Industrial Espionage (5):
Agents

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In the preceding four articles in this series, I have reviewed methods of industrial espionage and surveys about the dimensions of the problem. Today I look at information about who is attacking us from the National Counterintelligence Center (NACIC) which later became the Office of the National Counterintelligence Executive (ONCIX). As I mentioned in my first article, these agencies have been reporting annually to Congress since 1995 about foreign economic collection and industrial espionage. Their reports are freely available as PDF files from <http://tinyurl.com/cu34l>.

* * *

Early reports from NACIC/ONCIX blanked out the names of countries suspected or known to be engaging in foreign industrial espionage against the USA; however, later editions began publishing lists. The countries mentioned in early reports were Algeria, Armenia, Azerbaijan, Belarus, China, Cuba, Georgia, India, Iran, Iraq, Israel, Kazakhstan, Kyrgyzstan, Libya, Moldova, Pakistan, Russia, Syria, Taiwan, Turkmenistan, Ukraine, and Uzbekistan.

In the 2000 Annual Report, respondents to the NACIC survey of a few (about a dozen) Fortune 500 companies reported that the top countries involved in industrial espionage cases involving their firms were (in order of importance) China, Japan, Israel, France, Korea, Taiwan, and India.

By 2002, the ONCIX Annual Report commented, “The laundry list of countries seeking US technologies in 2001 was long and diverse. Some 75 countries were involved in one or more suspicious incidents. The most active countries in economic espionage, according to DSS data, were an interesting mix of rich and poor and “friend” and foe. Many of the richest nations aggressively sought the latest in advanced technologies both to upgrade their already formidable military infrastructures—particularly command, control, and communications—and to make their already sophisticated industries even more competitive with the United States. Most of the poorer countries, however, continued to exhibit a preference for older ‘off the shelf’ hardware and software to renovate their existing defensive systems and to develop countermeasures to provide them battlefield advantage. The search for lower technology goods by these less developed countries probably reflected their desire to bring in technologies that could be more easily integrated into their existing military structures; a number of these countries were probably not capable of utilizing the most sophisticated US technologies.”

The 2003 ONCIX report stated, “Foreigners from almost 90 countries attempted to acquire sensitive technologies from the United States in 2003, according to data compiled from across the [counterintelligence community], about the same number as in 2002.” That report also explained, “While foreign government officials were behind some of the incidents, they by no means accounted for the majority of collection attempts. For example, Defense Security Service (DSS) data show that [bullets added]
only about 15 percent of suspicious efforts to illegally acquire sensitive US military-related technology in 2003 directly involved foreign governments. Another 25 percent came from government-affiliated organizations or foreign companies that work solely or predominantly for foreign governments, according to DSS statistics. The remainder came from individuals (14 percent) claiming to be working for themselves and from company representatives (31 percent); in 15 percent of cases, there was no indication of affiliation.”

According to the latest ONCIX report available (2004), “Individuals from both the private and public sectors in almost 100 countries attempted to illegally acquire US technologies in FY2004, roughly the same number of countries as [in 2003]…. However, the report indicates a possible growth in government-sponsored industrial espionage: “foreign state actors accounted for about one-fifth of suspicious incidents and government-related organizations accounted for another 15 percent.” However, “Commercial organizations and private individuals with no known affiliation to foreign governments together accounted for nearly half—36 percent and 12 per cent respectively—of all suspicious incidents. In another 16 percent, the contractors were unable to determine the affiliation of the foreign parties involved in the elicitation.”

In summary, the enormous investment in US intellectual property has been a prime target for nations and firms eager to find shortcuts in the research and development process and thus to reduce their costs by stealing our information. In the next couple of articles, I look at some specific cases to illustrate the problem more vividly than by dry survey results.

* * *


M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2005 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.