Chapter 13
Cybercrimes Technologies and Approaches

WeSam Musa
University of Maryland – University College, USA

ABSTRACT

The growth of the Internet has changed our lives significantly. Not so long ago, computers used to be viewed as luxury items to have at home. People used to rely mainly on televisions and newspapers as the primary sources of news. Today, the Internet has become an essential service to depend on for many industries, such as news agencies, airports, and even utility companies. This was the beginning of a new-trillion-dollar industry: the Internet industry. However, the Internet was designed to be an open, academic tool, never to be secure. As a result, cybercrimes, cyber warfare, and other cyber illegal activities have spread to become a significant portion of Internet traffic. Cybercrimes often challenge law enforcement. It is difficult to know the exact location where an attack originated, and there are no cyber borders between nations. As a result, fighting cybercrimes requires international cooperation. The purpose of this chapter is to shed some light on motives of cybercrimes, technologies used by hackers, and solutions that can be adopted by individuals, organizations, and governments. This chapter also presents the United States (USA) and international perspectives on cybercrimes and privacy laws. In summary, individuals, organizations, and nations have roles to play in achieving security and reducing cyber risks.

INTRODUCTION

In the early 1980s, when the Advanced Research Projects Agency Network (ARPANET) developed the Transport Control Protocol/Internet Protocol (TCP/IP), the world became connected through the Internet. Nowadays, the Internet has a profound impact on society. Social interactions, economies, and fundamental life simply depend on cyberspace. The Internet, and more broadly cyberspace, has allowed social interaction worldwide. It has allowed sharing of information and freedom of expression – such as what occurred during the Arab Spring. Social media services, such as Twitter and Facebook played an instrumental role in the Arab Spring movements. While the cyber world brings economical and social benefits, it is also vulnerable. The Internet was never designed to be secure. Identity theft, cybercrimes, cyber warfare, and others cyber illegal activities started surfacing due to lack of appropriate security controls. According to Symantec's annual security report, the

DOI: 10.4018/978-1-4666-6324-4.ch013

numbers of cyber-targeted-attacks are increasing. Cyber attacks target everyone including small companies, large companies, government agencies, executives, and even sales people (Symantec, 2012). The global economy is being affected by cybercrime activities.

Cybercriminals are using sophisticated methods to gain unauthorized access to information systems to steal sensitive data, Personality Identifiable Information (PII), or even classified materials. Some of the creative methods that attackers use to gain unauthorized access are backdoor programs, spear phishing attacks, and social engineering. Tini, Netcat, Wrappers, EXE maker, Pretator, Restorator, and Tetris are well-known backdoor tools that can be used by attackers to setup a backdoor that allows them to connect into the computer systems. Phishing is a technique that attackers use by sending email messages with false links claiming to be a legitimate site in an attempt to acquire users' personal information. Social engineering is a powerful human-based technique that bypasses all network countermeasures by relying on human weakness to gain unauthorized access to the network. The technique targets certain personal, such as helpdesk, or executives by creating an artificial situation by exerting pressure to release the needed information.

Countries may misuse cyberspace for spying on other nations. For example, U.S. National Security Agency (NSA) is being accused for spying on world leaders and listening to 100s of millions of phone conversations worldwide. Additionally, cybersecurity incidents could disrupt water resources, power plants, healthcare, or financial institutions. A study conducted by McGraw (2013) concluded that the U.S IT infrastructure is highly vulnerable to deliberate attacks with possibly disastrous effects. The current cybersecurity technical approaches for many nations do not provide adequate computer or network security. With no surprise, President Obama has declared that, "cyber threat is one of the most serious economic and national security challenges we face as a nation" (Obama, 2012). Similarly, in 2013, in order to fight cybercrimes, the European Commission established the European Cybercrime Centre (EC3) at the European police headquarters in the Netherlands.

For the above stated reasons, governments across the world have started to collaborate by developing cybersecurity strategies. The European Union (EU) has created a cybersecurity strategy that consists of seven pillars. These pillars focus on using cyberspace to befit economically, socially, and even politically. Furthermore, the EU has put forward a framework to set the actions required to build a strong and effective countermeasures against cyber threats. In May 2013, the European Union Agency for Network and Information Security received a new authority, granting it the power to make bigger difference in protecting Europe's cyberspace. Furthermore, the U.S. has passed an executive order in 2013 to develop cybersecurity performance standards to reduce cyber risks to critical infrastructure. In addition, the United Nations Economic and Social Council (ECOSOC) has initiated an international treaty seeking to bring into line national criminal laws of cybercrimes, such as fraud, child pornography, and hate crimes.

The objective of this chapter is to provide an overview of the historical background, and trend of cybercrimes technologies and approaches. This chapter will also discuss relationship between the U.S. and global Internet operations in terms of international collaboration efforts to fight cybercrime activities. The chapter will also cover broader implications for relationships between civil liberties, innovation, and security.

MOTIVES OF CYBERCRIMINALS

Cybercrime by definition is committing an illegal act using a computer or network device (Musa, 2013). Cyber warfare, cybercrime, cyber espionage, and cyber terrorism are all similar activities,