mail (email), world wide web (www) sites and conferencing. Moreover, network agents are poised to benefit from future increases in the speed of communications, dramatic reduction in the cost of communications increases in bandwidth, vastly expanded connectivity, and integration of communication with computing technologies. Such technologies are highly advantageous for Netwar actor whose constituents are geographically dispersed (Arquilla & Ronefeldt, 1997).

The means by which information technology is used by terrorist groups to maintain control over their networks is briefly discussed below:

**Communications**

Micheale Zinini and Sean J.A.Edwards in their report on "The Networking of Terror in the Information Age", state that IT can be used to plan, coordinate, and execute operations. Using the Internet for communication can increase speed of mobilization and allow more dialogue between members, which enhances the organizations flexibility, since tactics can be adjusted more frequently, individuals with a common agenda and goals can form, sub-groups, meet at a
Terrorism

target, locate, conduct terrorist operations and they readily terminate the relationships and re-disperse (Zannini & Edwards, 1999).

The Bin Laden network appears to have adopted information technology to support its network mode of operations. According to reporters who visited Bin Laden's headquarters in a remote mountainous region of Afghanistan, the terrorist financier has modern computer and communications equipment. Bin Laden allegedly used satellite phone terminals to coordinate the activities of the groups dispersed operations and has ever devised counter measures to ensure his safety while using such communications systems. Satellite phones reportedly travel in separate convoys from Bin Laden; he also refrains from direct use, often dictating his message to an assistant who then relays it telephonically from a different location. Bin Laden's operatives have used CD-ROM disks to store and disseminate information on recruiting, bomb making, heavy weapons and terrorist operations (Whine, 1998). US intelligence agencies recently obtained computer-disk copies of six volume-training manuals used by Bin Laden to train his recruits. Egyptian computer experts who fought alongside Bin Laden in the Afghan conflict are said to have helped him devise a communications network that relies on the web, email and electronic bulletin board so that members can exchange information.

Counter terrorist operations targeting Algerian Armed Islamic Group (GIA) bases in 1990s uncovered computers and diskettes with instructions for the instructions for the construction of bombs. In fact, it has been reported that the GIA makes heavy use of floppy disks and computers to store and process orders and other information for its members, who are dispersed in Algeria and Europe (Whine, 1998). Among terrorist organizations, posting material to inform its members of its activities are the previously noted Hizb ut-Tahrir whose posting provides details, including time and date of its regular meetings around the UK. The militant Islamic group Hamas also uses the Internet to share and communicate operational information. Hamas activists in the United States use chat rooms plan operations and activities. Hamas' use of pass worded and
coded messages, clearly presents problems for security agencies. A recent article in Jane’s foreign report suggested that the Islamic security services have been unable to crack the code used by Hamas. Operatives use e-mail to coordinate actions across Gaza, West Bank and Lebanon. Hamas has profited to a great extent on secure information exchange on the Internet because counter terrorism intelligence cannot accurately monitor the flow and content of all Internet traffic.

“According to Israelis, the unidentified terrorists are using the Internet. Without offering evidence, investigators in the security service, Shin Beth, assert that a full range of instructions for terrorist attacks, including maps, photographs, directions, codes and even technical details of how to use the bombs, are being transferred through the Internet. They suspect that many of the instructions are sent from Britain, where they say that the Islamic/Palestine organization, Hamas has its main “European base” (Whine, 1998).

**Connectivity**

Terrorist recruitment and financing have been enhanced by computer networks. There have been reports of various supremacists groups in the United States using the Internet for financial gain. It has also been found that terrorist groups such as Peru’s Shining Path have websites where supporters seek to export the revolutionary products like t-shirts, posters and videos.

IT has given the opportunity for individuals and groups to reach and influence a larger audience that was previously only reserved for well organized, state funded terrorist organizations. It represents, in many respects, the “death of distance”. The physical distance and national boundaries which used to distant terrorist from their conspirators, their audience and their targets seem to have faded away in the world of modern telecommunications and the Internet.
One of the spokesman is reported to have said, "The service is very important for the morale of the resistance fights. They are always very happy to know that people around the world are backing them".

Other groups include "news agencies" which take in postings from other Islamic sites and reproduce them. Foremost among them is MSA News, originating in the state of Ohio. On their site one can see messages from the HS, GIA and Yakub Zaler, among others.

A posting on June 25 1996, advertised a FIS rally to take place in London Trafalgar Square on July 7, on behalf of "FIS leaders unjustly detained in Algeria and all prisoners of faith". The contact address was given as the Algerian community in Britain, operating from a west London post office box. The speakers were advertised as Tahir De LaNive of the Islamic council for the defense of Europe, Dr. Amaniar, spokesman for the Afghan Mujahedeen, Dr. Abdul bari of the Islamic forum in Europe, Dr. Fuzal Khan, leader of Al-Mujahajiroun in Mauritius, Prof. Francious Burgat, Institute of Research and studies of the Arab world and Muslims (Whine, 1998). Another news agency is Quds Press, which advertises itself as the first Arabic online news agency reproducing communiqués in English and Arabic, and it appears to have offices in London and Amman.

The site of the campaign for the Defense of Legitimate Rights (CDLR) contains also postings from groups not connected with it, as does Global Media Monitoring, the site of the London based journalist, Parvez Sayed. One of the terrorist sites that particularly aims its message to the outside worlds is that connected linked to Hizb-ut-Tahir, the Islamic Liberation Party. This first UK based site was hosted by Imperial College London. But soon after following complaints to the college authorities, the site was pulled down temporarily, until a new host could be found. They now post in their names Hizb-ut-Tahir and as Khalifa, providing Internet based access to their hard-copy material, their literature and their regional activities. Omar Bakri Mohamed the
leader of Al-Mujahiroun, (The emigrants) was the founder of Hizb-ut-Tahir in Britain. He later split from it, claiming differences with middle based leadership. It has been reported that he also provides details of its activities as well as lists of its hard-copy publications and contacts on his website (Whine, 1998).

Another evangelical Islamist organization, Al Muhrabitun, also posts regularly providing details of its activities and its historical development.

The fact that many terrorists now have direct control over the content of their message offers father opportunities for perception management, as well as for image manipulation, special effects and deception.

An Internet presence can prove advantageous for mobilizing “part time cyber terrorists”-individuals not directly affiliated with a given terrorist group who nonetheless support its agenda and whom malicious software tools and instructions available at a terrorist web site. This scenario would closely resemble the initiative taken by both the Israeli and Palestinian governments which have encouraged private citizens to download computer attack tools and become involved in the conflict surrounding that the al-Aqsa intifadah (Arquilla and Ronefeldt, 1997).

Nearly all the terrorists groups have a web presence. Hizbollah manages multiple web sites. Web sites can also be used to refine or customize recruiting techniques. Recording which types of propaganda receive the most browser hits could help tailor a message for a particular audience using some the same marketing techniques employed by commercial enterprises, terrorism servers could capture information about the users who browse their websites and then later contact those who seem most interested. Recruiters may also use more interactive Internet
technology to roam online chat room and cyber cafes looking for respective members of the public, particularly young people. Electronic bulletin board and user nets can also serve as vehicles for reaching out to potential recruits. Interested computer users around the world can be engaged in long-term cyber relationship that could lead to friendship and eventual membership (news.com).

Sample of the websites belonging to the terrorist groups:

<table>
<thead>
<tr>
<th>Group Name</th>
<th>Country of Origin</th>
<th>Web address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Almurabeton</td>
<td>Egypt</td>
<td><a href="http://www.almrabeton.org">www.almrabeton.org</a></td>
</tr>
<tr>
<td>Al-Jama’ah Al Islamiyyah</td>
<td>Egypt</td>
<td><a href="http://www.webstorage.com/~azzam/">www.webstorage.com/~azzam/</a></td>
</tr>
<tr>
<td>Hizb Al-Ikhnan</td>
<td>Lebanon</td>
<td><a href="http://www.hizbollah.org">www.hizbollah.org</a></td>
</tr>
<tr>
<td>Al-Muslimoon</td>
<td></td>
<td><a href="http://www.almanar.com.lb">www.almanar.com.lb</a></td>
</tr>
</tbody>
</table>

Two London based opponents of Al-Saud, dr. Muhammad Al Masari of the committee for the Defense of Legitimate Rights(CDLR) and his erstwhile colleague Dr.Saad al Faqqih, now leader of the movement for Islamic reform, have embraced the Internet as a tool. Another Saudi opposition group in the USA has set up its own world wide web homepage while a number of the Internet discussion groups based in USA provide a means for dissidents to air their views and contact one another. The London based Bahrain opposition movement, The Bahrain Freedom Movement (BFM), also uses the net to spread their message, just as they used newsletters or posters in the past. Due to the limited Internet access in Saudi Arabia and Bahrain, their propaganda campaigns have been targeted mainly at western audience and their compatriots living in the west. They have, therefore only begun to exploit the potentialities of their new medium. Once networks spread within the Gulf countries then the net will enable dissidents to exchange information about events much more easily than at present. Once opposition groups gain more sophistication they will be able to deploy a full range of offensive information warfare techniques, not restricted to psychological warfare propaganda (Arquilla & Ronefeldt, 1997)
Information Technology Tools used by Terrorists

Encryption

One tool that has become important to terrorist is encryption, as it allows activists to protect communications and stored information from government interception.

Encryption is a software tool that uses various scrambling techniques to make data unreadable to anyone other than the intended recipient. Internet users who make purchases online are undoubtedly familiar with one form of encryption, the Secure Socket Layer (SSL) technology used to safely transmit credit card account numbers to e-commerce web sites (Denning, 1999). By encrypting a message original text is manipulated so that it can be read only by using a key that unlocks the encryption and makes the text readable. The encryption technology that has been rated highly reliable is the public key encryption system. It has two keys – private and public. The user of the system distributes the public key to his/her clients. The message intended for the user can be encrypted using the public key. The encrypted message can only be decrypted using the corresponding private key. As the user is the only owner of the private key, nobody else can read the encrypted message.

As this technology provides a highly reliable encryption mechanism that is quite difficult to crack, it should be positive news for persons who value privacy. Apart from its obvious role in upholding and furthering the human rights initiatives, the strong encryption technology that helps conduct secured transactions will naturally augment the commercial transactions over the Internet.
One major argument against the free wide circulation of this technology is that it can be used by antisocial elements and political terrorists to safely correspond and co-ordinate their nefarious activities against the legally established systems. Terrorist networks can protect their vital communication flows through readily available commercial technology, such as encryption programs.

Michelle Zanini and Sean Edwards in their RAND report state that Animal Liberation Front cells in North America and Europe use encryption program (PGP) to send coded email and share intelligence (Zannini & Edwards, 1999). New encryption programs emerging in the market are becoming so sophisticated that coded emails may soon be extremely difficult to break. Rumors persist that the French police have been unable to decrypt the hard disk on a portable computer belonging to a captured member of the Spanish/Basque organization ETA. FBI Director Louis Freeh said last March during closed-door testimony on terrorism before a Senate panel said (Freeh, 2000), "Uncrackable encryption is allowing terrorists - Hamas, Hezbollah, Al-Qaeda and others - to communicate about their criminal intentions without fear of outside intrusion. They're thwarting the efforts of law enforcement to detect, prevent and investigate illegal activities."

**PGP**

PGP is one of the best examples of encryption software. Human rights activists in Guatemala, credited their use of Pretty Good Privacy (PGP) with saving the lives of witnesses to military abuses (Denning, 1999).

PGP was originally developed by a Colorado engineer and activist, Phil Zimmermann, who wanted to make strong encryption available to the public for privacy protection against government eavesdroppers. The software can be downloaded from the site at: pgpi.org (Denning, 1997). During the installation of the program it automatically installs plug-ins into mail clients.
installed in the system. The plug-ins help to use the PGP features such as sending encrypted messages directly from the mail client’s interface. The plug-ins is available for popular mail clients such as Eudora and Outlook.

The software was export-controlled, but however without the knowledge of Zimmermann someone quickly posted it on a foreign Internet site from where it could be downloaded by anyone, anywhere, despite export regulations. After this incident there have been several other encryption tools that have been posted on Internet sites. Ever since, this has become a major topic of debate that the availability of such tools demonstrates the weakness of export controls.

Denning states that this is one factor driving export policy towards increased liberalization. But other factors have also contributed, including the role of encryption in electronic commerce and a concern that export controls harm the competitiveness of industry. However, that drive is countered, by a concern that the widespread availability of encryption tools over the Internet will make it tougher for law enforcement and intelligence agencies to gather intelligence from communication interceptions.

U.S. officials say Bin Laden’s organization Al-Qaeda. It is believed that he uses money from Muslim sympathizers to purchase computers from stores or by mail. Officials say that Bin Laden’s followers download easy-to-use encryption programs from the Web and have used the programs to help plan carry out the following three of their most recent plots (Arquilla & Ronefeldt, 1997):

(ii) Khalil Deek, an alleged terrorist arrested in Pakistan in 1999, used encrypted computer files to plot bombings in Jordan at the turn of millennium, U.S. officials say. Authorities found Deek’s computer at his Peshawar, Pakistan, home and flew it to the National Security Agency in Fort Meade, Md. Mathematicians, using supercomputers, decoded the files, enabling the FBI to foil the plot.

(iii) Ramzi Yousef, the convicted mastermind of the World Trade Center bombing in 1993, used encrypted files to hide details of a plot to destroy 11 U.S. airliners. Philippines officials found the computer in Yousef’s Manila apartment in 1995. U.S. officials broke the encryption and foiled the plot. Two of the files, FBI officials say, took more than a year to decrypt.

Attorney General Janet Reno told a presidential panel on terrorism headed by former CIA John Deutsch states that extremist groups not only use encryption to disguise their e-mails but their voices, too (usatoday.com). Encryption programs are capable of scrambling telephone conversations when the phones are plugged into a computer.

**E-Mail Bombs**

Intentional bombardment of servers with thousands of messages at once, distributed with the aid of automated tools, can be termed as ‘E-Mail Bombing’. It effects in completely jamming a recipient’s incoming e-mail box, making it impossible for legitimate e-mail to get through. An e-mail bomb hence can also be viewed as a form of virtual blockade. Although e-mail bombs are often used as a means of revenge or harassment, they have also been used to protest government policies.

U.S. intelligence authorities characterized the Tamil Guerillas’ attack as the first known attack by terrorists against a country’s computer systems. The ethnic Tamil guerrillas were said to have swamped Sri Lankan embassies with thousands of electronic mail messages (Radu, 2001). The
messages read "We are the Internet Black Tigers and we are doing this to disrupt your communications." The Liberation Tigers of Tamil Eelam, which had been fighting for an independent homeland for minority Tamils, claimed responsibility for the 1998 incident.

The e-mail bombing consisted of about 800 e-mails a day for about two weeks. As cited by Denning, William Church, editor for the Centre for Infrastructural Warfare Studies (CIWARS), observed that "the Liberation Tigers of Tamil are desperate for publicity and they got exactly what they wanted ... considering the routinely deadly attacks committed by the Tigers, if this type of activity distracts them from bombing and killing then CIWARS would like to encourage them, in the name of peace, to do more of this type of "terrorist activity". The attack was successful in causing fear in the embassies.

The Kosovo conflict also witnessed one of the few e-mail bombing incidents in history. The protestors on both sides e-mail bombed government sites (cnn.com). According to a report, NATO spokesman Jamie Shea reported that their server had been saturated at the end of March by one individual who was sending them 2,000 messages a day. Fox News reported that when California resident Richard Clark heard of attacks against NATO's Web site by Belgrade hackers, he retaliated by sending an e-mail bomb to the Yugoslav government's site. After a few days, 500,000 e-mails brought the site down. Though he did not claim full responsibility, he claimed to have played a part. His Internet service provider, Pacific Bell, cut off his service, as his actions violated their spamming policy.

The San Francisco-based Institute for Global Communications (IGC) was forced to terminate its link with the Basque People's Journal after outraged Spaniards sabotaged the company's computer system by overloading it with a barrage of junk e-mail in 1997 (Denning, 1999). The protestor's wanted the site pulled, their objective was censorship. They bombarded IGC with thousands of bogus messages routed through hundreds of different mail relays. As a result, mail
was tied up and undeliverable to IGC's e-mail users, and support lines were tied up with people who couldn't get their mail. The attackers also spammed IGC staff and member accounts, clogged their Web page with bogus credit card orders, and threatened to employ the same tactics against organizations using IGC services. The only way IGC could stop the attack was by blocking access from all of the relay servers.

IGC pulled the site on July 18, but not before archiving a copy so that others could put up mirrors. Within days of the shutdown, mirror sites appeared on half a dozen servers on three continents. Chris Ellison, a spokesman for the Internet Freedom Campaign, an English group that was hosting one of the mirrors, said they believe "the Net should prove an opportunity to read about and discuss controversial ideas." The New York-based journal maintained their objective was to publish "Information often ignored by the international media, and to build communication bridges for a better understanding of the conflict." An article by Yves Eudes in the French newspaper Le Monde said the e-mail bomb attack against the IGC site represented an "unprecedented conflict" that Ahas opened up a new era of censorship, imposed by direct action from anonymous hackers." (Denning, 1999).

About a month after IGC removed the controversial Basque journal Euskal Herria Journal from its servers, Scotland Yards Anti-Terrorist Squad shut down Internet Freedom's U.K. Web site for hosting the journal. According to a press release from Internet Freedom, the squad claimed to be acting against terrorism. Internet Freedom said it would move its news operations to its U.S. site.

Euskal Herria Journal case illustrates the power of protestors on the Internet. Though IGC chose to ignore the e-mail demands of protestors and continued to host the controversial site, they could not survive the e-mail bomb attack. The case also illustrates the power of the Internet as a tool for freedom of speech. Denning states that because Internet venues for publication are rich and dispersed throughout the world, it is extremely difficult for governments and hacktivists alike to
keep content completely off the Internet. It would require extensive international cooperation and, even then, a site could operate out of a safe haven that did not sign on to international agreements.

**Flight Simulator**

It has been reported that the raids that took place in Florida, where the September 11th attackers lived, officials seized desktop and laptop computers. When they examined the contents of the computer's hard drive, they found information on piloting and crop dusting downloaded from the Internet, as well as a flight simulator program, Microsoft's Flight Simulator software. This has identified Microsoft's Flight Simulator in the media as a possible source of information and inspiration for the terrorists (usatoday.com).

After reports of the September 11th attackers using flight simulators there has been a debate over how much flying can really be learned in computer-based trainers.

Major airlines own and operate sophisticated flight simulators, which cost millions of dollars. It has been reported that at least two of the hijackers were trained on a Boeing 727 simulator facility, in South Florida, in one of the professional schools which is equipped with the flight simulator (usatoday.com).

Experts believe that with the advanced PC-based simulators that are available today, that it would not be unreasonable to expect that someone could learn how to operate the instrumentation of a large jet by using off-the-shelf technology, such as Microsoft Flight Simulator (Gladstone, 2001).

Embry-Riddle, the world's largest university specializing in aviation, shares a flight simulator on its campus with the Flight Safety Academy in Vero Beach. University officials confirmed that suspect Waleed Al Sheri, a WTC attacker, graduated in 1997 with a bachelor's degree in aeronautical science and experienced flight and simulator training.
History of Flight Simulator

In 1979, Bruce Artwick, an electrical engineering graduate student from the University of Illinois along with Stu Moment both the owners of a software company named SubLogic, decided to take the model from Artwick’s graduate thesis (a model of the flight of an aircraft, displayed on a computer screen) one step further and developed the first Flight Simulator program for the Apple-II (bleep.demon.co.uk). It was followed shortly by a version for the Radio Shack TRS-80. Both versions completely coded in their respective machine-code. In January 1980 Sub LOGIC FS1 hit the consumer market. By 1981 Flight Simulator was reportedly the best selling title for the Apple.

In November 1982 Microsoft Flight Simulator 1.01 hit the stores as one of the first PC entertainment titles, shortly after followed by version 2. MS-FS featured a new and sophisticated co-ordinate system for the FS-world, developed by Bruce Artwick. And as with all subsequent releases this first version already demanded so much from computer resources that people had to run to the computer stores to buy bigger and faster machines, primarily for the sake of running Flight Simulator.

Hundreds of utilities are available on Microsoft’s Flight Simulator, which are used to customize the simulator so it replicates the instrumentation of whatever type of airplane one wants to fly—from a Cessna 172S single-engine trainer to the Boeing 747-400 jumbo jet.

The Microsoft Flight Simulator provides the “background material,” said David Silbergeld, who frequently writes reviews of computer-based simulations. “Whatever utility you add on is used for the instrumentation.”

For the most part, the largest markets for these products are in the United Kingdom, Germany and Japan. Software packages range from about $40 to $100. The flight simulators for the Boeing 767 and 757 happen to be very precise. By the end of 1997 Microsoft claimed to have sold not less
than 10 million copies of all versions of FS, making it the best sold software title in the entertainment sector. And in 2000 Microsoft Flight Simulator was taken up in the Guinness Book of Records with 21 million copies sold per June 1999.

Pilots love can familiarize themselves with the controls ... take a look and play around. The simulator is very accurate.

In the simulator, a pilot can practice taking off from New York’s JFK Airport, turn left until heading due west, and see the skyline of Manhattan. “What you see in the box would be what you’d see in a night scene — The World Trade Center was, in fact, simulated,” said Sam Woolsey, a retired United and PanAm captain living in California (nationaldefensemagazine).

Jerry Weltsch, a senior aerospace analyst at Frost & Sullivan Aerospace and Defense Research Group assessed that the Microsoft program is only for desktop use. He concluded that doesn’t give the feel of the aircraft. It is like a familiarization tool. He stated that as it relies on a mouse or joystick to fly the airplane; one does not gain hands-on experience with the controls (Ballengar, 2001).

However, Weltsch asserted that a familiarity with behavioral responses to certain controls in the cockpit and a familiarity with how the instruments on the cockpit panel look are acquired for sure. This helps gain a thorough understanding of altitude, air speed, ground speed, direction relative to switches on the panel and how the airplane responds to certain inputs.

Flight Simulator 2002 comes with a new artificial intelligence system that generates air traffic around and between airports. It also has enhanced virtual cockpits with working instruments. Maps and graphs show the operators how well they maintain course and altitude. A “graphical flight planner,” is used to plot the route from departure to destination on an interactive map.

According to Weltsch, the hijackers, trained in flight simulators under the supervision of well trained flight instructors. They gained experience of flying in the simulator. They may have used
Microsoft Flight Simulator 2000 just to see what it would look like—from the cockpit of the type of airplane they were going to use, with the panel in front of them—to fly into the World Trade Center.

According to the FBI press reports, the 19 suspected terrorists received flight training from at least 10 U.S. flight schools.

**Steganography**

Another technology the terrorists may have used is steganography. According to Markus Kuhn (about.com), "Steganography is the art and science of communicating in a way which hides the existence of the communication. In contrast to cryptography, where the enemy is allowed to detect, intercept and modify messages without being able to violate certain security premises guaranteed by a cryptosystem, the goal of steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second secret message present"

Although not widely used, digital steganography involves the hiding of data inside a sound or image file. Steganalysis is the process of detecting steganography by looking at variances between bit patterns and unusually large file sizes.

A person who views the picture file with a secret message will only see the normal picture without any distortion; where as the intended recipient can view the data using a steganographic tool. The effect is that the sender can transmit a message without ever communicating directly with the receiver. There is no e-mail between them, no remote logins, and no instant messages. All that exists is a picture posted to a public forum, and then downloaded by anyone sufficiently enticed by the subject line (both third parties and the intended receiver of the secret message) (about.com).
<table>
<thead>
<tr>
<th>POSSIBLE USES OF STEGANOGRAPHY</th>
<th>DRAWBACKS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Used to combine explanatory information with an image (like doctor's notes accompanying an X-ray)</td>
<td>Could accidentally degrade or render an image misleading</td>
</tr>
<tr>
<td>Embedding corrective audio or image data in case corrosion occurs from a poor connection or transmission</td>
<td>Could counteract and be counterproductive with the original image</td>
</tr>
<tr>
<td>Peer-to-peer private communications</td>
<td>Doesn't hide the fact that an e-mail was sent negating the purpose of secret communications</td>
</tr>
<tr>
<td>Posting secret communications on the Web to avoid transmission</td>
<td>Someone else with a steganography detection and cracking tool could expose the message</td>
</tr>
<tr>
<td>Copyright protection</td>
<td>A form of this already exists, called digital watermarking, but requires use of separate hardware tools because steganographic software can't use separate hardware tools. Steganographic software also can't protect the watermark.</td>
</tr>
</tbody>
</table>

There have been reports about possible use of Steganography technology by terrorists, however there are no concrete evidence to prove this.

The first allegation of terrorist groups using steganography technology was made USA Today in February this year. The report said that "hidden in the X-rated pictures on several pornographic Web sites and the posted comments on sports chat rooms may lie the encrypted blueprints of the next terrorist attack against the United States or its allies".

The Pentagon's daily newsletter Early Bird carried an article on October 18th, warning that Al Qaeda was planning a "major biological attack". "The warning was believed to have been based on an analysis made by former National Security Agency instructor and experimental nuclear physicist, Dr Robert Koontz. The article said that Dr Koontz had "discovered evidence on the Internet that Osama bin Laden was planning a major biological warfare campaign, using more
than one form of germ agent. According to Koontz, the Al Qaeda leader was using "coded"
illustrations to signal and direct additional sleeper agents purportedly already armed with
biological weapons" (Lyman, 2001).

However, there has been no substantial evidence given by the FBI proving the use of
steganography by terrorists.
Information Technology to Counter Terrorism

President Clinton’s administration saw the biggest economic growth in history with the innovation of the new information era. During his eight-year presidency, President Clinton used information technology to help create a record period of economic prosperity for the United States. During President Clinton's administration, policies were introduced to advance computing and communications programs and funding was increased into key areas of IT through a number of initiatives.

Even after his presidency, the former president has been a devoted lobbyist of Information Technology.

President Clinton spoke to BBC World Click Online presenter, Stephen Cole, from the 2002 World Congress on Information Technology (WCIT) in Adelaide after addressing delegates on the information divide between rich and poor countries. He explained how he believes the availability of just one Internet-connected computer in a remote or poor area would make an enormous difference. President Clinton said, "I believe that technology gives us a chance to skip a whole generation in time in the development of educational, economic, health and environmental advances in the poorest countries in the world".

President Clinton also discussed the implications of being in an interdependent 'global village' in terms of global warming and terrorism and suggested how IT can help to combat terrorism by using it more efficiently to track patterns of behavior via information management systems. President Clinton said, "You can look for patterns, then if someone with an American visa has ten addresses they are either really rich or up to no good...You can also use Information Technology
Information Technology to Counter Terrorism

President Clinton’s administration saw the biggest economic growth in history with the innovation of the new information era. During his eight-year presidency, President Clinton used information technology to help create a record period of economic prosperity for the United States. During President Clinton's administration, policies were introduced to advance computing and communications programs and funding was increased into key areas of IT through a number of initiatives.

Even after his presidency, the former president has been a devoted lobbyist of Information Technology.

President Clinton spoke to BBC World Click Online presenter, Stephen Cole, from the 2002 World Congress on Information Technology (WCIT) in Adelaide after addressing delegates on the information divide between rich and poor countries. He explained how he believes the availability of just one Internet-connected computer in a remote or poor area would make an enormous difference. President Clinton said, "I believe that technology gives us a chance to skip a whole generation in time in the development of educational, economic, health and environmental advances in the poorest countries in the world".

President Clinton also discussed the implications of being in an interdependent 'global village' in terms of global warming and terrorism and suggested how IT can help to combat terrorism by using it more efficiently to track patterns of behavior via information management systems.

President Clinton said, "You can look for patterns, then if someone with an American visa has ten addresses they are either really rich or up to no good...You can also use Information Technology
to build better protections for your water systems, your transportation networks and certainly to build walls against cyber terrorism... so a big part of dealing with this terrorist threat will be maximizing the use of technology for defensive purposes."

Experts agree that technology has a role to play in protecting the US from terror attacks. But they warn that much depends how that technology is used in practice. In the aftermath of September 11th, it emerged that various government agencies had information that might have helped prevent the attacks. But the problem was that the data were spread over different bodies and different computer systems (news.bbc.co.uk).

"A piece of data in isolation may mean absolutely nothing, but put together with other fragments of data, it may suddenly paint a picture," explained said Dr Ruth David, president of Anser, an independent research institution in the US (news.bbc.co.uk).

The FBI is increasingly relying upon technologies to counter terrorism. The FBI has a state of the art, on-line computer database known as the Terrorist Information System (TIS) containing information on suspected terrorist groups and individuals. The system has over 200,000 individuals and over 3000 organizations or enterprises. The individuals indexed include not only subjects of investigations but also known or suspected members of terrorist groups, associates, contacts, victims and witnesses. The organizations or enterprises include not only terrorist groups but also affiliated organizations or enterprises. TIS allows the FBI to rapidly retrieve information and to make links between persons, groups or events (Tritak, 2000).

**New IT for detection, prevention, remediation, and attribution of attacks**
Promising to play a central role in the future prevention, detection, and remediation of terrorist acts, "information fusion" is defined as the use of computer technology to acquire data from many sources, integrate these data into usable and accessible forms, and interpret them. Such processed data can be particularly valuable for decision makers in law enforcement, the intelligence community, emergency-response units, and other organizations combating terrorism. Not surprisingly, an inherent problem of information fusion is data interoperability—the difficulty of merging data from multiple databases, multiple sources, and multiple media. In the book Making the Nation Safer: The Role of Science and Technology in Countering Terrorism, the Committee on Science and Technology for Countering Terrorism of the National Research Council has proposed ways in which information fusion can be utilized for security (NATIONAL ACADEMIES PRESS, 2002).

**Prevention:** Security checkpoints have become more important and more tedious than ever at airports, public buildings, sporting venues, and national borders. But the efficiency and effectiveness of checkpoints could be significantly improved by creating information fusion tools to support the checkpoint operator in real time. For example, future airport-security stations could integrate data received from multiple airports to provide a more global view of each passenger's luggage and activities on connecting flights. The stations could use data-mining methods to learn which luggage items most warrant hand-inspection, and they could capture data from a variety of biometric sensors to verify the identities of individuals and search for known suspects (NATIONAL ACADEMIES PRESS, 2002).

**Detection:** Intelligence agencies are routinely involved in information fusion as they attempt to track suspected terrorists and their activities, but one of their primary problems is managing the flood of data. There are well-known examples in which planned terrorist activity went undetected despite the fact that relevant evidence was available to spot it. The evidence was just one needle in a huge haystack. Future intelligence and law-enforcement activities could therefore benefit
enormously from advances in automatic interpretation of text, image, video, sensor, and other kinds of unstructured data. This would enable the computer to sort efficiently through the massive quantities of data to bring the relevant evidence (likely combined from various sources) to the attention of the analyst (NATIONAL ACADEMIES PRESS, 2002).

*Response:* Early response to biological attacks could be supported by collecting and analyzing real-time data, such as admissions to hospital emergency rooms and veterinary offices or purchases of drugs in grocery stores, and integrating it with background information about the affected patient’s residence and job address. Prototype systems are already under development, including one that monitors real-time admissions to 17 emergency departments near Pittsburgh, to generate profiles of ER visits, and discern patterns of activity. If anomalous patterns emerge that may signify an outbreak of some new pathogen, system administrators can quickly alert health officials (NATIONAL ACADEMIES PRESS, 2002).

Many other opportunities exist for such computer-aided “evidence-based decision making.” For example, the monitoring of activity on computer networks might flag potential attempts to break through a firewall; or sensor networks attached to public buildings might flag patterns of activity within the building that suggest suspicious behavior. In these kinds of cases, because the data is voluminous and derives from a variety of sources, an unaided decision maker might have difficulty detecting subtle patterns.

As a general proposition, the development of tools that provide human analysts with assistance in doing their jobs has a higher payoff (at least in the short to medium term) than tools that perform most or the analyst’s entire job. This places a greater emphasis on approaches that use technology to quickly sift large volumes of data to flag potentially interesting data items for human attention (as opposed to approaches that rely on computers to make high-level inferences themselves in the absence of human involvement and judgment).
A final dimension of information fusion is non-technical, that is, disparate institutional missions may well dictate against a sharing of information at all. Underlying successful information fusion efforts is a desire to share information. It is impossible to fuse information belonging to two agencies if those two agencies do not communicate with each other. Establishing the desire to communicate among all levels at which relevant information could be shared may have a larger impact than the fusion that might occur due to advances in technology.

**Data Mining**

With the proliferation of data warehouses, data mining tools are flooding the market. Data mining methodology extracts hidden predictive information from large databases. Their objective is to discover hidden gold in your data. Many traditional report and query tools and statistical analysis systems use the term "data mining" in their product descriptions. Exotic Artificial Intelligence-based systems are also being touted as new data mining tools. The ultimate objective of data mining is knowledge discovery. That's where technology comes in: for true knowledge discovery a data mining tool should unearth hidden information automatically (Thuraisingham, 2002).

A typical commercial application of data mining is fraud detection for credit cards, telephone calls, and insurance claims (by learning from historical data on transactions known to be fraudulent). Other applications are in assessing mortality risk for medical patients (by learning from historical patient data) and predicting which individuals are most likely to make certain purchases (by analyzing data on other individuals’ past purchasing). The majority of these commercial data-mining applications involve well-structured data. Limitations of the current commercial technology include the inability to mine data that is a combination of text, image, video, and sensor information (that is, data in "non-structured" formats) as well as the inability to incorporate the knowledge of human experts into the data-mining process. Despite the significant
value of current machine-learning algorithms, there is also a need to develop more accurate learning algorithms for many classes of problems (Thuraisingham, 2002).

This technology may prove to be a powerful tool to search for information about suspected people.

Language Technologies

The area of language technologies has developed a wide variety of tools to deal with very large volumes of text and speech. The most obvious commercial examples are the Web search engines and speech-recognition systems that incorporate technology developed with Defence Adavanced Research Projects Agency (DARPA) and National Science Foundation (NSF) funding. Other important technologies include information extraction (e.g., extraction of the names of people, places, or organizations mentioned within a document), cross-lingual retrieval (e.g., does an Arabic e-mail message involve discussion of a chemical weapon?), machine translation, summarization, categorization, filtering (monitoring streams of data), and link detection (finding connections). Most of these approaches are based on statistical models of language and machine-learning algorithms (American Institute of Physics, 2000).

A great deal of online information, in the form of text such as e-mail, news articles, memos, and pages on Web sites, is of potential importance for intelligence applications. Research is needed on methods for accurately extracting from text certain structured information such as descriptions of events, that is, the date, type of event, actors, and roles. Research is needed to handle multiple languages, including automatic translation, cross-lingual information retrieval, and rapid acquisition of new languages. Other important areas of future research are link detection (related to the normalization problem mentioned above) and advanced question answering.

Evidence Combination
Many of the techniques used to combine information from multiple sources, as in video indexing or meta search engines, are ad hoc. Current research on principle-based methods for reasoning under uncertainty needs to be extended and tested extensively in more demanding applications. This is a key technical problem, with widespread implications for many of the applications mentioned above—e.g., how to combine evidence from hospital admissions and from nonprescription drug purchases to detect a probable bioterrorist attack; how to combine evidence from face recognition and voice print to estimate the likely identity of a person; or how to combine evidence from multiple sensors in a building to detect anomalous activity (NATIONAL ACADEMIES PRESS, 2001)

Technologies to Address Future Passenger Screening Requirements

There has always been a trade-off between technology performance and public acceptance when it comes to technological improvements in airport security screening. Major concerns over health effects rises everytime a change is done to the metal-detection portals.

Imaging Technologies

Imaging technologies can produce an image of the human body underneath the clothes. The amount of detail presented by the images depends upon the technology used. However, none of the technologies gives images with photographic quality. Operators view and interpret these images. (NATIONAL ACADEMIES PRESS, 1996).

Imaging technologies are classified as either passive or active.

Passive screening- Here the natural radiation emitted by the human body is detected and analyzed. There is minimal concern about radiation.

Active imaging – This involves irradiating the body with x-rays or millimeter waves and analyzing the radiation scattered from the body.
In both these imaging procedures any object (e.g., metallic weapons or explosive materials) that emits or scatters radiation differently from the human body will appear different from the background on the image. Currently, images are viewed and interpreted by an operator. Research is required in developing effective, automated image-interpretation capabilities that would eliminate the operator from the routine screening process as such routines are always prone to human error.

Images that are produced by these technologies are of sufficiently high quality to make them effective for screening passengers (NATIONAL ACADEMIES PRESS, 1996). However, when the perceived level of threat is low, passengers, crews, and others passing through screening checkpoints are likely to object to having images of their bodies displayed. There are many concerns about the use and storage of the data used to generate images. Researchers believe that procedures, such as having operators of the same sex view the images or moving operators away from the screening checkpoints, could allay concerns. Financial and logistical deterrents of these procedures make imaging technologies extremely unattractive for use as primary screening systems at all checkpoints. It is difficult to quantify the level of threat at which the public would start accepting such invasion of privacy however it is highly important to do it before putting any such imaging technologies to use.

There have been a lot of concerns about health effects when talking about implicating such imaging technologies. However, the levels of radiation exposure required for image production are insignificant compared to the levels experienced during many other common activities, including airplane flights. It can be seen that most of the concerns have more to do with only perception. Hence it is necessary to address these perception and bring to the knowledge of the people that these radiations are not harmful. (NATIONAL ACADEMIES PRESS, 1996).
Trace-Detection Technologies

Trace-detection technologies work by physically collecting samples of air or material from clothing or bodies of individuals and use the samples to infer the presence of dangerous materials. Sampling the air around individuals or touching them to remove particles of explosive materials from them or their belongings (NATIONAL ACADEMIES PRESS, 1996). There are many techniques that can be used to identify chemical compounds of interest. The specifications of the chemical-identification technologies are less likely to cause passenger concern than the sample collection techniques.

Trace-detection technologies are still in the development phase, especially with regard to methods of sample collection and matching appropriate sampling techniques with chemical-identification technologies. Therefore, it is more difficult to comment on specific passenger screening scenarios involving trace-detection technologies.

Sample collection for trace-detection technologies entails the physical transfer of material from the person being screened to the screening equipment. Although sampling the air around a person is less intrusive, however it is likely to be less effective, than touching the person to collect a sample. When considering technologies that require touching, one of the major concerns is people's aversion to being touched either by inanimate objects, such as bars or fronds, or by operators wielding hand-wand devices. It is extremely difficult to address this issue as the desire to preserve distance from strangers is deeply ingrained and is often influenced by basic cultural and religious beliefs. It is not likely to change the optimum distance people maintain between themselves and others through public information campaigns as this varies greatly from person to person and from culture to culture (NATIONAL ACADEMIES PRESS, 1996). Concerns about privacy, about initiating physical contact, and the transmission of disease may prove to be significant hurdles to implementing new technologies.
Trace-detection technologies are also being considered for use in screening hand-carried baggage and personal electronic devices. There are likely to be less intense objections to touching these items than objections to touching people themselves. One effective way of transporting material from a person to screening equipment may be by collecting samples from areas that a person is likely to have touched. Samples collected from boarding cards may be a practical and less intrusive way of implementing trace-detection technologies in passenger screening.

The major limitation of present language and image technologies is that their accuracy and performance, despite significant progress, need to be considerably improved. This is particularly true for counterterrorist systems where the data may be very noisy (that is, surrounded by irrelevant information) and sparse. Work is needed on improved algorithms for image interpretation and speech recognition. Many of these research issues are specific to problems arising in a particular medium that is, recent progress on face recognition has come primarily from understanding how to extract relevant image features before applying machine learning methods, though this approach may not be applicable to machine learning in other contexts. However, new research is also needed on perception based on mixed media—e.g., speech recognition based on sound combined with lip motion (NATIONAL ACADEMIES PRESS, 1996).

**Research required for effective deployment of Information Technology**

Though the potential of Information Technology is recognized, information systems security, especially in its operational dimensions, has received far less attention and focus than the subject deserves in light of a growing U.S. military dependence on information dominance as a pillar of its war fighting capabilities. A thorough understanding of how information technology can be deployed to reduce risks is highly essential.
Information and Network Security

A broad overview of some of the major issues in information and network security is contained in the Computer Science and Technology Board (CSTB) report *Cyber security Today and Tomorrow: Pay Now or Pay Later* (*NATIONAL ACADEMIES PRESS*, 2002).

Despite diligent efforts to create an effective perimeter defense for computer and telecommunications systems, penetration by a determined adversary is highly likely. Software flaws, lax procedures for creating and guarding passwords, compromised insiders, and non-secure entry points all lead to the conclusion that watertight perimeters cannot be assumed. Nevertheless, strengthening defensive perimeters is helpful, and this section deals with methodologies (those of today and tomorrow) that can detect or confine an intruder and, if necessary, aid in recovery from attack by taking corrective action.

The need for information systems security and trust can be formulated in terms of several major requirements:

- **Data confidentiality**--controlling who gets to read information in order to keep sensitive information from being disclosed to unauthorized recipients, e.g., by preventing the disclosure of classified information to an adversary;

- **Data integrity**--assuring that information and programs are changed, altered, or modified only in a specified and authorized manner, e.g., by preventing an adversary from modifying orders given to combat units so as to shape battlefield events to his advantage;

- **System availability**--assuring that authorized users have continued and timely access to information and resources, e.g., by preventing an adversary from flooding a network with bogus traffic that delays legitimate traffic such as that containing new orders from being transmitted; and
• **System configuration**—assuring that the configuration of a system or a network is changed only in accordance with established security guidelines and only by authorized users, e.g., by detecting and reporting to higher authority the improper installation of a modem that can be used for remote access (NATIONAL ACADEMIES PRESS, 2002).

The requirement for accountability cuts across these four requirements. Accountability is knowing who has had access to information or resources. The listing shows that security means a lot more than protecting information from disclosure (e.g., classified information). According to the DOD, much of the information on which military operations depend is not classified. Though the disclosure of this information may not cause any harm, the alteration or a delay in transmitting it certainly could. Access to unclassified information can always present a threat to some extent (e.g., access to personnel medical records used to enable blackmail attempts).

Satisfying these security requirements requires a range of security services, including:

- **Authentication**—ascertaining that the identity claimed by a party is indeed the identity of that party. Authentication is generally based on what a party knows (e.g., a password), what a party has (e.g., a hardware computer-readable token), or what a party is (e.g., a fingerprint);

- **Authorization**—granting of permission to a party to perform a given action (or set of actions);

- **Auditing**—recording each operation that is invoked along with the identity of the subject performing it and the object acted upon (as well as later examining these records); and

- **Non-repudiation**—the use of a digital signature procedure affirming both the integrity of a given message and the identity of its creator to protect against a subsequent attempt to deny authenticity (NATIONAL ACADEMIES PRESS, 2002).
IT and C4I for Emergency Response

The creation, communication, analysis, and exploitation of information have always played a key role in military strategy and operations. However, the recent advancement in the development of information and communications technologies has dramatically influenced the military operations in realizing the strategic role of information. Positioning effective exploitation of these technology advances as a critical success factor in military affairs. The technological advancement has become the drivers and enablers for the "nervous system" of the military. Military operations are relying upon technology to develop its command, control, communications, computers, and intelligence (C4I) systems, to more effectively use the "muscle" side of the military, namely the weapons and platforms and troops. The growing importance of C4I systems reflects an information technology-driven transformation of strategy and operations similar to what is occurring across almost every segment of society (NATIONAL ACADEMIES PRESS, 1999).

There are many options for helping to facilitate interoperable crisis communications among emergency-response agencies. For example, it is likely that some portion of the public networks will survive any disaster; emergency-response agencies could use it to facilitate interoperability if there are mechanisms for giving them first priority for such use. A second option is to allocate dedicated spectral bands for emergency responders and to require by law that they use those frequencies. A third option is to mandate frequency and waveform standards for emergency responders so that they are interoperable. A fourth option is to develop technology to facilitate interoperable communications among emergency responders. Of course, these options are not mutually exclusive.

In addition, numerous computational and database facilities must be established to provide complete and real-time information to diverse constituencies whose information and
communication requirements, security needs, and authorizations all differ (NATIONAL ACADEMIES PRESS, 1999). These facilities must be established quickly, as minutes and even seconds matter in the urgent, early stages of an incident. Furthermore, tight security is essential, especially if the incident is the result of a terrorist attack, because an active adversary might try to subvert the communications or destroy data integrity. In addition, an atmosphere of crisis and emergency provides opportunities for hostile elements to overcome security measures that are normally operative under non-emergency circumstances; thus, another research area is how to build systems that permit security exceptions to be declared without introducing new vulnerabilities on a large scale.

Efforts to coordinate communications are complicated by the fact that emergency response to a large-scale incident has many dimensions, including direct on-the-ground action and response, management of the incident response team, operations, logistics, planning, and even administration and finance (NATIONAL ACADEMIES PRESS, 1999). Moreover, response teams are likely to include personnel from local, county, state, and federal levels.

In the book “Realizing the Potential of C4I: Fundamental Challenges”, the author suggests research in a number of areas can advance the state of the art for emergency response C4I systems, thereby improving their effectiveness for terrorist incidents.

In addition, it is stated, the development of better C4I systems for emergency response will have application to responding to natural disasters as well.

**Emergency Management of Communications Capacity**

In an emergency, extraordinary demands are placed on communications capacity. A disaster is likely to destroy some but not the entire communications infrastructure in a given area, leaving some residual capability. Meanwhile, the disaster provokes greater demands for communication from the general public. The result is often a denial-of-service condition for all, including emergency-communications services. The absence of a telephone dial tone in a disaster area is
common because of increased demands. Even under high-traffic but non-emergency situations, cell-phone networks are sometimes unable to handle the volume of users in a given cell because of statistical fluctuations. Nor is the Internet immune to such problems—congestion of shared Internet links, including both last-mile and aggregated feeder links, can cause lockouts to occur on facilities that are still operational in the disaster area (NATIONAL ACADEMIES PRESS, 1999).

Research is needed on using residual (and likely saturated) capacity more effectively, deploying additional (surge) capacity, and performing the tradeoffs among different alternatives. One problem in this area is the management of traffic congestion and the development of priority overrides for emergency usage (and prevention of the abuse of such authority). A second problem is that optimization algorithms for communications traffic that are appropriate in normal times may have to be altered during emergencies. For example, the destruction of physical facilities such as repeaters and the massive presence of debris could result in an impaired environment for radio-frequency transmissions. The rapid deployment of processors optimized to find weak signals in a suddenly noisier environment could do much to facilitate emergency communications (NATIONAL ACADEMIES PRESS, 1999). DSL systems, for example, can reallocate huge bandwidth to a single phone line by coordinating it with all the phone lines nearby (one can sometimes get 10 times the bandwidth if this is done right). Under normal circumstances, the interests of the other users would defeat such a system (with cross talk), but in an emergency those interests could be reprioritized.

Research is also needed for self-adaptive networks that can reconfigure themselves in response to damage and changes in demand and that can degrade gracefully. For example, in a congested environment, programmed fallback to less data-intensive applications (e.g., voice rather than video, text messaging rather than voice) may provide minimal communications facility. Even today, many cellular networks allow the passing of text messages. Also, public and private
elements of communications infrastructure could both be tapped to provide connectivity in a crisis, as happened in New York City on September 11.

In addition, the White House’s National Communications System office has moved to implement a wireless priority service that facilitates emergency recovery operations for the government and local emergency-service providers. This service will be implemented in phases, with an immediate solution available in early 2002 in selected metropolitan areas and a nationwide solution (yet to be developed) scheduled for late 2003. Further work after 2003 will concentrate on the development and implementation of third-generation technologies that enable high-speed wireless data services (NATIONAL ACADEMIES PRESS, 2000).

Security of Rapidly Deployed Ad Hoc Networks

The management of communications networks poses unique problems in a crowded, emergency disaster zone. Security must be established rapidly from the outset, as the terrorists might try to mix among the first responders. It is also necessary to determine a means for temporarily suspending people’s access to facilities, communications, and data without impeding the ability of those with legitimate need to use them. Yet this suspension process has to be done rapidly, given that minutes and seconds matter in severe emergencies.

Research is therefore needed on the special security needs of wireless networks that are deployed rapidly and in an ad hoc manner (NATIONAL ACADEMIES PRESS, 2002). (For example, ad hoc networks are not likely to have a single system administrator that can take responsibility for allocating user IDs.)

Information-Management and Decision-Support Tools

In a chaotic disaster area, a large volume of voice and data traffic will be transmitted and received on handheld radios, phones, digital devices, and portable computers. Nevertheless, useful information is likely to be scarce and of limited value. Thus, research is needed on “decision-
support” tools that assist the crisis manager in making the most of this incomplete information (NATIONAL ACADEMIES PRESS, 2002).

**Communications with the Public during an Emergency**

During a crisis, there is high need for channels to provide information to the public. Today, the radio, television, and often the Web play a vital role in providing such information, however, this information is not area specific and is usually generic. The authors of the book, "Making the Nation Safer: The Role of Science and Technology in Countering Terrorism," believes research is needed to identify appropriate mechanisms—new technologies such as “call by location” and zoned alert broadcasts—for tailoring information to specific locations or individuals. To be effective in interacting with individual users, ubiquitous and low-cost access is required. In addition, such systems should be highly robust against spoofing (entry by an intruder masquerading as a trusted host) so that only authorized parties can use them to send out information. For example, the current cell-phone system does not directly support these functions, but it might be possible to modify and exploit it to provide “reverse 911” service i.e., a one-way channel to those affected that provides a continual flow of relevant information and guidance. Such mechanisms would probably have to be locally self-sufficient, that is, the disaster might spare the local cell site. A temporary cell site could be deployed along with wireless alternatives, but access to central services might not be possible (NATIONAL ACADEMIES PRESS, 2002). Finally, providing information to those located outside the immediate emergency area gives important psychological comfort and helps to mitigate the disaster’s consequences. (For example, in the immediate aftermath of the September 11 attacks, “I’m alive” bulletin boards sprang up spontaneously.) Research is needed for establishing more effective means of achieving this objective—especially in updating the status of affected people—while compromising the local communications infrastructure to a minimal degree (NATIONAL ACADEMIES PRESS, 2002).
**Emergency Sensor Deployment**

During an emergency, responders need information about physical on-the-ground conditions that is sufficiently fine-grained and accurate to be useful. It is virtually inevitable that no preexisting sensor network will be in place to provide adequate information, so the deployment of sensors in response to a disaster is likely to be necessary. Depending on the nature of the emergency, sensor capacity would be needed to identify and track the spread of nuclear, chemical, or biological contaminants, characterize and track vehicular traffic, locate survivors (e.g., through heat emanations, sounds, or smells), and find pathways through debris and rubble. Developing robust sensors for these capabilities is one major challenge; developing architectural concepts for how to deploy them and integrate the resulting information is another.

**Precise Location Identification**

In a severe crisis, determining the location both of physical structures and of people is a major problem because of debris, airborne contaminants such as smoke and dust, and perhaps simply a lack of illumination. Therefore, technological solutions, such as embedded location sensors, are probably essential. Distributed sensor networks, either already in place or deployed in response to an incident, can be valuable information sources. While technologies like the Global Positioning System could also play a major role, airborne contaminants and equipment damage might render them ineffective. The information needs of the responders and those affected will thus require rapid access to accurate databases—of blueprints and building diagrams, for example. Research is needed to develop digital floor plans and maps of other physical infrastructure. The resulting data could be stored in geographic information systems (GIS), which would allow responders to focus on the high-probability locations of missing people (such as lunchrooms) and avoid dangerous searches of low-probability locations (such as storage areas). Research is needed in wearable computers for search-and-rescue operations so that responders could update the GIS in real time as they discover victims and encounter infrastructural damage. Another research area is in “map
ants"—distributed, self-organizing robots deployed in a disaster area to sense movement or body heat, for instance (NATIONAL ACADEMIES PRESS, 2002).

It may also be possible to develop technology to generate the data for accurate maps of a debris-strewn disaster location. Finally, keeping track of emergency responders' positions within a disaster area is an essential element of managing emergency response. Technology (similar to E-911 for cell phones) to monitor the progress of these individuals automatically is not yet available on a broad scale.

Mapping the Physical Infrastructure of IT

As noted above, the telecommunications infrastructure is for the most part densely connected; hence physical attack is unlikely to disrupt it extensively for long periods of time. However, the physical infrastructure of telecommunications (and the Internet) does not appear to be well understood (that is, immediate knowledge of where various circuits are located is unavailable), and there may well exist critical nodes whose destruction would have a disproportionate impact. On the other hand, knowing where these critical nodes are is difficult for both network operators and terrorists. Thus, an important priority is to develop tools to facilitate the physical mapping of network topology, and to begin that mapping now with the tools that are currently available. This is particularly important for converged networks over which both voice and data are carried (NATIONAL ACADEMIES PRESS, 2002).

As one example, consider that a firm that installs fiber-optic cables in a city's sewers is capable of mapping those sewers as well using a sewer-crawling robot that lays cable and tracks its position.

Characterizing the Functionality of Regional Networks for Emergency Responders

To develop mechanisms for coordinating emergency-response activities, it is necessary to understand what the various communications and computer networks of emergency responders in a given region are supposed to do. For example, managers from different agencies often speak
different “languages” in describing their needs, capabilities, and operational priorities; a common conceptual framework for these purposes would be enormously helpful for coordination of planning activities, yet one is not yet available. Sharing of information among the various providers of critical infrastructure and emergency-response agencies, even about common tasks and processes, has been a rather uncommon activity in the past (NATIONAL ACADEMIES PRESS, 2002).

The Impact of C4I in the past

The real-world impact of C4I technology in enhancing the effectiveness and security of the coalition forces was amply demonstrated during the Gulf War (USDOD, 1991). The allied forces depended upon highly tenuous C4I capabilities and relied on inadequate methods for construction and distribution of operational plans and execution of orders, collection and assessment of battle damage information, and coordination of operations on a global scale among systems ranging from highly sophisticated to significantly outdated (USDOD, 1991). A formidable capability was established in a span of six months for command and control of a multinational force in a region of the world where virtually no infrastructure previously existed to accommodate such complex operations. After the success of the Gulf War, C4I has been reported in numerous after-action media as a major force multiplier in the conflict. As stated by the Department of Defense these are the following ways in which C4I proved to be effective during the Gulf War:

* C4I systems supported through simultaneous suppression of enemy air defenses made highly effective, precise, orchestrated strikes on a variety of targets in Baghdad on the initial night of war, with extremely low casualties.
* The Global Positioning System allowed orchestrated movements of coalition armored forces to outflank Iraqi forces and engage them at the maximum effective range of coalition weapons.
Again in Bosnia, advanced C4I technology has provided forces with enhanced capabilities to detect, process, decide, and communicate. For example:

* The Predator Unmanned Aerial Vehicle has improved monitoring of compliance with the Dayton Peace Accord.

* Linked Operations-Intelligence Centers Europe systems have facilitated the sharing of intelligence among selected coalition partners.

* The Joint Surveillance Target Airborne Radar System supported the insertion of ground forces into Bosnia (NATIONAL ACADEMIES PRESS, 1999).

The war fighter who returned from the Gulf War strongly believed that improvement in C4I capability and interoperability would add more value to military operations than additional improvements in weapons. The continuous improvement in the precision and/or lethality of weapons has always been a priority; however, experts believe that such enhancements in capabilities may well result more from application of C4I improvements than from near-term advancements in weapons technology. (Zdon, 2001).
Planning for the Future

Planning for the future is also a critical dimension of any research agenda, though the resources devoted to it need not be large. New system architectures and technologies, such as switched optical networks, mobile code, and open source or multinational code development, will have different vulnerabilities and hence require different defense strategies. Similarly, new device types such as digital appliances, wireless headphones, and network-capable cell phones pose new challenges. Even today, it is hard to interconnect systems with different security models or security semantics; and unless we deal with this problem, it will become increasingly difficult in the future.

Furthermore, the characteristics of deployed technology that protect the nation against catastrophic IT-only attacks today (e.g., redundancy, system heterogeneity, and a reliance on networks other than the Internet for critical business functions) may not be efficient enough in the future. Indeed, some trends, such as deregulation, system monocultures, and the dominance of a smaller number of products, are pushing the nation’s critical infrastructure providers to reduce excess capacity, even though this is what provides much of the redundancy so important to reduced vulnerability (NATIONAL ACADEMIES PRESS, 1996).

For these reasons, researchers and practitioners must be vigilant to changes in network technology, usage and reliance on IT, and potentially decreasing diversity. In addition, research focused on the future is likely to have a slant that differs from those of the other research efforts described in this chapter. While the latter efforts might be characterized as building on existing bodies of knowledge (and are in that sense incremental), future-oriented research would have a more radical orientation: It would try to develop alternative paradigms for secure and reliable operation that would not necessarily be straightforward evolutions from the Internet and information technology of today. For example, one such pursuit might be the design of
appropriate network infrastructure for deployment in 2020 that would be much more secure than
the Internet of today. Another might be an IT infrastructure whose security relied on engineered
system diversity—in which deployed systems were sufficiently similar to be interoperable yet
sufficiently diverse to essentially be resistant to large scale attacks (NATIONAL ACADEMIES
PRESS, 1996).
Privacy and confidentiality

As pressure mounts for the government to collect and process more information, it becomes increasingly important to address the question of how to minimize the negative impacts on privacy and data confidentiality. Research is needed to provide policy makers with accurate information about the impact on confidentiality of different kinds of data disclosure. Research is also needed on new data-mining algorithms that discover general trends in data without requiring full disclosure of the individual data records. One example is data-mining algorithms that work by posing statistical queries to each of a set of databases, rather than gathering every data record into a centralized repository (Thuraisingham, 2002).

Another is zero-knowledge data mining, in which general trends in data can be uncovered without requiring full disclosure of individual data records. (However, note that for many applications such as badges and access tokens, personal information of the sort mentioned is not necessary; the only requirements are that the token be recognizable as valid and that it has been issued to the person presenting it. It doesn’t even have to have an individual’s name on it.)

A related issue is the fact that a sufficient aggregation of non-personally identified information can often be used to identify a person uniquely. For example, identifying someone as a man of Chinese extraction with a doctorate in physics who enjoys swing dancing, has an adopted 7-year-old daughter, and lives in upper-northwest Washington, D.C., is likely sufficient to specify a unique individual. Thus, the mere fact that information is disconnected from personal identifiers is no assurance that an individual cannot be identified if data are aggregated (O’neil & Demsey, 2000).
Conclusion

The thesis concludes that there is no doubt that our transition into the Information era has caused a major shift in the paradigm of the age old phenomenon of terrorism and military operations. Terrorism today is greatly influenced by the advance in information technology. The very same technology that we depend upon on a daily basis is being used by perpetrators to harm the safety of our existence. Information Age brings with it many security concerns and uncertainties. The modern information technology gives the opportunity to terrorists to cause havoc and chaos all over the world at the comfort of their homes. Information technology will play a major role in providing a wide range of options for the terrorists. Information technology is being used by terrorists both as a tool as well as a target.

Information technology has greatly enhanced the shift of terrorist organization from a hierarchical form to a networked form. Just as the businesses today are adopting network form of organizations for the relative flatness, flexibility and connectivity, terrorist organizations are also harnessing upon these advantages. Terrorists are increasingly relying upon information technology to manage their networked organizations. This is done through propaganda and communication. The Internet, the greatest innovation of the Information Age, plays a vital role helping the terrorists achieve this. It can be seen that Web sites are being used to great extent for propagation as well as information gathering. Computers and floppy diskettes were retrieved from the terrorist caves in Afghanistan which proves that terrorists today are also highly wired. Terrorists today are reported to be using many advanced information technology tools such as encryption, e-mail bombing, flight simulators; steganography etc., as most of these technologies comes with no regulatory policies.

Cyber space brought the world closer. National boundaries disappeared. What we weren’t aware of us that it also brought us closer to criminals, perpetrators and social enemies such as terrorists. The distance banished and space we lived together on, the cyber space became a favorable
platform for their actions. Cyberterrorism in its real sense has yet to occur. However, the vulnerabilities and susceptibilities of the national infrastructures cannot and should not be treated lightly. It is very important to consider the destructive effect of such an attack while designing strategic military operations. It can be noted that there are no compelling reasons to believe that cyber attacks will be any more deadly than conventional ones. The terrorist desire to escalate current levels of violence are as much dependent on who the groups are and what they hope to achieve, as upon the weapons they have at hand.

It is not enough to simply equate the effect of cyberterrorism with conventional terrorist attacks, but a much wiser approach will examine how the cyber environment both facilitates and influences a terrorist to pursue such an attack over a conventional one. It is also necessary to examine how a cyber attack effect the flow of information and cause the disability to take counter measures.

Information terrorism poses a great threat to all Third Wave nations. Increasing security and gathering accurate intelligence regarding any plans of attack that might be in consideration can ensure that the threat of terrorism is minimal and the effect is less destructive from which the United States can recover.

We certainly are, as Al Gore once noted that methods of warfare will continue to evolve as the revolution progresses. And hence the conceptions of national security will also have to evolve. There is no doubt that information warfare and information security must be incorporated into the national security agenda of any nation that is making the transition into the Information Age. Isaac Asimov notes that "Waiting for a crisis to force us to act globally runs the risk of making us wait too long" (Petersen, 1994). This can not be the case where information technologies are concerned, as they are the very foundation of today’s society. John Petersen points that a "philosophy comes bundled with every new technology; when one is embraced, the other is there as well "(Petersen, 1994).
According to Devost, the U.S. Military needs to adapt to new technology or it faces the prospect of allowing itself to grow flaccid and obsolete. The issues raised in this paper have no direct solution. There is a strong need for the awareness of the strengths and, more importantly, the weaknesses that technology brings to an organization (Julie, 1993).

The policy questions that dominate the issue of critical infrastructure protection –:

i) What and how limited is the role of the government.

ii) What is the most adequate infrastructure security

iii) How to determine appropriate standards

iv) What data does the government need from the people and why.

A few basic principles are emerging that should guide infrastructure protection efforts as stated by O’neil and Dempsey. (O’Neil & Dempsey, 2000):

* General or centralized monitoring of communications need not and should not be a chief or central component of the government’s response to computer security. There are other activities – notably the identification and closing of existing vulnerabilities – that should be given higher priority.

* Authority for increased monitoring of information systems is not required and should be rejected. Rather, the underlying laws for monitoring communications systems and accessing stored data should be strengthened.

* The role of the FBI and the (National Security Agency) NSA in computer security should be carefully limited: it has been demonstrated that their surveillance agendas trump their protective missions, and their activities are often so cloaked in secrecy as to generate understandable suspicion.

* Oversight of infrastructure protection should be institutionalized within the Executive Branch and should be accessible to the public. There should be established within the Executive Branch appropriate mechanisms for oversight of computer security issues, involving both industry representatives and privacy advocates.
* Congress must follow this issue carefully, and should insist upon periodic reports on the status, scope, and effectiveness of critical infrastructure activities, with special focus on monitoring and intrusion detection initiatives and the protection of privacy.

* In sum, while we acknowledge the need for government participation, especially in educating society about what is at stake, the government 's role in private sector infrastructure protection should be limited and largely advisory. The private sector should set information security standards, and the government should clearly define and limit what information it seeks from businesses and how that information will be used.

The following important conclusions have been drawn through this thesis:

* Technology has already been used by terrorist organizations in the past and will continue to be used.

* There is ongoing development in the field of information technology by strategic planners to use it both as an offensive weapon and as a weapon to cause an attack that would disrupt the infrastructure on which a nation depends.

* Information Technology has been effectively used by terrorist organizations to take advantage over network form of organization.

* Information Technology has been used in the past by American forces in the Gulf War.

* Those countries most capable of waging an information warfare are the ones that are most susceptible to such an attack.

* The globalization and digitization brought with the Information Revolution also brings us closer to hostile elements of the societies such as terrorists.

* Cyber attacks are easy to carry out. It is relatively inexpensive, can be carried out anonymously completely deniable. In addition to this, the fact that global economy solely depends upon the flow of information through computer networks, makes information war the perfect and most attractive weapon to a terrorist.

* The security solutions that we currently have lag far behind the potential threat (Yael, n.d.).
References


Chat about Internet Security and Denial of Service attacks (2000). CNN Online [WWW Page].


Freeh, Louis J. (2000). Cybercrime. Statement for the record before the Senate Select Committee on Intelligence. URL

http://homer.span.ch/~spaw1165/infosec/sts_en/


Infowar: Call For Floodnet Action for Peace in the Middle East [WWW Page]. URL
www.aec.at/infowar/NETSYMPOSIUM/ARCH-EN/msg00633.html


http://www.ndu.edu/irmc/publications/canberra_paper.htm
The Nautilus Institute Virtual Diasporas and global problem solving project papers. URL
http://www.nautilus.org/virtual-diasporas/paper/Lal.html


M2 Communications [WWW Page]. URL http://www.m2com.com/>


O’neil, Michael J. & Dempsey, James X. (2000). Critical Infrastructure Protection:


http://www.fpri.org/enotes/balkansturkey.19990326.radu.bombsforpeace.html

http://www.infowar.com/class_3/class3_q.html-ssi


The Terrorism Research Center. URL http://www.terrorism.com/terrorism/def.shtml


Webster’s Dictionary [WWW Page]. URL WWWebster Dictionary


