Cyberwarfare

Cyber warfare involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks.

Cyberwarfare involves the following attack methods:

Sabotage: Military and financial computer systems are at risk for the disruption of normal operations and equipment, such as communications, fuel, power and transportation infrastructures.

Espionage and/or security breaches: These illegal exploitation methods are used to disable networks, software, computers or the Internet to steal or acquire classified information from rival institutions or individuals for military, political or financial gain.

It should be pointed out that cyberwarfare can be and often is conducted in conjunction with regular military warfare.

One nation’s military leaders may attempt to sabotage an enemy’s computer system(s) in an attempt to disrupt the enemy’s combat operations.

Or, the military leadership of one nation may attempt to spy on an enemy via their computer system(s) to learn the enemy’s combat strategy.

Cyber Sabotage

Traditional espionage is not an act of war, nor is cyber-espionage, and both are generally assumed to be ongoing between major powers. Despite this assumption, some incidents can cause serious tensions between nations, and are often described as "attacks". For example:

- Massive spying by the US on many countries, revealed by Edward Snowden.
- The NSA's spying on Germany's Chancellor Angela Merkel.
- The NSA recording nearly every cell phone conversation in the Bahamas, without the Bahamian government's permission, and similar programs in Kenya, the Philippines, Mexico and Afghanistan.
- The "Titan Rain" probes of American defense contractors computer systems since 2003.

Titan Rain was the designation given by the U.S. federal government to a series of coordinated attacks on American computer systems; they were known to have been ongoing for at least three years. The attacks originated in Guangdong, China The activity known as "Titan Rain" is believed to be associated with a state-sponsored program of threat.

Titan Rain hackers gained access to many United States defense contractor computer networks who were targeted for their sensitive information, including those at Lockheed Martin, Sandia National Laboratories, Redstone Arsenal, and NASA.

The Office of Personnel Management data breach, in the US, widely attributed to China.
Out of all cyber attacks, 25% of them are espionage based.
In June 2015, the United States Office of Personnel Management (OPM) announced that it had been the target of a data breach targeting the records of as many as four million people. The final estimate of the number of stolen records is approximately 21.5 million. This includes records of people who had undergone background checks, but who were not necessarily current or former government employees. It has been described by federal officials as among the largest breaches of government data in the history of the United States. Information targeted in the breach included personally identifiable information such as Social Security numbers, as well as names, dates and places of birth, and addresses.
The data breach consisted of two separate, but linked, attacks. It is unclear when the first attack occurred but the second attack happened on May 7, 2014 when attackers posed as an employee of KeyPoint Government Solutions, a subcontracting company. The first attack was discovered March 20, 2014, but the second attack was not discovered until April 15, 2015.
On August 27, 2017, the FBI arrested a Chinese national suspected of helping to create the malware used in the breach.

Sabotage

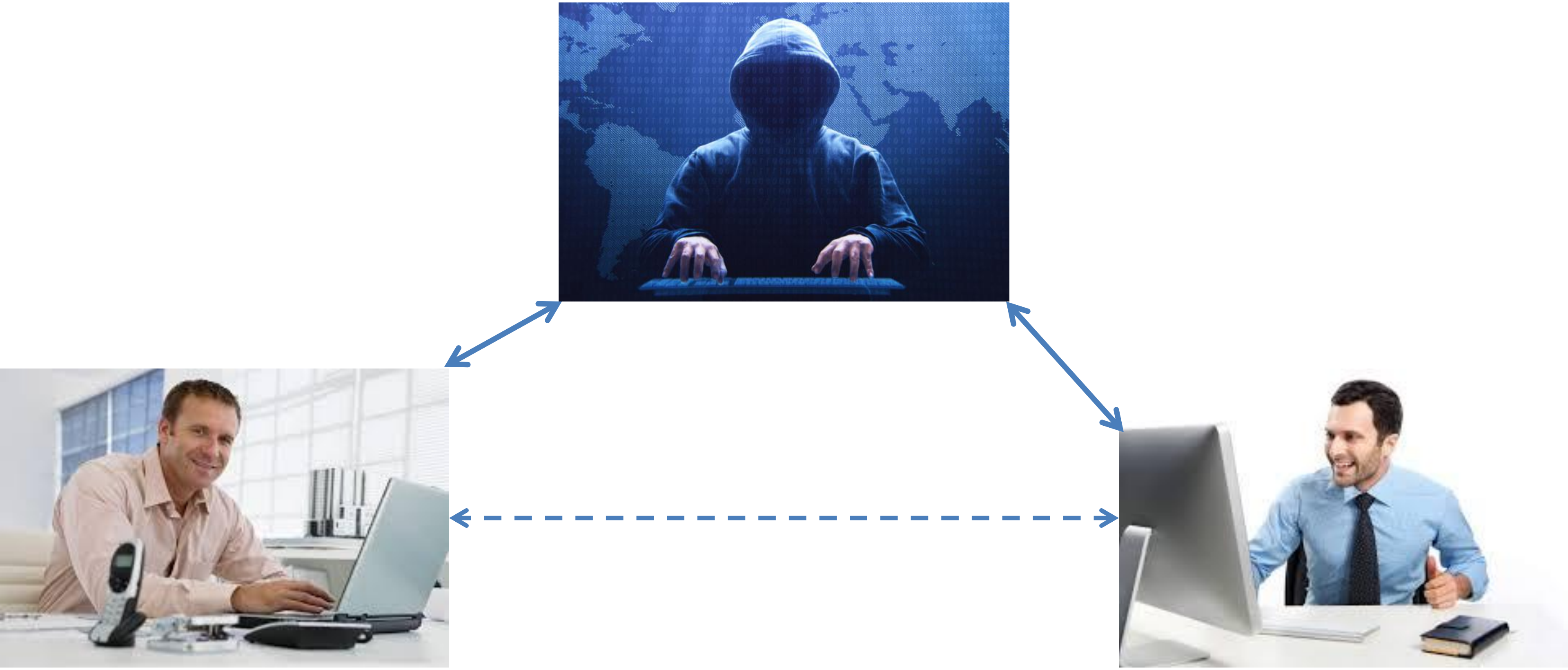
Computers and satellites that coordinate other activities are vulnerable components of a system and could lead to the disruption of equipment. Compromise of military systems, such as components that are responsible for orders and communications could lead to their interception or malicious replacement. Power, water, fuel, communications, and transportation infrastructure all may be vulnerable to disruption. The civilian realm is also at risk, in that security breaches have already gone beyond stolen credit card numbers, and that potential targets can also include the electric power grid, trains, or the stock market.

Some commonly used forms of cyber-sabotage include:

- Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks.
- Phishing and spear phishing attacks.
- Man-in-the-middle (MitM) attack.

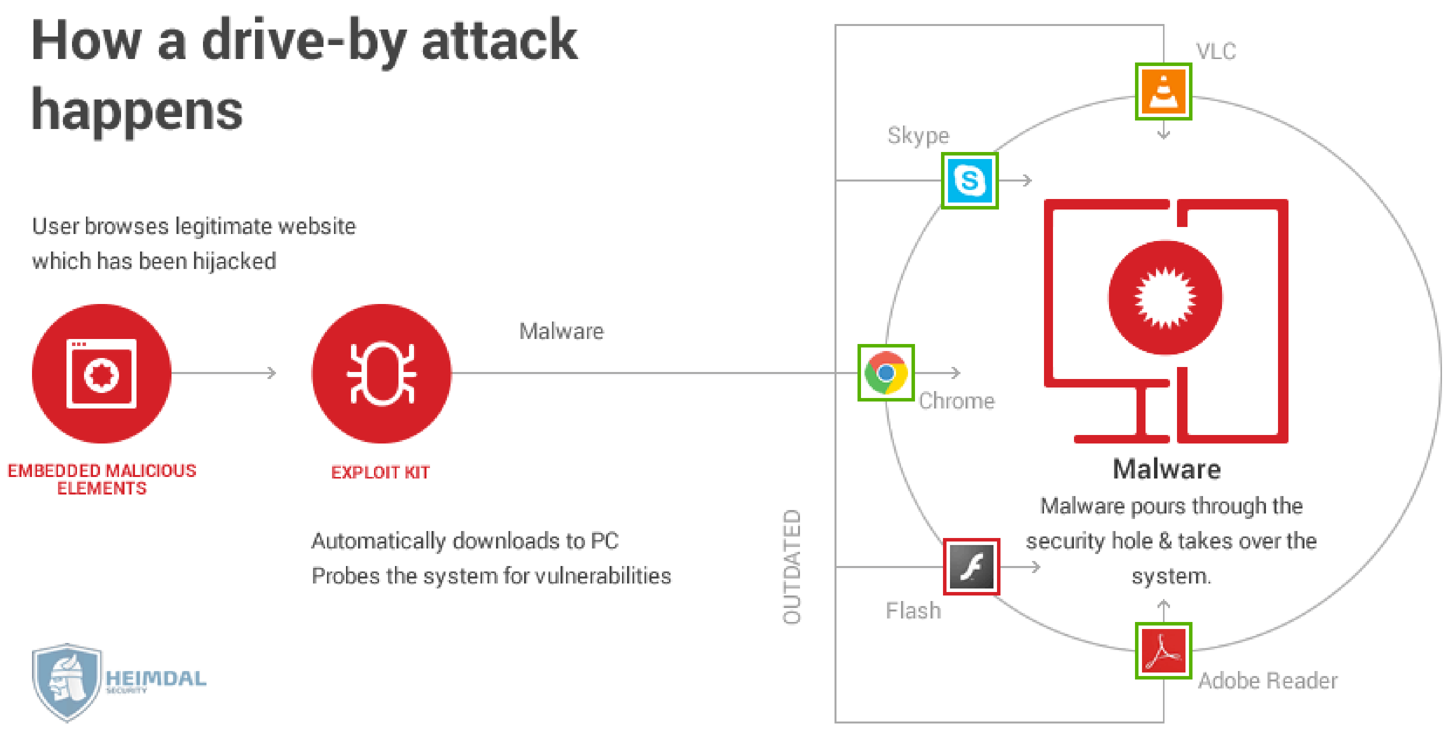
A man-in-the-middle attack requires three players. There’s the victim, the entity with which the victim is trying to communicate, and the “man in the middle,” who’s intercepting the victim’s communications. Critical to the scenario is that the victim isn’t aware of the man in the middle. One example of a MITM attack is active eavesdropping, in which the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.

Man in the Middle Attack



- Drive-by attack.

A drive-by download refers to the unintentional download of malicious code to your computer or mobile device that leaves you open to a cyberattack. You don't have to click on anything, press download, or open a malicious email attachment to become infected. A drive-by download can take advantage of an app, operating system, or web browser that contains security flaws due to unsuccessful updates or lack of updates. Unlike many other types of cyberattack, a drive-by doesn't rely on the user to do anything to actively enable the attack.



How a drive-by attack happens

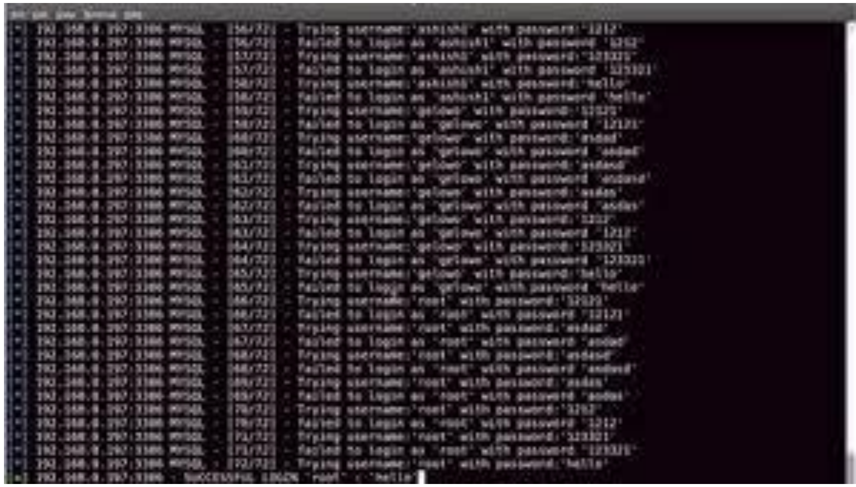
User browses legitimate website which has been hijacked

Automatically downloads to PC
Probes the system for vulnerabilities

Malware
Malware pours through the security hole & takes over the system.

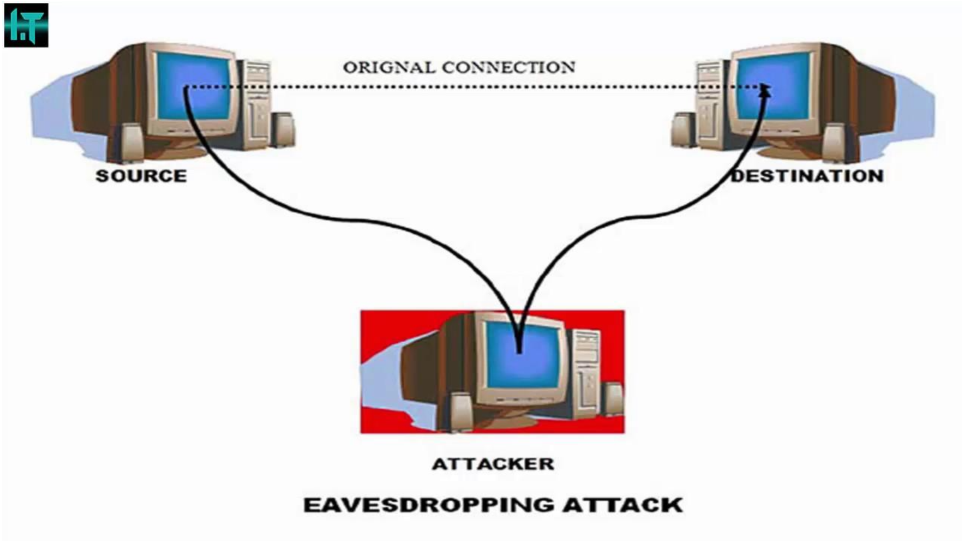
•Password attack.
Brute Force Pasword Attacks involve running through as many combinations of potential passwords as necessary to hit on the right one. Attacks will typically start with the commonest or most likely (“Password”, “1234567”, or birthdays if the target is known, etc.), then progress through mixtures of numbers, letters, and other keyboard characters. There are scripts and applications written specifically for this purpose, readily available for hackers to download from the Net.

PASSWORD
123456
123456789
12345
1234
123
MYSTERY
ROMANCE
SHADOW
TIGGER
SUNSHINE
102030
AJCUIVD289
DRAGON
BOOKWORM
READING
READER
PURPLE
MAGGIE
BOOKLOVER
PEANUT
CHARLIE
PRINCESS
MICHAEL
VAMPIRE
WRITER
WRITERSPACE
HANNAH
ANGELS
UNICORN
GINGER
BAILEY
MORGAN
COOKIE
LIBRARY
BUTTERFLY
FLOWER
ANDREW
MOTHER
ABC123
JOSHUA
MIDNIGHT
242424
654321
121212
12345678
PEPPER
MATTHEW
CHOCOLATE
BUSTER
AMANDA
JESSICA
JUNIOR
SUMMER
JENNIFER
JASPER
FREEDOM
DANIEL
THOMAS
MURPHY
CALLIE
1234567
SAMANTHA
PATRICK
BANDIT
101010
123123


```
[-] 192.168.0.197:3306 MYSQL - [56/72] - Trying username:'ashish' with password:'1212'
[-] 192.168.0.197:3306 MYSQL - [56/72] - Failed to login as 'ashish' with password '1212'
[-] 192.168.0.197:3306 MYSQL - [57/72] - Trying username:'ashish' with password:'123321'
[-] 192.168.0.197:3306 MYSQL - [57/72] - Failed to login as 'ashish' with password '123321'
[-] 192.168.0.197:3306 MYSQL - [58/72] - Trying username:'ashish' with password:'hello'
[-] 192.168.0.197:3306 MYSQL - [58/72] - Failed to login as 'ashish' with password 'hello'
[-] 192.168.0.197:3306 MYSQL - [59/72] - Trying username:'gelowo' with password:'12121'
[-] 192.168.0.197:3306 MYSQL - [59/72] - Failed to login as 'gelowo' with password '12121'
[-] 192.168.0.197:3306 MYSQL - [60/72] - Trying username:'gelowo' with password:'asdad'
[-] 192.168.0.197:3306 MYSQL - [60/72] - Failed to login as 'gelowo' with password 'asdad'
[-] 192.168.0.197:3306 MYSQL - [61/72] - Trying username:'gelowo' with password:'asdasd'
[-] 192.168.0.197:3306 MYSQL - [61/72] - Failed to login as 'gelowo' with password 'asdasd'
[-] 192.168.0.197:3306 MYSQL - [62/72] - Trying username:'gelowo' with password:'asdas'
[-] 192.168.0.197:3306 MYSQL - [62/72] - Failed to login as 'gelowo' with password 'asdas'
[-] 192.168.0.197:3306 MYSQL - [63/72] - Trying username:'gelowo' with password:'1212'
[-] 192.168.0.197:3306 MYSQL - [63/72] - Failed to login as 'gelowo' with password '1212'
[-] 192.168.0.197:3306 MYSQL - [64/72] - Trying username:'gelowo' with password:'123321'
[-] 192.168.0.197:3306 MYSQL - [64/72] - Failed to login as 'gelowo' with password '123321'
[-] 192.168.0.197:3306 MYSQL - [65/72] - Trying username:'gelowo' with password:'hello'
[-] 192.168.0.197:3306 MYSQL - [65/72] - Failed to login as 'gelowo' with password 'hello'
[-] 192.168.0.197:3306 MYSQL - [66/72] - Trying username:'root' with password:'12121'
[-] 192.168.0.197:3306 MYSQL - [66/72] - Failed to login as 'root' with password '12121'
[-] 192.168.0.197:3306 MYSQL - [67/72] - Trying username:'root' with password:'asdad'
[-] 192.168.0.197:3306 MYSQL - [67/72] - Failed to login as 'root' with password 'asdad'
[-] 192.168.0.197:3306 MYSQL - [68/72] - Trying username:'root' with password:'asdasd'
[-] 192.168.0.197:3306 MYSQL - [68/72] - Failed to login as 'root' with password 'asdasd'
[-] 192.168.0.197:3306 MYSQL - [69/72] - Trying username:'root' with password:'asdas'
[-] 192.168.0.197:3306 MYSQL - [69/72] - Failed to login as 'root' with password 'asdas'
[-] 192.168.0.197:3306 MYSQL - [70/72] - Trying username:'root' with password:'1212'
[-] 192.168.0.197:3306 MYSQL - [70/72] - Failed to login as 'root' with password '1212'
[-] 192.168.0.197:3306 MYSQL - [71/72] - Trying username:'root' with password:'123321'
[-] 192.168.0.197:3306 MYSQL - [71/72] - Failed to login as 'root' with password '123321'
[-] 192.168.0.197:3306 MYSQL - [72/72] - Trying username:'root' with password:'hello'
[+] 192.168.0.197:3306 - SUCCESSFUL LOGIN 'root' : 'hello'
```

- Eavesdropping attack.

An eavesdropping attack, also known as a sniffing or snooping attack, is an incursion where someone tries to steal information that computers, smartphones, or other devices transmit over a network. An eavesdropping attack takes advantage of unsecured network communications to access the data being sent and received. Eavesdropping attacks are difficult to detect because they do not cause network transmissions to appear to be operating abnormally.



Cyberterrorism

Cyberterrorism is the use of the Internet to conduct violent acts that result in, or threaten, loss of life or significant bodily harm, in order to achieve political or ideological gains through threat or intimidation.

Cyberterrorism is a complex concept, with some researchers using a narrow definition- relating to deployment by known terrorist organizations of disruption attacks against information systems for the primary purpose of creating alarm, panic, or physical disruption, while others employ a broader definition in which cyberterrorism overlaps considerably with the concept of cybercrime in general.

One way of understanding cyberterrorism involves the idea that terrorists could cause massive loss of life, worldwide economic chaos and environmental damage by hacking into critical infrastructure systems. The nature of cyberterrorism covers conduct involving computer or Internet technology that:

- is motivated by a political, religious or ideological cause
- is intended to intimidate a government or a section of the public to varying degrees
- seriously interferes with infrastructure

Critical infrastructure systems include:

- communication networks (telephone systems, media networks, etc.
- electric power generating systems
- air traffic control systems
- financial systems
- educational institutions
- transportation structures and systems
- state and local government institutions

Three levels of cyberterror capability have been recognized:

- 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 a coordinated attack 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.

As the Internet becomes more pervasive in all areas of human endeavor, individuals or groups can use the anonymity afforded by cyberspace to threaten citizens, specific groups (i.e. with membership based on ethnicity or belief), communities and/or entire countries, without the threat of capture, injury, or death to the terrorist that could result from the attacker actually being physically present.

Many believe that cyberterrorism is an extreme threat to countries' economies, and fear an attack could potentially lead to another Great Depression.

As the Internet continues to expand, and computer systems continue to be assigned increased responsibility while becoming more complex and interdependent, sabotage or terrorism via the Internet may become a more serious threat.

Dependence on the internet is rapidly increasing on a worldwide scale, creating a platform for international cyber terror plots to be formulated and executed as a direct threat to national security.

For terrorists, cyber-based attacks have distinct advantages over physical attacks. They can be conducted remotely, anonymously, and relatively cheaply, and they do not require significant investment in weapons, explosive and personnel.

The effects can be widespread and profound. Incidents of cyberterrorism are likely to increase. They will be conducted through denial of service attacks, malware, and other methods that are being developed today.

Just as cyberwarfare can be used in conjunction with military warfare, so cyberterrorism can be employed in conjunction with physical acts of terrorism.

While computer technology can be and is used to carry out acts of cyberterrorism, it can also facilitate terrorism in other ways.

It can be used as a means to gather intelligence about the individuals, groups, or societies which are the targets of cyberterrorism. [Terrorists can also engage in espionage against enemies- not just nation-states.]

The fact that it is a World-Wide web and that messages can be encrypted means that terrorists can communicate over great distances quickly and with little expense without concern about their messages being readily intercepted and read by targets.

Not only can terrorists communicate via the Internet, they can also disseminate propaganda and other forms of inflammatory hate speech against particular groups or individuals.

Terrorists can use the Internet as a means to wage psychological warfare. They can do this by deceiving targets into believing that an attack is imminent; or they can produce videos of military operations and/or executions. Both can raise the threat level in the targeted groups or societies.

The Internet can be used as a fundraising mechanism for terrrorists and their organizations.

It can also be used to recruit new members into their movement(s).

By putting out videos depicting attack skills and techniques, the Internet can help in the training of newly recruited terrorists.