Analysis of Cyberterrorism and Online Social Media

Chunying Wu [1], Juan Wang [1]

[1] Department of Military Management, China People's Police University, Lang fang City, Hebei Province, 065099,China

*Corresponding author's e-mail: 775251252@qq.com, 66267476@qq.com

Keywords: network terrorism;   Online Social media ; Anti-terrorism

Abstract. Cyberterrorism is terrorism in form of non-conventional security threats. In this paper, firstly, the definition of Cyberterrorism is elaborated, then the reasons of carrying on terrorism activities based on social media on the network in the recent years are be deeply analyzed, and finally the ways about anti-terrorism on the network is explored concisely.

1. Introduction

Since the birth of the term "cyberterrorism" in 1997, terrorist incidents have been carried out one after another by terrorists through the global popularization of the Internet. Cyber terror activities not only endanger the peaceful life of mankind, but also threaten human life, which will bring serious consequences to national public security, and even lead to armed conflicts. The world is facing a growing cyberterrorism, and the situation which is getting worse.

2. The definition of Cyberterrorism

As early as 1997, "Cyberterrorism" proposed by Dr. Barry C.Collin, refers to premeditated attack by terrorist organizations or terrorists on computer systems, programs and data[1]. What's more, British 2000 Anti-terrorism laws gives the definitions of Cyberterrorism legally. Now it is enriched with the development of network technology and diversity of terrorist activities, including all Internet activities involved terrorism, for example, promoting terrorism, recruiting new terrorists, teaching technology of terror and violence, raising funds, organizing and planning terrorist attacks, implementing cyber attacks and sabotage [2]. In recent years, Zhu Yongbiao and Ren Yan scholars have proposed that cyber terrorism refers to terrorism that uses the Internet as a tool or the network as an attack target. That is, cyberterrorism can be divided into two categories, namely, tool-type cyberterrorism and targeted cyberterrorism[3-4].

3. Cyberterrorism develops rapidly with online social media

3.1. Online social media is fast, convenient and low-cost and spreads information fast.

Terrorists initially established traditional websites to promote terrorism, but their production and maintenance costs are high, the number of visitors is limited, and the target is clearly traceable. Now with the rapid development of technology of network information interaction, information transmission and exchange are more convenient and efficient. Social media has become one of the most popular media types among Internet media in recent years [5]. Terrorist organizations or individuals can use the popular online forums, social networking sites, WeChat, Weibo and other social media to create accounts, promote terrorism and plan terrorist activities without spending any money. Compared with traditional websites, the releasing and spreading speed of a message in the new social media on the Internet has doubled or even increased exponentially, with an unimaginable speed.

3.2. Online social media users are used in large quantities and have a wide audience.

Online social media has become an important force for online content distribution[5]. China Internet Network Information Center (CNNIC) released the "42nd Statistical Report on Internet Development in China" On August 20th, 2018. By June 2018, China has 802 million Internet users, and user usage rate of WeChat friend circle is 86.9%, QQ space usage rate is 64.7% and Weibo and video users usage rate is 42.1%[6]. Terrorists make full use of the openness and anonymity, the characteristics of social media, and hide themselves in the dark in order to promote terrorism recruit associates, raise fund. When the police find out, they will close their accounts and quickly run away, shifting their positions like engaging in "guerrilla warfare". Since mid-2015, Twitter has blocked threatening 360,000 user accounts that take and promote terrorist activities[7].

3.3. Online social media is easy to be connected to finance to facilitate the transfer of funds or money laundering.

As the online financial system become mature gradually , many mobile APP social software have modules or links with financial platforms such as bank cards and Alipay to facilitate the entertainment and consumption of the public. In addition to traditional websites to accept donations to raise funds by links, terrorist organizations are trying to see for new ways on popular new social media to carry out fund transfers, raise funds, launder money and collect money.

4. The solution of Cyberterrorism based on online social media

We have a long way to go against terrorism on Internet. It is necessary to further improve the international anti-terrorism cooperation mechanism and coordinate operations, because terrorism involves the interests of many countries. In 2016, China promulgated and implemented the "Anti-Terrorism Law of the People's Republic of China" and the "Network Security Law of the People's Republic of China", and issued the "National Cyberspace Security Strategy"，which opened a new chapter in China's network anti-terrorism work. Under the vigorous development of new interactive technologies, attention should be paid to the establishment and improvement of network security legislation in the field of social media, establishing relevant laws and regulations, regulating social media operations to prevent terrorist organizations from using them to carry out terrorist activities. At the same time, the supervision of relevant departments should be strengthened. The network supervision department of the public security department should vigorously supervise and manage the network, and control the social media's network public opinion to be correctly oriented and establish an early warning and research mechanism for network public opinion. Once bad signs are found, they will be snuffed out in the "cradle" in a timely manner. Therefore, the research investment on network security should be constantly increased to turn passive defense into active defense. Besides, relevant government departments should actively promote anti-terrorism education to the public, raise people's awareness of vigilance, and make them understand its harm. What's more, the relevant departments should establish a psychological counselling station, actively use social media to tell the public how to conduct self-psychological adjustment under various circumstances through professional psychologists, and timely conduct psychological counselling for people with psychological problems.

References

[1] Collin B. The Future of cyberterrorism [J]. Chemical Engineering Progress, 1996, 13(2) : 1563－1568.

[2] LiuQigang, LiuChong. Study on the disposal mechanism of network terrorism[J]. Journal of Guizhou Police Officer Vocational College, 2016（5）:115-117.

[3] ZhuYongbiao, RenYan. International Cyberterrorism Study [M]. Chinese Academy of Social Sciences Press, 2014.07.

[4] XiaJing. Research on Current Situation and Improvement Strategy of Anti-Cyber terrorism in China [D], Nanchang University, 2017-5-1:14.

[5] CNNIC. The 41st Statistical Report on Internet Development in China[EB /OL]. http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201803/P020180305409870339136.pdf, 2018－03－05.

[6] CNNIC. The 42st Statistical Report on Internet Development in China ［EB /OL］. http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201808/P020180820630889299840.pdf, 2018－08－20.

[7] Sina science and technology. (2018). Twitter says it has suspended 360,000 terrorism-related accounts. http://tech.sina.com.cn/i/2016-08-19/doc-ifxvcsrm1864493.shtml.