Chapter 5.5
Female and Male Hacker Conferences Attendees: Their Autism-Spectrum Quotient (AQ) Scores and Self-Reported Adulthood Experiences

Bernadette H. Schell
University of Ontario Institute of Technology, Canada

June Melnychuk
University of Ontario Institute of Technology, Canada

ABSTRACT

To date, studies on those in the Computer Underground have tended to focus not on aspects of hackers' life experiences but on the skills needed to hack, the differences and similarities between insider and outsider crackers, and the differences in motivation for hacking. Little is known about the personality traits of the White Hat hackers, as compared to the Black Hat hackers. This chapter focuses on hacker conference attendees' self-reported Autism-spectrum Quotient (AQ) predispositions. It also focuses on their self-reports about whether they believe their somewhat odd thinking and behaving patterns—at least as others in the mainstream society view them—help them to be successful in their chosen field of endeavor.

INTRODUCTION

On April 27, 2007, when a spree of Distributed Denial of Service (DDoS) attacks started and soon thereafter crippled the financial and academic websites in Estonia (Kirk, 2007), large businesses and government agencies around the globe became increasingly concerned about the dangers of hack attacks and botnets on vulnerable networks. There has also been a renewed interest in what causes mal-inclined hackers to act the way that

DOI: 10.4018/978-1-61350-323-2.ch5.5

they do—counter to mainstream society's norms and values.

As new cases surface in the media—such as the December, 2007, case of a New Zealand teen named Owen Walker, accused of being the creator of a botnet gang and discovered by the police under Operation Bot Roast--industry and government officials, as well as the public have been pondering about whether such mal-inclined hackers are cognitively and/or behaviorally "different" from adults functioning in mainstream society.

This chapter looks more closely at this notion. The chapter begins with a brief discussion on botnets to clarify why the growing concern, reviews the literature on what is known about hackers—their thinking and behaving predispositions—and closes by presenting new empirical findings on hacker conference attendees regarding their self-reported Asperger syndrome predispositions. The latter are thought to provide a constellation of rather odd traits attributed by the media and mainstream society to males and females inhabiting the Computer Underground (CU).

CONCERNS OVER BOTNETS AND VIRUSES AND THEIR DEVELOPERS

A "bot," short form for robot, is a remote-controlled software program acting as an agent for a user (Schell & Martin, 2006). The reason that botnets are anxiety-producing to organizations and governments is that mal-inclined bots can download malicious binary code intended to compromise the host machine by turning it into a "zombie." A collection of zombies is called a "botnet.'

Since 2002, botnets have become a growing problem. While they have been used for phishing and spam, the present-day threat is that if several botnets form a gang, they could threaten—if not cripple--the networked critical infrastructures of most countries with a series of coordinated Distributed Denial of Service (DDoS) attacks (Sockel & Falk, 2009).

The Case of Bot Writer Owen Walker

It is understandable, then, why there has been considerable media interest in Owen Walker, who, according to his mother, suffers from a mild form of autism known as Asperger syndrome—often indicated in individuals by social isolation and high intelligence. Because of a lack of understanding about the somewhat peculiar behaviors exhibited by high-functioning Asperger individuals, Walker's peers allegedly taunted him during the formative and adolescent years, causing him to drop out of high school in grade 9. Unbeknownst to Walker's mother, after his departure from high school, Owen apparently became involved in an international hacking group known as "the A-Team" (Farrell, 2007).

In a hearing held on July 15, 2008, Justice Judith Potter discharged Owen Walker without conviction on some of the most sophisticated botnet cybercrime seen in New Zealand, even though he pleaded guilty to six charges, including: (i) accessing a computer for dishonest purposes, (ii) damaging or interfering with a computer system, (iii) possessing software for committing crime, and (iv) accessing a computer system without authorization. Part of a ring of 21 mal-inclined hackers, Walkers' exploits apparently cost the local economy around $20.4 million in US dollars. If convicted, the teen could have spent up to seven years in prison.

In his defense, Owen Walker said that he was motivated not by maliciousness but by his intense interest in computers and his need to stretch their capabilities. In her decision, Justice Potter referred to an affidavit from Walker in which he told her that he had received approaches about employment from large overseas companies and the New Zealand police because of his "special" hacker knowledge and talents. The national manager of New Zealand's police e-crime laboratory was quoted in the media as admitting that Walker had some unique ability, given that he appeared to be at the "elite" level of hacking (Gleeson, 2008).