Chapter 1.12
Deciphering the Hacker Underground:
First Quantitative Insights

Michael Bachmann
Texas Christian University, USA

ABSTRACT

The increasing dependence of modern societies, industries, and individuals on information technology and computer networks renders them ever more vulnerable to attacks on critical IT infrastructures. While the societal threat posed by malicious hackers and other types of cyber criminals has been growing significantly in the last decade, mainstream criminology has only recently begun to realize the significance of this threat. Cyber criminology is slowly emerging as a subfield of criminological study and has yet to overcome many of the problems other areas of criminological research have already mastered. Aside from substantial methodological and theoretical problems, cyber criminology currently also suffers from the scarcity of available data. As a result, scientific answers to crucial questions remain. Questions like: Who exactly are these network attackers? Why do they engage in malicious hacking activities? This chapter begins to fill this gap in the literature by examining survey data about malicious hackers, their involvement in hacking, their motivations to hack, and their hacking careers. The data for this study was collected during a large hacking convention in Washington, D.C, in February 2008. The study findings suggest that a significant motivational shift takes place over the trajectory of hackers' careers, and that the creation of more effective countermeasures requires adjustments to our current understanding of who hackers are and why they hack.

DOI: 10.4018/978-1-61350-323-2.ch1.12

INTRODUCTION

Deciphering the Hacker Underground: First Quantitative Insights

The recent attacks on Estonia's computer and network infrastructures were an event of such unprecedented magnitude that it sent shockwaves throughout the world. In April, 2007, pro-Russian hackers launched a month-long retaliation campaign for the removal of a World War II statue—a campaign that has become known as the first war in cyberspace. Using a technique known as Distributed Denial-of-Service (DDoS) attacks on a hitherto-unprecedented scale, the attackers managed to effectively shut down vital parts of Estonia's digital infrastructures. In a coordinated effort, an estimated one million remote-controlled computers from 178 countries were used to bombard with requests the Web sites of the president, the prime minister, Parliament and other government agencies, Estonia's biggest bank, and several national newspapers (Landler & Markoff, 2007). Members of the Kremlin-backed youth movement 'Nashe' later claimed responsibility for the attacks, which they described as an 'adequate response' intended to 'teach the Estonian regime a lesson' (Clover, 2009). The group of young Russians also emphasized that they acted on their own initiative, not on government orders.

While the description as the first cyber war remains controversial because nobody died or was wounded, the events in Estonia, nevertheless, demonstrate the devastating consequences of Internet-borne attacks. In reference to the events in Estonia, Suleyman Anil, the head of NATO's incident response center, later warned attendees of the 2008 E-Crime Congress in London that "cyber defense is now mentioned at the highest level along with missile defense and energy security." According to Anil, "we have seen more of these attacks and we don't think this problem will disappear soon. Unless globally supported measures are taken, it can become a global problem" (Johnson, 2008, p. 1).

Today, the Internet has developed into a mission-critical entity for almost all parts of modern societies. Although warnings of the societal threat posed by cyber attacks on critical network infrastructures have been heralded since the 1980s, it is only in recent years that the problem has made it onto the radar of governments. Partly due to the experiences of Estonia and later in the conflict between Russia and Georgia, countries around the globe are now reassessing the security situation of their key information systems. They are enacting new security measures to better protect their critical network infrastructures, and they are increasing their readiness to respond to large-scale computer incidents (NCIRC, 2008). In the United States, security experts went as far as to warn against an 'electronic Pearl Harbor,' a 'digital September 11,' or a 'cybergeddon' (Stohl, 2006).

The implementation of effective countermeasures against hacking attacks is facilitated by the vast amount of knowledge already accumulated in numerous computer science research projects (cf. Chirillo, 2001; Curran, Morrisey, Fagan, Murphy, O'Donnell, & Firzpatrick, 2005; Erickson, 2008). Several studies conducted by computer scientists and computer engineers have closely examined the technical details of the various attack methods and have produced a significant body of information that can now be applied to help protect network infrastructures (Casey, 2004). Unfortunately, the guidance provided by these studies is limited to only the technical aspects of hacking attacks and, sharply contrasting from the substantial amount of knowledge already gathered about how the attacks are performed, answers to the questions of who the attackers are and why they engage in malicious hacking activities continue to remain largely speculative. Today, the persons committing the attacks remain mysterious, for the most part, and scientific information about them continues to be only fragmentary.