Chapter 10
Fighting Cybercrime and Protecting Privacy:
DDoS, Spy Software, and Online Attacks

Javier Valls-Prieto
University of Granada, Spain

ABSTRACT

This chapter is about the use of large-scale databases that has increased considerably in the last two years. It is a powerful tool to predict future situations that may affect society. The use of an environmental scanner to fight cybercrime—as an organized crime—is the project for using this technique of large-scale databases to try to guarantee the security against the risk of new, developing forms of criminal activities. On the other hand, the use of large-scale databases utilizes a great amount of personal data to try to predict where and how organized crime or new forms of criminality will develop. This means that we have to evaluate the interests of security of society and the privacy of the person, and we have to find the way to balance both in a democratic society. There are important ethical issues to be considered in the employment of this new and unregulated instrument.

INTRODUCTION

Cybercrime, as a part of organized crime, is considered one of the most serious potential risks in twenty-first century society. Crimes such as cyber espionage, system attacks, child pornography, on-line fraud and extortion are a reality and may become worse. The World Economic Forum takes cyber attacks as having the most impact and the most considerable risk in the global area (WEF, 2013). And this risk is not only for private users but for governments and societies throughout the world. The problem found in cybercrime is that criminals can hide just waiting to attack, and moreover addition victims do not want to report the case in order not to amplify the issue. Many problems arise when considering how to fight this kind of criminality. One of them is the invisibility of the act. It remains confined to the net and only the perpetrator and the victim know about it. If the victim does not report anything to the police it is impossible to know that it has happened. But where the victim is a public institution the risks are so high for society that they cannot be allowed

DOI: 10.4018/978-1-4666-6324-4.ch010

to happen. Therefore, prevention is the only way to fight them. And that is exactly the idea behind the use of the Environmental Scanning. The use of robots to detect cybercrime is an effective tool because they work in the same environment, have the possibility of finding evidence and can predict future attacks.

To achieve these goals robots need to use large-scale databases with large quantities of personal information. But this poses a serious risk in using them in the fight against organized crime, and in particular, because of the conflict between the use of personal data and respect for human rights. Online criminal investigations are needed in the twenty-first century. As we have seen with the NSA investigations, the development of these robots is already a reality. A world with these cyber risks cannot be a democracy and a world without privacy, which also affects the right of freedom of speech, cannot be a democracy. Both are indispensable to live in a democratic society.

How to balance both is exactly the question that this paper seeks to solve. As it is a global problem both the EU legislation and projects on the protection of privacy and control of state investigations are going to be analysed. To this end, we are going to see from a criminological point of view how botnets work and how the European Union Law on the processing of personal data could control the use of big data on criminal investigations.

HOW THE BOTNETS WORK AND DESCRIPTION OF A FEW CYBERCRIME TYPES

Cybercrime has become an important topic for the police and security services. As has been pointed out by Clough the "rapid technological development continues, and will continue, to present new challenges" (Clough, 2012) and crime is not apart of these changes. According to Moore cybercrime covers plenty of crimes as intellectual property theft, child pornography, financial fraud, online harassment, identity theft, etc. (Moore, 2011) but some of them are only an online action with no a big difference to the offline world. That is why we are going to focus our work on the cybercrimes that all the process is online and has nearly nothing to do with the offline crime.

The three kinds of crimes that we are going to study (denying system attack, spy software and infrastructure online attacks) have points in common. Basically, the three of them involve the introduction of a malware in a computer that could be either the final-computer or a third part computer, from where the attack comes out but controlled by the botmaster.

Trying to explain the modus operandi is really complicated because it changes according to regions, groups of criminals and technology. Anyway, it is possible to identify some common points.

As we have said, these kinds of cyber attacks have to control computers to produce the result. The criminals use a botnet. 'Botnets' (a term derived from the words 'robot' and 'network') consist of a network of interconnected, remote-controlled computers generally infected with malicious software that turn the infected systems into so-called 'bots', 'robots', or 'zombies'. The legitimate owners of such systems may often be unaware of the fact of infection. Zombies within the botnet connect to computers controlled by perpetrators (known as 'command and control servers' or C&Cs), or to other zombies in order to receive instructions, download additional software, and transmit back information harvested from the infected system (UNODC, Comprehensive Study on Cybercrime, 2013).

Once the botnet is in the computer the hackers can control it. The classical way was to use the IRC chat system, but recently more sophisticated structures are being used (by working on TCP, UDP and ICMP protocols) (INFOSEC Institute, 2013). The first generation botnet was based on Command & Control Server (C&C) but it was quite easy to control by just shutting off the