The Spy Who Never Has to Go Out Into the Cold
Cyber Espionage

Laura Pinto Hansen
Western New England University, USA

INTRODUCTION

Cyber espionage is a fairly recent newcomer to means by which to steal trade secrets, classified government information, or consumer information. However, with the rise of the digital age beginning in the late 1950s, increasingly more documents are stored on mainframe and individual computers than compared to storage in conventional file cabinets. In fact, it is very unlikely that many institution store files these days on physical shelves, save older archives. Even then, the art of archiving reached the digital age some time ago. This has been exponentially so since the beginning of the Big Data age of the 21st century. In this chapter, we explore the types of cyber espionage, recent cases, as well as challenges to detecting, controlling cyber thievery and mayhem.

It is because of the vast amounts of data that are stored more efficiently on computers and in cyberspace, that these became the new frontiers for spies. Banks (2017, p 513) observes that "it seems that everyone is eavesdropping on everyone else…." Gone is the heyday of trench coat wearing spies wielding mini spy cameras in corporate headquarters, the stuff of Hollywood movies. Dark alley, middle of the night transactions, passing microfiche, audio tapes or video, or files, became increasingly unnecessary with the ease and speed of computer technologies.

A circular tautology exists: Technology has always created new advances in warfare (Roberts, 2017) and new advances are created during times of war, including in those conducted in cyberspace. Even art imitates life, with movies depicting elaborate fictional cybercrimes that are not so far-fetched. A handful are even based on true cases, as in the 2013 movie, *The Fifth Estate* (DreamWorks), depicting the infancy of the website, WikiLeaks.

Spying is considered business as usual in international relations, though nations publicly deny that they are involved in espionage. State-sponsored surveillance is common place and considered to be a necessary evil in order to maintain world order and promote national security. This challenges the principles of democracy and privacy. State-sponsored surveillance has its critics (Schmitt and Vihul, 2017). Comparisons have been made to George Orwell's 1948 novel, *1984*, where Big Brother is always watching: "If you want to keep a secret, you must also hide it from yourself." (Orwell, 2017, p 283)

On the other side of the argument, surveillance is argued to be a necessity in order to detect cyber attacks (Nissenbaum, 2005). The consequences of cyber intrusions by perceived hostile nations or "frenemies" (nations who are friendly for purposes of trade relations, but secretly economically and militarily compete with) are far reaching. As much as state-sponsored surveillance of governments is

DOI: 10.4018/978-1-5225-9715-5.ch017

commonplace, surveillance and cyber espionage are more likely to have an effect on the average citizen, much like other forms of white-collar crime, as compared to conventional crime. In many respects, there is far greater financial and political damage to be done in this day and age, because of the alarming amounts of sensitive information that is stored digitally.

More recent attention has been given to the ability to plant false information through the Internet, in order to engage in propaganda designed to confuse or divide nations' citizens. There is also the greater concern that whole cyber infrastructures could come tumbling down, with the ability of cyber spies or amateur hackers to infiltrate systems for purposes of sabotage, including energy and transportation.

DEFINING CYBER ESPIONAGE

As Randall Dipert (2013) argues, the terms "cyber attack" and to some extent, "cyber espionage" are loosely interchangeable, used to cover a wide range of cybercrimes. We should be clear that cyber espionage is more commonly thought to be limited to the theft of military or government secrets. A subset of cyber espionage is economic espionage, sometimes called industrial espionage, where governments attempt to gain information from foreign companies (Banks, 2017). A cyber attack or cyber warfare, on the other hand, implies that the act is for the purposes of bringing down whole systems, as in the example of viruses transmitted by bogus links imbedded in spam email.

One common means by which to obtain information from individuals is phishing. It is not restricted to attempts to gain personal financial information from employees. In recent decades, the use of company email exchanges has commonly been used to gain access to intellectual property and industry secrets. These are not easily detected schemes, as compared to the notorious Nigerian email scams. Increasingly the emails appear to be generated from legitimate sources, addressing employees by name within an organization, rather than the generic "Dear Sir or Madam". Sometimes initiated on the Dark Web, it is an effective way to gather information without hacking into sophisticated computer systems that might be heavily protected by more sophisticated cybersecurity systems. And because many are distributed through the Dark Web, the origins of the emails are difficult to detect. The Dark Web allows users to mask not only their identities, but their location.

Cyber espionage is not always limited to the theft of intellectual property. Espionage can also involve subterfuge where false or misleading information is planted. The most common current means by which to do so is through social media, including Facebook, Twitter, Instagram, and YouTube. Though these social media platforms have battled regulatory agencies to offer open access with few limitations, increasingly they have been asked to take a more active role in preventing foreign agents, acting as internet trolls, from agitating users, particularly during election cycles.

An additional form of cyber espionage is the use of malware for intelligence gathering and sabotage. These might not be isolated incidents, but rather can be ongoing campaigns by their designer, attacks presenting themselves within an advanced persistent threat (APT) (Wangen, 2015). Malware can come in a number of different forms, including temporary nuisances, as in the case of "bugs" or having far more devastating result, as in the example of a "Trojan horse". More commonly in cyber espionage, the use of spyware allows for information to be collected from individual computers, including keystrokes to obtain passwords or gather information about use. The lesser known, but in many respects, deadlier "rootkit", allows the user to evade detection and has the ability to alter software, including security systems.