Situational Sense Basic Threat Detection Using Situational Awareness And Common Sense

Human Performance and Situation Awareness MeasuresSituation Awareness Analysis and MeasurementField Trials of Health InterventionsHarbour Protection Through Data Fusion TechnologiesHidden SuccessIntroduction to Statistical Methods for BiosurveillanceCyber Situational AwarenessStatistics in a NutshellThe Owner's Role in Project Risk ManagementGlobal Infectious Disease Surveillance and DetectionCyberspace Safety and SecurityNetwork Security Through Data AnalysisSituational Awareness 101: Because What You Don't Know, Can Hurt You!Occupational Health and Safety in the Care and Use of Nonhuman PrimatesHow Smart Workers Use Situational Awareness to Improve SafetyBio-inspired Materials and Sensing SystemsModeling Human and Organizational BehaviorTen Strategies of a World-Class Cybersecurity Operations CenterFear ItselfThe CERT Guide to Insider ThreatsTerrorismNetwork Intrusion DetectionManaging epidemicsCrisis ManagementSituational SenseInfrared Technology XXIGray ManCan I See your HandsCybersecurity and Resilience in the ArcticAdaptive Cruise ControlSAR-Tracking Log BookCombatting Cybercrime and CyberterrorismNetwork Design and ManagementTactical Display for SoldiersTheory and Models for Cyber Situation AwarenessSmart Metering Technology and ServicesGoing GrayHandbook of Loss Prevention and Crime PreventionInsider Threats in Cyber SecurityS. A. F. E. Situational Awareness for Employees

Human Performance and Situation Awareness Measures

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.

Situation Awareness Analysis and Measurement

The Safe Training Program(TM) empowers you with the skills to establish behavior baselines in any setting, then proactively observe for anomalous behavior that could indicate threat. Whether you're trying to prevent workplace violence or spot indicators of insider threat; the S.A.F.E Training Program(TM) will empower your workforce to take ownership of their own security and of those around them.

Field Trials of Health Interventions

This book examines the human factors issues associated with the development, testing, and implementation of helmet-mounted display technology in the 21st Century Land Warrior System. Because the framework of analysis is soldier performance with the system in the full range of environments and missions, the book discusses both the military context and the characteristics of the infantry soldiers who will use the system. The major issues covered include the positive and negative effects of such a display on the local and global situation awareness of the individual soldier, an analysis of the visual and psychomotor factors associated with each design feature, design considerations for

auditory displays, and physical sources of stress and the implications of the display for affecting the soldier's workload. The book proposes an innovative approach to research and testing based on a three-stage strategy that begins in the laboratory, moves to controlled field studies, and culminates in operational testing.

Harbour Protection Through Data Fusion Technologies

Insider Threats in Cyber Security is a cutting edge text presenting IT and non-IT facets of insider threats together. This volume brings together a critical mass of well-established worldwide researchers, and provides a unique multidisciplinary overview. Monica van Huystee, Senior Policy Advisor at MCI, Ontario, Canada comments "The book will be a must read, so of course I'll need a copy." Insider Threats in Cyber Security covers all aspects of insider threats, from motivation to mitigation. It includes how to monitor insider threats (and what to monitor for), how to mitigate insider threats, and related topics and case studies. Insider Threats in Cyber Security is intended for a professional audience composed of the military, government policy makers and banking; financing companies focusing on the Secure Cyberspace industry. This book is also suitable for advanced-level students and researchers in computer science as a secondary text or reference book.

Hidden Success

Introduction to Statistical Methods for Biosurveillance

The title of this book: CAN I SEE YOUR HANDS refers to one of the key outcomes of this book--being able to tell whether or not people want to cause us harm. To put it very simply, if you can see someone's hands and they are not concealing them, holding a weapon or positioning to strike you, one's levels of trust and confidence can increase. This simple example can serve as a reminder to all of us in many of the complex moments we have to deal with, and difficult decisions we have to make, in everyday life.

Cyber Situational Awareness

Effective risk management is essential for the success of large projects built and operated by the Department of Energy (DOE), particularly for the one-of-a-kind projects that characterize much of its mission. To enhance DOEâ€™s risk management efforts, the department asked the NRC to prepare a summary of the most effective practices used by leading owner organizations. The studyâ€™s primary objective was to provide DOE project managers with a basic understanding of both the project ownerâ€™s risk management role and effective oversight of those risk management activities delegated to contractors.

Statistics in a Nutshell

Original edition published under title: Human performance measures handbook.

The Owner's Role in Project Risk Management

Motivation for the Book This book seeks to establish the state of the art in the cyber situational awareness area and to set the course for future research. A multidisciplinary group of leading researchers from cyber security, cognitive science, and decision science areas elab orate on the fundamental

challenges facing the research community and identify promising solution paths. Today, when a security incident occurs, the top three questions security admin istrators would ask are in essence: What has happened? Why did it happen? What should I do? Answers to the ?rst two questions form the core of Cyber Situational Awareness. Whether the last question can be satisfactorily answered is greatly de pendent upon the cyber situational awareness capability of an enterprise. A variety of computer and network security research topics (especially some sys tems security topics) belong to or touch the scope of Cyber Situational Awareness. However, the Cyber Situational Awareness capability of an enterprise is still very limited for several reasons: • Inaccurate and incomplete vulnerability analysis, intrusion detection, and foren sics. • Lack of capability to monitor certain microscopic system/attack behavior. • Limited capability to transform/fuse/distill information into cyber intelligence. • Limited capability to handle uncertainty. • Existing system designs are not very “friendly” to Cyber Situational Awareness.

Global Infectious Disease Surveillance and Detection

Situational Awareness 101 is fifty chapters designed to raise your level of "awareness" and teach both the average and the well educated person a wide diversity of skills that can be put into everyday use. From one chapter to the next it takes your mind to places you don't want to go, (without being mentally prepared.) The subject matter in this book addresses many real life scenarios and (rewires) the mind on how to avoid, prepare, and respond to an unusual array of situations and circumstances we're faced with in our everyday lives. What you can expect from reading this book is; Increased and Heightened Awareness of Your Surroundings. Avoidance, Detection, Preparedness, and Confidence Skill Levels Increased How to Respond Instead of React When Emergencies Arise. Why repetition is also predictable and why that can be a very bad thing. The safest rooms to stay in at hotels/motels. The number one thing that can ruin any trip no matter where you're at. How to turn the odds in your favor in many real life case scenarios. And many more real life scenarios.

Cyberspace Safety and Security

"While the public health philosophy of the 20th Century -- emphasizing prevention -- is ideal for addressing natural disease outbreaks, it is not sufficient to confront 21st Century threats where adversaries may use biological weapons agents as part of along-term campaign of aggression and terror. Health care providers and public health officers are among our first lines of defense. Therefore, we are building on the progress of the past three years to further improve the preparedness of our public health and medical systems to address current and future BW [biological warfare] threats and to respond with greater speed and flexibility to multiple or repetitive attacks." Homeland Security Presidential Directive 21 Bioterrorism is not a new threat in the 21st century -- thousands of years ago the plague and other contagious diseases were used in warfare -- but today the potential for catastrophic outcomes is greater than it has ever been. To address this threat, the medical and public health communities are putting various measures in place, including systems designed to pro-actively mon- itor populations for possible disease outbreaks"--Provided by publisher.

Network Security Through Data Analysis

Situational Awareness 101: Because What You Don't Know, Can Hurt You!

This book is a training aid and reference for intrusion detection analysts. While the authors refer to research and theory, they focus their attention on providing practical information. New to this edition is coverage of packet dissection, IP datagram fields, forensics, and snort filters.

Occupational Health and Safety in the Care and Use of Nonhuman Primates

Traditional intrusion detection and logfile analysis are no longer enough to protect today's complex networks. In this practical guide, security researcher Michael Collins shows you several techniques and tools for collecting and analyzing network traffic datasets. You'll understand how your network is used, and what actions are necessary to protect and improve it. Divided into three sections, this book examines the process of collecting and organizing data, various tools for analysis, and several different analytic scenarios and techniques. It's ideal for network administrators and operational security analysts familiar with scripting. Explore network, host, and service sensors for capturing security data Store data traffic with relational databases, graph databases, Redis, and Hadoop Use SiLK, the R language, and other tools for analysis and visualization Detect unusual phenomena through Exploratory Data Analysis (EDA) Identify significant structures in networks with graph analysis Determine the traffic that's crossing service ports in a network Examine traffic volume and behavior to spot DDoS and database raids Get a step-by-step process for network mapping and inventory

How Smart Workers Use Situational Awareness to Improve Safety

Today, when a security incident happens, the top three questions a cyber operation center would ask are: What has happened? Why did it happen? What should I do? Answers to the first two questions form the core of Cyber Situation Awareness (SA). Whether the last question can be satisfactorily addressed is largely dependent upon the cyber situation awareness capability of an enterprise. The goal of this book is to present a summary of recent research advances in the development of highly desirable Cyber Situation Awareness capabilities. The 8 invited full papers presented in this volume are organized around the following topics: computer-aided human centric cyber situation awareness; computer and information science aspects of the recent advances in cyber situation awareness; learning and decision making aspects of the recent advances in cyber situation awareness; cognitive science aspects of the recent advances in cyber situation awareness

Bio-inspired Materials and Sensing Systems

An Advanced Research Workshop (ARW) "Data Fusion Technologies for Harbour Protection" was held in Tallinn, Estonia 27 June–1 July, 2005. This workshop was organized by request of the NATO Security Through Science Programme and the Defence Investment Division. An ARW is one of many types of funded group support mechanisms established by the NATO Science Committee to contribute to the critical assessment of existing knowledge on new important topics, to identify directions for future research, and to promote close working relationships between scientists from different countries and with different professional experiences. The NATO Science Committee was approved at a meeting of the Heads of Government of the Alliance in December 1957, subsequent to the 1956 recommendation of "Three Wise Men" – Foreign Ministers Lange (Norway), Martino (Italy) and Pearson (Canada) on Non-Military Cooperation in NATO. The NATO Science Committee established the NATO Science Programme in 1958 to encourage and support scientific collaboration between individual scientists and to foster scientific development in its member states. In 1999, following the end of the Cold War, the Science Programme was transformed so that support is now devoted to collaboration between Partner-country and NATO-country scientists or to contributing towards research support in Partner countries. Since 2004, the Science Programme was further modified to focus exclusively on NATO Priority Research Topics (i. e. Defence Against Terrorism or Countering Other Threats to Security) and also preferably on a Partner country priority area.

Modeling Human and Organizational Behavior

Crisis management is an interdisciplinary subject field represented by theoretical problems, practical activity, people management and the art of crisis situation solving. Overall, the studies that this publication contains are to provide an overview of the state of the art mainly focused on crisis management cycle represented by certain phases and steps. Topics include also lessons learned from natural and man-made disasters, crisis communication, information systems in crisis management, civil protection and economics in crisis management. We hope that chapters of this book will provide useful information within crisis management issue for a wide audience.

Ten Strategies of a World-Class Cybersecurity Operations Center

Can scientists and engineers replicate Nature and develop systems that operate in extreme environments? Bio-inspiration is an established concept which is developing to meet the needs of the many challenges we face particularly in defence and security. This book explores the potential of bio-inspired materials and sensing systems together with examples of how they are being implemented. It is not an exhaustive study of the subject but provides an overview of how bio-inspired or -derived approaches can be used to enhance components, systems and systems of systems for defence and security applications. Readers will gain an awareness of the complexity and versatility of bio-inspired components as well as an understanding of how these technologies can be applied in a variety of operational scenarios. Consideration is given to using a conceptual model that can be deployed in distributed or autonomous operations. Using this model, bio-inspiration with behavioural science plays a major role in identification, movement, searching strategies and pattern recognition for chemical and biological detection. Examples focus on both learning new things from nature that have application to the defence and security areas and adapting known discoveries for practical use by these communities. This graduate level monograph provides an increased awareness of the need for more sophisticated, networked sensors and systems in the defence and security communities and will be of interest to both specialists in this area and science and technology generalists -- Back cover.

Fear Itself

The Gray Man is the antithesis of individual expression. He hides in the corners of conformity. He only flaunts a quotidian nature. He meanders through the mundane and occupies the ordinary. Individual expression and exceptionalism are his enemies. The Gray Man is the forgettable face, the ghost guy, the hidden human. Implementing the concepts is more than looking less tactical, less hostile, or less threatening. It is the willful abandonment of anything and everything that defines oneself as different. Using his unique "S" word conceptual approach featured in Appear to Vanish, camouflage and concealment expert Matthew Dermody discusses the concepts, tactics and mindset necessary to assimilate into any urban environment. From the safety-conscious international traveler to the SERE contingencies of the deep cover foreign operative, GRAY MAN is the definitive urban concealment resource.

The CERT Guide to Insider Threats

This book comprises an authoritative and accessible edited collection of chapters of substantial practical and operational value. For the very first time, it provides security practitioners with a trusted reference and resource designed to guide them through the complexities and operational challenges associated with the management of contemporary and emerging cybercrime and cyberterrorism (CC/CT) issues. Benefiting from the input of three major European Commission funded projects the book's content is enriched with case studies, explanations of strategic responses and contextual information providing the theoretical underpinning required for the clear interpretation and application of cyber law, policy and

practice, this unique volume helps to consolidate the increasing role and responsibility of society as a whole, including law enforcement agencies (LEAs), the private sector and academia, to tackle CC/CT. This new contribution to CC/CT knowledge follows a multi-disciplinary philosophy supported by leading experts across academia, private industry and government agencies. This volume goes well beyond the guidance of LEAs, academia and private sector policy documents and doctrine manuals by considering CC/CT challenges in a wider practical and operational context. It juxtaposes practical experience and, where appropriate, policy guidance, with academic commentaries to reflect upon and illustrate the complexity of cyber ecosystem ensuring that all security practitioners are better informed and prepared to carry out their CC/CT responsibilities to protect the citizens they serve.

Terrorism

Early detection is essential to the control of emerging, reemerging, and novel infectious diseases, whether naturally occurring or intentionally introduced. Containing the spread of such diseases in a profoundly interconnected world requires active vigilance for signs of an outbreak, rapid recognition of its presence, and diagnosis of its microbial cause, in addition to strategies and resources for an appropriate and efficient response. Although these actions are often viewed in terms of human public health, they also challenge the plant and animal health communities. Surveillance, defined as "the continual scrutiny of all aspects of occurrence and spread of a disease that are pertinent to effective control", involves the "systematic collection, analysis, interpretation, and dissemination of health data." Disease detection and diagnosis is the act of discovering a novel, emerging, or reemerging disease or disease event and identifying its cause. Diagnosis is "the cornerstone of effective disease control and prevention efforts, including surveillance." Disease surveillance and detection relies heavily on the astute individual: the clinician, veterinarian, plant pathologist, farmer, livestock manager, or agricultural extension agent who notices something unusual, atypical, or suspicious and brings this discovery in a timely way to the attention of an appropriate representative of human public health, veterinary medicine, or agriculture. Most developed countries have the ability to detect and diagnose human, animal, and plant diseases. Global Infectious Disease Surveillance and Detection: Assessing the Challenges -- Finding Solutions, Workshop Summary is part of a 10 book series and summarizes the recommendations and presentations of the workshop.

Network Intrusion Detection

A clear and concise introduction and reference for anyone new to the subject of statistics.

Managing epidemics

Crisis Management

Use this log book to record information regarding the search and recovery of lost/missing persons, fleeing suspects, and escaped felons. A useful law enforcement aid for annotating evidence during the course of a pursuit.

Situational Sense

Despite the technological advances, improved policing and security methods, and attempts to create safety through policy and legislation, the world is filled with danger and dangerous people. The choice to ignore these dangers or place misguided faith in a promised utopia puts you at greater risk. Your need

to pay attention to your surroundings and use common sense/critical thinking skills has never diminished. It will be even more important as American society grows more polarized. Using his insightful and easy-to-understand "S" word alliteration conceptual method and expounding upon the topic first introduced in Gray Man: Camouflage for Crowds, Cities, and Civil Crisis, Matthew Dermody breaks down the important elements of threat identification and response necessary for personal safety. SITUATIONAL SENSE is the perfect primer for travelers, college students, or anyone else wanting to identify threats before the need for assistance becomes a life or death situation. While threats can manifest with several uncertain or unpredictable variables, this book will help you identify conditions and scenarios in order to avoid many life-threatening encounters.

Infrared Technology XXI

The two volumes LNCS 11982 and 11983 constitute the proceedings of the 11th International Symposium on Cyberspace Safety and Security, CSS 2019, held in Guangzhou, China, in December 2019. The 61 full papers and 40 short papers presented were carefully reviewed and selected from 235 submissions. The papers cover a broad range of topics in the field of cyberspace safety and security, such as authentication, access control, availability, integrity, privacy, confidentiality, dependability and sustainability issues of cyberspace. They are organized in the following topical sections: network security; system security; information security; privacy preservation; machine learning and security; cyberspace safety; big data and security; and cloud and security;

Gray Man

"An extensive collection of significant documents covering all major and minor issues and events regarding terrorism. Government reports, executive orders, speeches, court proceedings, and position papers are presented in full text reprint"--Oceana Website.

Can I See your Hands

The Handbook of Loss Prevention and Crime Prevention, 5th Edition, is a trusted foundation for security professionals just entering the field and a reference for seasoned professionals. This book provides a comprehensive overview of current approaches to security and crime prevention, tools and technologies to put these approaches into action, and information on a wide range of specific areas within the field of physical security. These include school and campus security, cargo security, access control, the increasingly violent healthcare security environment, and prevention or mitigation of terrorism and natural disasters. * Covers every important topic in the field, including the latest on wireless security applications, data analysis and visualization, situational crime prevention, and global security standards and compliance issues * Required reading for the certification DHS selected for its infrastructure security professionals * Each chapter is contributed by a top security professional with subject-matter expertise

Cybersecurity and Resilience in the Arctic

An antidote to the culture of fear that dominates modern life From moral panics about immigration and gun control to anxiety about terrorism and natural disasters, Americans live in a culture of fear. While fear is typically discussed in emotional or poetic terms—as the opposite of courage, or as an obstacle to be overcome—it nevertheless has very real consequences in everyday life. Persistent fear negatively effects individuals’ decision-making abilities and causes anxiety, depression, and poor physical health. Further, fear harms communities and society by corroding social trust and civic engagement. Yet

politicians often effectively leverage fears to garner votes and companies routinely market unnecessary products that promise protection from imagined or exaggerated harms. Drawing on five years of data from the Chapman Survey of American Fears—which canvasses a random, national sample of adults about a broad range of fears—Fear Itself offers new insights into what people are afraid of and how fear affects their lives. The authors also draw on participant observation with Doomsday preppers and conspiracy theorists to provide fascinating narratives about subcultures of fear. Fear Itself is a novel, wide-ranging study of the social consequences of fear, ultimately suggesting that there is good reason to be afraid of fear itself.

Adaptive Cruise Control

Since 2001, the CERT® Insider Threat Center at Carnegie Mellon University's Software Engineering Institute (SEI) has collected and analyzed information about more than seven hundred insider cyber crimes, ranging from national security espionage to theft of trade secrets. The CERT® Guide to Insider Threats describes CERT's findings in practical terms, offering specific guidance and countermeasures that can be immediately applied by executives, managers, security officers, and operational staff within any private, government, or military organization. The authors systematically address attacks by all types of malicious insiders, including current and former employees, contractors, business partners, outsourcers, and even cloud-computing vendors. They cover all major types of insider cyber crime: IT sabotage, intellectual property theft, and fraud. For each, they present a crime profile describing how the crime tends to evolve over time, as well as motivations, attack methods, organizational issues, and precursor warnings that could have helped the organization prevent the incident or detect it earlier. Beyond identifying crucial patterns of suspicious behavior, the authors present concrete defensive measures for protecting both systems and data. This book also conveys the big picture of the insider threat problem over time: the complex interactions and unintended consequences of existing policies, practices, technology, insider mindsets, and organizational culture. Most important, it offers actionable recommendations for the entire organization, from executive management and board members to IT, data owners, HR, and legal departments. With this book, you will find out how to Identify hidden signs of insider IT sabotage, theft of sensitive information, and fraud Recognize insider threats throughout the software development life cycle Use advanced threat controls to resist attacks by both technical and nontechnical insiders Increase the effectiveness of existing technical security tools by enhancing rules, configurations, and associated business processes Prepare for unusual insider attacks, including attacks linked to organized crime or the Internet underground By implementing this book's security practices, you will be incorporating protection mechanisms designed to resist the vast majority of malicious insider attacks.

SAR-Tracking Log Book

Simulations are widely used in the military for training personnel, analyzing proposed equipment, and rehearsing missions, and these simulations need realistic models of human behavior. This book draws together a wide variety of theoretical and applied research in human behavior modeling that can be considered for use in those simulations. It covers behavior at the individual, unit, and command level. At the individual soldier level, the topics covered include attention, learning, memory, decisionmaking, perception, situation awareness, and planning. At the unit level, the focus is on command and control. The book provides short-, medium-, and long-term goals for research and development of more realistic models of human behavior.

Combatting Cybercrime and Cyberterrorism

The three-dimensional ghillie suit is the ultimate in personal camouflage. No other concealment technique or camouflage clothing pattern compares with its effectiveness. Detailed instructions summarize the different suit types and construction methods in this easy, step-by-step guide. A great resource for those interested in military and police snipercraft, hunting, paintball/airsoft, or wildlife photography. The ghillie suit provides the camouflage and concealment edge that produces resultswith hidden success!

Network Design and Management

Before new interventions can be used in disease control programmes, it is essential that they are carefully evaluated in "field trials", which may be complex and expensive undertakings. Descriptions of the detailed procedures and methods used in trials that have been conducted in the past have generally not been published. As a consequence, those planning such trials have few guidelines available and little access to previously accumulated knowledge. In this book the practical issues of trial design and conduct are discussed fully and in sufficient detail for the text to be used as a "toolbox" by field investigators. The toolbox has now been extensively tested through use of the first two editions and this third edition is a comprehensive revision, incorporating the many developments that have taken place with respect to trials since 1996 and involving more than 30 contributors. Most of the chapters have been extensively revised and 7 new chapters have been added.

Tactical Display for Soldiers

This manual provides concise and up-to-date knowledge on 15 infectious diseases that have the potential to become international threats and tips on how to respond to each of them. The 21st century has already been marked by major epidemics. Old diseases - cholera the plague and yellow fever - have returned and new ones have emerged - SARS pandemic influenza MERS Ebola and Zika. These epidemics and their impact on global public health have convinced the world s governments of the need for a collective and coordinated defense against emerging public health threats and accelerated the revision of the International Health Regulations (2005) entered into force in 2007. Another Ebola epidemic another plague epidemic or a new influenza pandemic are not mere probabilities the threat is real. Whether transmitted by mosquitoes other insects via contact with animals or person-to-person the only major uncertainty is when and where they or a new but equally lethal epidemic will emerge. These diseases all have the potential to spread internationally highlighting the importance of immediate and coordinated response. The diseases covered are: Ebola virus disease Lassa fever Crimean-Congo haemorrhagic fever yellow fever Zika Chikungunya avian and other zoonotic influenza seasonal influenza pandemic influenza Middle-East respiratory syndrome (MERS) cholera monkeypox the plague leptospirosis and meningococcal meningitis. Although originally developed as guidance for WHO officials this publication is available to a wide readership including all frontline responders - communities government officials non-State actors and public health professionals - who need to respond rapidly and effectively when an outbreak is detected.

Theory and Models for Cyber Situation Awareness

A comprehensive overview of different approaches to the measurement of situation awareness in experimental and applied setting, this book directly tackles the problem of ensuring that system designs and training programs are effective at promoting situation awareness. It is the first book to provide a all-inclusive coverage of situation awareness and its measurement. Topics addressed provide a detailed analysis of the use of a wide variety of techniques for measuring situation awareness and situation assessment processes. It provides a rich resource for engineers and human factors psychologists involved

in designing and evaluating systems in many domains.

Smart Metering Technology and Services

Until recently, the Arctic was almost impossible for anyone other than indigenous peoples and explorers to traverse. Pervasive Arctic sea ice and harsh climatological conditions meant that the region was deemed incapable of supporting industrial activity or a Western lifestyle. In the last decade, however, that longstanding reality has been dramatically and permanently altered. Receding sea ice, coupled with growing geopolitical disputes over Arctic resources, territory, and transportation channels, has stimulated efforts to exploit newly-open waterways, to identify and extract desirable resources, and to leverage industrial, commercial, and transportation opportunities emerging throughout the region. This book presents papers from the NATO Advanced Research Workshop (ARW) Governance for Cyber Security and Resilience in the Arctic. Held in Rovaniemi, Finland, from 27-30 January 2019, the workshop brought together top scholars in cybersecurity risk assessment, governance, and resilience to discuss potential analytical and governing strategies and offer perspectives on how to improve critical Arctic infrastructure against various human and natural threats. The book is organized in three sections according to topical group and plenary discussions at the meeting on: cybersecurity infrastructure and threats, analytical strategies for infrastructure threat absorption and resilience, and legal frameworks and governance options to promote cyber resilience. Summaries and detailed analysis are included within each section as summary chapters in the book. The book provides a background on analytical tools relevant to risk and resilience analytics, including risk assessment, decision analysis, supply chain management and resilience analytics. It will allow government, native and civil society groups, military stakeholders, and civilian practitioners to understand better on how to enhance the Arctic's resilience against various natural and anthropogenic challenges.

Going Gray

The field of occupational health and safety constantly changes, especially as it pertains to biomedical research. New infectious hazards are of particular importance at nonhuman-primate facilities. For example, the discovery that B virus can be transmitted via a splash on a mucous membrane raises new concerns that must be addressed, as does the discovery of the Reston strain of Ebola virus in import quarantine facilities in the U.S. The risk of such infectious hazards is best managed through a flexible and comprehensive Occupational Health and Safety Program (OHSP) that can identify and mitigate potential hazards. Occupational Health and Safety in the Care and Use of Nonhuman Primates is intended as a reference for vivarium managers, veterinarians, researchers, safety professionals, and others who are involved in developing or implementing an OHSP that deals with nonhuman primates. The book lists the important features of an OHSP and provides the tools necessary for informed decision-making in developing an optimal program that meets all particular institutional needs.

Handbook of Loss Prevention and Crime Prevention

Contains 63 papers covering 11 years of research on the progress and challenges in the design of Adaptive Cruise Control (ACC) systems and components. Subjects covered include: ACC sensors overview; Hybrid ACC systems; Interactive cruise control; Predictive safety systems; Brake actuation; ACC radar sensors; Vision sensors; and Miscellaneous ACC sensors.

Insider Threats in Cyber Security

Global energy context has become more and more complex in the last decades; the raising prices of fuels

together with economic crisis, new international environmental and energy policies that are forcing companies. Nowadays, as we approach the problem of global warming and climate changes, smart metering technology has an effective use and is crucial for reaching the 2020 energy efficiency and renewable energy targets as a future for smart grids. The environmental targets are modifying the shape of the electricity sectors in the next century. The smart technologies and demand side management are the key features of the future of the electricity sectors. The target challenges are coupling the innovative smart metering services with the smart meters technologies, and the consumers' behaviour should interact with new technologies and polices. The book looks for the future of the electricity demand and the challenges posed by climate changes by using the smart meters technologies and smart meters services. The book is written by leaders from academia and industry experts who are handling the smart meters technologies, infrastructure, protocols, economics, policies and regulations. It provides a promising aspect of the future of the electricity demand. This book is intended for academics and engineers who are working in universities, research institutes, utilities and industry sectors wishing to enhance their idea and get new information about the smart meters.

S. A. F. E. Situational Awareness for Employees

A compilation of four other published works by author Matthew Dermody. Titles include: Gray Man: Camouflage for Crowds, Cities, and Civil CrisisGray Woman: A Woman's Guide to Gray Man TacticsConversational Camouflage: Oratory Discretion and Pretexting for Behavioral ConcealmentSituational Sense: Basic Threat Detection Using Situational Awareness and Common Sense

Read More About Situational Sense Basic Threat Detection Using Situational Awareness And Common Sense

Arts & Photography
Biographies & Memoirs
Business & Money
Children's Books
Christian Books & Bibles
Comics & Graphic Novels
Computers & Technology
Cookbooks, Food & Wine
Crafts, Hobbies & Home
Education & Teaching
Engineering & Transportation
Health, Fitness & Dieting
History
Humor & Entertainment
Law
LGBTQ+ Books
Literature & Fiction
Medical Books
Mystery, Thriller & Suspense
Parenting & Relationships
Politics & Social Sciences
Reference
Religion & Spirituality
Romance
Science & Math
Science Fiction & Fantasy
Self-Help
Sports & Outdoors
Teen & Young Adult
Test Preparation
Travel