Chapter 5
Teaching New Dogs Old Tricks:
The Basics of Espionage Transcend Time

Neal Duckworth
American Military University, USA

Eugenie de Silva
University of Leicester, UK

ABSTRACT

This chapter discusses how the basics of espionage have remained the same, even in the digital age. The pendulum of espionage--and protection from it--has swung wide over the past century. Different public and private sectors have renewed focus on not only cyber protections, but on increased physical protection of critical assets and ensuring trusted personnel in the workforce. Within this chapter, the authors review the basics of protecting critical assets to ensure that changes in espionage can be mitigated at an early stage. While the techniques of espionage have many variables, especially in a digital age, the authors have established that the use of a risk assessment that focuses on identifying the threats, the specific variables or methods of espionage, and developing and implementing mitigation measures is of the utmost importance.

DOI: 10.4018/978-1-4666-9661-7.ch005

INTRODUCTION

To look to the past for answers to the questions of the present and the future could be deemed an entirely idealistic notion. However, it is this analysis of the past that can lead to the discovery of beneficial tactics and strategies to protect critical assets from theft, compromise, or destruction. There is no question that the art of espionage has changed since the stealing of secrets began, but one basic premise has remained consistent throughout global conflicts, the Cold War, and now in the digital age: the secrets that were stolen, compromised, destroyed, or disclosed were not properly safeguarded. Consider a few well-known personalities: the Federal Bureau of Investigation Special Agent Robert Hanssen, U.S. Army Private Bradley Manning, and National Security Agency Contractor Edward Snowden. Scholars of national security issues recognize these names as those persons responsible for overwhelming losses of classified information and damaging U.S. national security and diplomatic relationships. However, what about Boeing engineer Dongfan "Greg" Chung and Mo Hailong? Chung worked for 30 years for Boeing and passed trade secrets back to China on military planes and capabilities; he was convicted "of six counts of economic espionage and other federal charges for storing 300,000 pages of sensitive papers in his Southern California home" (Flaccus, 2010). Hailong was allegedly conspiring to steal trade secrets from U.S. organizations; and Hailong's case even led the U.S. attorney for the Southern District of Iowa to state that, "[t]he information that was stolen in this case has an estimated value of five to eight years' worth of research time […] [a]nd a minimum of $30 to $40 million" (Martin, 2014). Along these lines, it is imperative to recognize that not all cases of espionage involve the Intelligence Community (IC); other cases of espionage may focus on economic information, intellectual property, and other ways to increase a competitor's advantage.

Today's international media often reports the loss of information as a result of cyber-crimes and cyber espionage, with the "usual suspects" being unknown computer hackers or possibly an organized effort being orchestrated by a foreign nation. According to one report, it is even common for allies to suspect one another of economic espionage, which further exemplifies that "countries can be partners in traditional security matters yet competitors in business and trade" (Office of National Counterintelligence Executive, 2011). However, the traditional threat of espionage, which utilizes trusted employees to steal secrets, has not been eliminated with the expansion of cyber-crimes and cyber espionage. As public and private organizations respond to the expanded cyber threats, the most likely shift in tactics will be to return to the traditional method of coercing an organizational employee to gain access to facilities and information. It is important for organizations that invest so heavily on the prevention of cyber-crime and cyber espionage to not lose focus on mitigating the basic threats and vulnerabilities that could result in political, economic, and possibly even social havoc.

In the U.S. government, the identification and elimination of these threats is the responsibility of both counterintelligence and security officers. Counterintelligence serves as a more active approach that utilizes investigations, operations, collection, and analyses to both identify the foreign intelligence threat from outside and the possible corrupted trusted employees or insider threat(s). Security officers possess a much more agnostic approach to protection, and utilize an integrated protection plan which includes personnel, physical, information, and other types of security; it is often less important who or where the specific threat is from, whether it is a foreign intelligence service or a criminal.

While counterintelligence is primarily thought of as means to identify, neutralize, and exploit foreign intelligence organizations, such a strict interpretation leaves gaps based on different threats. State and