Open Source, Intelligence Cyberspace La Nuova Frontiera Della Conoscenza

Why do nations break into one another's most important computer networks? There is an obvious answer: to steal valuable information or to attack. But this isn't the full story. This book draws on often-overlooked documents leaked by Edward Snowden, real-world case studies of cyber operations, and policymaker perspectives to show that intruding into other countries' networks has enormous defensive value as well. Two nations, neither of which seeks to harm the other but neither of which trusts the other, will often find it prudent to launch intrusions. This general problem, in which a nation's means of securing itself threatens the security of others and risks escalating tension, is a bedrock concept in international relations and is called the 'security dilemma'. This book shows not only that the security dilemma applies to cyber operations, but also that the particular characteristics of the digital domain mean that the effects are deeply pronounced. The cybersecurity dilemma is both a vital concern of modern statecraft and a means of accessibly understanding the essential components of cyber operations.

Cyberwarfare: Information Operations in a Connected World puts students on the real-world battlefield of cyberspace! It reviews the role that cyberwarfare plays in modern military operations–operations in which it has become almost impossible to separate cyberwarfare from traditional warfare.

This book reports on research and developments in human–technology interaction. A special emphasis is given to human–computer interaction and its implementation for a wide range of purposes such as health care, aerospace, telecommunication, and education, among others. The human aspects are analyzed in detail. Timely studies on human-centered design, wearable technologies, social and affective computing, augmented, virtual and mixed reality simulation, human rehabilitation, and biomechanics represent the core of the book. Emerging technology applications in business, security, and infrastructure are also critically examined, thus offering a timely, scientifically grounded, but also professionally oriented snapshot of the current state of the field. The book gathers contributions presented at the 5th International Conference on Human Interaction and Emerging Technologies (IHIET 2021, August 27–29, 2021) and the 6th International Conference on Human Interaction and Emerging Technologies: Future Systems (IHIET-FS 2021, October 28–30, 2021), held virtually from France. It offers a timely survey and a practice-oriented reference guide to researchers and professionals dealing with design, systems engineering, and management of the next-generation technology and service systems.

In the last decade, the proliferation of billions of new Internet-enabled devices and users has significantly expanded concerns about cybersecurity. But should we believe the prophets of cyber war or worry about online government surveillance? Are such security concerns real, exaggerated or just poorly understood? In this comprehensive text, Damien Van Puyvelde and Aaron F. Brantly provide a cutting-edge introduction to the key concepts, controversies and policy debates in cybersecurity. Exploring the interactions of individuals, groups and states in cyberspace, and the integrated security risks to which these give rise, they examine cyberspace as a complex socio-technical-economic domain that fosters both great potential and peril. Structured around ten chapters, the book explores the complexities and challenges of cybersecurity using case studies – from the Morris Worm and Titan Rain to BlackEnergy and the Cyber Caliphate – to highlight the evolution of attacks that can exploit and damage individual systems and critical infrastructures. With questions for group discussion and suggestions for further reading throughout, Cybersecurity will be essential reading for anyone interested in understanding the challenges and opportunities presented by the continued expansion of cyberspace.

Military and Intelligence Cyber Decision-making

Conversations in Cyberspace

From Strategy to Implementation

The Decision to Attack

Internet Searches for Vetting, Investigations, and Open-Source Intelligence

Critical Infrastructure Protection Against Hybrid Warfare Security Related Challenges

The Tao of Open Source IntelligenceIT Governance Ltd

This book shows how open source intelligence can be a powerful tool for combating crime by linking local and global patterns to help understand how criminal activities are connected. Readers will encounter the latest advances in cutting-edge data mining, machine learning and predictive analytics combined with natural language processing and social network analysis to detect, disrupt, and neutralize cyber and physical threats. Chapters contain state-of-the-art social media analytics and open source intelligence research trends. This multidisciplinary volume will appeal to students, researchers, and professionals working in the fields of open source intelligence, cyber crime and social network analytics. Chapter Automated Text Analysis for Intelligence Purposes: A Psychological Operations Case Study is available open access under a Creative Commons Attribution 4.0 International License via link.springer.com.

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.

Forecasting new and emerging risks associated with new technologies is a hard and provocative challenge. A wide range of new and modified materials are being made available, and many of these have unknown consequences including nanomaterials, composites, biomaterials, and biocybernetics. Additionally, the greater complexity of man-machine processes and interfaces, the introduction of collaborative robots, and the excessive dependence on computers, as in the case of unmanned vehicles in transportation, could trigger new risks. Forecasting and Managing Risk in the Health and Safety Sectors is an essential reference source that combines theoretical underpinnings with practical relevance in order to introduce training activities to manage uncertainty and risks consequent to emerging technologies. Featuring research on topics such as energy policy, green management, and intelligence cycle, this book is ideally designed for government officials, managers, policymakers, researchers, lecturers, advanced students, and professionals.

Proceedings of the 5th International Virtual Conference on Human Interaction and Emerging Technologies, IHIET 2021, August 27-29, 2021 and the 6th IHIET: Future Systems (IHIET-FS 2021), October 28-30, 2021, France

Methodologies, Ethics, and Critical Approaches

Handbook of Intelligence Studies

The Five Disciplines of Intelligence Collection

Open Source Intelligence Investigation

Publications Combined: Studies In Open Source Intelligence (OSINT) And Information

Conversations in Cyberspace is a collection of insights on the current state of security and privacy in the Internet world. The book contains a brief introduction to some of the most used open-source intelligence (OSINT) tools and a selection of interviews with some of the key figures in industrial control systems (ICS), advanced persistent threat (APT) and online/deep web members organizations. It aims to be an introduction to the relationships between security, OSINT and the vast and complex world hiding in the deep web. The information provided will be beneficial to security professionals and system administrators interested in exploring today's concerns in database design, privacy and security-by-design, and deep web members organizations, including Cicada 3301, the Unknowns, Anonymous, and more.

This edited book promotes and facilitates cybercrime research by providing a cutting-edge collection of perspectives on the critical usage of online data across platforms, as well as the implementation of both traditional and innovative analysis methods. The accessibility, variety and wealth of data available online presents substantial opportunities for researchers from different disciplines to study cybercrimes and, more generally, human behavior in cyberspace. The unique and dynamic characteristics of cyberspace often demand cross-disciplinary and cross-national research endeavors, but disciplinary, cultural and legal differences can hinder the ability of researchers to collaborate. This work also provides a review of the ethics associated with the use of online data sources across the globe. The authors are drawn from multiple disciplines and nations, providing unique insights into the value and challenges evident in online data use for cybercrime scholarship. It is a key text for researchers at the upper undergraduate level and above.

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 This topical volume offers a comprehensive review of secret intelligence organizations and activities. Intelligence has been in the news consistently since 9/11 and the Iraqi WMD errors. Leading experts in the field approach the three major missions of intelligence: collection-and-analysis; covert action; and counterintelligence. Within each of these missions, the dynamically written essays dissect the so-called intelligence cycle to reveal the challenges of gathering and assessing information from around the world. Covert action, the most controversial intelligence activity, is explored, with special attention on the issue of military organizations moving into what was once primarily a civilian responsibility. The authors furthermore examine the problems that are associated with counterintelligence, protecting* *secrets from foreign spies and terrorist organizations, as well as the question of intelligence accountability, and how a nation can protect its citizens against the possible abuse of power by its own secret agencies. The Handbook of Intelligence Studies is a benchmark publication with major importance both for current research and for the future of the field. It is essential reading for advanced undergraduates, graduate students and scholars of intelligence studies, international security, strategic studies and political science in general.*

Spying in America in the Post 9/11 World

Cyber Warfare

The Tao of Open Source Intelligence

Defining Second Generation Open Source Intelligence (Osint) for the Defense Enterprise

Researching Cybercrimes

Information Operations

Interdisciplinary and multidisciplinary research is slowly yet steadily revolutionizing traditional education. However, multidisciplinary research can and will also improve the extent to which a country can protect its critical and vital assets. Applying Methods of Scientific Inquiry Into Intelligence, Security, and Counterterrorism is an essential scholarly publication that provides personnel directly working in the fields of intelligence, law enforcement, and science with the opportunity to understand the multidisciplinary nature of intelligence and science in order to improve current intelligence activities and contribute to the protection of the nation. Each chapter of the book discusses various components of science that should be applied to the intelligence arena. Featuring coverage on a range of topics including cybersecurity, economics, and political strategy, this book is ideal for law enforcement, intelligence and security practitioners, students, educators, and researchers.

A riveting account of espionage for the digital age, from one of America's leading intelligence experts Spying has never been more ubiquitous—or less understood. The world is drowning in spy movies, TV shows, and novels, but universities offer more courses on rock and roll than on the CIA and there are more congressional experts on powdered milk than espionage. This crisis in intelligence education is distorting public opinion, fueling conspiracy theories, and hurting intelligence policy. In Spies, Lies, and Algorithms, Amy Zegart separates fact from fiction as she offers an engaging and enlightening account of the past, present, and future of American espionage as it faces a revolution driven by digital technology. Drawing on decades of research and hundreds of interviews with intelligence officials, Zegart provides a history of U.S. espionage, from George Washington's Revolutionary War spies to today's spy satellites; examines how fictional spies are influencing real officials; gives an overview of intelligence basics and life inside America's intelligence agencies; explains the deadly cognitive biases that can mislead analysts; and explores the vexed issues of traitors, covert action, and congressional oversight. Most of all, Zegart describes how technology is empowering new enemies and opportunities, and creating powerful new players, such as private citizens who are successfully tracking nuclear threats using little more than Google Earth. And she shows why cyberspace is, in many ways, the ultimate cloak-and-dagger battleground, where nefarious actors employ deception, subterfuge, and advanced technology for theft, espionage, and information warfare. A fascinating and revealing account of espionage for the digital age, Spies, Lies, and Algorithms is essential reading for anyone who wants to understand the reality of spying today.

For more than 40 years, Computerworld has been the leading source of technology news and information for IT influencers worldwide. Computerworld's

award-winning Web site (Computerworld.com), twice-monthly publication, focused conference series and custom research form the hub of the world's largest global IT media network.

This report describes the evolution of open source intelligence, defines open source information and the intelligence cycle, and parallels with other intelligence disciplines, along with methods used and challenges of using off-the-shelf technology.

Hacking, Trust and Fear Between Nations

The Cybersecurity Dilemma

ICCWS 2020 15th International Conference on Cyber Warfare and Security

Digital Extremisms

How to Stop the Spies, Terrorists, Hackers, and Criminals You Don't Even Know You Encounter Every Day

Research Handbook on International Law and Cyberspace

Over 1,600 total pages ... CONTENTS: AN OPEN SOURCE APPROACH TO SOCIAL MEDIA DATA GATHERING Open Source Intelligence – Doctrine’s Neglected Child (Unclassified) Aggregation Techniques to Characterize Social Networks Open Source Intelligence (OSINT): Issues for Congress A BURNING NEED TO KNOW: THE USE OF OPEN SOURCE INTELLIGENCE IN THE FIRE SERVICE Balancing Social Media with Operations Security (OPSEC) in the 21st Century Sailing the Sea of OSINT in the Information Age Social Media: Valuable Tools in Today‘s Operational Environment ENHANCING A WEB CRAWLER WITH ARABIC SEARCH CAPABILITY UTILIZING SOCIAL MEDIA TO FURTHER THE NATIONWIDE SUSPICIOUS ACTIVITY REPORTING INITIATIVE THE WHO, WHAT AND HOW OF SOCIAL MEDIA EXPLOITATION FOR A COMBATANT COMMANDER Open Source Cybersecurity for the 21st Century UNAUTHORIZED DISCLOSURE: CAN BEHAVIORAL INDICATORS HELP PREDICT WHO WILL COMMIT UNAUTHORIZED DISCLOSURE OF CLASSIFIED NATIONAL SECURITY INFORMATION? ATP 2-22.9 Open-Source Intelligence NTTP 3-13.3M OPERATIONS SECURITY (OPSEC) FM 2-22.3 HUMAN INTELLIGENCE COLLECTOR OPERATIONS

The end of the Cold War and the emergence of terrorism; radicalized religion; the proliferation and commoditization of weapons of mass destruction (WMD); and the increased informational and economic power of Arabia, Brazil, China, India, Indonesia, Iran, Russia, and Venezuela, among others, have brought Information Operations (IO) to the forefront of the unified national security strategy. In the past year, IO has matured from an early emphasis on the protection of critical infrastructures and against electronic espionage, and is now more focused on content and on interagency information-sharing. The value of information all information, not only secret information and the value of global monitoring in all languages, 24/7, have been clearly established by the Undersecretary of Defense for Intelligence (USDI). This monograph defines and discusses three IO elements: " Strategic Communication (the message); " Open Source Intelligence (the reality); and, " Joint Information Operations Centers (the technology). These elements are further discussed in relation to six IO-heavy mission areas: " Information Operations generally; " Peacekeeping Intelligence (reactive); " Information Peacekeeping (proactive); " Early Warning (conflict deterrence, proactive counterterrorism); " Stabilization and Reconstruction Operations; and, " Homeland Defense and Civil Support.

This book explores the use of the internet by (non-Islamic) extremist groups, drawing together research by scholars across the social sciences and humanities. It offers a broad overview of the best of research in this area, including research contributions that address far-right, (non-Islamic) religious, animal rights, and nationalist violence online, as well as a discussion of the policy and research challenges posed by these unique and disparate groups. It offers an academically rigorous, introductory text that addresses extremism online, making it a valuable resource for students, practitioners and academics seeking to understand the unique characteristics such risks present.

The first comprehensive, research-based textbook on Internet-infused education, Educational Psychology and the Internet offers students an accessible guide to important issues in the field. Michael Glassman begins with an overview of the history that traces the evolution of the Internet and its significance for education. He outlines the current state of research, clearly defining terms that students will need to discuss larger concepts, such as hypertext and cyberspace. The second part of the book explores the practical applications of this research, which range from the individual-oriented to the generalized, including massive open online courses (MOOCs), open educational resources, and augmented reality. Key issues that affect teachers and students today, such as Net Neutrality and Creative Commons and Open Source licenses, are explained in straightforward terms, and often-overlooked differences - for example, between course management systems and learning management systems, and between blogs, social networking sites, and short messaging systems - are highlighted.

Duncan Hunter National Defense Authorization Act For Fiscal Year 2009, May 16, 2008, 110-2 House Report 110-652

Readings in Violence, Radicalisation and Extremism in the Online Space

Forecasting and Managing Risk in the Health and Safety Sectors

Spies Among Us

Violence and Society: Breakthroughs in Research and Practice

Social Media Analytics

This book examines the realities of living in the United States after the events of September 11th, 2001, and evaluates the challenges in gathering internal intelligence without severely compromising personal liberties. * Maps clarify America's security threats in a global and domestic context * Photographs depict historic events like the attacks of September 11, 2001, the Oklahoma City bombing, and the signing of the U.S. Constitution * Includes a bibliography of reference sources and recommended reading as well as an index of interviewees and quotations * A glossary explains the most commonly used terms in intelligence and homeland security

Ira Winkler has been dubbed "A Modern Day James Bond" by CNN and other media outlets for his ability to simulate espionage attacks against many of the top companies in the world, showing how billions of dollars can disappear. This unique book is packed with the riveting, true stories and case studies of how he did it-and how people and companies can avoid falling victim to the spies among us. American corporations now lose as much as $300 billion a year to hacking, cracking, physical security breaches, and other criminal activity. Millions of people a year have their identities stolen or fall victim to other scams. In Spies Among Us, Ira Winkler reveals his security secrets, disclosing how companies and individuals can protect themselves from even the most diabolical criminals. He goes into the mindset of everyone from small-time hackers to foreign intelligence agencies to disclose cost-effective countermeasures for all types of attacks. In Spies Among Us, readers learn: Why James Bond and Sydney Bristow are terrible spies How a team was able to infiltrate an airport in a post-9/11 world and plant a bomb How Ira and his team were able to steal nuclear reactor designs in three hours The real risks that individuals face from the spies that they unknowingly meet on a daily basis Recommendations for how companies and individuals can secure themselves against the spies, criminals, and terrorists who regularly cross their path

The skills and tools for collecting, verifying and correlating information from different types of systems is an essential skill when tracking down hackers. This book explores Open Source Intelligence Gathering (OSINT) inside out from multiple perspectives, including those of hackers and seasoned intelligence experts. OSINT refers to the techniques and tools required to harvest publicly available data concerning a person or an organization. With several years of experience of tracking hackers with OSINT, the author whips up a classical plot-line involving a hunt for a threat actor. While taking the audience through the thrilling investigative drama, the author immerses the audience with in-depth knowledge of state-of-the-art OSINT tools and techniques. Technical users will want a basic understanding of the Linux command line in order to follow the examples. But a person with no Linux or programming experience can still gain a lot from this book through the commentaries. This book’s unique digital investigation proposition is a combination of story-telling, tutorials, and case studies. The book explores digital investigation from multiple angles: Through the eyes of the author who has several years of experience in the subject. Through the mind of the hacker who collects massive amounts of data from multiple online sources to identify targets as well as ways to hit the targets. Through the eyes of industry leaders. This book is ideal for: Investigation professionals, forensic analysts, and CISO/CIO and other executives wanting to understand the mindset of a hacker and how seemingly harmless information can be used to target their organization. Security analysts, forensic investigators, and SOC teams looking for new approaches on digital investigations from the perspective of collecting and parsing publicly available information. CISOs and defense teams will find this book useful because it takes the perspective of infiltrating an organization from the mindset of a hacker. The commentary provided by outside experts will also provide them with ideas to further protect their organization’s data.

As industries are rapidly being digitalized and information is being more heavily stored and transmitted online, the security of information has become a top priority in securing the use of online networks as a safe and effective platform. With the vast and diverse potential of artificial intelligence (AI) applications, it has become easier than ever to identify cyber vulnerabilities, potential threats, and the identification of solutions to these unique problems. The latest tools and technologies for AI applications have untapped potential that conventional systems and human security systems cannot meet, leading AI to be a frontrunner in the fight against malware, cyber-attacks, and various security issues. However, even with the tremendous progress AI has made within the sphere of security, it's important to understand the impacts, implications, and critical issues and challenges of AI applications along with the many benefits and emerging trends in this essential field of security-based research. Research Anthology on Artificial Intelligence Applications in Security seeks to address the fundamental advancements and technologies being used in AI applications for the security of digital data and information. The included chapters cover a wide range of topics related to AI in security stemming from the development and design of these applications, the latest tools and technologies, as well as the utilization of AI and what challenges and impacts have been discovered along the way. This resource work is a critical exploration of the latest research on security and an overview of how AI has impacted the field and will continue to advance as an essential tool for security, safety, and privacy online. This book is ideally intended for cyber security analysts, computer engineers, IT specialists, practitioners, stakeholders, researchers, academicians, and students interested in AI applications in the realm of security research.

Putting the "I" Back Into DIME

Governing Cyberspace

Behavior, Power and Diplomacy

Human Interaction, Emerging Technologies and Future Systems V

Open Source Intelligence Methods and Tools

Open source, intelligence & cyberspace. La nuova frontiera della conoscenza

Violent behavior is an unavoidable aspect of human nature, and as such it has become deeply integrated into modern society. Examining violence through a critical and academic perspective can lead to a better understanding of its foundations and implications. Violence and Society: Breakthroughs in Research and Practice explores the social and cultural influences of violence on human life and activity. Focusin on emerging research perspectives, case studies, and future outlooks, this comprehensive collection is an essential reference source for graduate-level students, sociologists, researchers, professionals, and practitioners interested in the effects of violence in contemporary cult

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 architect large-scale data collection and analysis, and how to prepare the CSOC team for agile, threat-based response. If you manage, wor or are standing up a CSOC, this book is for you. It is also available on MITRE's website, www.mitre.org.

In the information age, it is critical that we understand the implications and exposure of the activities and data documented on the Internet. Improved efficiencies and the added capabilities of instant communication, high-speed connectivity to browsers, search engines, websites, databases, indexing, searching and analytical applications have made information technology (IT) and the Internet a vital issued for public a private enterprises. The downside is that this increased level of complexity and vulnerability presents a daunting challenge for enterprise ar personal security. Internet Searches for Vetting, Investigations, and Open-Source Intelligence provides an understanding of the implications the activities and data documented by individuals on the Internet. It delineates a much-needed framework for the responsible collection and of the Internet for intelligence, investigation, vetting, and open-source information. This book makes a compelling case for action as well as reviews relevant laws, regulations, and rulings as they pertain to Internet crimes, misbehaviors, and individuals' privacy. Exploring technologies such as social media and aggregate information services, the author outlines the techniques and skills that can be used to lev the capabilities of networked systems on the Internet and find critically important data to complete an up-to-date picture of people, employe entities, and their activities. Outlining appropriate adoption of legal, policy, and procedural principles—and emphasizing the careful and appropriate use of Internet searching within the law—the book includes coverage of cases, privacy issues, and solutions for common proble encountered in Internet searching practice and information usage, from internal and external threats. The book is a valuable resource on ho to utilize open-source, online sources to gather important information and screen and vet employees, prospective employees, corporate partners, and vendors.

Brantly investigates how states decide to employ cyber in military and intelligence operations against other states and how rational those decisions are. He contextualizes broader cyber decision-making processes into a systematic expected utility-rational choice approach to provide a mathematical understanding of the use of cyber weapons.

Cybersecurity

Cyberwarfare: Information Operations in a Connected World

Information Operations: Putting the "I" Back into DIME

Spies, Lies, and Algorithms

Hunting Cyber Criminals

Open Source Intelligence and Cyber Crime

In the past year, Information Operations (IO) has matured from an early emphasis on the protection of critical infrastructures and against electronic espionage and is now more focused on content and on interagency information-sharing. The value of information--all information, not only secret information--and the value of global monitoring in all languages, 24/7, has been clearly established by the Undersecretary of Defense for Intelligence (USDI). This monograph defines and discusses three IO elements: Strategic Communication (the message); Open Source Intelligence (the reality); and, Joint Information Operations Centers (the technology). It concludes with a strategic overview of the various conceptual and technical elements required to meet modern IO needs, and provides a requirements statement that could be tailored to the needs of any Combatant Commander, service, or agency.

This updated and expanded edition of Cyberspace in Peace and War by Martin C. Libicki presents a comprehensive understanding of cybersecurity, cyberwar, and cyber-terrorism. From basic concepts to advanced principles, Libicki examines the sources and consequences of system compromises, addresses strategic aspects of cyberwar, and defines cybersecurity in the context of military operations while highlighting unique aspects of the digital battleground and strategic uses of cyberwar. This new edition provides updated analysis on cyberespionage, including the enigmatic behavior of Russian actors, making this volume a timely and necessary addition to the cyber-practitioner's library. Cyberspace in Peace and War guides readers through the complexities of cybersecurity and cyberwar and challenges them to understand the topics in new ways. Libicki provides the technical and geopolitical foundations of cyberwar necessary to understand the policies, operations, and strategies required for safeguarding an increasingly online infrastructure.

Leading intelligence experts Mark M. Lowenthal and Robert M. Clark bring together an all new, groundbreaking title. The Five Disciplines of Intelligence Collection describes, in non-technical terms, the definition, history, process, management, and future trends of each intelligence collection source (INT). Authoritative and non-polemical, this book is the perfect teaching tool for classes addressing various types of collection. Chapter authors are past or current senior practitioners of the INT they discuss, providing expert assessment of ways particular types of collection fit within the larger context of the U.S. Intelligence Community. This volume shows all-source analysts a full picture of how to better task and collaborate with their collection partners, and gives intelligence collectors an appreciation of what happens beyond their "stovepipes," as well as a clear assessment of the capabilities and limitations of INT collection.

This revised and expanded edition of the Research Handbook on International Law and Cyberspace brings together leading scholars and practitioners to examine how international legal rules, concepts and principles apply to cyberspace and the activities occurring within it. In doing so, contributors highlight the difficulties in applying international law to cyberspace, assess the regulatory efficacy of these rules and, where necessary, suggest adjustments and revisions.

The History and Future of American Intelligence

Techniques, Tactics and Tools for Security Practitioners

A Practical Guide to Online Intelligence

Computerworld

Cyberspace in Peace and War, Second Edition

Ten Strategies of a World-Class Cybersecurity Operations Center

Cyber norms and other ways to regulate responsible state behavior in cyberspace is a fast-moving political and diplomatic field. The academic study of these processes is varied and interdisciplinary, but much of the literature has been organized according to discipline. Seeking to cross disciplinary boundaries, this timely book brings together researchers in fields ranging from international law, international relations, and political science to business studies and philosophy to explore the theme of responsible state behavior in cyberspace. . Divided into three parts, Governing Cyberspace first looks at current debates in and about international law and diplomacy in cyberspace. How does international law regulate state behaviour and what are its limits? How do cyber superpowers like China and Russia shape their foreign policy in relation to cyberspace? The second focuses on power and governance. What is the role for international organisations like NATO or for substate actors like intelligence agencies? How do they adapt to the realities of cyberspace and digital conflict? How does the classic balance of power play out in cyberspace and how do different states position themselves? The third part takes a critical look at multistakeholder and corporate diplomacy. How do global tech companies shape their role as norm entrepreneurs in cyberspace, and how do their cyber diplomatic efforts relate to their corporate identity?

Apply Open Source Intelligence (OSINT) techniques, methods, and tools to acquire information from publicly available online sources to support your intelligence analysis. Use the harvested data in different scenarios such as financial, crime, and terrorism investigations as well as performing business competition analysis and acquiring intelligence about individuals and other entities. This book will also improve your skills to acquire information online from both the regular Internet as well as the hidden web through its two sub-layers: the deep web and the dark web. The author includes many OSINT resources that can be used by intelligence agencies as well as by enterprises to monitor trends on a global level, identify risks, and gather competitor intelligence so more effective decisions can be made. You will discover techniques, methods, and tools that are equally used by hackers and penetration testers to gather intelligence about a specific target online. And you will be aware of how OSINT resources can be used in conducting social engineering attacks. Open Source Intelligence Methods and Tools takes a practical approach and lists hundreds of OSINT resources that can be used to gather intelligence from online public sources. The book also covers how to anonymize your digital identity online so you can conduct your searching activities without revealing your identity. What You'll Learn Identify intelligence needs and leverage a broad range of tools and sources to improve data collection, analysis, and decision making in your organization Use OSINT resources to protect individuals and enterprises by discovering data that is online, exposed, and sensitive and hide the data before it is revealed by outside attackers Gather corporate intelligence about business competitors and predict future market directions Conduct advanced searches to gather intelligence from social media sites such as Facebook and Twitter Understand the different layers that make up the Internet and how to search within the invisible web which contains both the deep and the dark webs Who This Book Is For Penetration testers, digital forensics investigators, intelligence services, military, law enforcement, UN agencies, and for-profit/non-profit enterprises

Hybrid conflicts are characterized by multi-layered efforts to undermine the functioning of the State or polarize society. This book presents results, recommendations and best practices from the NATO Advanced Research Workshop (ARW) "Critical Infrastructure Protection Against Hybrid Warfare Security Related Challenges", held in Stockholm, Sweden, in May 2016. The main objective of this workshop was to help and support NATO in the field of hybrid conflicts by developing a set of tools to deter and defend against adversaries mounting a hybrid offensive. Addressing the current state of critical infrastructure protection (CIP) and the challenges evolving in the region due to non-traditional threats which often transcend national borders – such as cyber attacks, terrorism, and attacks on energy supply – the widely ranging group of international experts who convened for this workshop provided solutions from a number of perspectives to counter the new and emerging challenges affecting the security of modern infrastructure. Opportunities for public-private partnerships in NATO member and partner countries were also identified. The book provides a highly topical resource which identifies common solutions for combating major hazards and challenges – namely cyber attacks, terrorist attacks on energy supply, man-made disasters, information warfare and maritime security risks – and will be of interest to all those striving to maintain stability and avoid adverse effects on the safety and well-being of society.

One of the most important aspects for a successful police operation is the ability for the police to obtain timely, reliable and actionable intelligence related to the investigation or incident at hand. Open Source Intelligence (OSINT) provides an invaluable avenue to access and collect such information in addition to traditional investigative techniques and information sources. This book offers an authoritative and accessible guide on how to conduct Open Source Intelligence investigations from data collection to analysis to the design and vetting of OSINT tools. In its pages the reader will find a comprehensive view into the newest methods for OSINT analytics and visualizations in combination with real-life case studies to showcase the application as well as the challenges of OSINT investigations across domains. Examples of OSINT range from information posted on social media as one of the most openly available means of accessing and gathering Open Source Intelligence to location data, OSINT obtained from the darkweb to combinations of OSINT with real-time analytical capabilities and closed sources. In addition it provides guidance on legal and ethical considerations making it relevant reading for practitioners as well as academics and students with a view to obtain thorough, first-hand knowledge from serving experts in the field.

Politics, Governance and Conflict in Cyberspace
Research Anthology on Artificial Intelligence Applications in Security
Breakthroughs in Research and Practice
Domestic Threat and the Need for Change
A Hacker's Guide to Online Intelligence Gathering Tools and Techniques
Educational Psychology and the Internet