AD-A279 882

JMENTATION PAGE

Form Approved
OMB No. 0704-0188

1b RESTRICTIVE MARKINGS

2a SECURITY CLASSIFICATION AUTHORITY

3 DISTRIBUTION/AVAILABILITY OF REPORT
APPROVED FOR PUBLIC RELEASE: DISTRIBUTION IS UNLIMITED.

2b DECLASSIFICATION / DOWNGRADING SCHEDULE

JUN 03 1994

4. PERFORMING ORGANIZATION REPORT NUMBER(S)

5 MONITORING ORGANIZATION REPORT NUMBER(S)

6a NAME OF PERFORMING ORGANIZATION	6b OFFICE SYMBOL (If applicable)	7a. NAME OF MONITORING ORGANIZATION
		Defense Personnel Security Research Center

6c. ADDRESS (City, State, and ZIP Code)	7b ADDRESS (City, State, and ZIP Code)
	99 Pacific Street Building 455, Suite E Monterey, CA 93940

8a. NAME OF FUNDING / SPONSORING ORGANIZATION	8b OFFICE SYMBOL (If applicable)	9 PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER

8c. ADDRESS (City, State, and ZIP Code)	10 SOURCE OF FUNDING NUMBERS			
	PROGRAM ELEMENT NO	PROJECT NO	TASK NO	WORK UNIT ACCESSION NO

11 TITLE (Include Security Classification)
Target Revitalization for Espionage in American Industry: New Directions for the Coming Decade

12. PERSONAL AUTHOR(S)
David L. Carter, Ph.D.

13a. TYPE OF REPORT	13b TIME COVERED	14. DATE OF REPORT (Year, Month, Day)	15 PAGE COUNT
Technical Report	FROM _____ TO _____	1993, September	76

16 SUPPLEMENTARY NOTATION

17 COSATI CODES			18 SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	Intelligence; espionage; security; security awareness; spying; security education

19 ABSTRACT (Continue on reverse if necessary and identify by block number)

The purpose of this research was to identify important U.S. targets of future espionage. Intelligence entities of foreign adversaries and allies alike have become more interested in certain types of information due to recent global economic and political changes. Data were collected from archival sources and through interviews with subject matter experts. The report summarizes significant economic and political trends, emerging espionage targets, and the implications of these changes for personnel security policy and security management.

20 DISTRIBUTION / AVAILABILITY OF ABSTRACT	21 ABSTRACT SECURITY CLASSIFICATION
☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT ☐ DTIC USERS	UNCLASSIFIED

22a NAME OF RESPONSIBLE INDIVIDUAL	22b TELEPHONE (Include Area Code)	22c OFFICE SYMBOL
ROGER P. DENK, Director, PERSEREC	(408) 646-2448	

DD Form 1473, JUN 86 Previous editions are obsolete SECURITY CLASSIFICATION OF THIS PAGE

S/N 0102-LF-014-6603

DTIC

TARGET REVITALIZATION FOR ESPIONAGE IN AMERICAN INDUSTRY:
NEW DIRECTIONS FOR THE COMING DECADE

by

DAVID L. CARTER, PH.D.
MICHIGAN STATE UNIVERSITY

A Grant Report Submitted to the

SECURITY AWARENESS AREA OF THE
PERSONNEL SECURITY RESEARCH INSTITUTIONAL AWARD PROGRAM

PERSONNEL SECURITY RESEARCH AND EDUCATION CENTER (PERSEREC)
OFFICE OF NAVAL RESEARCH
U.S. DEPARTMENT OF DEFENSE

94-16523

September 1993

This project was completed under a grant from the Personnel Security Research and Education Center (PERSEREC) of the Office of Naval Research, U.S. Department of Defense, Monterey, California. The views and conclusions expressed in this report are those of the author and do necessarily reflect those of PERSEREC, ONR, DoD, or Michigan State University.

6 02 01

EXECUTIVE SUMMARY

This project identified interactive economic and political strategic trends which will have an effect on the national security of the United States as we approach the millennium. This analysis addressed the probable espionage targets which are either non-traditional or have historically been of a low priority nature. With target definition, policy responses can be developed with respect to redefined personnel security issues, education/training needs, supervision, and personnel policy controls.

Target revitalization for espionage has a number of important factors which focus directly on personnel security issues. These include...

- ✔ Understanding changing espionage interests in order to provide new insights for potential breaches of security by personnel.
- ✔ Understanding changing targets to help increase security protection by imposing appropriate controls which will minimize both opportunity and "temptation."
- ✔ Knowledge of evolving targets helps to develop profiles of those who seek sensitive data and information.
- ✔ Industries which have traditionally received little or no attention with respect to espionage may be identified in order that a threat analysis can be conducted.
- ✔ Personnel expertise can be identified and focused toward those industries and disciplines where increased security is most likely to be needed.
- ✔ A re-development of organizational culture can begin as a means to respond to changing world situations; i.e., the "New World Order."

DTIC

RESEARCH QUESTIONS

Implicit from the discussion thus far, are five basic (yet interactive) research questions this project addressed...

- ✔ What espionage target changes have occurred or are anticipated to occur?
- ✔ What political and economic factors interact to make these changes? (i.e. What is the logic for these projections?)
- ✔ What broad implications do these factors have for personnel security?
- ✔ What policy directions should be taken to minimize the personnel security risk based on the research findings?
- ✔ What follow-up or future research needs are indicated from the findings?

The proverbial "bottom line" is that in the future—in fact, the near future—our view of national security is going to have to be broadened and redefined. While there is surely open discussion of issues such as economic intelligence threats and corporate espionage, the reality is that the national security structure is not changing in any marked degree. Traditional views of security risks remain and dogmatism is nearly institutionalized with respect to establishing a more comprehensive vision of national security.

For
Dist
A-1

A SHIFT IN FOCUS

We should not confuse "military threat" with "intelligence threat" The intelligence threat can best be seen in the shift from primary military collection of information and technology to collection of information which will build a stronger economic base to bring the countries of the former Soviet Union out of its severe economic depression and move it, eventually, into a position of economic power (Thomas, 1990). As one example, much of the vast Russian land has significant oil reserves. Efforts of both oil exploration and extraction have been very limited because of the lack of sophisticated technologies. If these technologies can be "developed" through intelligence sources, rather than purchase which would likely involve profit sharing, then the economic base would have an important element on which to solidify.

A fundamental argument made throughout this report is that the concept of national security must be broadened for the future. This, obviously, entails a wide range of policy change not to mention changing roles of critical elements of the intelligence community. Although change is difficult and time-consuming, we cannot afford to avoid it, or worse contest it, if the change is mandated by global events and required as a means to maintain both the sovereignty and quality of life in the United States. As noted in the *National Security Institute Advisory* (November, 1992:11), "Our greatest challenge in the 1990s is to protect our advanced technology from unauthorized disclosure to both friend and foe alike." Trade secret theft cost U.S. companies more than $100 billion dollars in lost revenues in 1992. If left unchecked, analysts estimate losses could grow an additional 50% by the year 2003.

Perhaps, then, an important role of government is to explore the role of the intelligence community in dealing with this problem. Certainly, it will be both difficult and controversial. How should the intelligence community attack economic issues?

- ✔ Should the intelligence community simply monitor international economic trends or target specific industries in which the U.S. is a substantial leader?
- ✔ Should the U.S. develop a comprehensive counterintelligence program to stop economic/industrial espionage in the U.S.?
- ✔ Should the U.S. actively develop covert strategies to perform industrial espionage for the benefit of the U.S.?
- ✔ If active espionage is performed, should the information be used as a policy tool or shared with U.S. industries? If the latter is the case, how would this be equitably accomplished?

These questions are not easily answered from a legal or ethical or policy perspective. These are, however, essential for a new national security perspective to be pondered. We must...

- ✔ ...redefine what secrets are. This includes encompassing the private sector *beyond* the defense industry to assist them from being victimized by corporate espionage.
- ✔ ...more explicitly articulate industrial espionage as it relates to economic homeostasis as a national security issue.
- ✔ ...broaden the role of personnel security to encompass the non-defense private sector in areas critical to the economic national security of the United States. This may include a new perspective of "clearances" as well as issues of training and threat awareness.
- ✔ ...recognize that in the corporate community, which is the greatest target of competitive espionage (e.g., high technology, pharmaceuticals, and chemical engineering), there needs to be more information given from the intelligence community of threats both in terms of the types of threats, source countries, targets of the espionage, and potential means of espionage.

- ✔ ...aggressively pursue for prosecution, people involved in economic and competitive intelligence. Commitment to prosecution and punishment to these individuals much match that traditionally afforded to persons involved in military espionage.

More explicitly, there are four primary reasons for the growth of competitive intelligence...

- ✔ With current communications, transportation, and data transfer, any market for any product can be invaded by a competing force in a short time period.
- ✔ Research and development is a labor-intensive, long term process; competitive intelligence can obviously shorten the time for R&D as well as significantly reduce costs. Simply put, it is cheaper and faster to steal a developed and tested idea than to develop it yourself.
- ✔ Competition is increasing globally while and currency is increasingly the most important weapon in a country's arsenal. Thus the need to (a) know what competitors products are and (b) beat competitors to the market becomes increasingly important.
- ✔ Continual creation of new products, services, and technologies means keeping abreast of changes in the marketplace is more difficult, consequently industrial espionage helps keep a competitor "in the race."

Important areas which must receive particular attention in the process of R^3 (R-cubed)—*Refocusing, Refining, Reallocating.*—as a means to prepare for the future of national security threats are...

- ✔ Personnel recruitment, evaluation, and development for *future responsibilities,* not today's.
- ✔ Special security programs currently in use—will they need to be re-tooled or, perhaps, eliminated and replaced?
- ✔ Personnel security requirements and processes including a re-definition of what personnel security is and a revisitation of the whole concept of clearances.
- ✔ Facilities use and allocation.
- ✔ Matters of collaboration and cooperation between intelligence community agencies and between the intelligence community and "critical" corporations, which include those beyond the traditional defense industry.
- ✔ The nature and operations of support services. What types of new support and research is needed for changing priorities?
- ✔ Budget planning processes and priorities.

In consideration of changing espionage targets, some important fundamental factors emerge which must be addressed by policy makers and agency administrators. Among these are...

- ✔ A renewal of the economy, a re-orientation of industry, and change of world politics leads to new national security threats.
- ✔ Within the intelligence community there needs to be an attitudinal change away from entrenched post World War II beliefs about international relations and toward the changing nature of the global community.
- ✔ National security needs to have a general re-definition. Traditional perspectives which were dominated by geo-political issues must now be viewed geometrically where concerns are more balanced between geo-political dynamics, multi-national social concerns (including the increasing

view of the U.S. "the world's police officer" as in the case of Somalia and Bosnia-Herzegovina), a world economy, and transnational business.

- ✔ The "Evil Empire" is being replaced by aggressive business competition and international crime.
- ✔ The threat-button of national security is changing from our pathology of scorn directed at the former Soviet Union and its ideological bloc, to a complicated admixture of "ally-competitors" (notably Japan and the European Community.)

The U.S. intelligence community must keep some important perspectives in light of these factors...

- ✔ The strategic threat against the United States and U.S. interests are at their lowest levels in nearly four decades, but we cannot totally discount threats to re-emerge. Among these potential threats are...
  - ✘ Return of authoritarian control in Russia and/or the Ukraine
  - ✘ Eastern European threats
  - ✘ North Korea
  - ✘ India and Pakistan (both of which have nuclear weapons)
  - ✘ Cuba
  - ✘ Iraq, Libya, Iran
  - ✘ China
- ✔ Particular world "hot spots" include...
  - ✘ Afghanistan
  - ✘ India
  - ✘ Tibet
  - ✘ Bangladesh
  - ✘ Cambodia
  - ✘ North Korea
  - ✘ Tajikistan
  - ✘ Sri Lanka
  - ✘ Bhutan
  - ✘ Burma
  - ✘ Taiwan
  - ✘ East Timor
- ✔ Disputed Territories
  - ✘ Bosnia-Herzegovina, Croatia, Yugoslavia
  - ✘ Peninsular Malaysia
  - ✘ Paracel Islands
  - ✘ Sabah
  - ✘ Kuril Islands
  - ✘ Spratly Islands
  - ✘ Senkaku Islands
- ✔ Nuclear Armed, Nuclear Capability, or Threshold Nuclear Capability
  - ✘ Russia
  - ✘ Kazakhstan
  - ✘ North Korea
  - ✘ Pakistan
  - ✘ Israel
  - ✘ Ukraine
  - ✘ China
  - ✘ Iraq
  - ✘ India
- ✔ Somalia, Bosnia and other humanitarian efforts hold unknown problems

INTERNATIONAL ORGANIZED CRIME

While general concern has been expressed in this report concerning the need to focus intelligence efforts toward economic and competitive intelligence, a related factor the intelligence community must address for national security is international organized crime. Globally, organized crime is changing radically with the traditional hierarchical structure and strong commitment within a given group (or "family") giving way to new models. More explicitly, organized crime on an international scale is increasingly entrepreneurial as has been found in investigations by the British National Criminal Intelligence Service (NCIS), the Dutch Centrale Recherche Informatiedienst (CRI), the German Bundeskriminalamt (BKA) and the Organized Crime Department of the Russian Ministry of Interior. Even the Italian Direzione Investigativa

Antimafia (DIA) has noted a subtle shift toward this more entrepreneurial model among the five major Mafia groups in Italy.

In sum, among the important factors of global organized crime to note with respect to this project are...

- ✔ Organized crime groups will do virtually *anything* to earn a profit.
- ✔ The inherent effect of organized crime groups, particularly multinational ones, is to undermine the legitimate social and economic stability of the countries it touches.
- ✔ Traditional views of organized crime as being a group of "thugs" which are a "police problem" must be changed to include a national security component.
- ✔ The line between organized crime, espionage, and illegitimate business practices is increasingly difficult to discern which, consequently, complicates investigations.
- ✔ Multinational organized crime groups are the norm, not the exception.

ESPIONAGE TARGETS

The phrase "Crown Jewels" has become a synonym in industry for its most prized possessions, whether they are products, patents, plans, processes, or any other intellectual property. The Crown Jewels are the most important economic weapons which are unique to a corporation's existence. From a broader perspective of the U S., this country collectively has its own Crown Jewels which must be protected from espionage.

Generally speaking, important targets of future espionage activities can be broken down into two broad categories...

1) Formulae, processes, components, structure, characteristics, and applications of new technologies. These include, but are not limited to,...
   - ✔ Fifth generation computer architecture
   - ✔ New computer chip designs and conductivity including biochip research
   - ✔ Biotechnology
   - ✔ Supercomputing and superconductivity
   - ✔ Processing capability
   - ✔ Holographic and laser research applications and modeling
   - ✔ Fiber optics
   - ✔ Aerospace technologies
   - ✔ Research in petrochemicals
   - ✔ Advanced materials
   - ✔ Advanced biotechnology methods
   - ✔ Medical technologies for treatment, wellness, and prevention, including pharmaceuticals
   - ✔ Advanced communications technologies and processes
   - ✔ Advances in satellite utilization and space technologies and applications
   - ✔ Electromechanical products and technologies
   - ✔ Optics technology
   - ✔ Telecommunications equipment, protocols, and technologies
   - ✔ Advanced cellular and wireless telecommunications technologies
   - ✔ Chemical process technology
   - ✔ Software development
   - ✔ Developments in integrated circuits
   - ✔ Packaging technology
   - ✔ Integration of all technologies

2) Factors associated with the marketing, production, and security of the new technologies. These include, but are not limited to,...
   - ✔ New technology release dates
   - ✔ Pricing information (wholesale and retail)
   - ✔ Marketing research on anticipated demand for the technologies
   - ✔ Marketing research on consumer profiles
   - ✔ Products which are needed for compatibility and applicability
   - ✔ Production time tables and product release dates
   - ✔ Production quantities
   - ✔ Market targets and schedules
   - ✔ Overseas marketing plans
   - ✔ Security equipment, sensors, and processes
   - ✔ Electronic banking equipment, interfaces, and protocols
   - ✔ Planned upgrade schedule for the technology
   - ✔ Planned changes of directions for the technology (somewhat similar to planned obsolescence)
   - ✔ Software developments particularly those which enhance new technologies, networking, and technological integration.

Beyond these broad categorical listings, future espionage targets can be defined in other, more explicit ways. Among them are...

- ✔ *Economic Targets*
  - ✘ Brokers
  - ✘ Bankers
  - ✘ Finance
- ✔ *Technology Targets*
  - ✘ Business
  - ✘ Research "Think Tanks"
  - ✘ Universities
  - ✘ Laboratories
- ✔ *Energy Exploration, Extraction, Processing and Use*
  - ✘ Oil
  - ✘ Gas
  - ✘ Goal
  - ✘ Nuclear
  - ✘ Solar
  - ✘ New Sources
- ✔ *Agricultural Targets*
  - ✘ Commodity Bankers
  - ✘ Agricultural Cooperatives
  - ✘ Forecasters
- ✔ *National/International Agreements*
  - ✘ Sales and Trade
  - ✘ Exchanges
  - ✘ Cartels

Based on the research and interviews for this study, it appears many of the methods will be the same or similar as ones already experienced in both national security espionage and industrial/economic espionage. In that discussions of these methods are available from other sources, they are summarily listed below for reference...

- ✔ Open sources (For example: Freedom of Information Act—FOIA—requests submitted to NASA, the FDA, Commerce Department, Defense Department, the EPA, and Department of Energy in addition to published government documents; government bidding specifications; opened bids; and articles in technical journals.)
- ✔ Attempting to hire "consultants" from the targeted firms and industries seeking people who have "inside information" on the explicit espionage

target. The consultation arrangement looks less sinister and appears to be a legitimate avenue for a professional to earn extra income (or at least an avenue easier for a person to rationalize their behavior).

- ✔ The use of "moles" (particularly by ethnic-related groups) whether they are professional employees or service employees working inside the industry. The "mole" will have unique access to information as a result of being "on the inside."
- ✔ Computer hacking and data transmission interruption.
- ✔ Compromising of employees, including blackmail and "set ups."
- ✔ Corrupting/bribing employees.
- ✔ Use of student researchers and university interns to gain access to research and technology (students from the sciences and marketing in particular).
- ✔ Surveillance and "snooping" around corporate employees including such things as listening to conversations in bars, going through trash, and similar activities.
- ✔ Signals interception and electronic eavesdropping, including...
  - ✘ Intercepting communications
  - ✘ Bugging
  - ✘ Fax Interception
  - ✘ Interception of communication
    - Microwave
    - Cellular
    - Satellite
    - Land line
- ✔ Burglary
- ✔ Use of janitorial and service-related personnel or businesses to gain access
- ✔ "Outsourcing"—the practice of contracting with individuals or companies to work on specific problems or elements of a new product. These people work for a wide range of companies and thus carry elements of the companies' secrets with them. Consequently, information will merge and move throughout the professional community as the contractors move. Foreign governments interested in industrial espionage can take advantage of this arrangement.
- ✔ Technologies and Techniques Which May Be Adapted to Serve as Detectors and Countermeasures for Espionage
  - ✘ Image Acquisition Using Gamma Backscatter
  - ✘ Magnetic Resonance Imaging
  - ✘ Pulsed Echo Inspection
  - ✘ Ultra-Trace Chemical Samples
  - ✘ Extremely Compact Embeddable Multichannel Global Positioning System Receivers
  - ✘ SAW (Surface Acoustic Wave) Sensor System for Identification of Substances
  - ✘ Ion Mobile Spectrometry (IMS) for Substance Detection
  - ✘ Visible and Near Infrared Reflectance
  - ✘ Optical Immunosensor
  - ✘ Panoramic Viewing Using a 3-D Line Scan Camera Technique
  - ✘ Remote Detection of Trace Effluenting Resonance Raman Spectrometry
  - ✘ Airborne Multispectral Scanner for Remote Sensing and Biomass Assessment of Substances
  - ✘ Tempest Systems
  - ✘ Real Time Multispectral Fusion for Wide Area Surveillance (WAS)
  - ✘ Wide Area Acoustic Intrusion Alarm and Tracking System
  - ✘ Micro-Miniature Radio Frequency Transmitters, receivers, and Recorders
  - ✘ Electronic Tags
  - ✘ Digital Microphone Array Systems

MOTIVATIONS FOR ESPIONAGE

Each case will involve an interaction of one or more factors, however, it appears the overwhelming motivation is *money*—increasingly so in recent years. Beyond the obvious monetary factor of increased "buying power" afforded by spying for profit, other factors have an important influence. For example...

- ✔ With shifts toward economic espionage, profitability of spying increases.
- ✔ Economic spying is not as repugnant as seeking traditional national security secrets.
- ✔ It is emotionally easier to spy for a political ally than a political foe.
- ✔ Economic spying does not have the punitive ramifications that is found with political/military espionage.

Beyond money, per se, there are several key characteristics which contribute to a person committing espionage. These factors essentially relate to the "quality of life" people experience both at home and at work. Security threats may include...

- ✔ ...a person who is unhappy on the job in general.
- ✔ ...a person who is unhappy with their location of assignment, particularly if it is perceived to be "off the beaten path."
- ✔ ...a person who feels they have been overlooked for promotion or merit salary increases.
- ✔ ...a person who feels they have been overlooked for commendations and awards.
- ✔ ...a person who does not feel they have been compensated for their contribution to the organization.
- ✔ ...a person faced with personal financial difficulties or stresses.
- ✔ ...a person facing personal problems, particularly if they feel that the "way out" of the problem is to "escape" or that they may "buy their way out of the problem."

Toffler (1990), in discussing the "info-wars" of the future, observed that it is inevitable that a "fusion of public and private intelligence" must occur. It is of paramount importance that we recognize this as a convention of policy for national security as we approach the millennium. It is time that a new corporate strategy in the intelligence community be developed. This includes new policy, new regulations, and new legislation. The need is not derived so much from the idea that strategic threats to national security have diminished, but that even an more ominous, less psychologically intimidating threat has emerged—economic espionage. It is less visible and less coercive, but extraordinarily dangerous to our national security. It is like a virus attacking our economic and, consequently, social systems. It can destroy us from within but never fire a shot. It is incumbent that we develop a remedy to this virus in order to protect the Crown Jewels of American inventiveness: The ability to create technological innovations and apply computerization to a vast array of uses.

TABLE OF CONTENTS

PREFACE

The importance of looking at the future is to anticipate changing problems and potential avenues to solve those problems. Visions of the future conjure illusions of streamlined, high technology devices which help us perform tasks at high speed with great efficacy. We envision problem solving simplified, job performance increasing, and a higher level of quality of life as a result of these innovations. To some extent this vision is accurate. For example, communications has evolved through a spectrum of devices and procedures ranging from signal lights, Morse code, telephones, low band radios, and high band transceivers with encoding capabilities. Beyond these are cellular telephones, microwave and satellite communications, facsimile transmission and computer conferencing with the so-called "interactive technology"—integrated computers, cable television, and telephones—on the horizon.

The future, however, is not only this immediate vision of technology and equipment. It also represents conceptual and operational changes in business and government. For example, high technology has increased the *efficiency* of people. But what about our *effectiveness*? Will such technologies help people to *qualitatively* perform their work better? The answer is not simple. Certainly with the ability to increase efficiency more information can be processed in a shorter amount of time. However, this increase in speed may come at a cost—the loss of truly understanding our goals, mission, and the need to re-define them in a changing society.

From this lesson we must recognize that the future embodies both "high tech" and "high touch" perspectives. It is clear that the intelligence community is evolving toward a philosophical change which integrates traditional national security concerns with issues related to economic intelligence and industrial espionage. The future roles of our intelligence community must look beyond the technological marvels which capture imagination. Instead, the future must *blend* the technology with a fundamental change in philosophy which breaks away from tradition in assessing the future threats to our national security. This report is directed toward this end.

An important element of this report is to challenge the *status quo*. Because it is directed toward exploring the future it does not approach issues of personnel security from a traditional perspective. Instead, it takes a broad view of national security issues we are likely to face in the future and places them in the perspective of how they must be addressed for change to occur.

Many people contributed to this report through interviews, sharing of information, and providing advice and direction. In the early stages of the project Maynard Anderson of DoD provided important advice and direction for study. Roger Denk of PERSEREC provided appreciated support and the assistance and patience of Jim Riedel, grant monitor from PERSEREC, is sincerely appreciated. Jim's quick responses to my inquiries and patient assistance were important elements for bringing this project to fruition. For the many security and law enforcement officials who contributed their time and expertise, I thank you all.

CHAPTER 1
INTRODUCTION

Because of global changes in political and economic forces, a "New World Order" is evolving which offers important changes in the relationship between the United States and other countries. Over the four and one-half decades following World War II, the primary national security focus has been the maintenance of military homeostasis and defense primarily directed toward the former Soviet Union and the Warsaw Pact countries. The world socio-political environment is now changing--somewhat akin to an international metamorphosis—and the intelligence community must respond to these changes.

Speculation has been offered on a variety of fronts with respect to these changes and their impact on the U.S. This project—designed as the first in an interlocking series—focuses these issues and offers a forecast of changing espionage targets. As global political ideologies and international relations change, so will threats to national security and, consequently, espionage. Similarly, as espionage targets are redefined in the global community, the methods, and even our vision of what personnel security threats are must be similarly redefined. Thus the need to forecast the changing trends—and targets—becomes of fundamental importance in order to effectively plan for security in the coming decade.

Importantly, this report also discusses the rationale of the forecasts and emphasizes what is perhaps the most difficult organizational and personnel challenge facing leaders in the intelligence and national security communities: Changing the organizational culture, and hence belief systems, of those employees working with classified information and intelligence. As will be discussed, this change of "vision" will come with difficulty, requiring diligence and commitment for the vision to transcend into policy.

It is important to re-emphasize a point established in the project proposal. The intent of this research was to project future espionage targets as the first step in a research series. Subsequent projects will focus on personnel security issues—both threats and precautions—which are related to these forecasts. Having stated this, the author has also ventured out somewhat to discuss a changing paradigm explicitly related to the way personnel security may be viewed in the future. This paradigm emerged as an applicable model during the course of the research for this project.

STATEMENT OF THE PROBLEM

This project identified interactive economic and political strategic trends which have an effect on the national security of the United States as we approach the millennium. This analysis addressed the probable espionage targets which are either non-traditional or have historically been of a low priority nature. With target definition, policy responses can be developed with respect to redefined personnel security issues, education/training needs, supervision, and personnel policy controls.

While speculation has been offered about the influence of evolving political and economic conditions as affecting U.S. national security, the material has been generally broad in scope. This project focuses the information both in terms of analysis and theory development as it relates to espionage targets.

During the course of this project it became apparent that changes in international relations were occurring at an unprecedented pace. Nearly every day new factors or unique "spins" emerged in media reports, research findings, and even expert opinions of issues. The rapidity of this change reinforces the need to forecast national security threats from a perspective that is both long-term and eclectic.

RELATIONSHIP TO PERSONNEL SECURITY

Target revitalization for espionage has a number of important factors which focus directly on personnel security issues. These include...

- ☑ Understanding changing espionage interests in order to provide new insights for potential breaches of security by personnel.
- ☑ Understanding changing targets to help increase security protection by imposing appropriate controls which will minimize both opportunity and "temptation."
- ☑ Knowledge of evolving targets helps to develop profiles of those who seek sensitive data and information.
- ☑ Industries which have traditionally received little or no attention with respect to espionage may be identified in order that a threat analysis can be conducted.
- ☑ Personnel expertise can be identified and focused toward those industries and disciplines where increased security is most likely to be needed.

☑ A re-development of organizational culture can begin as a means to respond to changing world situations; i.e., the "New World Order."

RESEARCH QUESTIONS

Implicit from the discussion thus far, are five basic (yet interactive) research questions this project addressed...

- What espionage target changes have occurred or are anticipated to occur?
- What political and economic factors interact to make these changes? (i.e. What is the logic for these projections?)
- What broad implications do these factors have for personnel security?
- What policy directions should be taken to minimize the personnel security risk based on the research findings?
- What follow-up or future research needs are indicated from the findings?

METHODS

This project used established qualitative research methods focused on content analysis and application of both inductive and deductive logic. The content analysis involved a wide array of disparate research, sources, and reports which addressed political, economic, and social issues. This process is closely akin to that used in the intelligence community for collating information, determining its veracity (both validity and reliability), and drawing policy-related conclusions.

Data collection included library research in diverse related disciplines, computer inquiries into appropriate data bases, review of unique limited distribution (unclassified) reports, and reviews of appropriate data bases. In addition, individuals with specific expertise in both the involved disciplines as well as personnel security were interviewed to gain their input on the project. Initial interviews focused on data gathering while follow-up interviews sought reactions and input related to both the findings and policy recommendations.

RESEARCH FOUNDATION AND PERSPECTIVES

The research related to this project represents an eclectic assortment of information ranging from traditional national security information, research related to the changing world social, economic, and political order; organized crime; competitive intelligence; and emerging technologies.

The foundation for this project addresses several factors which will interact to influence the environment surrounding intelligence targets and personnel security risks. These include...

- The dynamics and implications associated with the development of the European Community.
- The break-up of the Soviet Union and its move toward a market-based economy.
- The dissolution of the Warsaw Pact and subsequent movement toward market-based economies in Eastern Europe.
- The reunification of Germany.
- The rapidity of global economic and political changes.
- The rapid growth of economies and global reach of countries in the Pacific Rim.
- The desirability of U.S. technologies and market strategies by other countries—both traditional "friend" and "foe" alike.
- Changing world "hot spots."
- Emerging global powers and threats (both strategic and economic).

The proverbial "bottom line" is that in the future—in fact, the near future—our view of national security is going to have to be broadened and redefined. While there are some discussions of issues such as economic intelligence threats and corporate espionage, the reality is that the national security structure is not changing in any marked degree. Traditional views of security risks remain and dogmatism is nearly institutionalized with respect to establishing a more comprehensive vision of national security.

We should not confuse "military threat" with "intelligence threat" The intelligence threat can best be seen in the shift from primary military collection of information and technology to collection of information which will build a

stronger economic base to bring the countries of the former Soviet Union out of its severe economic depression and move it, eventually, into a position of economic power (Thomas, 1990). As one example, much of the vast Russian land has significant oil reserves. Efforts of both oil exploration and extraction have been very limited because of the lack of sophisticated technologies. If these technologies can be "developed" through intelligence sources, rather than purchase which would likely involve profit sharing, then the economic base would have an important element on which to solidify.

On May 28, 1989, an article in the *London Times* stated that then Soviet President Gorbachev ordered KGB Chief Kryuchkov to "sweep the world for the industrial and military secrets needed to transform the Soviet economy." In mid-1989 Soviet Under Secretary of Defense, General V. Sjabanov stated that in light of *glasnost* and *perestroika*, less money will be spent on arms, but more money will be spent on intelligence gathering. In April 1990, General Colonel Vladlen Mikhailov, chief of the GRU, stressed in an interview that the diminution of military capabilities will mean that the role of Soviet intelligence will increase. He also acknowledged that technical collection platforms, especially space reconnaissance, have been given a greater emphasis in conducting military intelligence (Thomas, 1990:6). There is no reason to believe that with the dissolution of the Soviet Union that these factors will change. Most of the intelligence resources and assets of the former Soviet Union are now in the hands of Russia and the Ukraine. Moreover, with the move toward market-based economies and the significant economic problems facing these two new countries, the need for economic intelligence is enhanced. Indeed, Russian intelligence sources have publicly stated that they plan to assist Russian businesses rebuild the economy (Sessions, 1991). This obviously means that the former KGB will more definitively direct its espionage activities to gain Western technology and expertise.

Related to these facets, Merritt (1991) observed that the move toward a profitable market economy coupled with the high education levels and low wages make Eastern Europe a prime contender in the global high technology arena. Add this with the need to play "catch-up" with the G7 countries as well as their expertise in conducting espionage, and it becomes clear why the Eastern Europeans are willing to aggressively move toward economic espionage.

Following the "end of the Cold War" American intelligence began to lack direction. There was indecision on what should be done and how it should be done. So much time and effort had been directed to understand the Soviets and their Warsaw Pact allies, comparatively little comprehensive and value-based intelligence was available on the rest of the world's hot spots and hot issues. The failure of American intelligence in predicting Iraqi intentions toward Kuwait serves as an example (Wirtz, 1990). Understanding the best options in the former Yugoslavia serves as another. Not forthrightly acting on what we know about the presence of economic intelligence is yet a third important facet.

Miscalculation in the use of intelligence not only wastes resources it also places us in much greater risk (Wirtz, 1990).

"Intelligence is essential for strategy formulation whether in sales, the military, or a corporation (Sigurdson and Nelson, 1990:20). It is the culmination of analyzing a wide array of information which is either open, gray, or secret. Ninety percent of all information needed in intelligence is open, while nine percent is gray and one percent secret. "Gray" information is that which is confidential, but not under rigid control. This is the information most likely gained through competitive intelligence. Moreover, the open information may establish the infrastructure of a critical issue, commodity or strategy, and the gray information simply completes the picture. It is the linchpin which gives meaning and utility. It is this information which needs to be revisited for security.

Too often intelligence is treated as a commodity; Instead, it should be viewed as a resource. It can only successfully exist when their are clearly articulated policy goals that are being sought and questions need to be answered to achieve those goals. Moreover, intelligence must be viewed on a continuum which relates to the quality and amount of raw information the intelligence is based, the quality of analysis, and cumulative knowledge of analysts and policy makers alike to give meaning to this intelligence in the real world (*see* Hastedt, 1990).

Johnson (1992-1993) observed that post-Cold War intelligence priorities should focus on global proliferation of nuclear, biological, and chemical weapons as well as the spread of conventional weapons. (An article in the May 21, 1993 issue of *USA Today* on the arms market even listed a black market price list for various Russian weapons. These ranged from $30 for night vision telescopes, $15,000 for a 125mm howitzer, and $23 million for a MiG-29 fighter.) Other priorities include drug trafficking, terrorism, understanding renegade countries (notably the Middle East but may include South America and eventually Africa), commercial intelligence, and the environment.

"American foreign policy in the nineties will have to choose its goals and targets much more carefully; the nation must learn to match ambitious goals with limited means" (Mead, 1993:11). Certainly, to borrow a phrase form the British, we need to look for greater "value for money." Given the large-scale dynamic impact of commercial espionage on the United States, this seems an important area on which to concentrate. But to be effective, we need to regress to the management philosophies of Frederick Winslow Taylor: We must select the right people for the right job; train them to do the job in the most efficient and effective way; and evaluate their performance on meaningful criteria, not personality or perception.

While we must remain vigilant to safeguard traditional defense secrets—from technology to the Order of Battle—this does not mean that we must avoid the broader, legitimate questions of changes in the national security structure. It is, perhaps, most appropriate to look toward this re-definition now as Vice-President Gore pursues the move toward greater efficiency in government following his task force report, *Reinventing Government*. The parallel between the desire for greater efficiency and a revisitation of our perspective of national security is closer than one may intuitively think. Both initiatives...

- ☑ ...require changes in administrative policy of the U.S. government.
- ☑ ...seek to increase efficiency and effectiveness of government operations.
- ☑ ...require attitudinal changes of personnel throughout the bureaucracy who are accustomed to a long-term process of doing things "the right way."
- ☑ ...are forward looking toward the next generation of government in light of a changing world and the role of the U.S. in the evolving global community.
- ☑ ...require commitment and dedication by government personnel in order for this "vision of change" to reach fruition.
- ☑ ...both will invigorate opponents who do not want to see a change in "business as usual."

Even *non*-classified—government and private—information is valuable. It makes personnel security—security consciousness, if you will—fall within a different perspective. We need to change our culture and ideas to address this. While traditionally espionage has not been an issue in this venue, part of our future efforts need to look at this. Perhaps taking a collective or synergistic view of non-classified information is the perspective which is needed. Certainly, it would appear that critically reviewing the responsibilities and processes of the intelligence community is philosophically consistent with "reinventing government."

CONSIDERING NATIONAL SECURITY

A fundamental argument made throughout this report is that the concept of national security must be broadened for the future. This, obviously, entails a wide range of policy change not to mention changing roles of critical elements of

the intelligence community. Although change is difficult and time-consuming, we cannot afford to avoid it, or worse contest it, if the change is mandated by global events and required as a means to maintain both the sovereignty and quality of life in the United States. As noted in the *National Security Institute Advisory* (November, 1992:11), "Our greatest challenge in the 1990s is to protect our advanced technology from unauthorized disclosure to both friend and foe alike."

Thus, it is important at the outset to establish the parameters of national security as it is related to economic issues. According to Executive Order 12333, *United States Intelligence Activities*, (1981)...

> Timely and accurate information about the activities, capabilities, plans and intentions of foreign powers, organizations, and persons, and their agents, is essential to the national security of the United States.

Without question, this is sufficiently broad to include economic espionage activities. In fact, one may argue from this wording that the intelligence community would be *obligated* to address economic intelligence issues if they impinge on the sovereignty and economic homeostasis of the United States. The Executive Order goes on to state that...

> The United States intelligence effort shall provide the President and the National Security Council with the necessary information on which to base decisions concerning the conduct and development of foreign, defense and *economic policy*, and the protection of United States national interests from foreign security threats (emphasis added).

Clearly, economic issues are encompassed within this specification. If economic espionage directed toward United States' companies and interests is being committed as part of the foreign policy of another country, countering this threat is clearly within the purview of the intelligence community. The question is somewhat more murky if the espionage is committed by a foreign corporate entity with the knowledge and lack of objection of its government. Even though questions will arise in any policy decision, the overwhelming concern is directed toward the protection of U.S. national security, which clearly includes economic security. As such, the argument can reasonably be made that economic/industrial espionage against private U.S. companies is within the purview of stated national security policy. The questions remain, therefore, on how that policy authorization should be directed and how the intelligence community should adapt, perhaps redefine, its role in this regard.

Richard Heuer (1993) observed that the...

> ...risk of betrayal of trust is inherent in human nature and does not depend upon the presence of an implacable foreign adversary. It depends only upon a marketplace for information or materiel (1993).

Clearly, industrial trade secrets, marketing information, and research and development information related to new products are in a marketplace of the global community wherein "betrayal of trust" appears to be a surprisingly available commodity.

CORPORATE/INDUSTRIAL ESPIONAGE

Trade secret theft cost United States' companies more than $100 billion dollars in lost revenues in 1992. If left unchecked, analysts estimate losses could grow an additional 50% by the year 2003 (*Time*, February 22, 1993). As a current illustration of corporate espionage, the former General Motors chief of purchasing has had charges filed against him by GM alleging that he stole company secrets, including marketing strategies, before joining Volkswagen of Germany (*Lansing State Journal*, May 22, 1993). While this particular case has been widely publicized, General Motors certainly has not been the only victim of corporate espionage. Among those other companies which have been victimized in various ways are IBM, DuPont, Texas Instruments, Corning Glass Works, Microsoft, Apple Computer, Celanese Corporation, General Electric, ITT, Boeing, Sikorsky Aircraft, Air Cruisers, Dow Chemical, Honeywell, and Monsanto. Certainly the list could go on, particularly in the cases of small companies who design and manufacture specialty products for which there is a large market, but limited competition. Similarly, items which have a high general consumer value—Levi's jeans, motion pictures on videotapes, popular toys, and audio recordings on cassette tapes—are also targets of theft and counterfeiting. The lessons from these practices also costs the American economy hundreds of millions of dollars every year.

A *Business Week* (October 14, 1991:96) article observed that, "Increasingly, economic intelligence-gathering—from tracking technology trends to passing foreign business secrets to domestic companies—is seen by many nations as key to their economic survival." Related to this, noted futurist Alvin Toffler, in his book PowerShift (1990), observed that there are several key reasons for growth in competitive intelligence/corporate espionage...

- The speed with which any market can now be invaded from the outside.
- The long lead times needed for research.
- Greater competition between companies and countries.
- Continual innovation and technological evolution spurs the desire to understand competitor strategies and products.

Add to these the rapid movement of the former Soviet-bloc toward market-based economies and the growth of regional economic common markets in Europe, North America, North Africa, and the Pacific Rim, then the incentives for corporate growth become even more evident. Importantly, the ability of any country's businesses to be profitable and predominant in a market is essential for national security, particularly has we merge into the "New World Order."

Economic espionage by a foreign national security intelligence agency is not new. Evidence exists by the U.S. intelligence community that Japan, France, Germany, Israel, and Russia have overtly charged their respective intelligence services to conduct economic intelligence in selected areas. Schweizer's research on the issue found that outside of Frankfurt, Germany "approximately thirty-six computer specialists and senior intelligence officials are working on a top-secret project to bring computer hacking into the realm of spying and intelligence" (1993:158). This was reinforced independently by the author's research in a discussion with a former Norwegian police official who is currently a corporate security director. In addition, a German official interviewed by the author also inferred this capability in the context of "the experimentation we are doing to get into the computers of criminals."

Many attempts to "reverse engineer" desired products—that is, obtain a desired product in order to take it apart to see how it was made—have simply not been an effective way to steal secrets. The reasons for this lack of success are (1) not all elements of components, compounds, or materials can be determined and/or (2) more is needed than formulae or recipes, instead *production processes* are also important. This is particularly true with respect to biotechnology. Thus, competing companies—and sometimes governments—will make efforts to commit corporate espionage or induce an employee to commit corporate treason. As Schweizer further observed...

> Intelligence and espionage, once the exclusive occupations of monarch and government, have become an important component of international business. No longer are spies employed only by national intelligence services. Large corporations around the world, particularly in Western Europe and Asia, now hire sophisticated agents to gather intelligence on competitors and other countries. Intelligence...is being privatized. Some of these corporations field networks of agents that, according to one former CIA Director, rival those of middle-sized countries (1993:251).

At an international conference at the British Police Staff College at Bramshill, a Russian General, a Hungarian police official, and a German Bundeskriminalamt (BKA) agent confirmed to the author that former intelligence agents from Eastern Bloc intelligence services—including ex-KGB and ex-Stasi agents—are "on the market" to sell their services and expertise to either

organized crime groups or for corporate espionage operations. They are, if you will, "intelligence mercenaries."

A KGB defector predicted that Moscow will step up its industrial espionage in the years ahead because of its deteriorating economic situation. The economic espionage would be subtle, frequently under the guise of offering to help U.S. businesses get established in the former Soviet Union (*The Washington Post*, October 29, 1991.) In this regard, evidence suggests that spying by the SVR (formerly the KGB) and other members of the former Warsaw Pact are continuing against the U.S. The difference, however, is a new intelligence mission toward economic intelligence (*The Washington Times*, October 29, 1991.) In support of this, the FBI has discovered that sophisticated espionage technology is being used more and more by foreign intelligence services to covertly obtain economic secrets from U.S. corporations as well as targeting the government for traditional political and military information. Similarly, a *National Security Institute Advisory* (1992:4) stated that "Numerous former KGB operatives are moving into the private sector, seeking lucrative careers in consulting and security work, and raising new concerns among U.S. counterintelligence officials about possible spying."

In an interview with *Time* magazine (April 20, 1992), former CIA Director Robert Gates stated...

> The KGB [in its traditional form] may have disappeared, but the interests of the Russian intelligence service in Western technology continues. We see operations, attempted recruitments. Their resources have been reduced, but they are more highly focused now than before. As a matter of fact, we sense that the [Russian] military intelligence, the GRU, has become more aggressive in seeking technical secrets.

Moreover, strong evidence exists that some industrial espionage activities have even involved organized crime groups. This is particularly true of the Japanese *Yakuza* and some of the Eastern European and North African organized crime groups. Indeed, many European companies, according to interviews in this study, are as concerned about organized crime groups who steal corporate secrets for sale on the open market as they are by competitors and state-supported industrial espionage efforts. (This will be described in greater detail later.)

THE ROLE OF AMERICAN CULTURE

According to a wide range of corporate security directors with whom these issues were discussed, the consensus was that despite losses, American business executives seem surprisingly naive of the "economic wars" which are

being pursued through industrial espionage. This is illustrated by the comparatively low investments in security by U.S. companies with perhaps the exception of defense contractors who are bound to have more rigid security controls. It should be emphasized that corporate security personnel recognize the problem, but have limited success in stressing its importance to management.

Why has the United States not responded to these threats? It is simply inconsistent with our culture and traditions; it violates our belief of "fair play" and seems incompatible with our philosophical beliefs of "due process" and "equal protection" embodied in the U.S. Constitution. In essence, it is a socio-legal characteristic of American culture. Beyond these factors are two other aspects of American society which are critical to our lack of response. First, Americans are a *present oriented* people. That is, our society emphasizes neither history nor the future to the extent that we emphasize the present. This is illustrated by fashion, language, movies, Nielson and Arbitron ratings, short terms of offices for elected officials, E-mail, computer services such as Prodigy and CompuServe, one or two year budget cycles, and commercials emphasizing us to "live for today" or "just do it" not to mention the rapid successes of facsimile machines and overnight package deliver services such as Federal Express and United Parcel Service. The significant point to note is that all of these icons of "Americana" indicate that it is contra-cultural to look very far into the future to both conceptualize and accept how change must occur. We celebrate the history of our country at nearly 220 years, yet it is but a fraction of the age of many of the world's societies. While we have made wonderful accomplishments, we still have a poor perspective of time. With this "present orientation" we are less likely to look very far into the future in order to anticipate the challenges ahead.

The other factor is that we tend to be *provincial*. That is, Americans tend to lack a global view of issues, perhaps because of the size and relative geographic isolation of our country. Perhaps this provincialism is best described in an observation a British Customs official made to the author. He said that Americans are the only people who, when asked where they were born, will respond with the name of a city or state instead of their country of birth. The problem with this tendency toward provincialism is that we tend not to view global issues from a realistic perspective, if at all. When confronted with global issues Americans tend to be uncertain of its effects or dismiss it because the link is not made between a global issue or event and one's own life or environment.

Adding to our "fair play" and legal perspectives, our "present" orientation, and our provincialism, the natural human penchant toward dogmatism magnified by the characteristics of the bureaucratic structure as found in government, it is no wonder that we have not embraced the fact that global corporate espionage is a destiny we must face in order to maintain our national security.

IMPORTANT QUESTIONS TO CONSIDER

Perhaps, then, an important role of government is to explore the role of the intelligence community in dealing with this problem. Certainly, it will be both difficult and controversial. How should the intelligence community attack economic issues?

- ☑ Should the intelligence community simply monitor international economic trends or target specific industries in which the U.S. is a substantial leader?
- ☑ Should the U.S. develop a comprehensive counterintelligence program to stop economic/industrial espionage in the U.S.?
- ☑ Should the U.S. actively develop covert strategies to perform industrial espionage for the benefit of the U.S.?
- ☑ If active espionage is performed, should the information be used as a policy tool or shared with U.S. industries? If the latter is the case, how would this be equitably accomplished?

These questions are not easily answered from a legal or ethical or policy perspective. These are, however, essential for a new national security perspective to be pondered.

A PERSPECTIVE

Throughout this research project it became clear that a fundamental perspective was needed in order to plan for future espionage threats. The watchword for this perspective in all aspects of our national security is *change*—the dogmatism we all experience coupled with the complexity of a bureaucratic institution, such as the government, makes any form of change seem alien, impossible, or inappropriate. Yet, as our society has evolved, our institutions have changed—albeit frequently with reluctance.

As an illustration, in his book *The Third Wave*, futurist Alvin Toffler describes major socio-economic "waves" the U.S. has experienced. Essentially, we began as an *agricultural society*, relying on agricultural production and trade as being the primary forces in moving society forward. With increased immigration and concomitant development of inventions and products, we moved into an *industrial wave*. With technological growth in the 1980s and increased heavy industry moving off-shore, the U.S. became increasingly embedded in the *information wave*. Technology as well as research and development (R&D) contributed significantly toward information being the

substantive industry. We successfully adjusted, with time, through the agricultural and industrial waves—we must now focus our resources on the information wave. Just as the "information wave" will drive our economy, it is also a prevalent factor in national security. This is particularly true since international relations have changed dramatically as we traverse the post-cold War era.

This writer is firmly convinced that the time has come to make a fundamental substantive change in viewing and protecting our nation's secrets. We must...

- ...redefine what secrets are. This includes encompassing the private sector *beyond* the defense industry to assist them from being victimized by corporate espionage.

- ...more explicitly articulate industrial espionage as it relates to economic homeostasis as a national security issue.

- ...broaden the role of personnel security to encompass the non-defense private sector in areas critical to the economic national security of the United States. This may include a new perspective of "clearances" as well as issues of training and threat awareness.

- ...recognize that in the corporate community, which is the greatest target of competitive espionage (e.g., high technology, pharmaceuticals, and chemical engineering), there needs to be more information given from the intelligence community of threats both in terms of the types of threats, source countries, targets of the espionage, and potential means of espionage.

- ...aggressively pursue for prosecution people involved in economic and competitive intelligence. Commitment to prosecution and punishment to these individuals much match that traditionally afforded to persons involved in military espionage.

These factors will be discussed throughout this report.

Personnel security must be forward looking and flexible; it must respond to changing conditions world over in order to ensure emerging threats to security do not reach fruition. In this regard, personnel security needs to clearly be on the cutting edge of all security issues.

CHAPTER 2
REVISITING SECURITY NEEDS AND ASSESSMENTS

The reader will note that this chapter is comparatively short. Yet, in the author's opinion the message is critically important to planning for future espionage threats. As such, it warrants being set apart. We are at a point of defining the future of national security to include new visions of concern and responses.

It cannot be overemphasized that the intelligence community—and consequently those in both the public and private sector "security establishments"—must begin a self-assessment process which is not locked to traditional perspectives of what national security is (including personnel security). A thoroughly creative, open view of the issues and threats must be done which is not bound by established parameters of current law, regulation, policy, custom or practice. This is not an easy endeavor to either perform or lead because many will respond. "We can't do that" or "That's not our job." The challenge and future, however, require that *creative* applications of the scientific method be exercised in order to explore change.

Noted astronomer Carl Sagan of Cornell University in his book *Broca's Brain*, made an important observation related to this concept. Referring to this process in the context of scientific thought, Sagan observed...

> Science is a way of thinking much more than it is a body of knowledge. Its goal is to find out how the world works, to seek what regularities there may be, to penetrate to the connection of things—from subnuclear particles, which may be the constituents of all matter, to living organisms, the human social community, and thence to the cosmos as a whole. Our intuition is by no means an infallible guide. Our perceptions may be distorted by training and prejudice or merely because of the limitations of our sense organs, which, of course, perceive directly but a small fraction of the phenomena of the world. ... Science is based on experiment, on a willingness to challenge old dogma, on an openness to see the universe as it really is. Accordingly, science requires courage—at the very least the courage to question the conventional wisdom. ... [T]he scientific cast of mind examines the world critically as if many alternative worlds might exist, as if other things might be here which are not. ... If you spend any time spinning hypotheses, checking to see whether they make sense, whether they conform to

> what else we know, thinking of tests you can pose to substantiate or deflate your hypotheses, you will find yourself doing science. (Sagan, 1979:13—14.)

Sagan's advice on the need to have a "willingness to challenge old dogma" and the "courage to question the conventional wisdom" are important keystones for a revisitation of policies, perspectives, and responsibilities related to national security. Following these paths are difficult because...

- *...it goes against our socialization.* Everything we have learned in our lifetime, including that which we learn at work—called occupational socialization—is the basis for our attitudes. Thus, challenging the norm is the same as challenging the validity of our belief systems.

- *...it is hard to be creative.* Innovation, originality, and new insight is a product of one of the most difficult of all human endeavors—creative thought. We cannot *force* ourselves to be creative, instead we have to *permit* ourselves the time to be creative.

- *...the bureaucratic structure inhibits creativity.* Bureaucracies, by their nature, have rigid organizational and behavioral controls which, consequently, discourage discretion. They reward adherence to rigid policy mandates and discourage any activities which are not consistent with the norm.

Forward-looking professionals must be aware of these problems and work at overcoming them in order to develop a vision for the millennium.

REFOCUSING, REFINING, REALLOCATING.

A revisitation of national security threats and the consequent role of the intelligence community requires a framework for directing self-study as well as a comprehensive vision. One way to reassess needs and explore pathways for the future may be referred to as R^3 (R-cubed)—*Refocusing, Refining, Reallocating.*

As noted earlier, with an evolving "New World Order" a changing global political climate, greater economic initiatives worldwide, and socio-political mandates which have greater diversity, the intelligence community will find it necessary to explore important new directions for the maintenance of national security. This exploration must go beyond speculation and research—it must move into the area of policy development, personnel training and a general change in both the *corporate ideology* and *corporate strategy* of the intelligence community.

Corporate ideology refers to the beliefs, values and responsibilities an organization holds in support of its mission. The corporate strategy reflects processes and procedures employed to attain goals in support of that ideology.

To begin, in order to prepare for the future, elements of the intelligence community must engage in a *comprehensive self-assessment of its current status*—managerially and operationally—in order to effectively explore the directions which are needed to best face the future. This self-assessment needs to embody the critical elements of R^3.

Refocusing refers to defining—in written form—what activities and concerns will be addressed by the intelligence community in the future. It requires a re-examination of the mission, goals and objectives and a re-statement of them as they fit the national security needs of the future

Refining refers to fine-tuning the infrastructure of intelligence organizations and processes to met future national security threats. Once the direction of the intelligence community agency has been formally refocused, then policies, procedures, job descriptions, security requirements, training and security countermeasures, must be adjusted to match the refocused mission. If the infrastructure does not functionally support the mission, goals, and objectives, then little forward progress can be made.

The final element of R^3 is *reallocation*. New organizational directions will most likely require a reallocation of resources (i.e., people, budget, equipment) in order to meet the needs of the refocused direction. For example, industrial espionage countermeasures would require new training, policy development and time for labor-intensive problem solving.

The application of R^3 is essential for implementing plans for the next generation of national security initiatives. Important areas which must receive particular attention in the R^3 process are...

- Personnel recruitment, evaluation, and development for *future responsibilities*, not today's.
- Special security programs currently in use—will they need to be re-tooled or, perhaps, eliminated and replaced?
- Personnel security requirements and processes including a re-definition of what personnel security is and a revisitation of the whole concept of clearances.
- Facilities use and allocation.
- Matters of collaboration and cooperation between intelligence community agencies and between the intelligence community and "critical" corporations, which include those beyond the traditional defense industry.

- The nature and operations of support services. What types of new support and research is needed for changing priorities?
- Budget planning processes and priorities.

Planning for the future must involve *substantive* change, not cosmetic change. Tinkering with such things as position titles, organizational alignment, and programmatic activities is insufficient. Radical surgery to the core philosophy is needed in order to introduce organizational change. This is a process which must be accomplished incrementally. There are several critical ingredients which are necessary for effective change to occur...

- There must be a stimulus for change—*Change Agent*
- There must be administrative commitment—*Stay Agent*
- Any change must be grounded in logical and defensible criteria—*Don't change simply to "shake up" the organization*
- Employees at all levels must be able to provide input—*Team Building*
- There must be a time for experimentation, evaluation, and fine-tuning—*Exploration of the Concept*
- Before change is introduced, you must communicate to all persons and enlist their support—*Don't leave employees in the dark*
- Change takes time in order to have an effect; major change may take a generation—*Time is a necessity; don't rush it*
- Recognize that not everyone will "buy in" to the change—*Complete support is improbable*
- Be flexible and open in your view of the change—*Many ideas are losers; maintain the freedom to fail*
- The chance always that you may be placed "on the hot seat" from a political perspective—*Change is risky*
- Change requires challenging conventional wisdom; or at least traditions—*Be ready for ridicule*
- The organization's evaluations system must measure and reward effective involvement in change—*Without rewards, failure is assured*

The "willingness to challenge old dogma" is not an easy thing to do, particularly in largely autocratic organizational structures. Our future, however, depends on it.

CHAPTER 3
THE CHANGING WORLD: THEORY AND REALITY

A phenomenon has occurred over the past few years that many of us would not have fathomed a half decade ago a radical change in the global political landscape has emerged. Scenes of people chipping away pieces of the Berlin Wall for souvenirs while exchanging conversations with the formerly feared East Berlin border Guards seemed surrealistic. Similarly, the rapidity with which Republics seceded from the Soviet Union leading to the former "Evil Empire's" transformation from a World Superpower to a collection of struggling new countries desperately trying to survive a metamorphosis into a democracy with a market-driven economy was remarkable. No less surprising was the speed with which the Warsaw Pact countries changed both directions and leadership while Germany was reunified. And the new relationship between Israel and the PLO, albeit fragile, is no less remarkable.

The euphoria of these world events brought calls for a reinvestment in America. This reinvestment speculated on new ways money could be invested through the so-called "peace dividend" with many suggestions for "down-sizing" both the military and the intelligence community. With the change of our attitudes toward former bitter adversaries becoming much more paternal, many began to assume that we were on the threshold of world peace. While the nuclear threat has indeed subsided, there are many obstacles in the way of world peace—obstacles which offer changing priorities for the U.S. military and intelligence communities which cannot be left unattended. Among the problems are...

- The remaining instability in the former Soviet Union, with particular concern for Russia and the Ukraine which maintain substantial nuclear arsenals and political forces which want to return to the previous world balance.

- The instability in Central Europe, notably the former Yugoslavia, but also the growing strife related to emigration particularly in Germany and France.

- The interminably unstable Middle East, particularly the political machinations of Libya, Iran, and Iraq.

- Growing nuclear capabilities from Pakistan, North Korea, Iraq, and China.

- Social, political, and economic strife which seems to pervade Africa.

- Growing worldwide organized crime which not only involves billions of dollars on an annual basis but substantially influences governments and governmental decisions in such diverse locations as Colombia, Russia, Poland, Mexico, and Italy, among others.

- Increased global competition in the marketplace leading to industrial espionage which drains billions of dollars from the U.S. economy annually.

The importance of these factors rests in the fact that new demands are being placed on the intelligence community—demands which are more diverse and, in many ways, non-traditional. Rather than neuter the intelligence community, we must redirect its efforts. Unfortunately, dogmatism from "traditionalists" and tunnel vision by others are, as noted earlier, significant barriers to effective change.

A global view must be taken to understand how these changes are affecting the United States and the roles of the intelligence community in this regard. The following discussion offers a theoretical view of how change is occurring.

FUNDAMENTAL FACTORS

In consideration of changing espionage targets, some important fundamental factors emerge which must be addressed by policy makers and agency administrators. To recap these, they are...

- A renewal of the economy, a re-orientation of industry, and change of world politics leads to new national security threats.

- Within the intelligence community there needs to be an attitudinal change away from entrenched post World War II beliefs about international relations and toward the changing nature of the global community.

- National security needs to have a general re-definition. Traditional perspectives which were dominated by geo-political issues must now be viewed geometrically where concerns are more balanced between geo-political dynamics, multi-national social concerns (including the increasing view of the U.S. "the

world's police officer" as in the case of Somalia and Bosnia-Herzegovina), a world economy, and transnational business.

- The "Evil Empire" is being replaced by aggressive business competition and international crime.

- The threat-button of national security is changing from our pathology of scorn directed at the former Soviet Union and its ideological bloc, to a complicated admixture of "ally-competitors" (notably Japan and the European Community.)

The U.S. intelligence community must keep some important perspectives in light of these factors.

- The strategic threat against the United States and U.S. interests are at their lowest levels in nearly four decades, but we cannot totally discount threats to re-emerge. Among these potential threats are...

  + Return of authoritarian control in Russia and/or the Ukraine
  + Eastern European threats
  + North Korea
  + India and Pakistan (both of which have nuclear weapons)
  + Cuba
  + Iraq, Libya, Iran
  + China

- Particular world "hot spots" include...

  + Afghanistan
  + Tajikistan
  + India
  + Sri Lanka
  + Tibet
  + Bhutan
  + Bangladesh
  + Burma
  + Cambodia
  + Taiwan
  + North Korea
  + East Timor

- Disputed Territories

  + Bosnia-Herzegovina, Croatia, Yugoslavia
  + Kuril Islands

+ Peninsular Malaysia
+ Spratly Islands
+ Paracel Islands
+ Senkaku Islands
+ Sabah

- Nuclear Armed, Nuclear Capability, or Threshold Nuclear Capability

  + Russia
  + Ukraine
  + Kazakhstan
  + China
  + North Korea
  + Iraq
  + Pakistan
  + India
  + Israel

- Somalia, Bosnia and other humanitarian efforts hold unknown problems

MANAGING INTELLIGENCE

The rapidity in growth and creation of technology as well as information exchange alters the way we manage intelligence. We must move from a somewhat contemplative environment to one of increased chaos as a result of rapid, on-going socio-economic change and changing foci of governments. How do we deal with this? One way is to recognize the "Crown Jewels" of America's secrets. These include the areas wherein the U.S. holds significant advantages over other countries—adversaries and friends alike—which must be protected.

Three important competitive edges the United States possesses and must maintain are...

- We are able to integrate technologies very successfully and effectively. The space program and military, *a la* Desert Storm, are good examples. In the private sector, the emerging "interactive technology" of computers, telecommunications and cable television serves as another illustration.

- The U.S. has the overall strongest computing power (including super computing) being applied to the widest areas of society.

- U.S. research and development initiatives have been perhaps the most productive in the world, yet, we are losing some ground, largely as a result of industrial espionage. Consequently, the U.S. R&D gap is not stable and may be narrowing. Moreover, since reverse engineering of American technologies and technological applications have not been very successful, industrial espionage has grown.

In some ways, the U.S. losses of headway in these areas has been a product of our cultural characteristics (e.g., openness, freedom, sense of "fair play" by unwritten rules) and inadequate security initiatives needed to protect the Crown Jewels. Among the problems are...

- Pure science and technology in American society are virtually impossible to control because of the openness of both our society and the scientific/research community in America.

- Related to this, most of the useful acquisitions of technologies and engineering developments by other countries has come from published documents—a significant amount of "open source" materials exists.

- Vigilance must be maintained on multi-lateral export controls of critical technologies with refinement to make controls more specific and enforceable to prevent massive exports of these materials (small amounts will inevitably be transferred out of the U.S.)

- We must broaden our Euro-centric views and attitudes to more inclusively look at the Far East and Pacific Rim in the short term and Africa and the Mid-East in the long term.

Importantly, we must recognize that increasingly the U.S. is moving from an *arms race* to an *information race*. As a result, we must prepare our policies, intelligence, foci, and psyche toward this direction.

As a post-war truth, Japan had to turn toward an economic strategic orientation rather than a military one. This is increasingly true with Eastern Europe and will likely occur with the traditional "Third World" areas of the globe, including...

- China
- India
- The Arab-Islamic World
- Niger-Kordofanian Africa
- The Hispanic Americas

Information, hence knowledge, is the central force driving economies, even manufacturing economies, of today. Business is the venue by which this knowledge is stimulated and converted to a socio-political force. The result is that industrial espionage—which has been occurring with dramatically increasing frequency over the past decade—must be viewed as a significant threat to our national security.

More explicitly, there are four primary reasons for the growth of competitive intelligence...

- With current communications, transportation, and data transfer, any market for any product can be invaded by a competing force in a very short time period.

- Research and development is a labor-intensive, long term process; competitive intelligence can obviously shorten the time for R&D as well as significantly reduce costs. Simply put, it is cheaper and faster to steal a developed and tested idea than to develop it yourself.

- Competition is increasing globally while and currency is increasingly the most important weapon in a country's arsenal. Thus the need to (a) know what competitors products are and (b) beat competitors to the market becomes increasingly important.

- Continual creation of new products, services, and technologies means keeping abreast of changes in the marketplace is more difficult, consequently industrial espionage helps keep a competitor "in the race."

A country's ability to develop and produce technologies determines power and influence" (Schweizer, 1993:30.) Technology gave the U.S. a quantum leap to become the world's single military superpower. We must respond to competitive intelligence threats in order to keep our technological edge on all fronts.

THE THEORETICAL DIMENSION

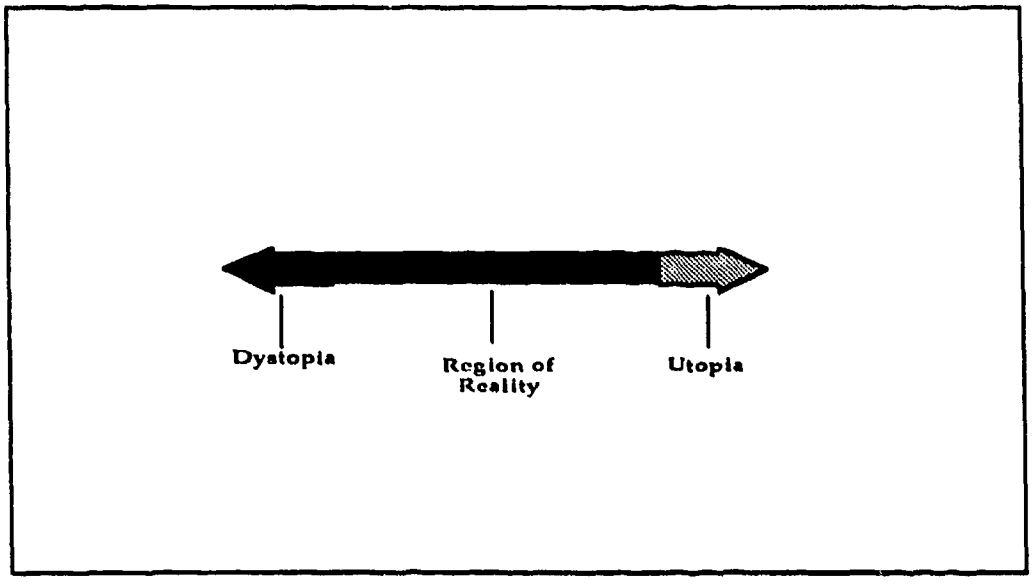
Strong theoretical reasons support the changing World Order and the consequent need to review intelligence mandates, strategies, and priorities. The phenomenon can be viewed on a continuum of social equilibrium with the extreme ends of the continuum representing utopia and dystopia. *Utopia* is a society where only good things occur. In utopia there is a world without hunger,

disease or war and all people are engaged in useful and meaningful work. Each social participant contributes to the betterment of society and does so in an ethical and fundamentally fair, selfless manner. Conversely, with *dystopia* one finds a society in chaos where social institutions have collapsed. Crime, corruption, hunger, and suffering are the foundations of this world where endless war and institutionalized depravity are salient features

The greater the conflict among social elements the greater the dystopia. The greater the social homogeneity, the greater the tendency to move toward the utopian end of the continuum. While there will be variance both between and within societies, most fall within the "region of reality"—an area of variance which has a centrist position on the continuum. When the social environment leans more toward the dystopic end of the continuum, conflict and social disintegration will increase. The converse is true when the social structure is more utopic.

As illustrated in Figure 3-1, these factors exist on a continuum, with the reality of life varying in the middle. Some societies tend to lean more toward one end of the continuum than the other, but all circumstances appear to be static rather than stable. Extremes do occur—Somalia represents an illustration of a highly dystopic society and Switzerland is a more utopic one—but all vary. As a global society, during the World Wars and even during the Bay of Pigs crisis in the Cold War, the world was leaning more toward dystopia. Fortunately, our shift on the continuum away from this position has occurred in the past several years.

FIGURE 3-1: CONTINUUM OF SOCIAL STABILITY



Our relationship with other societies will be influenced by our location on the continuum. During global crises, the value of military secrets and technology was quite high; as the crises subside, the value is diminished. For example, during the Cold War the U.S. intelligence community expended a great deal of effort (and money) to learn as much as possible about the capabilities and technology of the soviet MiG-29. Today, anyone who can travel to the Russian aerospace center at Zhukovsky can literally purchase a ride in the fighter piloted by a top Russian aviator. This same shift on the continuum—toward the utopian end of the scale—places premiums on other information. As a society becomes more ordered, it seeks a stronger economy and greater wealth. Consequently, information which helps strengthen the economy—such as, intellectual property which is frequently the target of industrial spying—becomes a higher priority target of espionage than the military secrets. Moreover, because of changes in the "World Order" the impact of economic loss to a country is truly a national security concern.

DIFFERENTIAL SOCIAL DISINTEGRATION

To build on the theoretical foundation, the optimum circumstance to protect national security and minimize espionage of all forms is to have *geo-homeostasis*. This is when elements of technology, economy, political ideology, and social evolution all move in synchronization. Each of these elements can be viewed as a wheel (or cycle) in global social systems. Geo-homeostasis—or world stability—is changed based on the relationship of each of these components as they relate to each other. The fundamental principles which drive this theory are as follows...

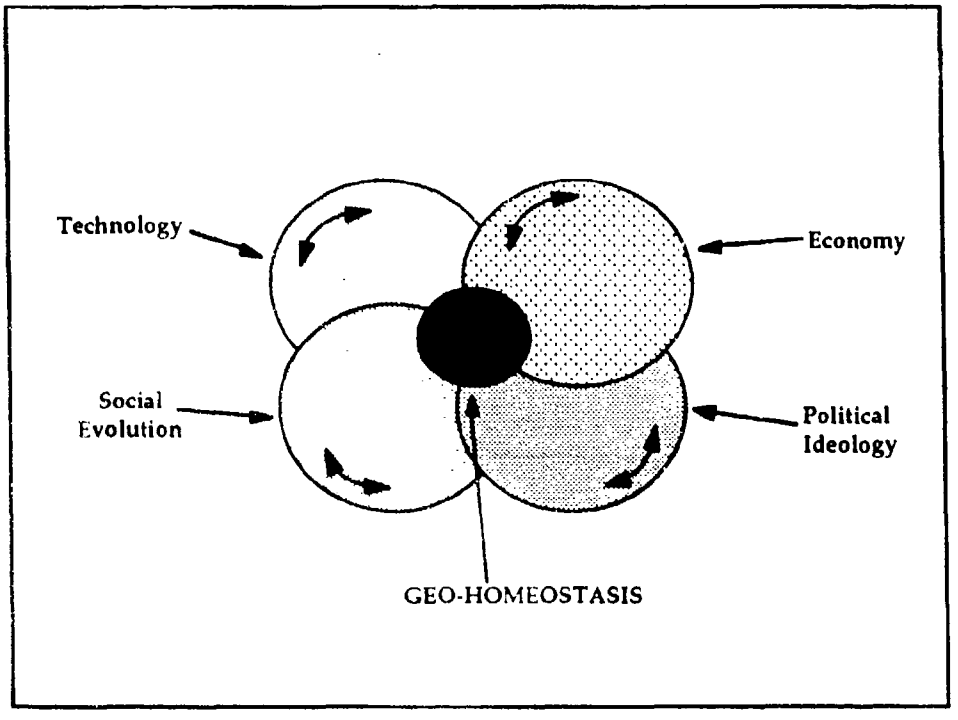
- The speed of each wheel in the model moves at different rates.
- The rate of movement of each component varies as they interact.
- All rates of change will vary depending on its location on the continuum of social stability.
- As the velocity of each component becomes increasingly different, they tear at the stability of the center, which is geo-homeostatic.
- As fissures occur in the components, greater geo-stress occurs consequently socio-political conflict erupts.

The differential forces which influence the future are similar to what Holden and Sapp refer to as *evolutionary dissonance*. In this concept, social friction is generated by the different speeds at which parts of society move. While time moves at a constant speed, change does not. Change is influenced, particularly in the area of national security, by four primary factors: technology, the

economy, social evolution, and political ideology. Each of these four elements, both within a society and between societies, moves at different rates. For example, as technology leaps ahead social change may be more spasmodic (such as, the resistance of older people to learn how to use a computer); it may even regress in some societies (such as in Iran when the fundamentalists came to power.) The greater the distinction between these evolutionary elements, the greater the conflict.

As another illustration closer to home, as technology leapt ahead in the U.S. to manufacture more reliable and powerful firearms, our social capacity to respond to these changes has not kept pace, with levels of violence increasing as an indicator of social stress. The economic environment is moving at still a different pace which is influencing crime and our political ideology on how to deal with crime and the economy is moving at a different speed yet, with disagreement on how to deal with these diverse problems. The net result is a slight shift toward dystopia where chaos, evidenced through rising rates of violence, increases.

FIGURE 3-2: MODEL OF FORCES AFFECTING GEO-HOMEOSTASIS



These are the factors which determine "importance" of commodities of all types and at all socio-political levels. As a simple example, during the cold war, geo-political homeostasis was threatened during conflicts in political ideology (i.e., Communism versus Democracy); social evolution (notably in the areas of

human rights and individual rights); economic disequilibrium, changing of economic standards particularly with the Pacific rim, notably Japan, becoming an important economic power; and the evolution of technology with the leading reasons for this change being economic growth and technological development related to the defense. With the break-up of the Soviet Union and dissolution of the Warsaw Pact, these components of geo-homeostasis changed.

Traditional national security concerns had three plateaus...

- PRIMARY: U.S.S.R. and Eastern Europe (Warsaw Pact)
- SECONDARY: Technology, Drugs and Terrorism
- TERTIARY: Third World Threats and Issues

With the socio-political changes occurring in the world, these three plateaus need to have greater balance. both in terms of attention and devotion of resources.

THE ROLE OF INTERNATIONAL ORGANIZED CRIME

While general concern has been expressed in this report concerning the need to focus intelligence efforts toward economic and competitive intelligence, a related factor the intelligence community must address for national security is international organized crime. A British intelligence official commented to the author that...

> The G7 countries clearly are worried about the theft of trade secrets and corporate investment by organized crime groups. The greatest worries are from Europe followed by Japan. For an unknown reason, America does not seem to react to this. American authorities appear to be caught in the disbelief that Soviet threats have been broadly reduced. Priorities, goals, ideas, and attitudes must be changed.

In a similar line of thought, a Dutch intelligence specialist echoed a related concern, observing...

> Maybe it is because of your great size or some scheme of your law, but American officials tend to view crime and espionage as two different responsibilities; two different concerns. Our view is that they are strongly related. Not crime like home burglaries and street robberies, but organized crime. We are absolutely convinced that organized criminals will do anything for money including drug trafficking, stealing large commodities of commercial goods, stealing U.N. shipments of food, and spying for whatever business or government will pay them. They have no loyalty beyond their

> profit. They [organized crime] are a substantial threat which cannot be discounted. Now with the break-up of the Soviet Union, we should focus on worldwide organized crime group, just as we focused on the KGB and Stasi. The damage they [organized crime groups] can do is far greater.

Historically in the United States organized crime has been viewed synonymously with the Italian/Sicilian Mafia or La Cosa Nostra. The character of organized crime began to change, however, as the Medellin and Cali drug cartels and Jamaican Posses made their presence felt on the streets of America. Moreover, the global impact of the Asian crime groups (e.g., Triads, Tongs and Yakuza) has been substantial.

Globally, organized crime is changing radically with the traditional hierarchical structure and strong commitment within a given group (or "family") giving way to new models. More explicitly, organized crime on an international scale is increasingly entrepreneurial as has been found in investigations by the British National Criminal Intelligence Service (NCIS), the Dutch Centrale Recherche Informatiedienst (CRI), the German Bundeskriminalamt (BKA) and the Organized Crime Department of the Russian Ministry of Interior. Even the Italian Direzione Investigativa Antimafia (DIA) has noted a subtle shift toward this more entrepreneurial model among the five major Mafia groups in Italy.

Many definitions and descriptions of organized crime exist all embodying certain basic principles. Perhaps best contemporarily viewed as continuing criminal enterprises, organized crime is characterized by...

- ☑ An accumulation of profit;
- ☑ Longevity in the pursuit of goals through illegitimate methods;
- ☑ A structure to further the group's crimes;
- ☑ A willingness to transgress border, laws, and custom in furtherance of their goals;
- ☑ A penchant toward violence; and
- ☑ The ability to corrupt government officials, police officials, and/or corporate officials

Emphasizing the trend of organized crime to go beyond drug trafficking, theft, and vice-related crimes, a Detective Chief Inspector of the British NCIS observed,

> Legitimate business never travels without criminal company. ...and like an ink spot, organized crime starts in one location, but spreads its dark shadow over any area it can easily invade

While perhaps a little melodramatic, the point is clearly illustrated.

In discussing the diversity of commodities in which Hungarian organized crime groups are interested in, a representative of the Hungarian National Central Bureau of Interpol told the author...

> Smuggling and black market alcohol, tobacco, and electronics are a foundation economy for organized crime in Hungary. It is hard to control because these are items people want. It's also hard to control because with the country's poor economic conditions, even an illegal economy adds jobs.

From a somewhat broader perspective, an official of the German BKA stated that...

> The political changes in Eastern Europe have clearly had an impact on the Federal Republic of Germany. We feel that Germany is becoming the new center for organized crime because of its growth here. This change is absolutely revolutionary.

According to law enforcement, criminal intelligence, and corporate security officials from a wide array of countries, among the increasingly coveted targets of entrepreneurial criminals are corporate secrets—information which can be easily transported and sold on the world market for high profits. This is not only the theft of the business secrets, it is the theft of future profits, the theft of jobs, and another step toward the undermining of a country's legitimate economy. Collectively, the monetary impact is staggering. Dr. Petrus Van Dyne, an economist and analyst with the Dutch Ministry of Justice estimates that "...the dollar amounts earned by entrepreneurial crime groups from commercial crime exceed the hundreds of millions of dollars earned in drug trafficking."

In sum, among the important factors of global organized crime to note with respect to this project are...

- ☑ Organized crime groups will do virtually *anything* to earn a profit.

- ☑ The inherent effect of organized crime groups, particularly multinational ones, is to undermine the legitimate social and economic stability of the countries it touches.

- ☑ Traditional views of organized crime as being a group of "thugs" which are a "police problem" must be changed to include a national security component.

- ☑ The line between organized crime, espionage, and illegitimate business practices is increasingly difficult to discern which, consequently, complicates investigations.

- ☑ Multinational organized crime groups are the norm, not the exception.

A SUMMARY NOTE

From the collective perspectives of military intelligence, economic intelligence, and organized crime as discussed in this chapter, there are several world "hot spots" which warrant attention from the United States intelligence community in the future. These are...

- Quebec
- Ukraine
- Russia
- Balkan states
- Eastern Europe (notably Czech Republic, Slovakia, and Hungary)
- Former Yugoslavia (Serbia, Croatia, Bosnia-Herzegovina)
- European Community
- North Korea
- Japan
- Significant (and disproportionate) economic growth in China
- Cuba
- U.S./Mexico Border
- South Africa
- Northwestern South America (notably, Columbia, Peru, Bolivia)

Future intelligence efforts should consider the broad of array of threats—military, political, industrial, economic, and criminal—which are likely to emerge from these locations.

CHAPTER 4
EMERGING ESPIONAGE TARGETS

Based on the material presented thus far, it should be apparent that forecasting future espionage targets requires an important fundamental factor: The intelligence community must shift its historical priorities (1) develop a broader perspective of national security threats and (2) provide greater balance of attention among the disparate threats which exist. While strategic military and nuclear threats unequivocally remain, the resonance of these threats are not superordinate above those posed by economic/industrial espionage. The issue is *national security*—we must recognize that the economic viability and world benchmark of the U.S. as *the* economic power in the world has clearly receded. This translates to a weakened national security. Economic espionage has clearly contributed to this and will most likely become more deleterious over the next decade.

To be sure, the loss of jobs and a significantly weakened economic state can be as devastating to the quality of life for American citizens as a warhead. While the emotional impact is not as dramatic, the substantive long-term impact is no less real.

As one example of the change, human intelligence (HUMINT) of the future will be less likely to resemble a person with the chameleon bravado and physical prowess to infiltrate hostile political groups, instead being more likely to resemble a "computer nerd" wearing an Apple T-shirt and carrying a notebook computer (complete with modem, of course.) A significant number of future "spies" will be "information archeologists." They will understand the value and structure of information, know how to assess its value from afar, locate it and retrieve it, be able to anticipate hazards and comparable risks, and be able to assess electronic artifacts as guideposts on the road to seeking the targeted treasure.

As another example of "balance," when dealing with high-profit consumer goods in the international market—such as jeans, computer games, wrist watches or videotapes—members of the intelligence community do not tend to view these things with the same importance as, for example, the military Order of Battle. Let's face it, textiles are not as "sexy" as nuclear weapons. Yet, as the "New World Order" continues to take shape these economically-based factors become increasingly paramount because of their broad appeal, their vitality for change, and their integral role in a country's socio-political and economic vitality.

The phrase "Crown Jewels" has become a synonym in industry for its most prized possessions, whether they are products, patents, plans, processes, or any other intellectual property. The Crown Jewels are the most important economic weapons which are unique to a corporation's existence. From a broader perspective of the U.S., this country collectively has its own Crown Jewels which must be protected from espionage. These include...

- High profit consumer products
- Technological innovations
- Software applications and innovations
- Information on corporate plans, research, and commodities
- High energy physics
- High temperature superconductivity
- Genetics and genetic engineering
- Emerging and future information technologies
- Technologies, machines and production practices/capabilities of the future
- Advanced materials
- Advanced biotechnology methods
- High-speed, environmentally clean transport
- Environmentally clean energy generation
- Resource saving and environmentally clean production processes in metallurgy and chemistry
- Efficient food production
- Medical technologies for treatment, wellness, and prevention (including pharmaceuticals)
- Advanced construction technologies
- Advances in safe, efficient, innovative, and environmentally clean nuclear power
- Advanced communications technologies and processes
- Advances in satellite utilization as well as space technologies and applications

When thinking about future espionage targets and threats, an important starting place is to "wipe the slate clean." Forget about traditional targets, "enemies," processes, reports, organizations, responsibilities, and concerns. Forget about our traditional vision of espionage and even the role of government. Think, instead, of being the marketing manager of a business which has a broad spectrum of high technology products for sale and in the research and development stage. How will you protect your corporate Crown Jewels? How can you help market your product to stay ahead of the competition? How can you help keep the creative juices flowing within your company without compromising the integrity of the information and ideas which are being developed? This is the emerging arena of national security which we must explore.

A key element in dealing with this new slate will be to understand the dynamics of computerization as a tool of espionage and threat.

UNAUTHORIZED ACCESS TO COMPUTERIZED INFORMATION

Computer-related crime and unlawful access to computer systems is still perceived by many to be distant—something that is possible, but somewhat unlikely. The traditional visage of crime happening to "someone else" appears to be even more prevalent with respect to unlawful computer access. Yet, the evidence is all too well documented that unlawful computer access has been linked to espionage, theft of trade secrets, access to critical economic information and simple theft of money. We, as a society, must take this threat more seriously with respect to both its impact on national security and its criminal potential.

Controls must be established in which are built around the unlawful computer access we have experienced. Moreover, these controls must be monitored and reinforced to minimize their security threat. Similarly, leadership is needed in the private sector to recognize the threats posed by computer-related crime.

Unlawful computer access and computer-related crime are aggravated by the network system designed to make computing more efficient—Internet, Milnet, and Bitnet serve as illustrations. These networks can serve as "electronic highways" linking government computers, contractors' computers, and university computers, around the globe. In a similar vein, the practice of *Electronic Data Interchange* (EDI) contributes to the complexity. The EDI connects parties for contract negotiations, sales, collections and other transactions—the computer becomes a vault and the EDI is the avenue to its treasures. Another avenue is the private computer network known as SWIFT (Society for World International Financial Transactions) which is a high-speed linkage carrying instruc' ns for most international bank transactions. Access to SWIFT permits tracking—even interrupting—significant international financial transfers between individuals, business, and governments. The value of unlawful access to SWIFT could do inestimable damage by an economic spy.

To better understand the nature of computer-related crimes, the author has developed a four-point typology...

- The computer is a target
- The c puter as an instrumentality
- The computer is incidental to other crimes
- Crime which is associated with the prevalence of computers

The computer is the target. The intent of this crime is to either obtain information fror e computer or to damage the computer's hardware or

programs by way of unlawful access to the system. This intrusion is usually committed by "superzapping" or becoming "super user." These terms refer to the process wherein the intruder—or "hacker"—first gain access to the computer's operating system where the masquerade as the computer system manager. From this point the intruder can gain access to virtually any file in the system as well as manipulate or modify any system hardware or software. More over, the intruder can even command the system to erase all evidence of the intrusion.

A wide array of crimes exist in this category—illustrations include...

- Theft of intellectual property (designs, trade secrets).
- Marketing (customer lists, pricing data, marketing strategies).
- Blackmail based information gained from computer files.
- Sabotage of intellectual property, marketing, pricing, personnel or any other critical file.
- Sabotage of operating systems and programs to impede the business process of a company or to create chaos.
- Unlawful access to criminal justice and other government records for various purposes, including...

  1) Access bid specifications and competitors
  2) Alter immigration information
  3) Change criminal history
  4) Change wants and warrants
  5) Creation of documents (driver's license, passport, automatic teller cards, etc.)
  6) Change tax records
  7) Access to intelligence files

- Techno-vandalism—"walking through a computer" and damage is caused, not for profit, but for the "challenge."
- Techno-trespass—"walking through a computer" just to explore—only looking, but violates privacy.

The computer is a instrumentality of the crime. In this category of computer abuse, it is the *processes* of the computer are used to facilitate the crime or intrusion. That is, it is not the information contained within the system's memory which is being sought, but the machinations which can be performed by the computer which are sought. For example, a thief may use a gun as an instrumentality to steal money from a person or the thief may use the computer as an instrumentality to take money from a person's bank account.

Typical crimes in this category may include...

- Fraud from use of ATM cards and accounts

- Money ("round offs" of monetary entries)
- Credit card fraud
- Fraud from transactions in the computer
- Telecommunications fraud

In the case of espionage—economic or strategic—a person may use the computer to locate important information or it may be used to copy sought-after data. In the latter circumstance, a hacker may instruct the computer to copy any information entered or produced by a given person or group of people and then place that copy in a special file which the hacker can access at any time. Rather than photographing or photocopying information which is sought, the computer's *processes* are being used to make a copy of the information.

The computer is incidental to other crimes. In a related vein, the computer is not always essential to commit a crime, but it can serve as an artifact related to the incident. That is, the essential crime could be committed without the computer, however, the system's presence simply helps facilitate the crime. Examples where this category of crime has occurred includes...

- Money laundering
- Off-shore banking
- Pedaphile Bulletin Board Service
- Organized crime records/books
- Murder (changing patient medical information in hospital computer)
- Bookmaking
- In a Georgia attempted murder case, a computer chip was altered and replaced in a Cadillac to make the car speed up and the brakes in operable.

In each of these cases, crimes have occurred without the computer, however the system simply increased the criminal's efficiency as well as making his/her discovery and prosecution more difficult.

Crime which is associated with the prevalence of computers. This is an area which has grown significantly with respect to economic espionage and theft of materials. In these offenses, the advent of micro-computers have produced new crime targets as well as competitive espionage targets. Crimes may include...

- Software piracy/counterfeit
- Copyright violations of computer programs
- Counterfeit equipment
- Black market computer equipment and programs

Just recently, the Microsoft Corporation identified a piracy ring operating out of Taiwan which was illegally reproducing Microsoft Windows and a variety of Microsoft Macintosh programs and selling these on the world market. The loss of income was estimated to be tens—if not hundreds—of millions of dollars. This type of loss to one American firm, multiplied times the wide variety of U.S. businesses which have similarly been victims, is a staggering loss to the American economy.

All of these crimes have international dimensions which can be accomplished with surprising ease as illustrated in the case of Cliff Stoll's *The Cuckoo's Egg*. Recognizing the significant impact of these crimes, the ease and speed with which they can be committed, the difficulty of detection, and the ease by which international borders can be crossed by nearly undetectable electronic impulses are all important which national security intelligence must face in the future. While important initiatives have already been directed toward computer-related issues of national security by NSA and others, the need to focus on computer-related *crime* in this international dimension is necessary.

INTELLECTUAL PROPERTY

Theft and alteration of *intellectual property* is increasingly centered around all issues of computer-related crime with a particularly strong influence on economic/industrial espionage. Intellectual property consists of concepts, ideas, planning documents, designs, formulae, and other information-based materials intended for products and/or services which have some commercial value or represent original thoughts or theses. Crime and ethical problems related to intellectual property can be divided into two categories...

1) Intellectual property with clear protection

   - Copyright
   - Trade Mark
   - Patent
   - Trade Secret

2) Intellectual property where protection can be debated

   - Non-protected research and development
   - Original concepts and ideas which have not yet been completed
   - Public domain information which has been modified with individual ideas and refinements

Intellectual property is increasingly being sought via industrial espionage because it tends to reflect a potentially valuable investment wherein lengthy

research and development efforts have been undertaken. Moreover, intellectual property that is in the process of long-term research is likely to be stored on computer media. These provide particular challenges for both protection and detection of theft.

ESPIONAGE TARGETS

Generally speaking, important targets of future espionage activities can be broken down into two broad categories...

1) *Formulae, processes, components, structure, characteristics, and applications of new technologies.* These include, but are not limited to...

   - Fifth generation computer architecture
   - New computer chip designs and conductivity including biochip research
   - Biotechnology
   - Supercomputing and superconductivity
   - Processing capability
   - Holographic and laser research applications and modeling
   - Fiber optics
   - Aerospace technologies
   - Research in petrochemicals
   - Advanced materials
   - Advanced biotechnology methods
   - Medical technologies for treatment, wellness, and prevention, including pharmaceuticals
   - Advanced communications technologies and processes
   - Advances in satellite utilization and space technologies and applications
   - Electromechanical products and technologies
   - Optics technology
   - Telecommunications equipment, protocols, and technologies
   - Advanced cellular and wireless telecommunications technologies
   - Chemical process technology
   - Software development
   - Developments in integrated circuits
   - Packaging technology
   - Integration of all technologies

2) *Factors associated with the marketing, production, and security of the new technologies.* These include, but are not limited to...

- New technology release dates
- Pricing information (wholesale and retail)
- Marketing research on anticipated demand for the technologies
- Marketing research on consumer profiles
- Products which are needed for compatibility and applicability
- Production time tables and product release dates
- Production quantities
- Market targets and schedules
- Overseas marketing plans
- Security equipment, sensors, and processes
- Electronic banking equipment, interfaces, and protocols
- Planned upgrade schedule for the technology
- Planned changes of directions for the technology (somewhat similar to planned obsolescence)
- Software developments particularly those which enhance new technologies, networking, and technological integration.

Beyond these broad categorical listings, future espionage targets can be defined in other, more explicit ways. Among them are...

- **Economic Targets**
  + Brokers
  + Bankers
  + Finance

- **Technology Targets**
  + Business
  + Research Institutes ("Think Tanks")
  + Universities
  + Laboratories

- **Agricultural Targets**
  + Commodity Bankers
  + Agricultural Cooperatives
  + Forecasters

- **Energy Exploration, Extraction, Processing and Use**
  + Oil
  + Gas
  + Goal
  + Nuclear
  + Solar
  + New Sources

- **National/International Agreements**
  + Sales and Trade
  + Exchanges
  + Cartels

METHODS FOR OBTAINING TARGETED INFORMATION

If we are concerned about what future espionage targets will be, then we must also be concerned about what methods will be used to acquire the information. Based on the research and interviews for this study, it appears many of the methods—in addition to unlawful computer-related access discussed previously—will be the same or similar as ones already experienced in both national security espionage and industrial/economic espionage. In that discussions of these methods are available from other sources, they are summarily listed below for reference...

- ☑ Open sources (For example: Freedom of Information Act—FOIA—requests submitted to NASA, the FDA, Commerce Department, Defense Department, the EPA, and Department of Energy in addition to published government documents; government bidding specifications; opened bids; and articles in technical journals.)

- ☑ Attempting to hire "consultants" from the targeted firms and industries seeking people who have "inside information" on the explicit espionage target. The consultation arrangement looks less sinister and appears to be a legitimate avenue for a professional to earn extra income (or at least an avenue easier for a person to rationalize their behavior).

- ☑ The use of "moles" (particularly by ethnic-related groups) whether they are professional employees or service employees working inside the industry. The "mole" will have unique access to information as a result of being "on the inside."

- ☑ Computer hacking and data transmission interruption.

- ☑ Compromising of employees, including blackmail and "set ups."

- ☑ Corrupting/bribing employees.

☑ Use of student researchers and university interns to gain access to research and technology (students from the sciences and marketing in particular).

☑ Surveillance and "snooping" around corporate employees including such things as listening to conversations in bars, going through trash, and similar activities.

☑ Signals interception and electronic eavesdropping, including...

- Intercepting communications
- Bugging
- Fax Interception
- Interception of communication
  - + Microwave
  - + Cellular
  - + Satellite
  - + Land line

☑ Burglary

☑ Use of janitorial and service-related personnel or businesses to gain access

☑ "Outsourcing"—the practice of contracting with individuals or companies to work on specific problems or elements of a new product. These people work for a wide range of companies and thus carry elements of the companies' secrets with them. Consequently, information will merge and move throughout the professional community as the contractors move. Foreign governments interested in industrial espionage can take advantage of this arrangement.

☑ Technologies and Techniques Which May Be Adapted to Serve as Detectors and Countermeasures for Espionage

- Image Acquisition Using Gamma Backscatter
- Magnetic Resonance Imaging
- Pulsed Echo Inspection
- Ultra-Trace Chemical Samples
- Extremely Compact Embeddable Multichannel Global Positioning System Receivers
- SAW (Surface Acoustic Wave) Sensor System for Identification of Substances
- Ion Mobile Spectrometry (IMS) for Substance Detection
- Visible and Near Infrared Reflectance

- Optical Immunosensor
- Panoramic Viewing Using a 3-D Line Scan Camera Technique
- Remote Detection of Trace Effluenting Resonance Raman Spectrometry
- Airborne Multispectral Scanner for Remote Sensing and Biomass Assessment of Substances
- Tempest Systems
- Real Time Multispectral Fusion for Wide Area Surveillance (WAS)
- Wide Area Acoustic Intrusion Alarm and Tracking System
- Micro-Miniature Radio Frequency Transmitters, receivers, and Recorders
- Electronic Tags
- Digital Microphone Array Systems

We must understand that while in the U.S. corporate trade secrets and the government remain as distinct entities, this is not the case with many other countries. Profitable businesses are viewed as important "natural resources" for a country and are therefore viewed as entities which need to have government attention and support, even through espionage. This fundamental difference in philosophy helps contribute to victimization of U.S. companies as well as the relative "hands off" attitude of government on these issues.

CHAPTER 5
MOTIVATIONS FOR ESPIONAGE

As noted previously, the primary purpose of this study was not to specifically articulate motivations for espionage, rather it sought to identify changes in the "espionage environment." As a natural outgrowth of this research, some motivational aspects emerged which warrant closer examination. There is a great deal of research available—the significant body of which was completed by PERSEREC—that empirically examines motivations. The current discussion is intended to give direction for motivations in light of the espionage trends which have been forecast.

Both national security and corporate security organizations have fundamental, yet diverse, responsibilities with respect to their role. These include...

- Prevention of theft and sabotage
- Investigation of losses and threats
- Protection of personnel
- Protection of assets
- Protecting the competitive position of the organization
- Damage control when a security breech has occurred
- Recovering losses
- Anticipating threats to security

One important dimension in achieving these is to understand how employees and others who may have critical access to the Crown Jewels may forsake loyalties and commit espionage.

THE FRAMEWORK FOR MOTIVATION

According to Wood and Wiskoff (1992), motivations for espionage have been...

- Money
- Ideology
- Disgruntlement/revenge
- Ingratiation
- Coercion
- Thrills/Self-Importance

Each case will involve an interaction of one or more factors, however, it appears the overwhelming motivation is *money*—increasingly so in recent years. As one illustration of this, the number of known spies recruited by foreign intelligence decreased, while volunteering increased dramatically, especially during the 1980s, with the volunteers clearly interested in financial gain (Wood and Wiskoff, 1992). Beyond the obvious monetary factor of increased "buying power" afforded by spying for profit, other factors have an important influence. For example...

- ☑ *With shifts toward economic espionage, profitability of spying increases.* The amounts of money which some people "earned" through espionage during the Cold War varied widely, with many payments being surprisingly small. One problem was that the value of information—such as military strategies, encryption codes, or equipment capabilities—was difficult for the spy to ascertain. However, with industrial/economic espionage, the explicit is profit-based. And while the person committing the theft may not know the exact value of the information which is being passed on, they *do* know it has value in the commercial marketplace and can thereby command a larger payment. In cases where the spy is a technical expert on the information being stolen, his/her knowledge of the uniqueness of the information will also help contribute to a larger fee.

- ☑ *Economic spying is not as repugnant as seeking traditional national security secrets.* The moral element of patriotic allegiance will always have some degree of influence on a person's decision of whether or not to spy. When selling national security secrets, a person knows they are tearing the fabric of our sovereignty as well as providing information which could lead to physical injury or death to others. In the case of economic spying, the most visible outcome—the ledger—has significantly less emotional impact; particularly when so many corporations are of a multinational nature. Consequently, it is easier to rationalize to oneself the act of industrial espionage.

- ☑ *It is emotionally easier to spy for a political ally than a political foe.* We know that governments and companies who seek economic intelligence include just as many, if not more, traditional political allies as it does political foes. There is always some degree of conscience in espionage with which the spy must reconcile. When the consumer of economic intelligence is viewed in the context of one which has traditionally been an ally to the United States, rationalization is, once again, easier.

☑ *Economic spying does not have the punitive ramifications that is found with political/military espionage.* The threat of punishment may be a preventive factor for some people who are attempting to decide whether or not to commit espionage. Since, generally speaking, the social condemnation of nearly all economic crimes, including industrial espionage, is significantly less than for political/military espionage, the punishment for those apprehended in economic crimes tends to be less harsh; many times being only a probated sentence. With the likelihood of more lenient punishment if caught coupled with the lower social condemnation of industrial espionage, the potential thief may decide that the potential benefits outweigh the risks.

Beyond money, per se, there are several key characteristics which contribute to a person committing espionage. These factors essentially relate to the "quality of life" people experience both at home and at work. Security threats may include...

☑ ...a person who is unhappy on the job in general.

☑ ...a person who is unhappy with their location of assignment, particularly if it is perceived to be "off the beaten path."

☑ ...a person who feels they have been overlooked for promotion or merit salary increases.

☑ ...a person who feels they have been overlooked for commendations and awards.

☑ ...a person who does not feel they have been compensated for their contribution to the organization.

☑ ...a person faced with personal financial difficulties or stresses.

☑ ...a person facing personal problems, particularly if they feel that the "way out" of the problem is to "escape" or that they may "buy their way out of the problem."

Supervisors, in particular, should be aware of these issues and be prepared for intervention should the manifestation of these factors become evident in employees. Other methods to deal with money and monetary-related motivations include...

- As part of employee psychological testing, diagnostic inquiries about people who are disproportionately motivated by materiality.
- Look for those who need money; particularly large sums of money in a short period of time which appears to be beyond one's current earning ability—e.g., Larry Wu-Tai Chin's gambling debt or Pollard's bankruptcy.
- Look for those people who seem to be almost desperately seeking a better or "upscale" lifestyle beyond simple upward mobility—i.e., always trying to win the lottery or trying "get rich quick" schemes)
- People who have no sense of corporate loyalty and or fail to subscribe to corporate values; a person who is somewhat of an "occupational sociopath."
- Develop an "Early Warning System" for disgruntled employees (no raises or pay grade advancements, no promotions, no choice of assignment, uncertainty about the draw down, any other factors that face an individual, particularly those where one cannot commiserate with others).

A Broader Perspective: The Tripartite Paradigm for Security Threats

In both the national security and corporate security environments, the threat paradigm has three fundamental elements...

- ☑ Motive
- ☑ Expertise
- ☑ Opportunity

Motive is the reason commits espionage; it is the moving force which prompts the idea to steal secrets and focuses attention on how the theft will occur. *Expertise* refers to the types of knowledge required to commit espionage and the ability to extract the intended information. It includes deciding what types of information are valuable, being able to select the most valuable information, and having the technical ability to access the information. In some cases this will require simply accessing a locked file, in other cases, more difficult security procedures must be compromised including, increasingly, computer access. *Opportunity* means that a person has access to critical information under circumstances wherein it can be stolen. The opportunity may be access as a result of one's work with the information or access as a result of collateral factors such as a custodian or service worker.

These three factors are not discrete or independent. Instead they are interactive, almost synergistic, in nature. That is, each factor "feeds" the other depending on a wide variety of internal and external factors. For policy analysis,

each of the three elements in the paradigm must be broken down into analytic stages...

- ☑ Stage 1: First know the espionage targets
- ☑ Stage 2: Establish controls for threats
- ☑ Stage 3: Institute contacts
- ☑ Stage 4: Revisit targets and threats

PROGRAMMATIC ELEMENTS RELATED TO PERSONNEL SECURITY

One way to operationalize the paradigm is to look at some basic assumptions of security supplemented with constructs related to this model. This permits a framework to implement policy related to the motive, expertise, and opportunity of security threats.

Assumption 1. To begin, the first assumption is somewhat cynical, relying on Douglas McGregor's Theory X of management only applied to the framework of personnel security. The assumption is that anyone will commit espionage. The questions are: What type of espionage will they commit? What kind of inducement is needed before they will commit espionage? How much inducement is needed before they will actually commit the act? While this assumption is largely inconsistent with current management philosophy, notably W. Edwards Demming's Total Quality Management (TQM), it is nonetheless a functional assumption which can be used to prevent espionage. Importantly, this should be viewed as an assumption of personnel security rather than management philosophy.

Assumption 2. The second assumption is that any employee who commits espionage is basically a thief—he/she "steals" information and "fences it" in a manner to meet his/her needs (i.e., a way to fulfill his/her motivations.) Those needs may be...

- Stealing for profit
- Stealing for food
- Stealing for sensation
- Stealing for arrogance
- Stealing for revenge (or "pay backs")

Importantly, this assumption views information and intellectual property as a commodity. Continuing with this line of thought, we must look for benchmark criteria which serve as critical elements in order to prevent espionage and the theft of corporate secrets. These benchmarks are...

☑ *Selection.* This refers to the recruitment and employment of personnel who have been screened for their substantive knowledge, competence, loyalty, psychological stability, and social stability. While selection is not fail-safe, it is an important beginning.

☑ *Training.* Beyond giving a new employee the substantive knowledge and procedures related to his/her new position, training can provide insights and threats related to security. Training should also include in-service sessions to present new information and reinforce security procedures.

☑ *Surveillance.* Maintaining control and observation of information which needs to be protected will decrease the likelihood of espionage. Surveillance not only includes observation but also sensor control of the information which reports whenever access to the information is made.

☑ *Supervision.* Supervisors must be vigilant to account for the behavior—and particularly changes in behavior—of personnel under their supervision. An alert supervisor may both identify when an employee has committed a security violation as well as perceive signs which could be the precursor of such violations if intervention does not occur.

☑ *Accountability.* Whereas surveillance refers to property or information control, accountability refers to control of individuals. Ensuring personnel are following procedures, performing efficiently and effectively, and adhering to organizational values will contribute greatly to continued personnel integrity.

☑ *Target Hardening.* Taking measures to protect information from being stolen will help reduce theft. Certain minimal efforts can be taken to generally improve security, however, the problem becomes one of balance. Determining the amount of money and effort to invest in protecting information must be balanced with the competing needs of "cost-benefits"—a process which sometimes pits security personnel versus research personnel versus marketing personnel versus management.

☑ *Positive Work Environment.* Having a good work environment, being supportive of one's place of work, and having a feeling of worth in the organization—a sense of ownership—will increase the employee's obligation and loyalty to the organization. As

these factors increase, the probability of espionage by employees will decrease.

- ☑ *Realistic Threat of Discipline for Wrong Doing.* Given the nature of information (and property) which is at issue in light of national security and economic intelligence, employees must also recognize that if they commit a security violation there is a realistic threat that they will be both identified and disciplined. Punishment must be swift and sure if it is going to have any significant preventive effect.

- ☑ *Positive Rewards.* Balancing the realistic threat of discipline is reinforcement of positive work and contributions to the organization. Supervisors and managers must provide a positive environment for work performed well by providing rewards, awards, and commendations. The spirit of cooperation is what should be engendered within the organization, not competition.

- ☑ *Reinforcement of Ethics and Values.* A statement of organizational values, reinforcement of ethical standards, and the obligations of professionalism must be engendered in all employees. At the least, all employees should subscribe to the most basic of all ethics—"Do no harm." This sense of moral obligation can be an important security precaution.

Collectively, these controls can help to (1) minimize opportunity; (2) channel expertise toward goals; and (3) help control motive. This perspective of treating information as a commodity is even more relevant as competitive intelligence becomes more dominant.

WHAT CAUSES SECURITY VIOLATIONS?—A SOCIAL-PSYCHOLOGICAL PERSPECTIVE

As espionage targets change, particularly with ideological issues becoming less prominent, there will be some shifting in the motivations for espionage. There is a strong body of research—notably sponsored by PERSEREC—which addresses these issues. For future threats, this research may need to be refocused into a different theoretical paradigm. The following is one model relying on social-psychological dynamics.

We seek simplicity in answers to difficult questions. Straight-forward, easily understood, intuitively acceptable explanations to problematic issues are easy to offer and accept. Unfortunately, experience has shown that most problems are more complex than they appear on the surface; consequently, the

solutions are also complex. Thus, suggestions that there is a single motivation for espionage is misleading. Rather, it is a complex social-psychological phenomenon with interacting variables which leads one to commit espionage against her/her government.

While these factors—which the author characterizes as stressors—do not "cause" espionage, per se. Problems arise when an employee begins to experience multiple stressors without a legitimate release mechanism. These stressors continue to accumulate until a release opportunity occurs. The employee's action may be either intentional or simply a reaction to circumstances. Regardless of the case, it results in misconduct. The critical factors are...

- *Social Isolation Stressors.* Included in this category are such factors as isolation from the community environment; authoritarianism; cynicism; and an occupationally-centric environmentally which mandates many aspects of one's work cannot be shared with others outside of the workplace because of their classified nature. A unique aura is socially attached to a classified work environment which isolates the employee from his/her family, neighbors, and extra-occupational friends. Being unable to talk about work except in a restrictive sense socially isolates the employee contributing to work-related stress. Related to this, the author would argue that working within a "classified environment" will increase levels of authoritarianism and cynicism, with these personality characteristics serving on a continuum which increases their effects as the employee becomes more immersed in a rigidly classified work environment.

- *Organizational Stressors.* These deal with all aspects of organizational life—both formal and informal. Specific stressors include administrative philosophy, peer pressure, poor role models, misdirected performance measures, the pressure for upward mobility, changing policies and procedures, job satisfaction, lack of training, specialization, morale, inadequate supervision and administrative control, internal organizational jealousies, and other factors which create conflict in organizational life.

- *Political Stressors.* Changing demands based on the evolving political philosophy of policy makers and fluctuations within the world political environment. These changes require adjustments in priority, processes, and targets. Ironically, it is most likely not the substantive nature of changing political mandates which create stress. Rather, it is the fact that

organizational change in processes and priorities alter the work environment in which the employee becomes both accustomed and comfortable. It is human nature to be dogmatic, thus any form of organizational change influenced by political processes will impose stress.

- *Functional Stressors.* These relate to the actual performance of one's duties and include role conflict, the use of discretion, the application of law and regulatory mandates, decision making responsibilities, and other operational activities one is called on to perform. The degree of stress will obviously vary between positions, but will nonetheless be present at all levels to some extent. If an employee does not have a good understanding of his/her responsibilities and is ill-prepared to handle them, stress will increase.

- *Personal Stressors.* These stressors are from an employee's off-duty life can clearly influence the way one performs on the job. These can include such things as family problems—illness, problems with children, marital stress, and so forth—or financial constraints. Personal problems cannot be left at home; they will inherently influence a person's daily behavior, including work decisions: such as the decision to steal secrets.

- *Physiological Stressors.* A change in one's physiology and general health may also affect an employee's decision-making, work performance, relationship with others, and general attitude about work ad one's employer. Fatigue from working extra duty time, the physiological impact of shift work, illnesses, and physiological responses to critical incidents (i.e., getting "pumped up" during a crisis) are all additional examples of this form of stress.

- *Psychological Stressors.* The impact of most of the other stressors will also contribute to psychological stress. Other factors include constant exposure to the changing political and organizational demands, the impact of resolving situations which have no definitive "right" or "wrong" answer, and internalization of fear or uncertainty about job-related responsibilities.

These stressors are not mutually exclusive. It is their interactive nature which lends support to their cumulative effect on employee behavior. As exposure to the stressors increase in both time and intensity without a control mechanism, the more the employee's self-control is eroded.

These stressors are further influenced by two important facets of the occupational culture which exist within the intelligence and defense communities. First is what might be called the *opportunity structure*. By the very nature of the national security environment and the need to have a security clearance for access to critical information, opportunity is afforded to individuals to obtain information which is critical, and thereby marketable. While safeguards are placed to minimize abuse of the opportunity structure—compartmentalization, supervision, duplicity—these safeguards are employed with variable controls, therefore lack reliability in their ability to protect information. Thus, the opportunity to steal secrets clearly exists if one develops the inclination.

A second aspect is what may be called the *invulnerability factor*. The knowledge of having free access to classified information, the ability to control that access to others, and the comparative rarity of people being discovered and prosecuted infers to the employee who decides to steal secrets that he/she is invulnerable to detection and apprehension. In fact, this feeling of invulnerability, I would argue, is what leads to increasing boldness on the thief's part which eventually arouses suspicions about their activities.

Of course, the control we rely the most on is self-policing to ensure employees adhere to their oath of office and subscribe to basic values of propriety. At a secondary level, we hope to minimize the potential for abusing one's access to information through the use of screening (i.e., clearances). A third level of security control is the threat of punishment—i.e., loss of job, criminal prosecutions—if an employee commits espionage. while these controls work for the bulk of employees, we know all too well, exceptions arise.

Program managers and administrators have the responsibility to employ administrative measures which can address the problems of espionage from both preventive and follow-up perspectives. Factors include...

- A clear statement of organizational philosophy and purpose; i.e., a corporate strategy
- Ethics and values
- Training
- Adequate supervision with regular training for supervisors
- An open personnel problem identification system supported by effective internal investigations
- Meaningful performance evaluations
- The availability of an Employee Assistance Program
- Clearly stated policies and procedures
- Trouble shooting and preventing programs

The inherent conclusion from these factors is that prevention of espionage goes beyond security practices and programming. It embodies the entire

management and human resource system of an organization in order to address the stressors. It is hypothesized that if these factors can be controlled through good management practice, including employment assistance resources, feeling of organizational loyalty, and "ownership" will be increased thereby minimizing the potential for one to commit espionage—even for money.

OTHER PREVENTIVE INITIATIVES

Beyond those concerns discussed above, there are other initiatives which may forestall some espionage motivations. Among them are...

- ☑ De-stigmatizing compromising situations; most notably homosexuality.

- ☑ Janitorial personnel and temporary workers, particularly those who have *access*, whether than be physical access to the facility or access to information, should have greater scrutiny and controls.

- ☑ Accountability and access controls should be particularly rigorous for temporary professionals—these individuals will have virtually no "ownership" in the organization's values and, as such, are more likely to pass on corporate secrets (whether for profit or through collateral work at other organizations.)

- ☑ Non-defense companies which are on developing technologies and applications need to develop a classification system for their intellectual property; couple this with a contractual agreement with employees at all levels related to liability (civil and criminal) for selling company secrets. The defense industry may give some guidance here.

- ☑ It may be reasonable to develop model legislation (criminal and civil liability) to deal with "classified" intellectual property in the non-defense industries.

- ☑ Corporations which may be targeted for economic espionage should place strict limitations—perhaps prohibiting—on outside consulting by employees.

- ☑ Careful evaluation of ethnic professionals, particularly those who are not U.S. citizens. This presents an unusual problem. Experience shows us that ethnic nationals have a greater tendency to commit espionage. However, being too restrictive

> to ethnic nationals also poses civil rights problems with respect to discrimination and equal protection. Because of immigration to the U.S. from a wide range of countries coupled with the increased social phenomenon in the United States where multiculturalism is emphasized, some employees may have a patriotic allegiance to another country.

While these issues are only peripherally related to the issues of this report, there relationship is worthy of note.

CHAPTER 6
SOME FINAL THOUGHTS

According to Tafoya (1990), any attempts to make projections about the future are limited in three significant ways:

- The future is neither fixed nor predetermined,
- The future is not predictable, and
- Individual choices and actions can influence and change the future.

In light of these factors, any forecasts are therefore probabilistic projections made with reference to known phenomenon and logical analysis of changing events, whether cosmopolitan or local in nature. Reasonable forecasts can be made about the future within parameters, however, these are subject to change by external events and/or events we manipulate. For example, we cannot conclusively state what future espionage threats will be faced by the United States, however, we can reasonably estimate them through an analysis of wide ranging economic, social, and political trends (what Tafoya refers to as ESP—clever!). If the trends indicate the probability of threats in a given area, we can then take steps to preclude, or minimize, the damage caused by such threats through various steps (policies) which "change the future."

A CRITICAL TOPIC: GIVING NEWLY LEARNED ECONOMIC/INDUSTRIAL SECRETS TO AMERICAN COMPANIES

The challenges are difficult. For example, consider the question: Should agencies of the U.S. intelligence community provide information related to foreign competing business to the American business sector? There are important issues which must be resolved to answer that question. They include issues which are...

- Ethical
- Legal
- Economic
- Strategic
- Political

These must be carefully examined and balanced for the "greater good"—it is not a dichotomous "yes/no" issue. The benchmark for "greater good" is the

national security of the United States; a benchmark by which measurement is difficult on matters related to international commerce. Moreover, decisions must be made in the context of the *future* environment, not within the constraints of today. To immediately respond "yes" or "no" is inappropriate because (1) the response is likely based on emotional "feeling" and (2) there has been insufficient study to determine the propriety of this in the long term. These factors are true for many questions on the future raised in this report.

At this point, the author does not support using our national security intelligence resources to commit espionage against other countries or corporations with foreign ownership. However, the author does not rule out this possibility as a future, legitimate role of the intelligence community, particularly in light of the "info-wars" observations made by futurist Alvin Toffler. As a country, we need to plan for this option. Careful consideration of how such operations would proceed as well as the conditions under which we would pursue economic intelligence. In essence, contingency plans should be researched and developed in the event that a point is reached where such operations are necessary for our national security.

Some of the issues which must be addressed in this planning include...

- ☑ What kind of intelligence resources would be most useful and in what application (e.g., human intelligence, remote sensing, signal intelligence).
- ☑ What limitations should be imposed.
- ☑ What are the domestic legal questions which must be resolved.
- ☑ What issues in international law might arise.
- ☑ What ethical issues must be considered.
- ☑ How are competitive intelligence targets defined.
- ☑ How is economic intelligence shared with U.S. companies.

BROAD-BASED INITIATIVES TO EXPLORE IN THE FUTURE

In order to provide better protection and more leverage to deal with industrial espionage cases, there are several broad-based goals which may considered in the future...

- ☑ Task force investigations of theft in the private sector, perhaps structured along the lines of the Organized Crime Drug Enforcement Task Forces (OCDETF).

- ☑ Develop more comprehensive and controllable trade agreements with other countries.

- ☑ Make industrial espionage a federal offense.

- ☑ Urge industry, particularly the non-defense high technology industries, to develop more comprehensive security controls.

- ☑ Provide greater regulatory protections for high-technology companies.

- ☑ Provide realistic oversight, guidance, and information concerning thefts of intellectual property, research, and technologies.

- ☑ Conduct research to explore new and innovative ways to both increase protection and investigate offenses.

- ☑ Creation of specific statutes preventing disclosure of proprietary data.

- ☑ "Tighten" security requirements of government contractors.

As a result of the research on the trends in espionage, we tend to have a pretty good picture of changes which are occurring in espionage targets. The biggest problems is that our *institutions* are not responding to this knowledge. That is, there is surprisingly little movement in the intelligence community, as well as the White House and Congress to make policy responses to these issues. From a personnel security issue at the outset, the initial response may sound somewhat simple, but is extremely difficult to attain—there needs to be a change in organizational culture with respect to *what* the crown jewels are; *who* has the knowledge to obtain or access the crown jewels, and *how* to best protect the crown jewels.

A change in organizational culture requires short term and long term responses with our ultimate goal of looking at the next *generation*, not just tomorrow. Much of this must begin with an educational process to ensure that everyone involved understands the issues, goals, needs, and processes in looking toward the future.

There are macro (policy, regulation, legislation) and micro (personnel training, awareness, supervision, control) issues involved. Significant change in the personnel security system is needed to meet changes in political and economic needs, thus the *macro* needs must be addressed, perhaps with the leadership of personnel security specialists.

Toffler (1990), in discussing the "info-wars" of the future, observed that it is inevitable that a "fusion of public and private intelligence" must occur. It is of paramount importance that we recognize this as a convention of policy for national security as we approach the millennium. It is time that a new corporate strategy in the intelligence community be developed. This includes new policy, new regulations, and new legislation. The need is not derived so much from the idea that strategic threats to national security have diminished, but that an even more ominous, less psychologically intimidating threat has emerged in the form of economic espionage. It is less visible and less coercive, but extraordinarily dangerous to our national security. It is like a virus attacking our economic and, consequently, social systems. It can destroy us from within but never fire a shot. It is incumbent that we develop a remedy to this virus in order to protect the Crown Jewels of American inventiveness: the ability to create technological innovations and apply computerization to a vast array of uses.

Perhaps the public health model to protecting our Crown Jewels is needed. We comprehensively define threats on a national basis which inherently includes private R&D work as well as trade secrets. Then we inoculate these resources by providing some measure of security assistance. The federal role would be one of leadership and resourcefulness. It would help identify those committing economic espionage to take precautions and prevention strategies.

If one says, "But that's not our role" or "That's not our responsibility," then I challenge you to think again and look to the future. Think geometrically and look at the changing socio-political and socio-economic global environment we now exist in—change is occurring rapidly in diverse directions. Our traditions must change to meet the techno-geo-economy of the future. We know the threats that are posed by economic espionage—information already gathered by both the intelligence community and corporate security professionals provide a strong argument. Make no mistake—the future threat is defined and crystal clear: Economic espionage by friends and foes alike.

BIBLIOGRAPHY

Andrano, Ralph and John J. Siegried. (eds.). (1980). *The Economics of Crime.* New York: John Wiley & Sons.

Aron, Leon. (1991). "The Russians Are Coming." *Policy Review.* (Fall):pp. 44—49.

Association of Former Intelligence Officers. (1993) "Industry Wants Counterintelligence, Not Economic Spying." *Periscope Newsletter.* Vol. 18, No. 2, p. 3.

Boren, David L. (1992) "The Intelligence Community: How Crucial?" *Foreign Affairs.* vol. 71, No. 3, pp. 52—62.

Borodin, Stanislav, D. (1990). "Crime Trends and Directions in the Criminal Policy of the USSR." *Soviet Criminology Update.* Rome, Italy: United Nations Interregional Crime and Justice Research Institute..

Bureau of Alcohol, Tobacco, and Firearms. (1989) *Jamaican Organized Crime.* (Unpublished mimeographed report.) Washington: BATF, Office of Law Enforcement, Intelligence Branch.

"Fifty Biggest Mafia Bosses." (1986). *Fortune International,* (No 23, November), pp. 20—32.

Center for the Study of Foreign Affairs. (1990). *Thinking About World Change.* Washington, DC: U.S. Department of State.

Colton, Kent W., et al. (1982). *Computer Crime: Electronic fund Transfer Systems and Crime.* Washington: Bureau of Justice Statistics.

Commission on Narcotic Drugs. (1990). *Development and Promotion of More Effective Action Against Illicit Drug Trafficking Through Regional Co-operation in Drug Law Enforcement.* Vienna, Austria: United Nations.

Commission on Narcotic Drugs. (1991). *Situation and Trends in Drug Abuse and Illicit Traffic.* Vienna, Austria: United Nations

Economic and Social Council. (1991a) *The World Economy at the End of 1990: Short-Term Prospects and Emerging Issues.* New York: United Nations.

Economic and Social Council. (1991b). *Impact of the Recent Evolution of the East-West Relations on the Growth of the World Economy, in Particular on the Economic Growth and Development of the developing countries, as Well as on International Economic Cooperation.* A report to the United Nations Secretary General. Geneva, Switzerland: United Nations.

Economic and Social Council. (1991c). *Report of the Commission on Narcotic Drugs on its Thirty-Fourth Session.* A report to the United Nations Economic and Social Council. Vienna, Austria: United Nations.

Eighth United Nations Congress on the Prevention of Crime and the Prevention Treatment of Offenders (UNCPC). (1990). *Effective National and International Action Against Organized Crime and Terrorist Criminal Activities.* Havana, Cuba: United Nations.

Executive Order 12333, *United States Intelligence Activities* (1981).

Florida Department of Law Enforcement. (1990). *Asian Organized Crime.* (Unpublished mimeographed report.) Tampa, FL: FDLE Intelligence Office, Tampa Division.

Fromkin, David. (1993) "The Coming Millennium: World Politics in the Twenty-First Century." *World Policy Journal.* (Spring), Vol. X, No. 1, pp. 1—8.

Gurov, Alexander I. (1990). "Issues Relating to Studies of the Criminal Career." *Soviet Criminology Update.* Rome, Italy: United Nations Interregional Crime and Justice Research Institute.

Heffernan, Richard J. (1991). "And the SPI Survey Says...." *Security Management.* (October), pp. 39—40.

Heuer, Richards J. (1992). *Achieving More With Less: An Ideal Continuing Evaluation Program.* A report prepared for the Central Intelligence Agency, Office of Security.

Heuer, Richards J. (1993). *Assessing Personnel Security Needs in the Post Cold War Era.* Draft Paper.

Holden, Richard and Allen Sapp. (1993) *Police: A Future of Utopia or Dystopia?.* Paper presented at the annual meeting of the Society of Police Futurists, International. (Baltimore, MD.)

Janssens, Edouard. (1989). "Surveillance and Security Agencies Transport of Money, Valuables, and Documents." Proceedings of the *XIIth International*

Course of Higher Specialization for Police Forces. International Centre of Sociological, Penal and Penitentiary Studies. Messina, Italy.

Johnson, Loch K. (1992-93) "Smart Intelligence." *Foreign Policy.* (Winter), Vol. 89, pp. 53—69.

Karchmer, Cliff. (1988). *Illegal Money Laundering.* Washington: Police Executive Research Forum.

Lee, Rensselaer W. and Scott B. MacDonald. (1993) "Drugs in the East." *Foreign Policy.* (Spring), No. 90, pp. 89—107.

Levenbach, Hans and James P. Cleary. (1984). *The Modern Forecaster: The Forecasting Process Through Data Analysis.* Belmont, CA: Lifetime Learning Publications.

Mack, John A. and Hans-Jürgen Kerner. (1975). *The Crime Industry.* Westmead, England: Saxon House, Ltd.

May, Ernest R. (1992) "Intelligence: Backing Into The Future." *Foreign Affairs.* Vol. 71, No. 3, pp. 63—72.

McGregor, Douglas (1960) *The Human Side of Enterprise.* New York, NY: McGraw Hill, Publisher.

Mead, Walter R. (1993) "An American Grand Strategy: The Quest for Order in a Disordered World." *World Policy Journal.* (Spring), Vol. X, No. 1, pp. 9—37.

Merritt, Giles. (1991) *Eastern Europe and the USSR: The Challenge of Freedom.* London, England: Euro Business Publishing Network.

National Institute of Justice. (1990). "Opening the Borders in the European Community: Perspectives on Internal Security." *International Summaries.* Washington, DC: U.S. Department of Justice, National Institute of Justice.

National Narcotic Intelligence Consumers Committee (NNICC). (1991). *The NNICC Report of 1990 Intelligence Data.* Washington, DC: Office of Intelligence, Drug Enforcement Administration.

Owen, Richard and Michael Dynes. (1990). *The Times guide to 1991: Britain Without Frontiers.* 2d ed. London, England: Times Books.

Savona, Ernesto Ugo. (1990). "Social Change, Organization of Crime and Criminal Justice Systems." *Essays on Crime and Development.* Rome, Italy: United Nations Interregional Crime and Justice Research Institute.

Schweizer, Peter. (1993) *Friendly Spies*. New York, NY: Atlantic Monthly Press.

Sessions, William B. (1991). "Counterintelligence Challenges in a Changing World." *FBI Law Enforcement Bulletin*. (September), pp. 1—4.

Sigurdson, Jon and Patricia Nelson. (1990) "Intelligence Gathering and Japan: The Elusive Role of Grey Intelligence." *International Journal of Intelligence and Counterintelligence*. Vol. 5, No. 1, pp. 17—34.

Stoll, Cliff. (1989). *The Cuckoo's Egg*. New York: Simon and Schuster.

Stone, Leroy. (1991). "I Spy A Myth." *Security Management*. (October), pp. 28—32.

Tafoya, William L. (1990) "Futures Research: Implications for Criminal Investigations." In J.N. Gilbert (ed.) *Criminal Investigation: Essays and Cases*. Columbus, OH: Merrill Publishing Company.

Thomas, Douglas. (1990). "Friendship Means More Intelligence Officers." *Global Reliance: A Publication of the U.S. Air Force, Office of Special Investigations*. (September/October), Vol. 16, No. 5: pp. 5—7.

Toffler, Alvin. (1971) *Future Shock*. New York, NY: Bantam Books.

Toffler, Alvin. (1981) *The Third Wave*. New York, NY: Bantam Books.

Toffler, Alvin. (1990). *PowerShift: Knowledge, Wealth and Violence in the 21st Century*. New York: Bantam Books.

Vlahos, Michael. (1990) *Thinking About World Change*. Washington, DC: Foreign Service Institute, U.S. Department of State.

von Lazar, Arpad. (1991). "Work and Unity: Germany the Morning After." *Harvard Business Review*. (March-April)pp. 32—44.

Wack, John P. and Lisa P. Camahan. (1989). *Computer Viruses and Related Threats*. Washington: U.S. Department of Commerce, National Institute of Standards and Technology.

Whitt, Darnell M. (1992). "Reform as Well as Retrenchment? Defense Management and the New World Order." *Comparative Strategy*. Vol 11, pp. 115—147.

Wirtz, James J. (1990) "Miscalculation, Surprise, and American Intelligence After the Cold War." *International Journal of Intelligence and Counterintelligence*. Vol. 5, No. 1, pp. 1—16.

Wood, Suzanne and Martin F. Wiskoff. (1992) *Americans Who Spied Against Their Country Since World War II*. Monterey, CA: PERSEREC.

Zvekic, Ugljesa. (1990). "Introductory Notes." *Essays on Crime and Development*. Rome, Italy: United Nations Interregional Crime and Justice Research Institute.