Counterintelligence Theory And Practice Security And Professional Intelligence Education Series

Counterintelligence Theory and PracticeThe Code of TrustNational Intelligence SystemsCurveballThwarting Enemies at Home and AbroadThe Man who Never wasNational Security IntelligenceNational, International, and Human SecurityIntelligence and Intelligence AnalysisFutureproofCyber WarfareCounterintelligence Theory and PracticeCases in Intelligence AnalysisHandbook of Scientific Methods of Inquiry for Intelligence AnalysisCyber-Security and Threat PoliticsDeceptionCounterintelligence Theory and PracticeThe Tao of Open Source IntelligenceThe End of IntelligenceINTELLIGENCE AND PRIVATE INVESTIGATIONTen Strategies of a World-Class Cybersecurity Operations CenterStrategic Security ManagementIntelligence and Surprise AttackInsider ThreatSecurity Education, Awareness, and TrainingThe Professional Protection OfficerCode Name Kindred SpiritThe Oxford Handbook of National Security IntelligenceGetting Agencies to Work TogetherSecurity Clearance Issues, Problems, Denials and RevocationsSecurityVaults, Mirrors, and MasksIntelligence ElsewhereTo Catch a SpyCounterintelligence Theory and PracticeScientific Methods of Inquiry for Intelligence AnalysisReasoning for Intelligence AnalystsAssessing the Tradecraft of Intelligence AnalysisEffective Physical SecurityConfronting the "Enemy Within"

Counterintelligence Theory and Practice

Ten Strategies of a World-Class Cyber Security Operations Center conveys MITRE's accumulated expertise on enterprise-grade computer network defense. It covers ten key qualities of leading Cyber Security Operations Centers (CSOCs), ranging from their structure and organization, to processes that best enable smooth operations, to approaches that extract maximum value from key CSOC technology investments. This book offers perspective and context for key decision points in structuring a CSOC, such as what capabilities to offer, how to architect large-scale data collection and analysis, and how to prepare the CSOC team for agile, threat-based response. If you manage, work in, or are standing up a CSOC, this book is for you. It is also available on MITRE's website, www.mitre.org.

The Code of Trust

A Classic in Counterintelligence—Now Back in Print Originally published in 1987, Thwarting Enemies at Home and Abroad is a unique primer that teaches the principles, strategy, and tradecraft of counterintelligence (CI). CI is often misunderstood and narrowly equated with security and catching spies, which are only part of the picture. As William R. Johnson explains, CI is the art of actively protecting secrets but also aggressively thwarting, penetrating, and deceiving hostile intelligence organizations to neutralize or even manipulate their operations. Johnson, a career CIA intelligence officer, lucidly presents the nuts and bolts of the business of counterintelligence and the characteristics that make a good CI officer. Although written during the late Cold War, this book continues to be useful for intelligence professionals, scholars, and students because the basic principles of CI

are largely timeless. General readers will enjoy the lively narrative and detailed descriptions of tradecraft that reveal the real world of intelligence and espionage. A new foreword by former CIA officer and noted author William Hood provides a contemporary perspective on this valuable book and its author.

National Intelligence Systems

Curveball

While many books have been written about private investigation, this text is different in that it does not deal with the subject from traditional perspectives. It examines how private investigation has grown, particularly since 9-11, into an exacting and sophisticated occupation. The book looks at the key issues in what it describes as private intelligence; that is, intelligence activities practiced by operatives other than law enforcement, national security, or the military. Eleven world experts contribute chapters addressing key practice issues concerning the skills, abilities, and knowledge necessary in the new realm of private intelligence. The initial three chapters provide a report on present-day private intelligence and offer an overview of the specifics of intelligence issues that follow. Eleven subsequent chapters take the reader progressively through various intelligence-related subjects. Major topics presented include: skills for intelligence-led private investigators, open source intelligence, target profiling, fraud intelligence, political intelligence, anti-terrorist and anti-gang intelligence, illicit organizations and financial intelligence, counterintelligence, clandestine communication methods, preparing a prosecution brief, legal issues for intelligence-led private investigators, and ethical issues for intelligence-led private investigators. Additionally, the text contains several features that will appeal to both students and instructors. These include a set of key terms and phrases, a number of study questions, and learning activities in each chapter. Written in a clear and concise style, the text provides a foundation of practical and useful information. It will be a most important and unique resource for undergraduate students in private investigation courses as well as intelligence practitioners and general readers interested in self-development study.

Thwarting Enemies at Home and Abroad

Cyber Warfare Techniques, Tactics and Tools for Security Practitioners provides a comprehensive look at how and why digital warfare is waged. This book explores the participants, battlefields, and the tools and techniques used during today's digital conflicts. The concepts discussed will give students of information security a better idea of how cyber conflicts are carried out now, how they will change in the future, and how to detect and defend against espionage, hacktivism, insider threats and non-state actors such as organized criminals and terrorists. Every one of our systems is under attack from multiple vectors - our defenses must be ready all the time and our alert systems must detect the threats every time. This book provides concrete examples and real-world guidance on how to identify and defend a network against malicious attacks. It considers relevant technical and factual information from an insider's point of view, as well as the ethics, laws and

consequences of cyber war and how computer criminal law may change as a result. Starting with a definition of cyber warfare, the book's 15 chapters discuss the following topics: the cyberspace battlefield; cyber doctrine; cyber warriors; logical, physical, and psychological weapons; computer network exploitation; computer network attack and defense; non-state actors in computer network operations; legal system impacts; ethics in cyber warfare; cyberspace challenges; and the future of cyber war. This book is a valuable resource to those involved in cyber warfare activities, including policymakers, penetration testers, security professionals, network and systems administrators, and college instructors. The information provided on cyber tactics and attacks can also be used to assist in developing improved and more efficient procedures and technical defenses. Managers will find the text useful in improving the overall risk management strategies for their organizations. Provides concrete examples and real-world guidance on how to identify and defend your network against malicious attacks Dives deeply into relevant technical and factual information from an insider's point of view Details the ethics, laws and consequences of cyber war and how computer criminal law may change as a result

The Man who Never was

The goal of Reasoning for Intelligence Analysts is to address the three distinct dimensions of an analyst's thinking: the person of the analyst (their traits), the processes they use (their techniques), and the problems they face (their targets). Based on a decade of academic research and university teaching in a program for aspiring intelligence analysts, this multidimensional approach will help the reader move beyond the traditional boundaries of accumulating knowledge or critical thinking with techniques to assess the unique targets of reasoning in the information age. This approach is not just a set of techniques, but covers all elements of reasoning by discussing the personal, procedural, and problem-specific aspects. It also addresses key challenges, such as uncertain data, irrelevant or misleading information, indeterminate outcomes, and significance for clients through an extensive examination of hypothesis development, causal analysis, futures exploration, and strategy assessment. Both critical and creative thinking, which are essential to reasoning in intelligence, are integrated throughout. Structured around independently readable chapters, this text offers a systematic approach to reasoning a long with an extensive toolkit that will serve the needs of both students and intelligence professionals.

National Security Intelligence

The United States is losing the counterintelligence war. Foreign intelligence services, particularly those of China, Russia, and Cuba, are recruiting spies in our midst and stealing our secrets and cutting-edge technologies. In To Catch a Spy: The Art of Counterintelligence, James M. Olson, former chief of CIA counterintelligence, offers a wake-up call for the American public and also a guide for how our country can do a better job of protecting its national security and trade secrets. Olson takes the reader into the arcane world of counterintelligence as he lived it during his thirty-year career in the CIA. After an overview of what the Chinese, Russian, and Cuban spy services are doing to the United States, Olson explains the nitty-gritty of the principles and methods of counterintelligence.

Readers will learn about specific aspects of counterintelligence such as running double-agent operations and surveillance. The book also analyzes twelve actual case studies to illustrate why people spy against their country, the tradecraft of counterintelligence, and where counterintelligence breaks down or succeeds. A “lessons learned” section follows each case study.

National, International, and Human Security

This book is the only one available on security training for all level of personnel. Currently, there are a handful of titles that cover guard forces and protection officers, but none that speak to security training for government, security, and non-security professionals. Chief Security Officers (CSO), security managers, and heads of security forces often have to design training programs themselves from scratch or rely on outside vendors and outside training companies to provide training which is often dry, stilted, and not always applicable to a specific corporate or government setting. "Security Education, Awareness and Training" addresses the theories of sound security training and awareness, then shows the reader how to put the theories into practice when developing or presenting any form of security education, training, motivation or awareness to organizational employees. Motivation is a key factor in how a trainer can make security essential to an organization and individual employees; it also speaks to the necessity of security and helps to shape policy and ways of making security inherent and "easy" for the employee to ensure a safe facility and working environment. Quite simply, there is no other book like this on the market today, and this one will be the one everyone turns to in order to learn and use for their own security programs. All three authors have at least 20 years each in one aspect of the security business or another, whether it be in program management, educational products, training, or research. But it should be added that, while working at the Department of Defense (DoD) Security Institute, we collaborated in developing and teaching an innovative course specifically for "security educators." The course attendees were individually tasked in their own organization to develop and execute educational security programs for their general employee populations. Usually they were starting from scratch rather than taking over from a previous security educator. Often these programs were described as "security awareness" programs, sometimes security education programs, an often security training. In those days the student clientele for the Security Educators" Seminar were drawn largely from industry and government agencies where the. These seminar attendees had many goals: safety, protection of proprietary information including protecting government and classified information, access control, coping with work-place violence, anti-terrorism, facility protection often a range of educational tasks rolled into the position description of a single person. What these professionals needed was not an understanding of security as we defined it, but skills and techniques for imparting awareness of vulnerabilities, threats, and consequences of ignorance; essential know-how to prevent bad things from happening; and strategies for enhancing motivations to do the right thing at the right time. We saw the central concept to be communication how to reach people, capture their attention, and ensure retention of essential information within security training programs. Over the years, there has always been the conflict between time, cost, and resources and the need for security awareness training. Now, it seems more corporations and government operations and facilities are willing to invest the time and money needed to properly train and

education employees. While technology and corporate dynamics have changed and developed, the need for security awareness training has remained, in fact, has never been greater. These fundamental issues of awareness, motivation, and communication have not changed, and the proposed book is the authors" attempt to fill such a need in security training. - Discusses how to establish and integrate a structured, internally consistent and coherent program from the ground up - Assess and analyze security program needs and audience and customize training accordingly - Numerous Appendices to help the security manager justify security spending on training initiatives - Notes in margins emphasize key points and make for easy reference in training preparation

Intelligence and Intelligence Analysis

Curveball answers the crucial question of the Iraq war: How and why was America’s intelligence so catastrophically wrong? In this dramatic and explosive book, award-winning Los Angeles Times reporter Bob Drogin delivers a narrative that takes us to Europe, the Middle East, and deep inside the CIA to find the truth–the truth about the lies and self-deception that led us into a military and political nightmare.

Futureproof

This book explores the political process behind the construction of cyber-threats as one of the quintessential security threats of modern times in the US. Myriam Dunn Cavelty posits that cyber-threats are definable by their unsubstantiated nature. Despite this, they have been propelled to the forefront of the political agenda. Using an innovative theoretical approach, this book examines how, under what conditions, by whom, for what reasons, and with what impact cyber-threats have been moved on to the political agenda. In particular, it analyses how governments have used threat frames, specific interpretive schemata about what counts as a threat or risk and how to respond to this threat. By approaching this subject from a security studies angle, this book closes a gap between practical and theoretical academic approaches. It also contributes to the more general debate about changing practices of national security and their implications for the international community.

Cyber Warfare

In their Second Edition of Cases in Intelligence Analysis: Structured Analytic Techniques in Action, accomplished instructors and intelligence practitioners Sarah Miller Beebe and Randolph H. Pherson offer robust, class-tested cases studies of events in foreign intelligence, counterintelligence, terrorism, homeland security, law enforcement, and decision-making support. Designed to give analysts-in-training an opportunity to apply structured analytic techniques and tackle real-life problems, each turnkey case delivers a captivating narrative, discussion questions, recommended readings, and a series of engaging analytic exercises.

Counterintelligence Theory and Practice

Spying, the “world’s second oldest profession,” is hardly limited to the traditional great power countries. Intelligence Elsewhere, nevertheless, is the first scholarly volume to deal exclusively with the comparative study of national intelligence outside of the anglosphere and European mainstream. Past studies of intelligence and counterintelligence have tended to focus on countries such as the United States, Great Britain, and Russia, as well as, to a lesser extent, Canada, Australia, France, and Germany. This volume examines the deep historical and cultural origins of intelligence in several countries of critical importance today: India, China, the Arab world, and indeed, Russia, the latter examined from a fresh perspective. The authors then delve into modern intelligence practice in countries with organizations significantly different from the mainstream: Iran, Pakistan, Japan, Finland, Sweden, Indonesia, Argentina, and Ghana. With contributions by leading intelligence experts for each country, the chapters give the reader important insights into intelligence culture, current practice, and security sector reform. As the world morphs into an increasingly multi-polar system, it is more important than ever to understand the national intelligence systems of rising powers and regional powers that differ significantly from those of the US, its NATO allies, and its traditional opponents. This fascinating book shines new light into intelligence practices in regions that, until now, have eluded our understanding.

Cases in Intelligence Analysis

With the exponential growth in the intelligence field in the last few years, the profession has grown much larger and its mission more complex. Government and private sector security agencies have recruited intelligence analysts to process what has become a voluminous amount of raw information flowing into these agencies' data collection systems. Unfortunately, there is an unmet need for analysts who are able to process these data. For this reason there are a growing number of colleges and universities that offer intelligence training so that candidates for analyst positions can take-up their duties without protracted on-the-job instruction. Handbook of Scientific Methods of Inquiry for Intelligence Analysis offers students in such courses a way of gaining the analytic skills essential to undertake intelligence work. This book acquaints students and analysts with how intelligence fits into the larger research framework. It covers not only the essentials of applied research but also explains the function, structure, and operational methods specifically involved in intelligence work. It looks at how analysts work with classified information in a security conscious environment, as well as obtaining data via covert methods. Students are left with little doubt about what intelligence is and how it is developed using scientific methods of inquiry.

Handbook of Scientific Methods of Inquiry for Intelligence Analysis

Cyber-Security and Threat Politics

A counterintelligence expert shows readers how to use trust to achieve anything in business and in life. Robin Dreeke is a 28-year veteran of federal service, including the United States Naval Academy, United States Marine Corps. He served most

recently as a senior agent in the FBI, with 20 years of experience. He was, until recently, the head of the Counterintelligence Behavioral Analysis Program, where his primary mission was to thwart the efforts of foreign spies, and to recruit American spies. His core approach in this mission was to inspire reasonable, well-founded trust among people who could provide valuable information. The Code of Trust is based on the system Dreeke devised, tested, and implemented during years of field work at the highest levels of national security. Applying his system first to himself, he rose up through federal law enforcement, and then taught his system to law enforcement and military officials throughout the country, and later to private sector clients. The Code of Trust has since elevated executives to leadership, and changed the culture of entire companies, making them happier and more productive, as morale soared. Inspiring trust is not a trick, nor is it an arcane art. It’s an important, character-building endeavor that requires only a sincere desire to be helpful and sensitive, and the ambition to be more successful at work and at home. The Code of Trust is based on 5 simple principles: 1) Suspend Your Ego 2) Be Nonjudgmental 3) Honor Reason 4) Validate Others 5) Be Generous To be successful with this system, a reader needs only the willingness to spend eight to ten hours learning a method of trust-building that took Robin Dreeke almost a lifetime to create.

Deception

Strategic Security Management, Second Edition provides security leadership and decision-makers with a fresh perspective on threat, vulnerability, and risk assessment. The book offers a framework to look at applying security analysis and theory into practice for effective security program, implementation, management and evaluation. Chapters examine metric-based security resource allocation of countermeasures, including security procedures, utilization of personnel, and electronic measures. The new edition is fully updated to reflect the latest industry best-practices and includes contributions from security industry leaders—based on their years of professional experience—including Norman Bates, Robert Emery, Jack Follis, Steve Kaufer, Andrew Rubin, Michael Silva, and Ken Wheatley. Strategic Security Management, Second Edition will be a welcome addition to the security literature for all security professionals, security managers, and criminal justice students interested in understanding foundational security principles and their application.

Counterintelligence Theory and Practice

A series of investigations, especially in Great Britain and the United States, have focused attention on the performance of national intelligence services. At the same time, terrorism and a broad span of trans-national security challenges has highlighted the crucial role of intelligence. This book takes stock of the underlying intellectual sub-structure of intelligence. For intelligence, as for other areas of policy, serious intellectual inquiry is the basis for improving the performance of real-world institutions. The volume explores intelligence from an intellectual perspective, not an organizational one. Instead the book identifies themes that run through these applications, such as the lack of comprehensive theories, the unclear relations between providers and users of intelligence, and the predominance of bureaucratic organizations driven by collection. A key element is

the development, or rather non-development, of intelligence toward an established set of methods and standards and, above all, an ongoing scientific discourse.

The Tao of Open Source Intelligence

Since the September 11, 2001, terrorist attacks, critics have charged that the Federal Bureau of Investigation, while qualified to investigate terrorist incidents after the fact, is not well equipped enough to adequately gather and assess information to prevent attacks. More intrinsically, many believe that given a predominant and deeply rooted law enforcement and prosecutorial culture, the bureau may not be able to change operational focus toward dedicated counterterrorism intelligence gathering and analysis. To better inform debate, researchers analyzed the domestic security structures of four allied countries--the United Kingdom, France, Canada, and Australia--weighing both their positive and negative aspects. (PW/PC)

The End of Intelligence

Since 9/11, the needs of intelligence agencies as well as the missions they conduct have increased in number, size, and complexity. This expanded and updated edition offers a way of gaining the analytic skills essential to undertake intelligence work. It acquaints students and analysts with how intelligence fits into the larger research framework, covering not only the essentials of applied research, but also the function, structure, and operational methods specifically involved in intelligence work. It looks at how analysts work with classified information in a security conscious environment as well as obtain data via covert methods.

INTELLIGENCE AND PRIVATE INVESTIGATION

OSINT is a rapidly evolving approach to intelligence collection, and its wide application makes it a useful methodology for numerous practices, including within the criminal investigation community.The Tao of Open Source Intelligence is your guide to the cutting edge of this information collection capability.

Ten Strategies of a World-Class Cybersecurity Operations Center

Counterintelligence Theory and Practice explores issues relating to national security, military, law enforcement, and corporate, as well as private affairs. Hank Prunckun uses his own experience as a counterintelligence professional to provide both a theoretical base and practical explanations for counterintelligence.

Strategic Security Management

Decision makers matching wits with an adversary want intelligence—good, relevant information to help them win. Intelligence can gain these advantages through directed research and analysis, agile collection, and the timely use of guile and theft. Counterintelligence is the art and practice of defeating these endeavors. Its purpose is the same as that of positive intelligence—to gain advantage—but it

does so by exploiting, disrupting, denying, or manipulating the intelligence activities of others. The tools of counterintelligence include security systems, deception, and disguise: vaults, mirrors, and masks. In one indispensable volume, top practitioners and scholars in the field explain the importance of counterintelligence today and explore the causes of—and practical solutions for—U.S. counterintelligence weaknesses. These experts stress the importance of developing a sound strategic vision in order to improve U.S. counterintelligence and emphasize the challenges posed by technological change, confused purposes, political culture, and bureaucratic rigidity. Vaults, Mirrors, and Masks skillfully reveals that robust counterintelligence is vital to ensuring America's security. Published in cooperation with the Center for Peace and Security Studies and the George T. Kalaris Memorial Fund, Edmund A. Walsh School of Foreign Service, Georgetown University.

Intelligence and Surprise Attack

Effective Physical Security, Fifth Edition is a best-practices compendium that details the essential elements and latest developments in physical security protection. This new edition is completely updated, with new chapters carefully selected from the author’s work that set the standard. This book contains important coverage of environmental design, security surveys, locks, lighting, and CCTV, the latest ISO standards for risk assessment and risk management, physical security planning, network systems infrastructure, and environmental design. Provides detailed coverage of physical security in an easily accessible format Presents information that should be required reading for ASIS International’s Physical Security Professional (PSP) certification Incorporates expert contributors in the field of physical security, while maintaining a consistent flow and style Serves the needs of multiple audiences, as both a textbook and professional desk reference Blends theory and practice, with a specific focus on today’s global business and societal environment, and the associated security, safety, and asset protection challenges Includes useful information on the various and many aids appearing in the book Features terminology, references, websites, appendices to chapters, and checklists

Insider Threat

This clear and concise new edition offers a comprehensive comparison of national, international, and human security concepts and policies. Laura Neack skillfully argues that security remains elusive because of a centuries-old ethic insisting that states are the primary and most important international actors, that they can rely ultimately only on themselves for protection, and that they must keep all options on the table for national security. This is particularly apparent with the increase in “glocalized” terrorism and the forced migration of millions of people. Although security as a concept can be widened to encompass almost any aspect of existence, Neack focuses especially on security from physical violence. Case studies throughout bring life to the concepts. New cases in this revised edition include the Syrian refugee crisis and the responses from European states, the growth and reach of jihadist terrorist groups and the unilateral and multilateral military actions taken to confront them, drug trafficking organizations and the Mexican government’s failure to protect citizens, the overt use of preventive war

by major and regional powers and the increasing American reliance on drone warfare, multilateral "train-and-assist" operations aimed at peacekeeping and counterterrorism in Africa, UN civilian protection mandates in Libya and Côte d'Ivoire and their absence in Syria, and how terrorism and refugee crises are intimately connected. The first edition of this book was published under the title Elusive Security: States First, People Last in 2007.

Security Education, Awareness, and Training

Using espionage as a test case, The End of Intelligence criticizes claims that the recent information revolution has weakened the state, revolutionized warfare, and changed the balance of power between states and non-state actors—and it assesses the potential for realizing any hopes we might have for reforming intelligence and espionage. Examining espionage, counterintelligence, and covert action, the book argues that, contrary to prevailing views, the information revolution is increasing the power of states relative to non-state actors and threatening privacy more than secrecy. Arguing that intelligence organizations may be taken as the paradigmatic organizations of the information age, author David Tucker shows the limits of information gathering and analysis even in these organizations, where failures at self-knowledge point to broader limits on human knowledge—even in our supposed age of transparency. He argues that, in this complex context, both intuitive judgment and morality remain as important as ever and undervalued by those arguing for the transformative effects of information. This book will challenge what we think we know about the power of information and the state, and about the likely twenty-first century fate of secrecy and privacy.

The Professional Protection Officer

Designed for university students in the burgeoning field of intelligence studies and professional training classes, Counterintelligence Theory and Practice provides all the elements required for a successful counterintelligence operation. Exploring issues relating to national security, military, law enforcement, as well as corporate private affairs, Hank Prunckun uses his experience as a professional to explain both the theoretical basis and practical application for real counterintelligence craft. Each chapter contains key words and phrases and a number of study questions and learning activities that make the book a comprehensive tool for learning how to be a counterintelligence professional.

Code Name Kindred Spirit

Collaboration between government agencies, an old joke goes, is an unnatural act committed by nonconsenting adults. Eugene Bardach argues that today's opinion climate favoring more results-oriented government makes collaboration a lot more natural--though it is still far from easy. In this book, Bardach diagnoses the difficulties, explains how they are sometimes overcome, and offers practical ideas for public managers, advocates, and others interested in developing interagency collaborative networks. Bardach provides examples from diverse policy areas, including children, youth, and family services; welfare-to-work; antipollution enforcement; fire prevention; and ecosystem management.

The Oxford Handbook of National Security Intelligence

The former director of intelligence at the U.S. Department of Energy describes the investigation that focused on Los Alamos scientist Wen Ho Lee, who was suspected of giving nulcear warhead secrets to the Chinese.

Getting Agencies to Work Together

National security intelligence is a vast, complex, and important topic, made doubly hard for citizens to understand because of the thick veils of secrecy that surround it. In the second edition of his definitive introduction to the field, leading intelligence expert Loch K. Johnson guides readers skilfully through this shadowy side of government. Drawing on over forty years of experience studying intelligence agencies and their activities, he explains the three primary missions of intelligence: information collection and analysis, counterintelligence, and covert action, before moving on to explore the wider dilemmas posed by the existence of secret government organizations in open, democratic societies. Recent developments including the controversial leaks by the American intelligence official Edward J. Snowden, the U.S. Senate's Torture Report, and the ongoing debate over the use of drones are explored alongside difficult questions such as why intelligence agencies inevitably make mistakes in assessing world events; why some intelligence officers choose to engage in treason against their own country on behalf of foreign regimes; and how spy agencies can succumb to scandals -including highly intrusive surveillance against the very citizens they are meant to protect. Comprehensively revised and updated throughout, National Security Intelligence is tailor-made to meet the interests of students and general readers who care about how nations shield themselves against threats through the establishment of intelligence organizations, and how they strive for safeguards to prevent the misuse of this secret power.

Security Clearance Issues, Problems, Denials and Revocations

Two schools of thought now exist in security studies: traditionalists want to restrict the subject to politico-military issues; while wideners want to extend it to the economic, societal and environmental sectors. This book sets out a comprehensive statement of the new security studies, establishing the case for the broader agenda.

Security

This book tracks post 9/11 developments in national security and policing intelligence and their relevance to new emerging areas of intelligence practice such as: corrections, biosecurity, private industry and regulatory environments. Developments are explored thematically across three broad sections: applying intelligence understanding structures developing a discipline. Issues explored include: understanding intelligence models; the strategic management challenges of intelligence; intelligence capacity building; and the ethical dimensions of intelligence practice. Using case studies collected from wide-ranging interviews with leaders, managers and intelligence practitioners from a range of practice

areas in Australia, Canada, New Zealand, the UK and US, the book indentifies examples of good practice across countries and agencies that may be relevant to other settings. Uniquely bringing together significant theoretical and practical developments in a sample of traditional and emerging areas of intelligence, this book provides readers with a more holistic and inter-disciplinary perspective on the evolving intelligence field across several different practice contexts. Intelligence and Intelligence Analysis will be relevant to a broad audience including intelligence practitioners and managers working across all fields of intelligence (national security, policing, private industry and emerging areas) as well as students taking courses in policing and intelligence analysis.

Vaults, Mirrors, and Masks

The Oxford Handbook of National Security Intelligence is a state-of-the-art work on intelligence and national security. Edited by Loch Johnson, one of the world's leading authorities on the subject, the handbook examines the topic in full, beginning with an examination of the major theories of intelligence. It then shifts its focus to how intelligence agencies operate, how they collect information from around the world, the problems that come with transforming "raw" information into credible analysis, and the difficulties in disseminating intelligence to policymakers. It also considers the balance between secrecy and public accountability, and the ethical dilemmas that covert and counterintelligence operations routinely present to intelligence agencies. Throughout, contributors factor in broader historical and political contexts that are integral to understanding how intelligence agencies function in our information-dominated age. The book is organized into the following sections: theories and methods of intelligence studies; historical background; the collection and processing of intelligence; the analysis and production of intelligence; the challenges of intelligence dissemination; counterintelligence and counterterrorism; covert action; intelligence and accountability; and strategic intelligence in other nations.

Intelligence Elsewhere

Insider Threat: Detection, Mitigation, Deterrence and Prevention presents a set of solutions to address the increase in cases of insider threat. This includes espionage, embezzlement, sabotage, fraud, intellectual property theft, and research and development theft from current or former employees. This book outlines a step-by-step path for developing an insider threat program within any organization, focusing on management and employee engagement, as well as ethical, legal, and privacy concerns. In addition, it includes tactics on how to collect, correlate, and visualize potential risk indicators into a seamless system for protecting an organization’s critical assets from malicious, complacent, and ignorant insiders. Insider Threat presents robust mitigation strategies that will interrupt the forward motion of a potential insider who intends to do harm to a company or its employees, as well as an understanding of supply chain risk and cyber security, as they relate to insider threat. Offers an ideal resource for executives and managers who want the latest information available on protecting their organization’s assets from this growing threat Shows how departments across an entire organization can bring disparate, but related, information together to promote the early identification of insider threats Provides an in-depth explanation

of mitigating supply chain risk Outlines progressive approaches to cyber security

To Catch a Spy

Security Clearance Issues, Problems, Denials and Revocations (If you have a security clearance with no issues, then you don't need this book. If, however, you are worried about any aspect of your security clearance, then you absolutely need this book!) Attorney Ronald C. Sykstus first started handling security clearance matters as a prosecutor in the United States Army. Subsequent to that, he defended active-duty soldiers and officers who were having their clearances revoked. He has continued his security clearance defense practice as a civilian lawyer since he left the United States Army with an honorable discharge. Ron is very aware of the importance of having a security clearance for obtaining meaningful and well-compensated employment, both within the government and in the private contracting industry. This book covers all aspects of the security clearance. It is especially geared toward people who not only run into problems with their existing security clearance, but also for those who have concerns about getting a security clearance and making sure that their clearance or job is not jeopardized down the road. This book addresses people's concerns at all phases of the security clearance process, and it does so in a way that makes sense and is easy to understand.

Counterintelligence Theory and Practice

Counterintelligence Theory and Practice explores issues relating to national security, military, law enforcement, and corporate, as well as private affairs. Hank Prunckun uses his own experience as a counterintelligence professional to provide both a theoretical base and practical explanations for counterintelligence.

Scientific Methods of Inquiry for Intelligence Analysis

Security is a defining characteristic of our age and the driving force behind the management of collective political, economic, and social life. Directed at safeguarding society against future peril, security is often thought of as the hard infrastructures and invisible technologies assumed to deliver it: walls, turnstiles, CCTV cameras, digital encryption, and the like. The contributors to Futureproof redirect this focus, showing how security is a sensory domain shaped by affect and image as much as rules and rationalities. They examine security as it is lived and felt in domains as varied as real estate listings, active-shooter drills, border crossings, landslide maps, gang graffiti, and museum exhibits to theorize how security regimes are expressed through aesthetic forms. Taking a global perspective with studies ranging from Jamaica to Jakarta and Colombia to the U.S.-Mexico border, Futureproof expands our understanding of the security practices, infrastructures, and technologies that pervade everyday life. Contributors. Victoria Bernal, Jon Carter, Alexandra Demshock, Zaire Z. Dinzey-Flores, Didier Fassin, D. Asher Ghertner, Daniel M. Goldstein, Rachel Hall, Rivke Jaffe, Ieva Jusionyte, Catherine Lutz, Alejandra Leal Martínez, Hudson McFann, Limor Samimian-Darash, AbdouMaliq Simone, Austin Zeiderman

Reasoning for Intelligence Analysts

How can the United States avoid a future surprise attack on the scale of 9/11 or Pearl Harbor, in an era when such devastating attacks can come not only from nation states, but also from terrorist groups or cyber enemies? Intelligence and Surprise Attack examines why surprise attacks often succeed even though, in most cases, warnings had been available beforehand. Erik J. Dahl challenges the conventional wisdom about intelligence failure, which holds that attacks succeed because important warnings get lost amid noise or because intelligence officials lack the imagination and collaboration to “connect the dots” of available information. Comparing cases of intelligence failure with intelligence success, Dahl finds that the key to success is not more imagination or better analysis, but better acquisition of precise, tactical-level intelligence combined with the presence of decision makers who are willing to listen to and act on the warnings they receive from their intelligence staff. The book offers a new understanding of classic cases of conventional and terrorist attacks such as Pearl Harbor, the Battle of Midway, and the bombings of US embassies in Kenya and Tanzania. The book also presents a comprehensive analysis of the intelligence picture before the 9/11 attacks, making use of new information available since the publication of the 9/11 Commission Report and challenging some of that report’s findings.

Assessing the Tradecraft of Intelligence Analysis

This report assesses intelligence analysis across the main U.S. intelligence agencies and makes a number of recommendations, some of which parallel initiatives that have begun in the wake of the December 2004 legislation, for instance, create a Deputy Director of National Intelligence as a focal point for analysis, establish a National Intelligence University, build a Long Term Analysis Unit at the National Intelligence Council, and form an Open Source Center for making more creative use of open-source materials.

Effective Physical Security

"The chapters on the exercises are a treasure chest of material to work with, covering a whole array of scenarios. . . . I think virtually every page and topic could spark robust and spirited classroom discussion starting with the text title itself." —Ronald W. Vardy, University of Houston "Most students have very little or no background [in this subject area], so Clark’s work is great to introduce students to intelligence and the analytical disciplines . . . a really excellent book that fills a gaping hole in the public literature and is of genuinely great value to both students and practitioners." —Carl A. Wege, Professor Emeritus, College of Coastal Georgia Bridging the divide between theory and practice, Deception: Counterdeception and Counterintelligence provides a thorough overview of the principles of deception and its uses in intelligence operations. This masterful guide focuses on practical training in deception for both operational planners and intelligence analysts using a case-based approach. Authors Robert M. Clark and William L. Mitchell draw from years of professional experience to offer a fresh approach to the roles played by information technologies such as social media. By reading and working through the exercises in this text, operations planners will learn how to build and conduct a

deception campaign, and intelligence analysts will develop the ability to recognize deception and support deception campaigns. Key Features New channels for deception, such as social media, are explored to show readers how to conduct and detect deception activities through information technology. Multichannel deception across the political, military, economic, social, infrastructure, and information domains provides readers with insight into the variety of ways deception can be used as an instrument for gaining advantage in conflict. Contemporary and historical cases simulate real-world raw intelligence and provide readers with opportunities to use theory to create a successful deception operation. A series of practical exercises encourages students to think critically about each situation. The exercises have several possible answers, and conflicting raw material is designed to lead readers to different answers depending on how the reader evaluates the material. Individual and team assignments offer instructors the flexibility to proceed through the exercises in any order and assign exercises based on what works best for the classroom setup.

Confronting the "Enemy Within"

Eight previous iterations of this text have proven to be highly regarded and considered the definitive training guide and instructional text for first-line security officers in both the private and public sectors. The material included in the newest version covers all the subjects essential to the training of protection officers. This valuable resource and its predecessors have been utilized worldwide by the International Foundation for Protection Officers since 1988, as the core curriculum for the Certified Protection Officer (CPO) Program. The Professional Protection Officer: Practical Security Strategies and Emerging Trends provides critical updates and fresh guidance, as well as diagrams and illustrations; all have been tailored to the training and certification needs of today’s protection professionals. Offers trainers and trainees all new learning aids designed to reflect the most current information and to support and reinforce professional development Written by a cross-disciplinary contributor team consisting of top experts in their respective fields