Abstract:

Cyber terrorism is the wave of the future for terrorists and extremist. Other than physical attacks such as the bombing of U.S. Embassies and the September 11th, 2001 attacks on the World Trade Center etc. terrorists have found a new way to cause destruction. This paper gives the definition of cyber terrorism; its potential and suggests an approach to the minimization of its dangers. From a psychological perspective, two greatest fears of modern time are combined in the term “cyber terrorism”.

Cyber terrorism is the convergence of terrorism and cyberspace. It is generally unlawful attacks and threats of attack against computers, networks, and the information stored in several sectors.

Keyword: Terrorism, Cyber terrorism, Extremist, Convergence, Cyberspace.

[1] INTRODUCTION

According to national research council, “Tomorrow’s terrorist may be able to do more damage with a keyboard than with a bomb”. According to George smith, Co-editor, vmyths.com, “Terrorists are interested in creating bloodshed and terror”. If we ask 10 people what ‘cyber terrorism’ is, we will get at least nine different answers! When those 10 people are computer security experts and their task is to create various forms of protection against ‘cyber terrorism’. This discrepancy is comedic to rather than worrisome.

The Internet doesn’t rise to this level of impact in a way that a truck bomb does similarly many other organizations or research fellow gives a different answer about “cyber terrorism”. The term was coined in the 1980s by Barry Collin, a senior research fellow at the Institute for Security and Intelligence in California, who in 1997 was attributed for creation of the term "Cyber terrorism", defined cyber-terrorism as the convergence of cybernetics and terrorism. Another example would be hacking into hospital databases and changing patient information in a way that would cause patients to die due to false medication dosage or allergies to foods or medicines changing patient information in a way that would cause patients to die due to false medication dosage or allergies to foods or medicines.

“Cyber terrorism” is the use of computer network tools to harm or shut down critical national infrastructures like energy, transportation, government operations [2]. “Cyber terrorism” is an attractive option for modern terrorists, who value its anonymity, its potential to inflict massive damage, its psychological impact, and its media appeal. The term “cyber terrorism” is becoming increasingly common in the popular culture. With the globalized nature of the Internet, perpetrators can launch cyber-attacks from anywhere in the world and route the attacks through
servers of third-party countries like the cyber-attacks on Sony, a private corporation with headquarters in Japan, an attack on the United States. The conclusion looks to the future and argues that we must remain alert to real dangers while not becoming victims of overblown fears.


Cyber Terrorism is the same like physical terrorism, except that they use computers to make attacks[1]. An example of cyber terrorism would be hacking into the CIA or FBI to intimidate or coerce the American people.

There have been several stumbling blocks to creating a clear and consistent definition of the term “cyber terrorism”. “The use of computer network tools to shut down critical national infrastructures (e.g., energy, transportation, government operations) or to coerce or intimidate a government or civilian population”. There are two views that exist for defining cyber terrorism; effects-based and internet-based. In an effects-based situation cyber terrorism exists when computer attacks result in a situation where fear is generated which is similar to a traditional terrorist attack. In an internet-based situation attacks are done to cause harm or severe economic damage. One of the first recorded cyber-terrorist attacks was in 1996 when a computer hacker allegedly associated with the White Supremacist movement temporarily disabled a Massachusetts Internet service provider (ISP) and damaged part of the ISP's record keeping system.

Countries with most cyber terrorism as in 2002:-

![Pie chart showing countries with most cyber terrorism in 2002.](image)

In the first half of 2002, there were more than 180,000 Internet based attacks on business. Attacks against the Internet increase at an annual rate above 60%.

Thus, use of information technology and means by terrorist groups and agents constitute cyber-terrorism. Other activities, so richly glamorized by the media, should be defined as cybercrime[5].

Kumar BhashkarPoddar, Md. Kashif, GauravJha

Cyber terrorism is an attractive option for the terrorists for the following reasons:

- First, easy to access.
- Second, it is cheaper than other terrorist methods. The terrorist needs only a computer and online internet connection. They do not need to buy weapons like, guns and explosives etc.
- Third, more difficult to get caught than other traditional methods.
- Fourth, little or no regulation, censorship, or other forms of government control.
- Fifth, potentially huge audiences spread throughout the world.
- Sixth, fast flow of information.
- Seventh, inexpensive development and maintenance.
- Eighth, can be done from anywhere.
- Ninth, can affect more people.

Today there are more than 40 terrorist organizations that maintain websites and use different languages. Their websites provide information about the organization and some of their purposes are to change public opinion, weaken public support for a governing regime, and even take them down.

- From the Middle East
  - The Unix Security Guards (Islamic group)
  - The Popular Front for the Liberation of Palestine
  - The Anti - India Crew
- From Europe
  - The Irish Republican Army
  - The Basque ETA movement
  - Israel and Pakistan groups fighting each other using cyber-attack.

Cyber terrorism has the potential to affect directly a larger number of people than traditional terrorist methods, thereby generating greater media coverage, which is ultimately what terrorists want.

[4] Prevention by the Cyber terrorism

There are no hard-and-fast rules that will prevent cyber-terrorism in all cases, but there are some basic rules and regulations that the organizations and the firms should take to safeguard its information and digital assets.

- Secure systems with hardware and software protection.
- The Operating system and software’s should be regularly updated.
- A strong password policies should be enforced, regularly change the passwords, always use passwords that include a combination of numbers, letters and other characters and never store them in the computer.
Cyberterrorism: A dangerous weapon

- Antivirus system should be installed and kept them up to date and run regular checks to detect and remove any problems.
- High fidelity intrusion detection systems and firewalls should be employed.
- Regular checks to make sure security precautions are followed.
- Follow news and computer information reports about new threats.
- All the unnecessary services should be disabled.

Hence, we need to understand the importance of secure passwords, virus protection software, and the like.

**[5]Conclusion**

In today’s society it is apparent that cyber terrorism is a problem especially since it can be difficult to determine if an attack is from a hacker or from a hacker that is a terrorist or terrorist group. The next generation of terrorists are now growing up in a digital world, one in which hacking tools are sure to become more powerful, more simple to use, and easier to access.

Looking at the history of cybercrime it has been shown that there is definitely a need for more protection. Knowing that cyber terrorism exists is the first step to a solution. Always keep secure the hardware and software, use a strong password policy, install antivirus and kept them up to date, the unnecessary services should be disabled. Never give the personal information to any unknown person.

**References:**


Kumar Bhashkar Poddar, Md. Kashif, Gaurav Jha