

International Terrorism

Second Grade Students

International Relations Department

Lecture 11

Cyber Terrorism

Lecturer: Sara H Ali

As early as 1990, **the National Academy of Sciences** began a report on computer security with the words, “We are at risk. Increasingly, America depends on computers. . . . Tomorrow’s terrorist may be able to do more damage with a keyboard than with a bomb.”

quote from **Walter Laqueur**, one of the most well known figures in Terrorism studies: “The electronic age has now made cyberterrorism possible”.

Definition of cyber Terrorism

It is generally understood as an act that is

- – executed via cyberspace by individuals, groups or organizations who are directly influence by some terrorist movements or/and its leaders. motivated by a desire to effect political or ideological change. leading to violence that reaches physical and psychological repercussions beyond the immediate victim or target.

US Department of State's Define Cyber Terrorism as:

- “Cyberterrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against non-combatant targets by sub-national groups.
- **Cyber terrorism is the convergence of cyberspace and terrorism and it is different from cybercrimes, such as data theft, bank fraud.**
- Two main forms of this terrorist threat must be differentiated:
 - 1. Hybrid cyber terrorism
 - 2. pure cyber terrorism.

Hybrid Cyber Terrorism

Hybrid cyber terrorism is the use of the Internet for terrorist activities such as propaganda, recruitment, radicalization, fundraising, data mining, communication, training, and planning for actual terrorist attacks.

1- Propaganda and Psychological Warfare:

The Internet is being used by terrorists and terrorist organizations to spread and manage their propaganda through information warfare, to impart their ideology, to conduct psychological warfare as well as to radicalize and recruit new members from all over the world, through terrorist websites, online magazines, and various social media platforms (such as Facebook, Twitter, Instagram, youtube, etc).

2- Communication and Networking:

Terrorists groups have used social media platforms (like Telegram) and encrypted messaging system applications (such as Kik, SuperSpot, Wickr, Whatsapp), online gaming chat rooms, coded messages or steganography for covert discussions, direct and private communications purposes (that includes networking with other members of the group, interaction with recruits and supporters) and planning and coordination of physical attacks as well as planning hacking operations.

3- Fundraising:

Funding for terrorist related activities (acquire weapons or support the war effort by providing funds to the families of fighters) is no longer simply done through charity organizations. Instead, it is also being done by donation through social media platforms and blogs, and the use of the bitcoin digital currency.

4- Data Mining, Recruitment and Training:

Terrorists are using the Internet for data mining to collect information of particular places and individuals as potential targets for attacks as well as recruitment. Already in the case of the attacks of 11 September 2001, the al-Qaeda operatives used the Internet to collect information such as flight times and to share information and coordinate their attacks.

2- Pure Cyber Terrorism

- Pure cyber terrorism refers to direct attacks on a victim's cyber infrastructure (such as computers, networks, and the information stored therein) to achieve the political, religious and ideological objectives. Destructive and disruptive cyber terrorism can be further differentiated:
 - – Destructive cyber terrorism is the manipulation and corruption of information system functions to damage or destroy virtual and physical assets. The most popular weapon is the use of computer viruses and worms.
 - – Disruptive cyber terrorism is described as hacking designed to take down websites and disrupt the normal lifestyle, which relies on critical infrastructure supporting medical utility, transportation, and financial systems.