Intelligence Threat Handbook

Operations Security Information Series

The **Interagency OPSEC Support Staff (IOSS)** was created to support the National OPSEC Program by providing tailored training, assisting in program development, producing multimedia products and presenting conferences for the defense, security, intelligence, research and development, acquisition and public safety communities. Its mission is to help government organizations develop their own, self-sufficient OPSEC programs in order to protect U.S. programs and activities.

Our **Vision** is secure and effective operations for all National Security Mission activities.

Our **Mission** is to promote and maintain OPSEC principles worldwide by assisting our customers in establishing OPSEC programs, providing OPSEC training and conducting OPSEC surveys.

Our **Goal** is to be recognized as the leader and preferred provider of value-added OPSEC products and services.

PURPLE DRAGON:

In the early days of the Vietnam War, the U.S. lost an alarming number of pilots and aircraft. To reverse that trend, a team was assigned to analyze U.S. military operations. The team, "Purple Dragon," discovered that crucial planning information was being disclosed through routine patterns of behavior. Countermeasures were quickly initiated. Purple Dragon's analytic process, called **OPerations SECurity or OPSEC**, was used by the military for the next 20 years. In 1988, President Reagan formalized its use throughout the government and created the IOSS to provide training and guidance to the national security community.

The Intelligence Threat Handbook was researched, written and designed for IOSS by the Centre for Counterintelligence and Security Studies, cicentre.com.

Table of Contents

(U) Overview

(U) The purpose of this handbook is to provide unclassified threat reference information for Operations Security (OPSEC) personnel and managers. This handbook explains the categories of intelligence threat, provides an overview of worldwide threats in each category, and identifies available additional resources for obtaining threat information and outside assistance. The information presented has been drawn entirely from open-source reference material and, therefore, may be disseminated to the largest possible audience in order to increase the awareness of intelligence threats targeting U.S. government and industry.

(U) OPSEC is a set of procedures and methodologies that provides a way for program, project, or facility managers to implement cost-effective measures to protect their programs and staff from exploitation by adversaries. The key to effective OPSEC is to determine both what critical information most needs to be protected and how a potential adversary would most likely attempt to exploit weaknesses to obtain that information. An organization's OPSEC officer must understand the range of threats that confront the organization. Although many categories of threat that may be considered, most OPSEC activities focus initially on the intelligence collection threat.[1]

(U) While U.S. organizations and their staff are the targets of a large number of intelligence collectors worldwide, the specific collection methodologies deployed against U.S. targets are limited. Moreover, intelligence methodologies tend to change only slowly and are intended to be used against many targets. The starting point for the OPSEC manager is to become familiar with the intelligence procedures and methodologies used by adversaries, to determine how an intelligence attack on his facility would most likely be carried out. In the wake of the 11 September 2001 terrorist attack on the United States, attention to intelligence procedures and methodologies has

become even more critical, because experience indicates that every successful terrorist attack has been preceded by at least one successful intelligence attack to gather information about the intended target.

Every successful terrorist attack has been preceded by at least one successful intelligence attack to gather information about the intended target.

(U) This handbook will provide OPSEC officers with information on how intelligence collection programs most often target and collect against individuals and institutions of interest. To simplify study of the different ways in which U.S. critical information is targeted by foreign collection programs, this handbook focuses on the collection mechanisms, strategies, and capabilities of the Russian Federation and the People's Republic of China. Although often targeting the same information, Russia and China approach their collection operations from very different intelligence perspectives.[2] This complicates the OPSEC process of determining threat, risk, and effective countermeasures.

(U) More details on specific intelligence organizations of other U.S. intelligence adversaries are included in Appendix A. Information about available U.S. Government resources is provided in Appendix B.

(U) Nature of the Threat

(U) Intelligence threat, as it applies to OPSEC, is defined as the intention and capability of any adversary to acquire and exploit critical information. The purpose of the acquisition is to gain a competitive edge or diminish the success of a particular U.S. program, operation, or industrial activity.[3]

(U) Changing Nature of the OPSEC Challenge

(U) While the end of the Cold War caused a dramatic drop in the military threat to U.S. security interests, it also gave rise to a significant increase in the OPSEC threat. Although there has been an easing of political and military tensions since the collapse of Soviet-style communism, there has not been a corresponding reduction in the level of espionage and other activities threatening the United States. In fact, foreign intelligence activities have grown in diversity and complexity over the last several years. OPSEC must become more diverse in order to confront the evolving threat environment. That environment now also includes a large number of terrorist organizations.

(U) Changing Nature of the Intelligence Environment

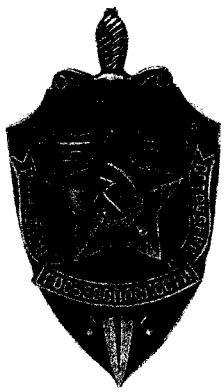
(U) *More Exchange Programs*

(U) A natural byproduct of less antagonistic relations with former military adversaries has been an increase in exchange programs. Because of this, U.S. facilities have been flooded with large numbers of foreign students, research scholars, and commercial delegations. Such exchanges, in turn, create increased opportunities for knowl-

edgeable staff members of U.S. facilities to travel overseas on reciprocal visits—far from U.S. security and counterintelligence capabilities.

(U) Several other factors have combined to create significant changes in the overall OPSEC environment. Now, in addition to individual-country threats, there are transnational groups, such as terrorists, organized criminals, and economic competitors that engage in traditional intelligence collection activities.[4] This has been made possible by the fall of the Soviet Union, an event which threw many professional intelligence officers out of work, with little but their intelligence skills to fall back on.

(U) *A KGB Intelligence Training Connection*



(U) With the emergence of many newly independent states in Africa and Asia in the 1960s, the KGB founded the Foreign Intelligence Training Center in Moscow to provide special courses for the intelligence services of the new countries. This training was of a lesser quality than that provided to Soviet intelligence personnel or intelligence officers from former Bloc countries.[5]

(U) The fall of communism turned the training situation topsy-turvy. There now was very little demand for large-scale specialized training for former Soviet citizens, and no such interest at all from the Bloc. Intelligence instructors became more available for third-world students, and the those nations in turn became more interested in the training, since it no longer came with a strong dose of communist indoctrination and potential Soviet political interference. The KGB Training Center quickly evolved into a commercial entity.[6]

(U) One current Training Center intelligence professor put it this way to a former colleague:

> (U) *"Now we are after money, not ideology. In 1991, of course, if a foreign entity like the Cali Cartel openly asked us to train their personnel, we would refuse. If, however, the Cartel was smart enough to use a cover such as calling themselves personnel security officers from a Colombian or international bank, then we didn't mind training them. After all, in 1991, the government destroyed our jobs and threw us on the streets. We have to take care of ourselves. International crime is not our problem; for us, the name of the game is survival."*[7]

(U) Russian intelligence professors are available on a pay-as-you-go basis to teach the following courses to all who are interested: international security threats; agent networks; recruitment strategy and tactics; agent handling; countersurveillance theory and practice; signals intelligence and eavesdropping operations; and counterintelligence strategy, tactics, and practices.[8]

(U) *More Joint Ventures*

(U) In the United States, many facilities formerly dependent on defense contracts have found themselves in search of continued sources of funding. They have commonly responded to this challenge by instituting commercial joint ventures with private concerns. This has increased opportunities for information to flow outward and created direct economic incentives for sharing as much information as possible. The realities of joint-venture economics opens a de facto official umbrella for establishing and nurturing close relationships with those potential collectors of intelligence who also have a commercial dimension. In some cases, the same resources that were formerly dedicated to defense technical research and production are now designated for joint-venture technical commercial projects with entities representing former U.S. military adversaries.

(U) *The Internet*

(U) The current information explosion via computers and the Internet has also changed the OPSEC environment. Computers are constantly growing faster and more powerful while becoming smaller. In the past, just locating a possible source of desired information was a considerable stumbling block in the path of U.S. intelligence adversaries. With rise of the Internet and vast increases in data-storage capabilities, this is no longer the case. Many American businesses, including the military, use computers to communicate and store most information. Most have their computers internally networked to facilitate better and faster communication (Intranet or LAN). They also have external access to the Internet, and advertise their wares and capabilities on websites.

(U) While the Internet is a superb vehicle for advertising and informing the population at large, many businesses have not yet found the correct, and often delicate, balance for posting information on the Internet-thereby creating a virtual OPSEC nightmare. This E-business explosion, and often unchecked posting of information on websites, has made it much easier for foreign countries, non-government entities, and even motivated individuals to locate and focus on specific targets and feast on the information given away so freely.

(U) For example, Russia's Center for Automated Data Exchanges (once subordinated to the KGB and now believed to play a central role in the computer intelligence collection activities of its successor agency, the SVR) is a client of several on-line databases such as those provided by the Library of Congress, LEXIS/NEXIS, U.S. National Technical Information Service, and the International Atomic Energy Agency, and has direct access to data networks in the U.S., Canada, France, Germany and the United Kingdom. The Russians also have established accounts with multiple Internet service providers such as America Online, CompuServe, and the European

Union's EuNet.[9] Russia is only one country of many to have these capabilities; there are at least 20 others considered "critical countries" on various U.S. government lists at any given time.[10]

Many businesses have not yet found the correct, and often delicate, balance for posting information on the Internet thereby creating a virtual OPSEC nightmare.

(U) Collectors around the world dedicated to the Internet collection effort no longer have to leave their homes to gather information; they can access it from the comfort of their armchairs in seconds rather than traveling for days and spending vast amounts of money to locate a source that may or may not have the morsel of information they seek.