Coronavirus (COVID-19) and the Spread of Cyberterrorism Attacks

Sonny Zulhuda

Associate Professor, Ahmad Ibrahim Kulliyyah of Laws, International Islamic University in Malaysia (IIUM)

Since the World Health Organization (WHO) announced in March 2020 that the new coronavirus (COVID-19) became a global pandemic, increased caution and care have been given to contain its spread. Some have used websites to obtain more information about the pandemic, while others have been busy sharing messages on social media. E-activities such as on-line meetings, distance learning, or sharing video clips have become new habits, especially during the lockdown period imposed by many countries.

Cyberspace security

With the increasing fear and social anxiety of the pandemic, in addition to the strict lockdown procedures, this panic has given rise to dangerous and illogical behavior, including cyberspace security. Hundreds of millions of people have had to work or study from home. Cyberspace has become a tempting space for hackers and cyberterrorists to corrupt everything.

This is confirmed by the news and reports which stated that many abusive practices and cyberattacks emerged in cyberspace during the pandemic. WHO indicated that the number of cyberattacks that targeted international bodies had increased five times last April. Cyber threats in Malaysia reached over 80%, while the number of cyberattacks in Indonesia reached 88 million attacks from January to April 2020. India stated that the number of security cyberattacks supported by government-bodies targeting countries had increased during this period. All these news confirm that COVID-19 crisis is a major cause of the spread of cyberattacks.

Identifying gaps

The significant rise in cyberattacks affecting both organizations and individuals can be viewed as a danger warning for counterterrorism workers. This increase indicates that there are certain gaps in the information infrastructure related to the country's

public or private affairs (such as the Internet and large data) which are exploited by terrorist organizations to carry out their cyberattacks. Dr. Alex Schmid, from the International Center for Counter-Terrorism (ICCT) in the Hague, asserts that the growth of terrorist organizations at present is due to many factors, including the effects of globalization, such as the liberalization of financial markets, external and electronic banking services and the exploitation of Internet networks for abusive purposes.

Terrorist organizations and cyber-criminal groups have always been targeting governance systems to exploit weaknesses in them, which has led the United States government to state that it will not allow criminal groups to exploit the pandemic to threaten the lives of Americans. These terrorists are certainly keen to take advantage of the pressures caused by the pandemic on government institutions to exploit the emerging security gaps affecting cyberspace infrastructure for their subversive and terrorist interests and objectives.

Cyberspace exploitation

Terrorists exploit the Internet by various means, and there are major reasons for the increase in the exploitation of cyberspace by terrorists during the pandemic, given the availability of factors that facilitate such exploitation.

1. People's eagerness to gain information as many are keen to gather more information about the pandemic.

Individuals' behavior in dealing with the Internet changes during pandemics because they become more eager to access and disseminate information, and are more likely to click on any links or sources in the Internet. In fact, criminals and cyberterrorists quickly adapt to this emergency behavior and take advantage of opportunities to spread malicious programs by exploiting unlicensed links, fake emails, or misleading messages.

2. Telecommuting (working from home) allows cyber criminals to exploit unprotected computer systems.

The new rules of social distance, lock-down and self-quarantine have forced millions of people to work and study from their homes, using less protected computers and in a less technically supportive environment, compared to the ideal working facilities and the technical support which was provided before the pandemic.

3. Use external applications during lockdown period, especially unlicensed ones.

The overuse of external on-line platforms such as social media, e-meeting platforms, and cloud services which are under-protected or beyond the control of the employer, leads to many sensitive security risks and causes many other security problems.

COVID-19 pandemic and terrorism

One of the persistent questions in this regard is that does COVID-19 pandemic allow for the spread of terrorist attacks? To answer this question, several issues should be considered:

1) Terrorists are always keen to exploit the gaps of cyberspace. The new habits which have emerged during lockdown periods led many people to access cyberspace more, thus making it easier to conceal the identity of terrorists or some terrorist activity in cyberspace, given the significant increase in reliance on Internet networks.

2) There are no signs of any decline in cyberterrorism activities during the pandemic. Several reports have indicated that terrorists have been doing their best to make the most of this epidemic crisis. The Chief of the United Nations Peacekeeping Force stated in June 2020 that the COVID-19 pandemic posed many complex security challenges in the Sahel and Africa as terrorist groups are doing their best to take advantage of the pandemic by attacking national and international forces. Several sources indicate that terrorists take advantage from the hardship imposed by the pandemic to undermine countries' powers and destabilize governments.

3) Many cyberattacks target critical information infrastructure (critical services or basic services) which is considered a key source for maintaining essential social functions, or on the health, economic or social welfare level. If this structure is disrupted, it will cause considerable damage due to the inability to protect and maintain these functions.

Real examples

One example of such attacks targeting critical information infrastructure took place in the Czech Republic when a terrorist group electronically attacked the computer system of a university hospital in Brno, disrupting one of the largest COVID-19 screening laboratories in the Republic. Also, the ransom program targeting the information system of the Public Health Management in Champaign, Illinois, United States, threatened to disrupt the public health system used to manage information on the COVID-19 pandemic.

In Taiwan, the state-owned energy company was reportedly attacked by the ransom

program. Japan Telecom stated that some criminals hacked its internal network and stole the data of 621 customers. Some sources warned that Germany's critical infrastructure was at risk also of Russian piracy. In Indonesia, a high-level on-line meeting of the National Information Technology Council was vandalized by a hacker who viewed inappropriate and abusive files of other participants. This incident caused much embarrassment and considerable fanfare among participants, and exposed the sensitive information discussed at the meeting to the risk of diversion.

All these incidents confirm that the critical information infrastructure is greatly targeted by cyberattacks during pandemics which could be a first step towards further terrorist attacks.

Information governance

The most prominent risk factors resulting from the outbreak of COVID-19 have created many gaps which provided an attractive environment for terrorist attacks. In his analysis, Schmid asserts that terrorist organizations need to finance their attacks from various sources and that the cyberspace congestion would be an excellent source of financing, an opportunity for data theft, extortion, electronic fraud schemes and the breach of on-line banking facilities.

In addition, terrorists exploit the Internet to promote their ideological and political goals to attract individuals, gain sympathy and promote their goals. Therefore, they are keen to expand their networks over the Internet as it brings many benefits contributing to their interests. The spread of media can be exploited for this purpose as well.

Cyberattacks on critical infrastructure confirm the strength of terrorist groups' determination to harm their targets and to continue their terrorist acts, all of which could turn into a dangerous cyberterrorist threat.

COVID-19 pandemic has posed difficulties for individuals and governments in averting terrorist threats. There is an urgent need to develop a comprehensive framework for information governance and to make sustained efforts to ensure the safety, security and strength of cyberspace. The devastating consequences of COVID-19 pandemic have exacerbated these intractable threats, requiring those responsible for critical information infrastructure or essential services, government actors and private organizations to strengthen their security, preventive, protection and response measures to avoid and limit terrorist threats. This must be based on a firm basis of information governance and compatible with legal and technical aspects.