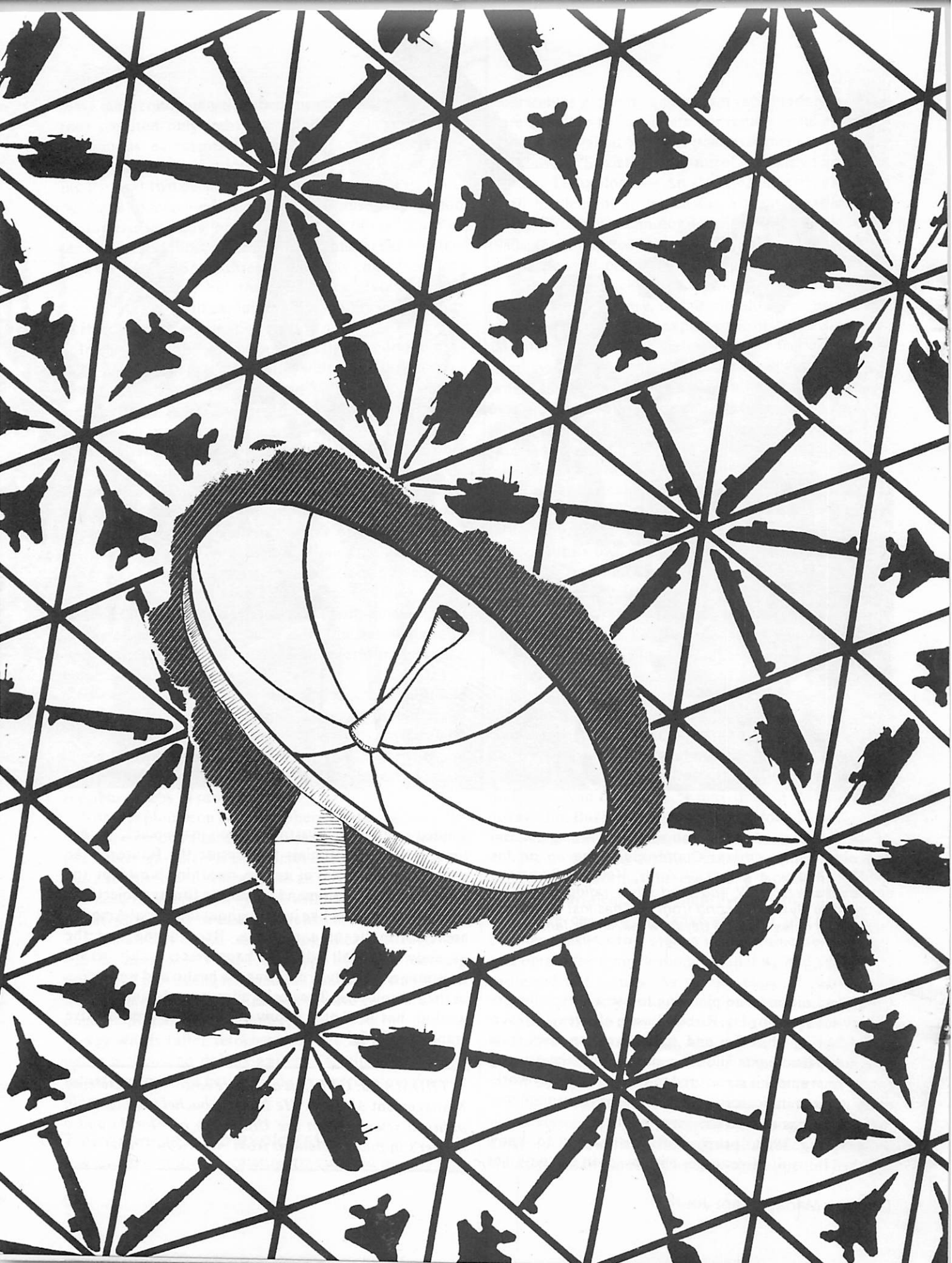
Defense Management Journal

Fourth Quarter 1986

Defense Logistics: A New Day Dawning



Information security: the hidden force multiplier

By NOEL D. MATCHETT

Loss of sensitive technological data compromises national security and wastes tax dollars; under the aegis of a major new program, defense officials are implementing cost-effective measures to safeguard such information.

In November 1983, concerned that foreign adversaries were intercepting and exploiting sensitive information about major weapon systems, Secretary of Defense Caspar W. Weinberger directed that a mechanism be developed to protect such information. In response, the director of the National Security Agency issued National Communications Security Instruction 6002 (June 1984), "Protection of Contractor Telecommunications," and the assistant secretary of defense (command, control, communications, and intelligence) signed DoD Instruction 5210.74, "Security of Defense Contractor Telecommunications," on June 26, 1985. The focus of attention now is the speed, effectiveness, and efficiency with which the Department of Defense and the contractor community can implement these new policies in the face of current budgetary constraints. This article outlines the origins of the issue and offers a rationale, strategies, and challenges to government and industry people directly affected by the program.

Information security in the context of the discussion below refers to telecommunications and computer security; it includes the protection of information during transmission as well as the security of critical data bases and processes. The difficulty inherent in determining the effectiveness of information security distinguishes it from physical and personnel security. As evidenced by recent espionage cases, good counterintelligence operations can produce a reasonably accurate picture of the effectiveness of personnel and physical security programs. Likewise, officials are frequently able to uncover thefts of classified and embargoed technology.

But an organization can assess the effectiveness of information protection measures (or the lack thereof) only with great difficulty. Exploitation of a communications system by intercepting plain text, for example, or breaking a cipher by means of a copied key may leave no trace whatsoever. Nor can one detect someone who is intercepting a signal being broadcast into the ether. And those who steal information in electronic form by copying a file typically leave no evidence unless extremely sophisticated audit trails and electronic logs are in place. Put simply, an organization often does not even know that a problem exists.

But more information is surfacing on the scope and effectiveness of foreign efforts to exploit U.S. telecommunications and computer systems. Despite the extreme precaution adversaries take to protect this type of intelligence, the body of knowledge dealing with the issue is steadily growing, and national policy is to share it as much as possible with those who need to understand it. The fundamental problem is that transmission and storage procedures threaten the integrity and privacy of militarily valuable information. A brief history of the growth of telecommunications will clarify the broader ramifications of this simple statement.

The vulnerability of technology

Until the 1950s, copper cable was the dominant long-haul medium. In the early years of that decade, micro-

ILLUSTRATION BY ERIC D. MATCHETT

wave radio communications became more cost-effective—they required only individual plots of real estate, not continuous easements—and as a result, tremendous growth in telecommunications capacity took place during the next two decades. However, microwave technology has also increased vulnerability because propagation characteristics allow people in the path of the transmitter's beam and those close to the antenna to easily intercept the signals. Some threats obviously come from foreign governments, but the electronics revolution has placed intercept and exploitation capability in the hands of the dedicated amateur as well.

In the 1970s, the great boom in satellite communications provided very high quality, wide-band service over broad areas of the country, and vulnerability became even greater. Why? Nearly all down-link beams from satellites carrying traffic between points in the United States cover the entire U.S. mainland as well as Cuba. Estimates indicate that as many as 1.5 million private citizens have antennas which directly access those satellite down-links. And only modest modifications are necessary to adapt a system capable of receiving commercial entertainment channels to one that can receive business and government communications as well. The cost of setting up a system to intercept satellites can be under $3,000. Though some satellites with time-division, multiple-access systems require more sophisticated equipment to exploit, access is still within a serious hobbyist's capabilities.

The push toward cellular radio has created additional vulnerabilities. Stories abound of the old mobile radio telephone system that was accessible to anyone who could operate a ham radio. While the frequencies are different, cellular radio systems today are just as interceptible dozens of miles away.

Nor is exploitation of unenciphered radio signals difficult. One needs an antenna, a receiver, and a demodulator. Other equipment is sometimes necessary to penetrate more sophisticated systems, but an adversary often does not need to intercept a system with the same degree of fidelity that a user or carrier requires in order to operate it. Even a noisy signal can yield significant intelligence. Furthermore, new VLSI technology is greatly reducing the cost of processing information, putting it well within home computer capabilities. Microwave receivers, low-noise amplifiers, and computers able to sort on the basis of key words (after reformatting) are all available for under a thousand dollars apiece. Certainly, cost alone would never deter a national adversary from intercepting these systems.

The damage from exploitation

The demand for information transmitted quickly and accurately is growing, and as that information becomes more valuable to legitimate consumers, it likewise becomes more valuable to our potential enemies. A recent publication, "Soviet Acquisition of Militarily Significant Western Technology — An Update," describes in great detail the lengths to which the Soviets go to acquire critical Western technology. In one case in the early 1980s, they budgeted more than $3 million for acquisition of a single semiconductor memory test system.

Admittedly, much illegal high-technology acquisition is due to theft, bribery, or unscrupulous companies and individuals who subvert export controls. However, critical information about state-of-the-art technology, defense systems and their capabilities, development approaches, design, and research continues to be available over unprotected communication systems and in ineffectively protected data bases. Easy access to that data provides an invaluable window into the technical heart of our systems for those who choose to look.

An adversary can reap tremendous benefits from this information in several areas. Advanced development information alone can save a nation millions, or even billions, of its own research and development dollars in acquiring a similar or improved product. It can also greatly hasten the date of initial operating capability and increase the effectiveness of countermeasures. Equally unsettling, the U.S. has paid for the system out of its own limited budget, only to receive greatly diminished return on its investment.

When an adversary obtains test results identifying strengths and weaknesses of a particular system prematurely, we also lose an important force multiplier — our adversaries' uncertainty about the system. The tank, plane, or ship may look the same to the program manager and user. And the operator may think it performs as it always did. But compared to a system for which information safeguards were adequate, its real value in the overall defense posture has declined sharply.

Advance information enables a hostile nation to develop equivalent or even improved systems much faster and more cheaply. An adversary can precisely tailor countermeasures to a system's most vulnerable features and obtain them much sooner than if we had adequately protected test results. As the secretary of defense has argued, a modest premium for good information security is well worth the cost because, spent wisely, it is highly leveraged money. In fact, the nation can ill afford to discount the defense budget by giving its adversaries an advantage due to inadequate information protection.

Estimates put the telecommunications component of a major system at 3 to 8 percent of the program's budget, and guidelines indicate that expenditures for satisfactory security initially amount to 10 percent of total telecom-

U.S. NAVY PHOTO

munications costs. Once designed into the system, the security component costs less than half that amount to operate. In other words, if telecommunications account for 5 percent of the budget on a major defense program, securing the entire program will add another half percent—10 percent of 5 percent — to the price tag. Operating the security system will cost even less and in effect create a force multiplier by ensuring that our adversaries remain uncertain about overall program technology and capabilities.

Progress to date

The first step taken to improve the nation's information security was to define the scope of the problem. The Defense Department was then able to quickly determine that many forms of communication were vulnerable — among them, voice, data, radio, satellite, and microwave — and that we needed a comprehensive strategy to deal with the problem. Developing that strategy has been an ongoing effort, as technology and our understanding of the issues and the threats have evolved. But the broad outlines became clear relatively early. A two-phased approach was in order: the backbone communication links first, followed by end-to-end security.

Rapid changes in the telecommunications industry forced a rethinking of the traditional philosophy governing security development. Officials concluded that to accomplish both bulk and end-to-end security, DoD would have to closely collaborate with the industry that is creating the telecommunications revolution. The government has to set security standards which industry will incorporate into its telecommunications and information-processing products. Additionally, the government must take a leading role in creating the market, for the approach will not work unless the government is willing to pay the legitimate costs of protection. Continued acceptance of nonsecure voice, data, and carrier systems by federal users only sends the wrong message and destroys the credibility necessary for the program to succeed.

National policy reflects the changing role of the government and of the National Security Agency in particular. Presidential Directive 24, signed by President Jimmy Carter in November 1977, recognized for the first time at the national level the importance of protecting unclassified sensitive information. Its replacement, National Security Decision Directive 145, signed by President Ronald Reagan in September 1984, significantly enhances the government's ability to help the defense, civil, and commercial sectors. It establishes a structure to deal comprehensively with a national problem. The secretary of defense, who is the executive agent, and the director of the National Security Agency, who is the national manager, now have the means to develop, disseminate, and utilize the necessary technology in the broad areas required.

Not all threats to information security are as elaborate — or as visible — as the Cosmonaut Yuri Gagarin, a Soviet vessel depicted here; some are available for modest sums of under a thousand dollars.

The strengthened charters are part of the market strategy. In addition, the secretary of defense has signed two documents, designated National Communications Security Committee-10 and -11, which require that government and contractor communications bearing sensitive information be protected. National Communications Security Instruction 6002, endorsed by the secretary in October 1984, enunciates policy concerned with funding, and DoD Instruction 5210.74, signed in June 1985, establishes a mechanism for incorporating costs into defense contracts. It answers the key question, "Who pays?"

While much remains to be done, various elements in the Defense Department have already taken steps to protect sensitive information. Thus, all communication services for which DoD contracts must consider security and, if certain criteria are present, include appropriate requirements in the request for proposals. The largest such program to date is the Defense Commercial Telecommunications Network, a billion-dollar, satellite-based communication system which has a circuit protection requirement. In addition, officials review all new contracts for protection requirements. The more than 80,000 current contracts administered by the department's commercial communications office are also reviewed at renewal.

One of the most dramatic responses to the challenge has come from the National Security Agency's communications security organization, now the directorate for information security. The agency recognized that the telecommunications revolution was creating new products within 2 to 5 years, rather than ten to twenty as before. As a result, old-style development and procurement processes were not responsive to the nondevelopmental telecommunications items and automatic data processing systems being used by the military and their contractors. The challenge was to broaden the base of security products and at the same time speed up their availability.

The National Security Agency therefore joined forces with major communications carriers and vendors to initiate several very successful programs. In one such effort, the data encryption standard endorsement program, the agency contributes cryptographic and system security expertise, while the carriers and vendors supply state-of-the-art telecommunications development and production capability. These companies are the very people creating the communications revolution. The success of the data encryption standard program and the development of a mutually beneficial approach to transferring sensitive security technology to firms holding appropriate clearances have become the foundation of a major new initiative, the commercial communications security endorsement program.

Under this program, qualified vendors develop products that meet government security specifications, but they target them to attractive market areas. The approach ultimately enables the government to obtain a broad range of technologies, products, and services that meet its needs, while industry is able to spin off products for the commercial, nongovernment market. The objective is to support the security needs of the private sector and at the same time reduce development costs for the more focused national security market.

Thanks to these programs, protected carrier service, plus 32 categories of equipment, each containing hundreds of models and endorsed by the data encryption standard program, as well as initial products developed under the commercial communications security endorsement program are now available to government and private industry. The *Information Security Bulletin* (formerly the *Telecommunications Protection Bulletin),* published by the National Security Agency's industrial relations staff, provides the contact points for industry representatives. A related initiative allows qualified users to directly purchase from authorized vendors secure voice and secure data cryptography to protect classified information. In addition, three competing vendors—AT&T, Motorola, and RCA—are developing an advanced, low-cost, secure voice terminal, scheduled to be available in 1987. The vendors' unique value-added features will give users a choice among models.

The commercial communications security endorsement program is also sponsoring an effort to embed security in various personal and mainframe computers, interfaces, networks, and terminals. Work is under way on standards needed to provide end-to-end cryptographic interoperability for key management, and products have begun to be available. For computer security, users can find a list of companion software and hardware in the *Evaluated Products List for Trusted Computer Systems,* put out by the National Security Agency's National Computer Security Center. Broad changes in handling and accounting rules for cryptographic products are also in progress; the objective is to maintain security control while allowing users greatly expanded access and utilization.

Program manager's role

How can a defense program manager benefit from these new tools and policies? Consider the government program manager. His or her task is to manage the program politically and technically, keep it on schedule and within budget, and ensure that it performs as required. Unauthorized disclosure of data related to the system's research, development, testing, capability, or

operational strategy discounts the program's value and renders the system less effective to those who operate and depend upon it.

For example, when the Soviets obtained documentation on just one item, the F18 fire control radar, they gained several major advantages:

- A baseline for airborne radar countermeasures to the F18.
- Technology for equipping the latest generation of Soviet fighters with state-of-the-art, lookdown-shootdown radar.
- A 5-year savings in development time.
- Savings of over $50 million in development costs.

The value of such information to our adversaries is obvious, and whether stolen from data bases, intercepted, or obtained by other means, it will be exploited. As more and more documentation is processed and stored in electronic form, threats to telecommunications and data bases will continue to grow.

Program personnel, both in government and industry, need up-to-date information about the threat to their programs and steps they can take to guard against it. Above all, program managers, who often are not telecommunications experts, must understand the value of information security to their program. Prudent protective measures increase the value of the system to the United States; consequently, secure communications are an essential part of the program. The cost of adequate information protection is modest, and such measures should be an absolute requirement of doing business. The force multiplier effect adds significant value to the program, and contractors need to work closely with government contracting officials to ensure mutual compliance and satisfaction.

National support is clearly present. At the October 1985 meeting of his National Security Telecommunications Advisory Committee, President Reagan specifically expressed concern about protecting information in our nation's telecommunications and computer systems from hostile intelligence threats. He asked the chief officers and company presidents who comprise the committee to devote energy and thought to those technologies and policies that will improve our national information security posture. The Defense Department and the National Security Agency stand ready to assist program managers in fulfilling the president's expressed intent.

Placing protection requirements in the request for proposals is the single most important action a government program manager can take. By requiring protection and paying for it, the government strongly signals its support to the industry which provides security technology. Such support is crucial. If contractors are to implement protection in a smart, aggressive manner, the government must hold up its end of the bargain by allowing legitimate costs. To penalize a contractor who puts in appropriate protective technology and incurs higher overhead costs as a result would be self-defeating.

Serious government interest in protection benefits the contractor and his program manager too. For the latter, the necessary support from corporate telecommunications, security, and automatic data processing is easier to obtain. The contractor can also better protect the company's communications and sensitive corporate data, both of which are increasingly the target of hostile intelligence services and competitors. The growing terrorist environment makes good security a prudent investment as well. Thus, the serendipitous benefits to a corporation can be significant when top company officials support those program managers who implement protective measures.

Auditors have a stake in this area too. Because information protection is relatively new and the Federal Acquisition Regulations are undergoing revision, the auditor's role is still taking shape. Start-up problems will be inevitable, and precedents must be established. But efforts can begin to move forward, even without every "i" dotted and every "t" crossed. Auditors, contractors, and the information security community must cooperate to ensure intelligent, accurate, fair, and fast implementation of national policy.

Solid foundations for a robust information security program are definitely in place, but hard work remains for both government and industry. Developing security technology that keeps pace with new computer and communication systems is an ongoing requirement. Additionally, we must agree upon cost-effective procedures for implementation, installation, and operation of the systems. Those contractors who have incorporated security systems early, in what is admittedly a transition period, must receive support. They can deliver better defense systems and should reap the benefits in competing for procurements. The ultimate payoff is a more efficient and effective national defense, made possible by secure information, the hidden force multiplier. DMJ

NOEL D. MATCHETT is president of Information Security Inc., which he founded in 1985. Prior to retiring from federal service, he was area executive and director of data network security at the National Security Agency, where he served for 19 years. Mr. Matchett earned a bachelor's degree from Haverford College and a master's degree in mathematics from Rutgers—The State University; he has also done extensive work in probability and operations research at the doctoral level.
