Date: July 5, 2020
To: Mr. Jim Pereira
From: Abhijith Umesh
Subject: Combating cybercrimes and terrorist activities in the world of internet.

Today, internet is an inseparable component of human beings, employed in length and breadth of the world. It is used by infants to old people and makes its presence in tiny devices like handheld mobile phones to huge datacenters. We rely on internet for tasks like buying commodities, performing banking activities, social media and entertainment. The moment we step out of the house, we are the slaves of GPS and many queries are solved at an arm's reach by the use of search engines. Although fantastic, many of these activities are eavesdropped by cybercriminals. They search for patterns to execute an attack. The advancement in the field of internet is also a boon for terrorism.

Further to throw light on the issue, terrorist organizations try to fund their activities by engaging in online criminal activities like credit card fraud. Terrorist purchase airplane tickets, global positioning devices and armor that provide direct tactical support for their operations. In addition, the easy availability of detailed maps of countries from services such as Google Earth aid terrorism activities. The topology of white house and other prominent places like the seven wonders of the world is at one's disposal which can be ingeniously used to sketch a plan. It is to be noted that AL Qaeda commander had planned a precision attack by using a tablet and google maps [1]. Terrorists now have a chance to approach targets that would otherwise be utterly unassailable, such as air traffic control systems and national defense systems by the use of information technology. It can be seen that internet is neither simply a potential vehicle for carrying out attacks nor a potential target, however internet is powerful tool to communicate words, images and sounds over long distances. This makes it easy to grab tools required to carry out an attack from long distances. For example, powerful armory developed in one part of the world is now easily available in other places by means of easy communication channels. All these have led to a new concept of "cyberterrorism" which can be defined as the use of internet to perform disruptive activities and intimidate the civilian population and government [2].

Although cyber-terrorism is spiraling in the world, it remains concealed and hence becomes intractable. This is a boon for cyber-terrorists as they complete missions with no risk of being identified. It takes very minimal efforts for the criminals to exploit a vulnerability once identified. They can hack a defense website or aircraft station to obtain all the necessary information without leaving a trace. Terrorist also use the social media for propaganda purposes. Videos and images can be easily posted in blogs to allure the young. Lone wolves for example are individuals who interact with persons/groups having similar ideologies and express their disgruntlement on social media [5].

Stuxnet, a malicious computer worm, is one of the epitomes of cyber terrorism. Stuxnet functioned by targeting Microsoft windows operating system and compromised programmable logic controllers collecting information on industrial systems causing a system damage thereby

putting the system to vulnerability. National security agency (NSA) is a national level intelligence agency which is tasked with the protection of United states communications networks and information systems. Edward Joseph Snowden was a whistleblower who copied and leaked highly secretive information from the NSA. Though he was charged for violating the government norms, such kind of information leaks can be effectively used by the criminals to chalk out a cyberattack.

Though cybercrime is increasing at a high rate, effective measures can be taken to combat it. Firstly, content blocking can be performed that prevents users from accessing specifically targeted illegal content from servers using the techniques of encryption. Further violence/counter attacks arising in social media must be detected and curbed [4]. Another way to prevent the threat is by discovering certain aberrant characteristics. Additionally, it is possible to employ the techniques of artificial intelligence that enables us to develop autonomous computer systems that are built on the principles of self-tuning, self-management and self-diagnosis [6].

Lastly, I want to say that our company can aim at combating the cyberterrorism. Firstly, software products must be thoroughly tested for cyber-attacks before release. Solutions could also aim at detecting people who tend to influence the society in the social media by uploading videos or writing blog posts about terrorism. Further, we can design products that detect malware and prevent unscrupulous ways of accessing the data from air traffic control systems and national defense systems. Additionally, we can detect the fraud transactions being made and combat it, thereby preventing the terrorists from buying air tickets and other accessories needed to carry out their operation. Also, we can write extensions to google map application which will grab information from users who try to pose security threat to heritage buildings. In addition, we can identify those criminals using the concepts of machine learning that detects a user as a fraud or legitimate based on some of the predefined attributes. Finally, we can use extra caution and experienced system administrators who will restrict access to some of the crucial materials in our organization in the case they notice some activities that deviate from the norm. All these will put a check on cyberterrorism.

Citations

[1] https://www.dailymail.co.uk/news/article-5642361/Al-Qaeda-appears-use-Google-Maps-plan-terrorist-attack-new-propaganda-video.html
[2] James A. Lewis, Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats, December 2002.
[3] Max Kilger, Integrating Human Behavior into the Development of Future Cyberterrorism Scenarios
[4] Borka Jerman, Missing Solutions in the Fight against Cybercrime and Cyberterrorism – the New EU Research Agenda.
[5] Babak Akhgar and Andrew Staniforth, Cyber Crime and Cyber Terrorism Investigator's Handbook, 125
[6] Roumen Trifonov, et al., Artificial Intelligence in Cyber Threats Intelligence.