Cyber Terrorism Through Social Media: A Categorical Based Preventive Approach

Alaattin Parlakkılıç*
*Department of Management Information Systems, Ufuk University, Turkey

Tel: +090-3125867494, e-mail:alaattin.parlakkilic@ufuk.edu.tr

ORCID ID: 0000-0002-6834-6839

Research Paper Received: 07.12.2018 Revised: 25.12.2018 Accepted: 30.12.2018

Abstract: This paper deals with the categorical cyber terrorism threats on social media and preventive approach to minimize their issues. While dealing with the threat of cyber terrorism in social media, The United Nations Office for Drug and Crime categorical approach propaganda, financing, training, planning, execution, and cyber attacks are determined. In order to prevent cyber terrorism in social media, measures in social spam, campaigns, misinformation and crowdturfing, and other practical techniques have been revised to provise a categorical approach. Combating and measures may involve improving the response to cyber threats by using security technologies; developing and improving situational awareness, analytic risk mitigation scanning, adoption of international criminal law penalties and most importantly providing a holistic information security education to people and organisations that may be at risk from cyber terrorism.

Keywords: Social media, cyber terrorism, prevention, threats, security.

1. Introduction

The number of cyber attacks has been increased in recent years and has made cybersecurity concern for people, nations and the globe. The social media makes it possible to communicate with people who have any social media accounts. The dissemination of information through social media is fast, easy and superior to any other media. In the world, there have been approximately 2.67 billion people using social media and is expected that there will be 2.95 billion by 2020 [1]. This situation brings many problems to solve. Online attacks, terrorist activity, and cyberterrorism are most to exist. The term cyberterrorism was originated by Barry Collin in 1980 and it has spread widely and quickly to be used.

Cyber Terrorism in social media is used for money laundering, identity theft, online fraud, cyber attacks, and others. Such the situation, methods have been used to prevent illegal operations [2]. Therefore, solving cyber terrorism in the internet and social media, it would be perhaps more accurate to refer to it The United Nations Office for Drug and Crime (UNODC) categorization which divides this into six main areas, namely propaganda, financing, training, planning, execution, and cyber attacks in 2012 [11]. In this study, the following questions are investigated to be answered:

- What are the threat categories in social media for cyber terrorism?
- How do attackers use social media for cyber terrorism?
- What are the mitigations for cyber terrorism in social media?

This paper is organized as follows. Section 2 reviews social media and cyber terrorism in social media. Section 3 describes cyberterrorism categories through social media. Finally, Sections 4 report measures to be taken for cyberterrorism through social media

2. Literature review

Social Media is simple, flexible and inexpensive, with its global prevalence and increasing level of use, and it is one of the mass media. Massive use of social media, national security, and strategic interests may be subject to negative impacts [3].

As platforms such as Facebook and Twitter are exposed to a multifaceted interaction with geo-economic and sociocultural elements, it is important to constantly monitor how they develop, to analyze how they work and to measure their potential. In this process, it is aimed that states will be able to monitor, report and neutralize the potentially offensive character of social media and to preserve security [4].

2.1. Social Media Analysis

The social media analysis has increased with the growth of websites using social networks. Many software to monitor and analyze the social networks were developed. Analysis tools perform following duties [5]:

- Monitoring: search information in the Internet environment using information retrieval languages;
- Analysis: process information and visualize in reports.

Social media analysis was done for information passing through the network; for its scope; for its specific paths, for discovering of non-obvious relations and for identifying nodes that are directly or indirectly associated in social media [6].

2.2.Cyber Terrorism Using Social Media

Cyber terrorism is an electronic attack to a particular target from both the internal and external networks that infiltrate from different sources with the different set of motivations. Another spesific definition by Janczewski and Colarik [24] defines cyber terrorism as: "cyber terrorism means pre-mediated, politically motivated attacks by sub national groups or clandestine agents or individuals against information and computer systems, computer programs, and data that results in violence against non-combatant targets" [24]. Cyber terrorism aims to damage, compromising and by-passing security measures for harmfulness [7].

The term 'cyber terrorists' known as 'hackers' can be an individual aim to damage target's reputation. However, hackers can malign the reputations of organizations, people and even their psychological situation. The targets are generally computer networks [8].

Social media is a suitable area for cyber terrorism. Because of the accessibility, affordability, and broad reach of social platforms, terrorist groups use social media to realize their objectives within the borders of the country and outside. Governments and agencies use preventive tools to stop terrorist bad efforts. Today, 90% of cyber terrorist attacks are done on the internet through social media [9].

Much effort is needed to reduce cyber attacks. An attack model makes it possible to recognize the current situation and future cyber attacks. With the Lockheed-Martin Intrusion Kill Chain (IKC) model, it shows the seven steps the attacker has followed to plan and execute an attack. The IKC stages are as follows [10]:

- Information Gathering: collecting information for the target.
- Weaponization: developing malicious code for vulnerabilities
- Delivery: deploying the payload to the targets
- Exploitation: executing the malicious code.
- Installation: install malicious programs.

3. Cyberterrorism categories through social media

The Internet is a powerful political instrument for cyber terrorists to forward their goals. Cyber terrorists and their organizations start to utilize the Internet to expand and improve their operations. However, when coping with attacks of cyberterrorism, it is wise to control harmful use of the Internet by cyber terrorists. The UNODC described threats for social media. Social media platforms offer terrorists to spread their message more quickly and effectively. UNODC categorized threats in six area as propaganda, financing, training, planning, execution and cyber attacks [11]. The categories are explained briely as follows:

a.Propaganda: Social media has increased the publicity of cyber terrorists by spreading their ideas with virtual tools. Terrorists try to reach out globally to sympathizers by so-called incitement, recruitment, and radicalization. But sometimes the disseminators can be unaffiliated but are sympathetic to the ideology of a terrorist organization [12].

b.Financing: The financial resources search can comprise direct approaches, electronic commerce, virtual payment systems, and legal any financial organization. Terrorists use Web sites dedicated to the activities for controling the money flow with secret detection methods. Social media are used to coordinate financial campaigns involve 'sponsors' and may get many amounts of cash. Terrorists can reach a large audience by peer-to-peer mobile applications such as WhatsApp and Viber or more secure ways. And sometimes donors are also a priority target group. Financing terrorist activities are done through charity organizations. Donation can be done through social media with bitcoin or with any method [13].

c.Training: Training recruits by using the Internet involves using the information to produce arms and to launch attacks. Virtual training tools are used to reach target groups and organized journals are used like Al-Qaida's Inspire. Terrorists use the Internet for collecting information about places and individuals. Recruitment is done by monitoring Facebook profiles and conversation whether they are genuine sympathizers. Terrorists add sympathizers as friends and engage in private after ensuring individuals' faithfulness. Terrorist disseminates training materials for physical attacks, and instructions to equip necessary skills for cyber defense and to improve offensive capabilities [12].

d.Planning: Dissemination of jihadism have made an important contribution to the ability of terrorists to communicate, plan, conscript, organize, and train through social media. Internet resources make it easier to plan an attack. Intelligence gathering from social media (e.g. Google earth) can be done and also they use encryption not to be discovered [14].

e.Execution: The attacks execution are hard to be detected when terrorist use right precautions when connect. The terrorists use and make chaos by targeting important infrastructures. Vulnerabilities are much and the outcomes are high. The strategies against cyberterrorism can be improved. But the threat from cyberterrorism should not be vastly overstated [15].

f. Cyber attacks: A cyber attack can be done at any time or place. The motivations behind the cyber-attacks are depending on the terrorist intention, hacktivism, and terrorist authorities.

Organizations should take drastic protection against cyber-attacks, assess cyber readiness, expand the resilience capacity and adopts security regulations. Cyber attacks graded from installing spyware to destroy the infrastructure. Social media attacks target

websites with large user bases and use as a delivery mechanism by stealing user accounts [16].

4. Combating Cyberterrorism in social media

Social media are exceptionally evolving and are covering, so, it is important to monitor and take measure for their bad effects. Threats in the social media spectrum are limitless and wide-range. Specifically, new kinds of threats like social spam, campaigns, misinformation and crowdturfing, and other techniques improve information theft and threats [17].

4.1. Social Spam

Spams might damage reputation, so it needs to be stopped or avoided. The needs in practices are spammy or disingenuous and require managing spam accounts and monitoring the channels regularly, providing terrorists to collect dust intentionally, acting fast and remaining vigilant and measurements as follows [18]:

- Do not automatically follow people
- Turn off commenting
- Block spam accounts
- Reduce the hashtags
- Avoid bulk messages and
- Report fake reviews.

4.2.Campaigns

Social media can often go unmonitored or misused as it floods supporters with irrelevant advertisements and requests. Faking reports can be distasteful and quite disturbing. Important measures are as follows [19]:

- Create appropriate content
- Make sure images aren't offensive
- Think about risk factor
- Avoid bad timing and
- Be sure for references.

4.3. Misinformation

While searching for actual news, it's possible to confront with misinformation. However, some modern technologies can be used to destroy false reports and find the right forms from social media at the time of crises. In real controls and valid scoring, new platforms better direct social media after disasters [20].

Due to the speed and ease of spread, it is difficult to neutralize the information. Social networks provide a basis for people to express their intentions and prescriptive beliefs by spreading information quickly without confirming whether they are true or not. Combating misinformation is a complex task, and here are some important points to do [21] :

- Know the source
- Compare reports for real information
- Do not present stories only by looking at the headlines
- Avoid exaggeration
- Consider the scope of the topic
- Check images with visual search and
- Fix your micro-messages.

4.4.Crowdturfing

A combination of "crowdsourcing" and "astroturfing", crowdturfing is a new spamming phenomenon that artificially mobilizes large numbers of users to support reputations, companies, organizations, products, or even opinions. The money-operated posters can produce the desired result of positive or negative opinions, combined with coordinated attacks, to attract attention or to induce curiosity. With this method, it can mislead the online users and lead to cyber-rumors to put individuals or businesses in a compromising position or at serious risk. Here are measures to prevent crowdturfing [22]:

- Ask for feedback
- Create contests and giveaways
- Poll or survey fans.

4.5. Some Practical Techniques

Criminals masquerade themselves in social media while gathering information.

Security measures and the following strategies can be implemented [23]:

- Use current antivirus software
- Keep all software up-to-date
- Learn basic security measures
- Know your friends well
- Never provide sensitive information
- Use secure and differentiate passwords.

5. Conclusion

This paper presents with the categorical cyber terrorism threats on social media and preventive approach to minimize the effects of cyber terrorism. In order to prevent and combat with cyber terrorisms, the issues summarised below should be focused and achieved.

- The categorical approach summarised should be considered.

- Measures in social spam, campaigns, misinformation and crowdturfing, and other practical techniques should be taken into account.

- The review showed that terrorists spread their ideas with virtual tools; have financial resources by a direct approach, e-commerce, online payment systems, and the legitimate organizations; plan, communicate, organize, recruit, and train terrorists through social media; exploit and attack by targeting critical infrastructures and vulnerabilities. These issues should be under investigation.

- Security technologies like firewall, intrusion detection and prevention system, spam filter, anti-malware, and anti-virus tools should be used for mitigation and response of attacks.

- Cyber terrorism measures should be preventive for information infrastructure in terms of security policy and criminal special rule's allocation. Governmental situational awareness, analytic risk mitigation scanning, and adoption of international criminal law penalties can be applied. A comprehensive education and awareness program for users and the public on cyberterrorism can contribute to decreasing cyberterrorism.

It can be concluded that combating cyber terrorisms requires more attention, knowledge, support, coordination, and experts. The managers/rulers should take actions on the issues given in this article.

References

[1]. L. Kirichenko, T. Radivilova, and A. Carlsson. "Detecting cyber threats through social network analysis: short survey." CoRR abs/1805.06680, 2018.

[2]. R. B. Broadhurst, Chapman-Schmidt, D. Maxim, S. Orlando, B. Sabol, and H. Woodford-Smith. "Cyber Terrorism: Research Review", Australian National University, Cybercrime Observatory, Canberra, DOI: 10.13140/RG.2.2.19282.96964, 2017

[3]. J.K. Kimutai. "Social. Media and National Security Threats: A Case Study of Kenya", http://www.erepository.uonbi.ac. ke/ bitstream/handle /11295/76667/ Kimutai_Social%20 Medi %20And%20 National%20Security%20Threats%20A%2 0 Case%20 Study%20Of%20Kenya.pdf? sequence=4,2014 (Article)

[4]. A Montagnese.“Impact of social media on National Security”,Published MA Thesis. University of Rome, 2012

[5]. W. Marcellino, L.M. Smith, C. Paul, L. Skrabala. Monitoring Social Media, https://www.rand.org/content/dam/rand/ pubs/research_ reports/RR1700/RR1742/ RAND_RR1742.pdf, 2017 (Report)

[6]. D. Prakash, S. Surendran., “Detection and Analysis of Hidden Activities in Social Networks”, IJCA, Volume 77 – No.16, 2013

[7]. R. Littlefield. “Cyber Terrorism: understanding and preventing acts of terror within our cyber space”, https://littlefield.co/cyber-terrorism-understanding-and-preventing-acts-of-terror-within-our-cyber-space-26ae6d53cfbb , 2017 (Article)

[8]. S. Narula, N. Jindal. “Social Media, Indian Youth and Cyber Terrorism Awareness: A Comparative Analysis”. J Mass Communicat Journalism 5:246. doi:10.4172/2165-7912.1000246, 2017

[9]. A. Aly, S. Macdonald, L. Jarvis and T. M. Chen. “Introduction to the Special Issue: Terrorist Online Propaganda and Radicalization”, Studies in Conflict & Terrorism, 40:1, 19, DOI: 10.1080/1057610X.2016.1157402, 2017

[10]. D. Galinec, D. Možnik and B. Guberina. “Cybersecurity and cyber defence: national level strategic approach”, Automatika, 58:3, 273-286, DOI: 10.1080/00051144.2017.1407022, 2017

[11]. United Nations Office on Drugs and CrimeThe use of the internet for terrorist purposes. United Nations Office on Drugs and Crime, pp.3-13. Available at: https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf, 2012.

[12]. K. Shaffer. “ 10 ways to get started fighting internet propaganda”, https://pushpullfork.com/getting-started-fighting-internet-propaganda/, 2017

[13]. M. Nazır. “How To Use Socıal Medıa Effectıvely In “The Medıa Mıx”, https://wearesocial.com/blog/2018 /01/use-social-media-effectively-media-mix , 2018

[14]. H.H. Willis, A.R. Morral, T.K. Kellyand J. Medby. Estimating Terrorism Risk. MG-388-RC. Santa Monica, CA, RAND Corporation, 2005

[15]. A. Chuipka, The Strategies of Cyberterrorism: Is Cyberterrorism an effective means to Achieving the Goals of Terrorists? https://ruor.uottawa.ca/bitstream/ 10393/35695/1/CHUIPKA%2C%20Adam%2020169.pdf, 2017

[16]. M. Sreenu. “A General Study on Cyber-Attacks on Social Networks.” IOSR Journal of Computer Engineering (IOSR-JCE) , vol. 19, no. 5, 2017

[17]. L. Kyumin, J. Caverlee, James and P. Calton. “Social spam, campaigns, misinformation and crowdturfing”, 199-200. 10.1145/2567948.2577270.

[18]. L. K. Williams. “ How to Prevent Social Media Spam from Damaging Your Brand”, 2017

[19]. Isentia, “How to avoid a social media campaign disaster”, https://www.isentia.com/news/blog/ideas/how-to-avoid-a-social-media-campaign-disaster, 2018

[20]. D. Talbot. "Preventing Misinformation from Spreading through Social Media", https://www.technologyreview.com/s/514056/preventing-misinformation-from-spreading-through-social-media/, 2013.

[21]. Paul Krugman, How to avoid spreading fake news when big stories break, https://mashable.com/201710/03/how-to-avoid-spreading-misinformation-online/#, TY5opc_ Jxmqm, 2017

[22]. R. Spiegel. " 3 Ways To Benefit From Social Media Crowdsourcing", Https://Www.Socialmediaexaminer.Com /3-Ways-To-Do-Social-Media Crowdsourcing, 2011

[23]. Preparisi, Social Media Threats. Https://Www.Americanbar.Org/Content/Dam/Aba/ Events/State_Local_Government/2017/Homeland-Security/Social-Media-Threats Checklist. Pdf, 2017

[24]. L. Janczewski and A. Colarik, Cyber warfare and cyber terrorism (1st ed., pp. 13–14). Hershey [Pa.]:Information Science Reference, 2008.