**Chapter 1: Omar and Carfizz**

**By**

**Natnael Kebede**



**University of Dallas**

**2020**

This Paper Submitted in Partial Fulfillment of the Requirements for

CYBS 7359 – Penetration Testing and Vulnerability Assessment

Spring 2020

Presented to Dr. Renita Murimi

1. How has the World Wide Web enabled terrorism?

The World Wide Web enabled terrorism by being the fastest and best way for America’s enemies to connect and launch an attack against people. Additionally, it provided a safe virtual environment for terrorist groups such as al-Qaeda, its affiliates, and its splinter groups to reach each other easily.

1. In your opinions, who are the two audiences of online terrorism?

In my opinion, the two audiences of online terrorism are potential terrorists and the counter-terrorists who chased them (analysts, researchers, and counterterrorism experts inside or outside intelligence agencies.

1. How easy is it to gather social media information?

It is easier to gather social media information for analysts and researchers outside of intelligence agencies. That is, with terrorists flocking to social media, the experts no longer need classified reporting to be aware of what terrorists were up to.

1. Research: Pastebin

Pastebin was a popular code-sharing site that went live on September 3, 2002. The site allows also allows one to upload and share text online by using a specific URL. Once the text has been uploaded, users are also entitled to edit and share it as well. Pastebin eventually became the place for hackers to hang out. For instance, the Hacker group Lulz Security (LulzSec) once posted a file containing information related to the attacks on the website. It contained information such as people’s names, addresses, dates of birth, phone numbers, and email addresses that were captured (Brian, 2011).

1. In chapter 1, the author created a summary titled “6 Reasons Not to Join Shabaab”. This summary was based on observations of Omar’s online activity, online conversations with Omar and other OSINT techniques. Have you observed parallels online where information is curated by third parties?

I have observed parallels online where third parties curate information. One of those was Radicalisation and al-Shabaab recruitment in Somalia, a study conducted by Anneli Botha and Mahdi Abdile from the Institute for Security Studies organization. The study was based on interviews from former al-Shabaab fighters and details typical al-Shabaab recruits, factors for their recruitment such as religious identity, socioeconomic circumstances (education, unemployment), political circumstances, and the need for a sense of belonging. Furthermore, it identifies their regrets after joining and why they shouldn’t have joined the organization in the first place (Abdile & Botha, 2014).

1. What is the notion of an online gloom period? Do similar gloom periods exist for cybersecurity incidents?

The notion of an online gloom period indicates an interval when someone remains hiding their virtual identity before exposing themselves through actions. The actions, in turn, accomplish the goals they have set before coming out.

In my opinion, similar cybersecurity incidents exist. One example is when an attacker that has been hiding in an organization’s network, collecting information, and analyzing patterns before it executes its actions to cause damage to the victim.

1. Who is an online influencer? What role does an influencer play in online activities?

An online influencer is someone who uses social media to spread information supporting a particular ideology rapidly. An influencer plays a critical role in online activities by creating a behavioral change among their audience (targets) so that that they execute tasks in the way that influencer had planned.

1. How important is cross-domain knowledge in cybersecurity?

Cross-domain knowledge is vital in cybersecurity. This importance is because security operations are interdependent and certainly require a collaborative effort among different security teams. This technique, in turn, allows one to address risks effectively, respond to incidents, and keep sensitive data secure and in compliance with set regulations.

1. What is behavioral economics? What are its applications to cybersecurity?

Behavioral economics refers to a field of study that explains how people behave instead of how they should and make decisions based on emotional, cultural, and social factors.

Behavioral economics can be applied to cybersecurity to understand the human factor better, decision-making process, and motivations. That is, according to Dan Ariely, a professor of psychology and behavioral economics at Duke University, behavioral economics plays a critical role in Cybersecurity by allowing security experts not just to create security but to create appreciation. It asserts that creating security with no appreciation results in people not valuing the security and willing to participate in it (Ariely, 2008). With cybersecurity being a combined effort, I agree with dan in that users' (employees’) buy-in to security controls is vital to accomplish organizational security objectives. This scenario becomes crucial with management and executives as they need to utilize behavioral change to influence employees.

1. How will AI change social media?

AI will change social media in various ways. It can manipulate audiences to follow someone, map users’ thoughts, and provide propagandists with exceptional speed and power to continuously magnify their message.

1. The author states that a solution to the evils of social media can be found in the birthplace of global jihad. Why would this assumption be valid?

The assumption that a solution to the evils of social media can be found in the birthplace of global jihad would be a valid solution. This solution is the case since successful mechanisms for users and countries to survive and thrive in our social media, including utilizing systems for good purposes, requires that influential bad habits (such as the ones exercised by jihad groups) get eradicated from the root one step at a time. This scenario confirms with what the author mentions too. That is, the eradication involves pursuing a social media counterattack against the world’s existing evil social media habits.

References

Abdile, M., & Botha, A. (2014). Radicalisation and al-Shabaab recruitment in Somalia. Retrieved from https://issafrica.s3.amazonaws.com/site/uploads/Paper266.pdf

Ariely, D. (2008). Behavioral Change in Cybersecurity, with Dan Ariely. Retrieved from https://www.marmaladebox.com/podcast/behavioural-change-dan-ariely/

Brian, M. (2011). Pastebin: How a popular code-sharing site became the ultimate hacker hangout. Retrieved from https://thenextweb.com/socialmedia/2011/06/05/pastebin-how-a-popular-code-sharing-site-became-the-ultimate-hacker-hangout/