E-Terrorism and Counter Measures

Mahmoud Al-Hamdan,

Strategic researcher in countering terrorism, Jordan

Extremist organizations have employed modern technology to achieve their destructive and terrorist purposes. Accordingly, terrorists perceive Internet with its various technologies, sites and social media pages, as an important and easy way to perpetrate their illegal extremist activities. They may also target some websites and computerized systems of parties hostile to them in order to achieve their goals.

Terrorism Reformulation

In their paper "From Terrorism to Cyber Terrorism: The Case of ISIS", "Dominika Helena Giantas" and "Dimitrios Stergiou" consider electronic terrorism as a new version of traditional terrorism. It has been redefined to tailor to technical progress and the use of digital space as a realm of terrorism. They define "cyber-terrorism" as: "a high-impact attack using computers or computerized systems or threats to attack information systems by foreign activists; to terrorize countries or societies and force them to fulfil specific social or political objectives" They describe it as a result of the combination of traditional terrorism and the digital space, in which the latter becomes the means and realm for carrying out terrorist acts.

Samer Muayyad Abd al-Latif in his book "Electronic Terrorism and How to Confront It" concluded after reviewing the development of electronic terrorism concept that it is : "unlawful attacks or threats of attacks on computers, networks, or electronically stored information for retaliating or blackmailing governments, peoples, or the entire international community to force or influence them in order achieve specific political, religious or social goals".

Michael Kenney explains some of cyber-terrorism attributes according to the following table:

Attribute	Cyber-attack	Cyber-warfare	Hacktivism	Cyber-terrorism
Computer attack targeting other computers, computer systems, or the information they contain	✓	✓	✓	✓
Attack in pursuit of political, social, or religious aim		✓	✓	✓
Attack part of broader hostilities between belligerents, usually states or their proxies		✓		
Attack produces physical violence against persons, property or critical infrastructure				✓
Attack causes widespread fear or physical intimidation beyond immediate victims				✓

The analysis of the previous table clarifies that the classification of cyber-terrorism is not concerned with the scope and extent of attacks as much as it is concerned with the method and field of cyber activities. This type of terrorism aims to produce material violence towards individuals and materials accompanied by a state of panic among the victims and the general public.

Forms of Cyber Terrorism

In his book, "Strategies to Counter Terrorism and Extremism", Mahmoud Al-Farajat divides electronic terrorism forms into two types:

First: Direct use of the Internet: where extremist groups employ Internet to get the required impact directly on computerized systems connected to the Internet to achieve their goals, and the most prominent forms are:

1. **Cyber Threat:** Threatening to terrify people by harming individuals or their families, using e-mail, forums, social media, or media platforms.

Among its types are theft of data and files, blackmailing targeted parties, the use of data to kill, or the threat to hack websites and place terrorist organizations flags on

them, with intimidation and threats messages.

2. **Service Denial,** or electronic bombing, a form of net abuse consisting of sending large volumes of email to an address in an attempt to make it crash and become unable to serve users and subscribers.

3. **Destruction of systems, data and information:** the use of hacking files and electronic viruses to target the basic electronic systems, files and sensitive data of official and private institutions.

Second: Indirect use of the Internet: by exploiting available websites and applications, or creating websites or applications for terrorist organizations, or exploiting various communication applications. The most prominent uses are:

1. **Communications:** They are used because of their low cost, ease of use in communication and speed, ease of concealment, availability of various modern communication tools, and their transgression of geographical borders, which facilitated the processes of safe communication and contact among extremist groups leaders, their members and supporters.

2. **Promotion and recruitment:** by attracting new members to terrorist organizations, through coordination between the organization center and the new members, by using secure and encrypted communication programs. ISIS and others succeeded in recruiting many sympathizers by using these means, and bringing them to spheres of influence and conflict areas such as Syria and Iraq.

3. **Financing, armaments and logistical support services:** The use of digital currency, the most famous of which is Bitcoin, provided a suitable financial environment for extremist groups; to transfer money, use it and provide their needs, especially weapons, away from hostile security and intelligence oversight. It was also used to penetrate banking systems and steal from bank accounts and credit cards, to provide the necessary liquidity.

4. **Training, planning and managing traditional operations:** by broadcasting training courses; security, intelligence, operational, and tactical ones, and those that are related to the security of cyber operations, electronic terrorism activities, and lectures on ideological mobilization.

Confronting Cyber-terrorism

There are challenges that face endeavors to confront cyber-terrorism, the most important of which are related to the rapid developments in technology field, the development of stealth tools and blocking of tracking techniques, and the advancement of location change programs. Therefore, ways to confront this type of

terrorism can be arranged according to the following phases:

Phase one: Political and Organizational measures: They include the following:

- **Cyber policies:** A country's policy, at both local and international levels, determines its orientations in cyberspace. It seems that some of the major powers that are active in cyberspace, such as China and Russia, have reservations towards this field as they view cyber globalization as an infringement on the sovereignty of nation states, and that no state could control the content circulating among its citizens via the Internet under cyber globalization. Therefore, each country set up the required barriers, established its own national networks within the framework of the global Internet, according to its own controls, and succeeded in that. Most major countries have started, moreover, to adopt intermediary cyber groups to work in their favor, such as armies or "electronic flies".

- **Regulatory and legislative aspects:** Legal legislation, which takes into account the substantive and formal aspects, plays an important role in facing cyber-terrorism at state level. Legislation must regulate work in the digital field by establishing specialized entities under special laws, identifying the nature of crimes and the appropriate and dissuasive penalties for them and covering all aspects related to criminalization, penalties and formal procedures such as seizure, investigation, arrest, etc.

- **Cyber strategies:** A country's cyber strategy determines its orientation in this field. It includes all policies and other related aspects, such as entities authorized to regulate and control digital activities, keeping the legislations up to date with the developments in this area and paying attention to raising users' awareness of potential risks.

- **Regional agreements and international cooperation:** Bilateral agreements among states include the legal aspects required for cooperation in investigating cyberspace incidents. As for cyber alliances among states or with the private sector, bilateral agreements are important in tracking and investigating incidents and exchanging information on the most prominent methods criminals use, main digital seals and electronic fingerprints of terrorist organizations and the latest software and cyber weapons. This helps to determine the identity of the party that carries out cyber-terrorist attacks and facilitates targeting them.

Some experts do not support the alliance of major powers with developing countries in everything, i.e., developing countries should not open their digital space to these countries but seek partial cooperation instead. Countries can ally with prominent and

active cyber-security companies, especially local ones, provided that their alliance is based on the state's ability to control these companies. As for foreign companies, countries should be wary of them and treat them the same as major powers.

Phase two: Cyber security and intelligence measures

It is important for cyber-security authorities to raise awareness and carry out counter cyber intelligence measures to uncover and address the gaps in local systems, develop measures to counter attacks, carry out the required technical investigations, coordinate with law-enforcement agencies and other relevant entities, follow up with latest cyber activities and new cyber weapons, monitor digital space and users' commitment to locally and internationally established standards, cooperate with their regional and international counterparts, employ local hackers and recruit them to form on-line armies for their benefit.

Phase three: Technical measures

This phase includes developing software, applications, tools and electronic infrastructure required for the confrontation, as follows:

1. **Create Firewalls:** as the first line of defense for systems and information. They are software to protect systems and data and detect attacks.

2. **User account security measures and identification methods:** it includes protecting official and classified accounts. The individual is the main element in this aspect as system administrators must set the required automatic and manual means to verify the identity of the user.

3. **Data Encryption:** it is one of the methods used to protect data before sending them via the Internet or storing them. If an unauthorized party obtains the data, this process will prevent or delay the use of data.

4. **Public-key cryptography:** it adopts the technique of encrypting the data by the sender, dividing it into parts, and distributing it to several servers in different regions of the world. The receiver, on the other hand, can only collect these data using an encryption key (such as Freenet technology).

5. **Encrypted hopping technology:** this technology relies on the transmission of encrypted data from the sender through several consecutive nodes in the network, as each node adds an encryption until it reaches the receiver. This technique was used in the Dark Secret Network (Tor).

6. **Virtual Private Network:** it is a virtual sub-network on the Internet,

categorized, as Linknet the American network, as a secret private network connected to security, intelligence and government agencies related to countering cyber-terrorism. Organizations and countries use some private networks which are developed for private use among employees and managers, are partially isolated from the Internet and are subject to the permanent supervision of specialists to protect them.

7. **Air-gapping technology:** it is a technology used by control, supervision and computing systems of the sensitive infrastructure and data management, by isolating the systems completely from the Internet through developing technical gaps, which can be removed only according to specific confidential procedures and at secret times.

8. **Keylogger:** a technology used by cyber-intelligence to spy on the devices used by criminal and extremist organizations, using the required software to hack into the systems of these organizations and send spyware to the target in the digital space.

9. **Honey-cell, or bait:** is a technique used by cyber-intelligence by placing unreal information on a server to be a bait for terrorists, according to a well-structured plan. It aims to recognize and identify terrorists' activities, potentials and locations.

10. **Business continuity technology:** it means that data continue to be used by using backup copies. Usually, backup copies are kept automatically according to a specific programming managed by the system administration or the concerned security authority.

Summary

Competent authorities will be able to confront cyber-terrorism if they are able to define its concept accurately, and then determine their priorities in developing protection, follow-up and investigation procedures.

The inclusion of the competent authorities' view of this concept enables them to identify the required measures to confront cyber-terrorism activities, which range from technical, legislative, regulatory and political measures, in addition to regional and international cooperation in this field.