JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 06, ISSUE 01 , 2019

An Empirical Study Of Cyber Terrorism

N.K SINGH
Department of computer science ,BIT Mesra, nksingh27@gmail.com

ANURAG SINHA
anuragsinha257@gmail.com
Department of computer science and IT, UG SCHOLAR Amity University Jharkhand, Ranchi, Jharkhand (India)

Abstract

Over the past two decades there has developed a voluminous literature on the problem of cyber terrorism. The themes developed by those writing on cyber terrorism appear to spring from the titles of Tom Clancy's fiction, such as Clear and Present Danger, The Sum of All Fears and Breaking Point, or somewhat more cynically, Patriot Games. This essay examines both the gap between the presumed threat and the known cyber terror behaviors and the continuing literature which suggests an attack is imminent. It suggests that at least part of the explanation lies both in the continuing failure to distinguish between what Denning (Activism, hacktivism, and cyber terrorism: The internet as a tool for influencing foreign policy, 1999) referred to as hactivism and cyberterrorism and also the failure to distinguish between the use of digital means for organizational purposes (information, communication, command and control) and the use of digital communications to actually commit acts of terror.

Introduction

Defining cyber terrorism:-

Cyber terrorism can be explained as internet terrorism. With the advent of the internet, individuals and groups are misusing the anonymity to threatenindividuals, certain groups, religions, ethnicities or beliefs.

Types of cyber terror capability:-

Cyber terrorism can be broadly categorized under three major categories:

- Simple: This consists of basic attacks including the hacking of anindividual system.
- Advanced: These are more sophisticated attacks and can involvehacking multiple systems and/or networks.
- Complex: These are coordinated attacks that can have a large-scaleimpact and make use of sophisticated tools.

The following three levels of cyber terror capability are defined by Montereygroup:-

- Simple-(Unstructured) The capability to conduct basic hacks against individual systems using tools created by someone else. The organization possesses little target analysis, command, and control, or learning capability.

- Advanced-(Structured)The capability to conduct more sophisticated attacks against multiple systems or networks and possibly, to modify or create basic hacking tools. The organization possesses an elementary target analysis, command and control, and learning capability.

- Complex-(Coordinated) The capability for a coordinated attack capable

  of causing mass-disruption against integrated, heterogeneous defenses (including cryptography). Ability to create sophisticated hacking tools. Highly capable target analysis, command, and control, and organizationlearning capability.

Concern:-

Cyber terrorism is becoming more and more prominent on social media today. As the Internet becomes more pervasive in all areas of human endeavor, individuals or groups can use the anonymity afforded by cyberspace to threaten citizens, specific groups (i.e.with membership based on ethnicity or belief), communities and entire countries, without the inherent threat of capture, injury, or death to the attacker that being physically present would bring. Many groups such as Anonymous, use tools suchas denial-of-service attack to attack and censor groups who oppose them, creating many concerns for freedom and respect for differences of thought.

Many believe that cyber terrorism is an extreme threat to countries' economies, and fear an attack could potentially lead to another Great Depression. Several leaders agree that cyber terrorism has the highest percentage of threat over other possible attacks on U.S. territory. Although natural disasters are considered a top threat and have proven to be devastating to people and land, there is ultimately little that can be done to prevent suchevents from happening. Thus, the expectation is to focus more on preventative measures that will make Internet attacks impossible for execution.

As the Internet continues to expand, and computer systems continue to be assigned increased responsibility while becoming more complex and interdependent, sabotage or terrorism via the Internet may become a more serious threat and is possibly one of the top 10 events to "end the human race."[28] People have much easier access to illegal involvement within the cyberspace by the ability to access a part of the internet known as the Dark Web. The Internet of Things promises to further merge the virtual and physical worlds, which some experts see as a powerful incentive for states to use terrorist proxies in furtherance of objectives.

Dependence on the internet is rapidly increasing on a worldwide scale, creating a platform for international cyber terror plots to be formulated and executed as a direct threat to national security. For terrorists, cyber-based attacks have distinct advantages over physical attacks. They can be conducted remotely, anonymously, and relatively cheaply, and they do not require significant investment in weapons, explosive and personnel. The effects can be widespread and profound.

ISSN- 2394-5125 VOL 06, ISSUE 01 , 2019

Incidents of cyber terrorism are likely to increase. They will be conducted through denial of service attacks, malware,and other methods that are difficult to envision today. One example involves the deathsinvolving the Islamic State and the online social networks Twitter, Google, and Facebooklead to legal action being taken against them, that ultimately resulted in them being sued.

In an article about cyber attacks by Iran and North Korea, The New York Times observes, "The appeal of digital weapons is similar to that of nuclear capability: it is a way for an outgunned, outfinanced nation to even the playing field. 'These countries are pursuing cyberweapons the same way they are pursuing nuclear weapons,' said James A. Lewis, a computer security expert at the Center for Strategic and International Studies inWashington. 'It's primitive; it's not top of the line, but it's good enough and they are committed to getting it.'

Examples of Cyber terrorism

An operation can be done by anyone anywhere in the world, for it can be performed thousands of miles away from a target. An attack can cause serious damage to a critical infrastructure which may result in casualties. Attacking an infrastructure can bepower grids, monetary systems, dams, media, and personal information.

Some attacks are conducted in furtherance of political and social objectives, as the following examples illustrate:

- In 1996, a computer hacker allegedly associated with the White Supremacist movement temporarily disabled a Massachusetts ISP and damaged part of the ISP'srecord keeping system. The ISP had attempted to stop the hacker from sending outworldwide racist messages under the ISP's name. The hacker signed off with the threat: "you have yet to see true electronic terrorism. This is a promise."

- In 1998, ethnic Tamil guerrillas attempted to disrupt Sri Lankan embassies by sending large volumes of e-mail. The embassies received 800 e-mails a day over a two-week period. The messages read "We are the Internet Black Tigers and we're doing this to disrupt your **communications." Intelligence authorities characterized it as the first known attack by** terrorists against a country's computer systems.

  During the Kosovo conflict in 1999, NATO computers were blasted with e-mail bombs and hit with denial-of-service attacks by hacktivists protesting the NATO bombings. In addition, businesses, public organizations and academic institutes received highly politicized virus-laden e-mails from a range of Eastern European countries, according toreports. Web defacements were also common. After the Chinese Embassy was accidentally bombed in Belgrade, Chinese hacktivists posted messages such as "We won't stop attacking until the war stops!" on U.S. government Web sites.

- In March 2013, The New York Times reported on a pattern of cyber attacks against U.S. financial institutions believed to be instigated by Iran as well as incidents affecting South Korean

financial institutions that originate with the North Korean government.

- Pakistani Cyber Army is the name taken by a group of hackers who are known fortheir defacement of websites, particularly Indian, Chinese, and Israeli companiesand governmental organizations, claiming to represent Pakistani nationalist and Islamic interests. The group is thought to have been active since at least 2008, and maintains an active presence on social media, especially Facebook. Its members have claimed responsibility for the hijacking of websites belonging to Acer, BSNL, India's CBI, Central Bank, and the State Governmentof Kerala.

Prevention from Cyber terrorism and laws against it.

a) Existing Law Organic Law No. 2015-26 of 7 August 2015 on the Fight against Terrorism crimes and repression of money laundering.

b) − Law No. 2008-01 of 8 January 2008 concerning the revision and completion of the Telecommunications Code promulgated by Law No. 2001-01 of 15 January 2001.

c) − Law No. 2005-51 of 27 June 2005, on electronic transfer of funds.

d) − Organic Law No. 2004-63 of 27 July 2004, on Protection of personaldata (in process

e) − Law No. 2004-05 of 3 February 2004 on computer security.

f) - Law No.2000- 83 of august 2000 on electronic commerce.

- Telecommunication Code promulgated by Law No. 2001-01 of 15January 2001.

- Budapest Convention on Cybercrime (Treaty No. 185) of the Council of Europe which can be considered the international reference framework)

. b) Laws and Codes sui generis:

- Law on the Fight against Cyber Crime.
- Digital Code.

Some Institutional capacity are:-Executive mechanisms:

* National Counter-Terrorism Commission.
* Tunisian Commission of Financial Analysis.
* Ministry of the Interior.
* Fusion Centre for the Fight against Terrorism and Organized Crimes.
* Ministry of Communication Technologies and Digital Economy.
* Technical Agency of Telecommunications.
* National Agency for Computer Security.

ISSN- 2394-5125 VOL 06, ISSUE 01 , 2019

* Tunisian Internet Agency.

* National Digital Certification Agency.

* Ministry for Relation with Constitutional Institution, Civil Society and Human Rights.

*National Instance of Personal Data Protection.

Judicial mechanisms:

Judicial courts:

*Courts of First Instance / the Counter Terrorism Judicial Pole.

* Courts of Appeal.

* Court of Cassation.

Military Justice:

* Permanent Military Tribunal of 1st Instance of Tunis.

* Military Court of Appeal.

Recommendation

Taking into consideration all the efforts undertaken to govern the area of information and communication technology, some more major shortcomings to prevent cyber terrorist acts from occurring and/ or to safeguard citizens and human rights, including those of the presumed terrorists, must be noted here: − The non-compliance of many public structures with the legal and regulatory measures in this area represents a serious threat that can benefit terrorists to penetrate information systems.4 − In the context of open government, there is a lacking framework to adjust the classification ofsensitive data, such as those on critical infrastructures, and the problem of the non- dissemination of data to the new kinds of threats posed by cyber terrorists as presentedin this paper. − The absence of a framework that regulate the use of social media networks by citizens as well as government agencies to track and monitor terrorist organizations or individuals; it must be noted, however, that any regulation can constitute a restriction of the freedom of the Internet represented by access, freedom ofexpressions and information, privacy and data protection.

References

1. Canetti, Daphna; Gross, Michael; Waismel - Manor, Israel; Levanon, Asaf; Cohen, Hagit (2017-02-01). "How Cyber attacks Terrorize: Cortisol and Personal Insecurity Jump in the Wake of Cyber attacks". Cyber psychology, Behavior, and Social Networking. 20 (2): 72–77. doi:10.1089/cyber.2016.0338. Hower, Sara; Uradnik, Kathleen (2011).

3. Cyber terrorism (1st ed.). Santa Barbara, CA: Greenwood. Pp. 140–149.

4. Matusitz, Jonathan (April 2005). "Cyber terrorism:". American Foreign Policy Interests. 2:137–147.

5. Laqueur, Walter; C., Smith; Spector, Michael (2002). Cyber terrorism. Facts on File. pp. 52–53.

6. "India Quarterly : a Journal of International Affairs". 42–43. Indian Council of World Affairs. 1986: 122. The difficulty of defining terrorism has led to the cliche that one man's terrorist is another man's freedom fighter

7. Worth, Robert (June 25, 2016). "Terror on the Internet: The New Arena, The New Challenges". New York Times Book Review: 21. Retrieved 5 December 2016.

8. "What is cyber terrorism? Even experts can't agree". Archived from the original on November 12, 2009. Retrieved 2009-11-05.. Harvard Law Record. Victoria Baranetsky.November 5, 2009.

9. "Latest viruses could mean 'end of world as we know it,' says man who discoveredFlame", The Times of Israel, June 6, 2012

10. "Cyber espionage bug attacking Middle East, but Israel untouched — so far", The Timesof Israel, June 4, 2013

11. Harper, Jim. "There's no such thing as cyber terrorism". RT.