WORLD THREATENING CYBERTERRORISM

Abdul Sattar Abdul Rahman

Journalist & Researcher

Given the cutting-edge technologies of communication, terrorism has entered into a new era, making the world reconsider the current manifestations of terrorism, which is no longer limited to its traditional forms that can be identified and targeted; rather, terrorism has become cross-border in such a fashion that is difficult to control simply by closing or securing borders. Terrorist groups have become concerned with the ubiquity of the ideology and the recruitment of elements via the internet. Training camps have moved from the real world to the virtual world. It is no longer required to train individuals on a camp deep into one of the caves or mountain peaks or any strongholds: new elements can receive training along with associated information even from terrorist group websites.

Terrorist plans and tools have changed over time, and the specter of cyberterrorism is looming large on the horizon, through which terrorists target government infrastructures, information systems and military bases. As such, a valid question in this context is: "What is cyberterrorism?" What are the risks and opportunities of countering and overcoming cyberterrorism?

Cyberterrorism

In the 1980s, Barry Collin, senior research fellow at the Institute for Security and Intelligence in California, coined the term "cyberterrorism" in reference to the confluence of cyberspace and terrorism. Later in 1998, the CSIS Global Organized Crime Project of the Center for Strategic and International Studies in Washington D.C. published a report entitled '*Cybercrime, Cyberterrorism and Cyberwarfare*: *Averting an Electronic Waterloo*' which was the first key contribution to this field. Although cyberterrorism has become popular in recent years, and has become a major threat globally, especially with the increasingly growing development of communication technologies, and the exponentially heavy dependence of people on the internet and social media, there is no commonly agreed global definition of cyberterrorism as such! The definitions of cyberterrorism are numerous across the FBI, the US Department of

Defense, NATO, and other relevant institutions and research centers; now we have about 27 working definitions. The common ground among all these definitions is that cyberterrorism is the point where terrorism converges and intersects with cyberspace, which differs from cybercrime, data theft, bank fraud and the like.

Global Media

Cyberspace holds great appeal for all terrorist organizations, given the role assumed by global media through cyberspace; a fatal two-edge weapon. Daesh is considered the most threatening terrorist organization to the internet safety and security, as it is used for propaganda purposes, recruiting, financing, gathering information, coordinating terrorist attacks and mobilizing sympathizers from different parts of the world. Daesh has recruited a media army specializing in electronic media, operating under various alias.

There are factors that tempt terrorist organizations to use cyberterrorism: terrorism can be perpetrated from anywhere in the world, and the offender does not need to be in the location of the terrorist act, as the internet connections necessary to carry out such a terrorist attack using any modern mobile phone are widely available. The speed of electronic attacks does not depend on the speed of the internet connection used by the attacker; rather, the high speed of the internet connection used by computers under attack can be exploited. Viruses and other malware programs can mushroom as quickly as possible without the need for further interference by the attacker.

Terrorist acts committed through the internet can be kept anonymous and not traceable and remain intractable through anonymization services and similar camouflaging techniques, such as the use of computers controlled by piracy. In addition, digital evidence can be falsified intentionally. The temptation to cyberterrorism is further compounded by the low cost of the internet, the large number of targets that can be aimed at and many of these targets may not be adequately protected.

Given these temptations, various terrorist and extremist groups rushed to and jostled for owning sites on the internet, especially social networks; some of which own more than one site and in more than one language in order to introduce the organization, its history, foundations, activities, political and social backgrounds, ideological and political goals, the news update, attacks aimed at the target opponents, academia, intelligentsia, government authorities and security services.

For instance, Daesh has further enhanced its electronic capabilities by incorporating its cyber-arms, such as "Ghost Caliphate," "Sons Caliphate Army," "The Caliphate Cyber Army," and "Kalashnikov E-Security" in what was called The United Cyber Caliphate Hacker Group. Over the recent years, a group of Daesh pirates have been able to hack and destroy some websites, spreading extremist propaganda, including the websites of the British Ministry of Health, the Royal Malaysian Police, Malaysia Airlines, the French TV5 network and its stations, and the US Central Command.

Two Overlapping Types of Terrorism

Since there is no clear and commonly agreed definition of the concept of cyberterrorism, two different types of terrorism overlap: pure cyberterrorism and hybrid cyberterrorism.

Pure cyberterrorism relates to direct attacks on the victim of cyber-infrastructure, such as computers, networks and stored information to achieve various goals, including but not limited to destroying the functions of information systems, breaking down virtual and physical assets, blocking websites, and disrupting daily life by targeting the computer-managed infrastructure, such as medical facilities, stock exchanges, transportation, financial systems and the like.

Hybrid cyberterrorism refers to the terrorist use of cyberspace in various activities, such as:

1. Propaganda and psychological warfare: For instance: Daesh has seven media agencies, in addition to 37 media offices in different countries. Al-Qaeda has a media arm called Sahab;
2. Safe communication and networking: The aim is to send encrypted messages and information for clandestine discussions, and to plot and plan attacks, and the murder of the French priest in Normandy in July 2016 is a case in point; the murderers received the instructions via the internet;
3. Recruiting new members: A 2015 FATF report reveals that the network has become the most used tool for recruitment and support for terrorist organizations;
4. Training: This aims to publish training manuals explaining how to carry out attacks and manufacture explosives at the sites of such organizations;
5. Fundraising;
6. Collecting information on potential human targets.

Serious Risks

E-bombs are among the most notorious methods used to carry out electronic terrorism operations, such as disrupting and disturbing communications, tapping calls, broadcasting misleading information, mimicking voices, especially the voices of military leaders to issue dangerous orders, sabotaging computer networks through viruses, and wiping out device memory, obstructing the flow of funds, changing the course of deposits and breaking down power stations. For such a covert purpose, a special e-bomb, known as the CBU 49, was prepared; from such an e-bomb, several bombs were fired into the air, fully destroying power stations.

In a research paper about "The Future of Cyber-Terrorism" presented at the Eleventh Annual International Symposium on Criminal Justice Issues by Barry Coleen, a formidable list of potential cyber-terrorism activities that threaten the future of humanity is brought to focus, including the most infamous acts of vandalism:

- Remote access to control systems of grain silos, changing iron supplement levels to harm the health of consumers;
- Remote adjustments of the infant formula to harm the health of infants;
- Disrupting banks, international financial transactions and stock exchanges to undermine the economic systems;
- Remote manipulation of remediation of pharmaceutical industry components;
- Changing the pressure in gas lines and the loads of electrical networks, causing terrible explosions and fires;
- Attacking air traffic control systems, causing two civil planes to collide, by accessing the sensors in the cockpit. This is also possible on trains.

If the previous threats of cyberterrorism were merely theoretical perceptions that nothing as such, thankfully, by the grace of Allah and divine providence, has ever occurred, then this does not mean resignation and acquiescence; rather, this calls for outdoing and outperforming terrorists and proactively understanding their line of thought, hence preparing to nip their terrorist ideologies in the bud.

Necessary Confrontation

The first international efforts to counter cybercrime and digital terrorism date back to three decades, when Interpol discussed in 1981 the possibility of developing legislation on cybercrime. Progress since then has been slow, but it has accelerated

after the end of the Cold War. The establishment of the Cyberspace Law Institute at Georgetown University in 1995 may have been an indicator of the problem awareness. Countries have adopted many initiatives at the national, bilateral, regional or international levels in order to protect the global information infrastructure from the threat of cyber-threats. The world countries have also made concerted efforts to find new legislative frameworks that address such an emerging phenomenon by developing a new concept of national security, moving to international cooperation.

Fortunately, the world is aware of the risks of cybercrimes and seeks to confront and address such cyberterrorism by adopting an international strategy to secure cyberspace, through a set of laws and initiatives, such as the International Multilateral Partnership Against Cyber-Terrorism (IMPACT) that aims to bring together international efforts for government sectors, the private sector and civil society to meet the increasingly growing threats of cyberterrorism, gathering visions and ideas about training and exchanging experiences, establishing many websites to counter terrorism and protecting cybersecurity. These sites have been a meeting point and springboard for information security experts and politicians to discuss the threat of cyberterrorism and confrontation methods. This includes but not limited to the "SITE" intelligence group, which is an intelligence agency specialized in monitoring terrorism via the internet, investigating the primary sources of terrorists, monitoring their conversations and propaganda. In the aforementioned research paper, Barry Coleen provides a list of the elements that must be addressed when creating a program to counter cyberterrorism:

- Building a team to counter cyberterrorism on time armed with unique resilience;
- Changing the method in which we counter cyberterrorism;
- Collaborating and sharing intelligence information in new methods;
- Eliciting assistance and support from the individuals who well understand the war we face;
- Being aware of the new rules, new technologies and new players. Unlike traditional terrorists, if a cyber-terrorist loses today, such a cyber-terrorist does not perish, rather, he or she learns more and gain further experience from what he or she had failed to do, and hence will use that experience in a new successful attempt sometime in the future.

In their research study titled "An International Study on the Risk of Cyber-Terrorism" published in 2019, Ponnusamy and Rubasundram, add in other necessary research elements to counter cyberterrorism:

- Creating a strong and coordinated international framework for countering cyber-terrorism, reached at and agreed by governments and regulatory bodies to exchange intelligence and other forms of cooperation;
- Providing more education for public and private sector institutions to develop technologies that may be vulnerable to cyber-terrorism and to ensure that security is at always given a prime priority when creating new systems;
- Developing a safe technology to identify suspicious activities by analyzing public and private data, and making computers and systems much less vulnerable.

Tough Challenges

Cyberterrorism threats are on the increase in parallel with the increasingly growing number of the internet users constantly and exponentially. Given the fast-paced growth of computer technologies, and despite the fact that governments have stepped up security measures to counter such threats, including monitoring via the internet, such efforts are faced by a spate of daunting obstacles; most companies and applications use end-to-end encryption to protect the privacy of their users, while terrorists navigate across platforms and applications with the highest level of protection and encryption.

Almost all reports reveal that the number of Dark Web and the Onion Router users is on the increase compared to other browsers due to privacy concerns and anonymous identity preferences, which increases the risk of cyberterrorism. The concern of the internet users is mounting, with the pressure of the civil society institutions building up in the face of strict legislation issued by governments to counter terrorism on the internet. When British Home Secretary Amber Rudd expressed her intention to change the law to increase the prison sentence from 10 years to 15 years for people who constantly watch terrorist content on the internet, she was met with great objections.

Given the increasingly growing number of the internet users around the world that have reached more than 4.5 billion users and the lack of security awareness along with the glaringly heavy dependence on online communications to provide services, the difficulties of combating the threats of cyberterrorism are downright on the increase. Driven by these triggers, and the imperative of facing these threats is becoming more palpable.

It is true that government sectors all over the world have launched strict regulations, programs, policies, laws and various other measures in order to counter such threats; however, it remains a pitched battle that constantly needs continued

surveillance and intelligence, especially with the development and growth of threats, and their negative effects on governments, companies and individuals in terms of their business, information, privacy and security.