B15   The Facebook® Faker: Case Study of an Online Romance Scam Turned Dangerously Physical

Richard D. Walter, MA*, 1879 Chenango St, Montrose, PA 18801; and Peter R. Stephenson, PhD*, Norwich Univ, 158 Harmon Dr, Dewey Hall, Rm 221B, Northfield, VT 05663

The goal of this presentation is to provide an example of the use of Cyber-Physical Crime Assessment (CPCA) techniques to characterize a crime, crime scene, and suspect, thus informing the investigation. The presenters will describe the case and apply CPCA to explain its ramifications and how CPCA might be used as an investigative tool to support a digital forensic investigation.

This presentation will impact the forensic science community by suggesting that CPCA may be useful for predicting the point at which a cyber-stalker, cyber-bully, or cyber-harasser may resort to actions and violence in the physical world. The case study supports Jaishankar's space-transition theory in cyber criminology.[1] It represents one type of romance scam where the scammer uses social media to troll for and groom victims before attempting contact in the physical world. This case study is part of the presenters' on-going research into CPCA and its direct applicability to digital forensic investigations.

DK is a 49-year-old male who entraps women and men using Facebook®, arranges meetings with them, and escalates many of those meetings to sexual encounters often with (up to 79%) violent assault. Over his history, DK has engaged with at least 84 victims. Typically, he engaged the victims using a variety of subterfuges. Likewise, he often attempted to develop a real-world relationship at the point where he perceived that he was not achieving adequate control over his victims online.

DK is overweight, indigent (living in shelters when he does not have a victim with whom to live), and expert in the use of the Internet and social media, which he accesses either from a library or using a victim's computer and Internet connection. He is reported by one of his victims to "…sleep no more than four hours per night" spending much of the rest of his time online.

He represents himself on Facebook® as younger, a bodybuilder, extremely wealthy, an ex-FBI agent, and a former private sniper who was paid by the kill. None of these is true. He uses a variety of aliases and is suspected of both identity theft and child abuse. In interviews with his 84 victims, several have indicated that he raped them; however, most women with whom he has been involved did not report him because he was careful to engage initially in consensual sex and, where possible, cohabitate with his victims.

DK represents the Power Reassurance (PR) sub-type and spikes over into the power assertive (PA) sub-type when he can no longer satisfy his need for control of his victim.[2] The PR sub-type is characterized, among other things, by the actor living in a personal fantasy. The fantasy drives his actions. The PA sub-type is characterized by aggressive assertiveness.

In the case of DK, he lives in the fantasy that he is the person he represents himself to be (PR). Then he attempts to engage his victim in *his* fantasy and, when he no longer can control his victim, he exerts more power and his actions become PA. When he no longer can exert control through his online presence, he attempts to move the relationship into the real world, often with violent results.

Analysis of chat logs, a sting operation, video of interviews with DK in the media, his emails, and tracking of his numerous Facebook® presences has allowed the presenters to develop a very clear picture of DK's behavior. Additionally, the presenters have had access to computing devices (including laptops, tablets, and smart phones) that DK used extensively. Applying CPCA to the forensic analysis of these devices allowed the presenters to test the viability of considering the computing device as a crime scene that could be analyzed in much the same way that a crime scene investigator analyzes a physical crime scene.

References:

1. Jaishankar, K. (2008). Space Transition Theory of cyber crimes. In Schmallager, F., & Pittaro, M. (Eds.), *Crimes of The Internet.* (pp.283-301) Upper Saddle River, NJ: Prentice Hall.
2. Stephenson, Peter, Richard Walter, "Cyber Crime Assessment," hicss, pp.5404-5413, 2012 45th Hawaii International Conference on System Sciences, 2012

Facebook®, Crime Assessment, Cyber Crime