Open Source Intelligence Reader

Momentous social events result from the sum of micro-level changes in daily individual life, and by observing and fusing publicly available data, such as web searches and other internet traffic, it is possible to anticipate events such as disease outbreaks. However, this ability is not without risks, and public concern about the possible consequences of improper use of this technology cannot be ignored. Opportunities for open discussion and democratic scrutiny are required. This book has its origins in the workshop Internet-Based Intelligence for Public Health Emergencies and Disease Outbreak: Technical, Medical, and Regulatory Issues, held in Haifa, Israel, in March 2011. The workshop was attended by 28 invited delegates from nine countries, representing various disciplines such as public health, ethics, sociology, informatics, policy-making, intelligence and security, and was supported by the NATO Science for Peace and Security Programme. Its starting point was the 2009 outbreak of swine flu in Mexico. The book includes both scientific contributions presented during the meeting and some additional articles that were submitted later. Interactions between public health and information and communication technologies are destined to be of great importance in the future. This book is a contribution to the ongoing dialogue between scholars and practitioners, which will be essential to public acceptance and safety as we rely more and more on the internet for predicting trends, decision-making and communication with the public.
Algorithms for Automating Open Source Intelligence (OSINT) presents information on the gathering of information and extraction of actionable intelligence from openly available sources, including news broadcasts, public repositories, and more recently, social media. As OSINT has applications in crime fighting, state-based intelligence, and social research, this book provides recent advances in text mining, web crawling, and other algorithms that have led to advances in methods that can largely automate this process. The book is beneficial to both practitioners and academic researchers, with discussions of the latest advances in applications, a coherent set of methods and processes for automating OSINT, and interdisciplinary perspectives on the key problems identified within each discipline. Drawing upon years of practical experience and using numerous examples, editors Robert Layton, Paul Watters, and a distinguished list of contributors discuss Evidence Accumulation Strategies for OSINT, Named Entity Resolution in Social Media, Analyzing Social Media Campaigns for Group Size Estimation, Surveys and qualitative techniques in OSINT, and Geospatial reasoning of open data. Presents a coherent set of methods and processes for automating OSINT Focuses on algorithms and applications allowing the practitioner to get up and running quickly Includes fully developed case studies on the digital underground and predicting crime through OSINT Discusses the ethical considerations when using publicly available online data
Eye-Opening Techniques Shed New Light on Open Source Intelligence Collection and Analysis.Author Michael Bazzell has been well known and respected in government circles for his ability to locate personal information about any target through Open Source Intelligence (OSINT). In this book, he shares his methods in great detail. Each step of his process is explained throughout fifteen chapters of specialized websites, application programming interfaces, and software solutions. Over 200 resources are identified with narrative tutorials and screen captures. This book will serve as a reference guide for anyone that is responsible for the collection of online content. It is written in a hands-on style that encourages the reader to execute the tutorials as they go. The search techniques offered will inspire analysts to "think outside the box" when scouring the internet for personal information. Much of the content of this book has never been discussed in any publication. Always thinking like a hacker, the author has identified new ways to use various technologies for an unintended purpose. This book will improve anyone's online investigative skills. Among other techniques, you will learn how to: Search The Twitter API for GPS data, Locate "hidden" Myspace content, Use search operators to increase results, Generate maps of video media by location, Search multiple networks for people, Monitor all network traffic for keywords, Create API calls to get instant information, Properly extract content from websites, Create replicas of an entire website, Locate deleted and previous versions of websites, Search past archives of online classifieds data, Locate all user profiles by searching user names, Obtain user created documents, photos, & videos, Analyze digital photograph metadata for information, Conduct reverse image searches to identify aliases, Use software applications to automate searching, Locate additional information about website owners, andCreate personal web forms for API searching
Please note that the content of this book primarily consists of articles available from Wikipedia or other free sources online. Pages: 24. Chapters: AltLaw, Co-occurrence networks, Commercial intelligence, Dan Butler (civil servant), DigitalGlobe, Eliot A. Jardines, Factiva, Foreign Broadcast Information Service, GhostNet, Intellipedia, Jane's Information Group, Joint Publications Research Service, LexisNexis, List of intelligence gathering disciplines, MilSuite, National Open Source Enterprise, NATO Open Source Intelligence Handbook, NATO Open Source Intelligence Reader, Newsknowledge, Open-source intelligence, Open Source Center, Open Source Information System, Robert David Steele, Ronald A. Marks, Shephard Group, SITE Institute, Space Imaging Middle East, World-Check, World Basic Information Library, Zapaday.
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.
"Open Source Intelligence: Reader 2.0 is published to ensure the dissemination of useful information that is not yet available doctrinally but is vital to successful intelligence support for national policymakers, military warfighters and acquisition managers, law enforcement professionals, and competitive intelligence professionals from the business community"--Forward.
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.

The Routledge Companion to Intelligence Studies provides a broad overview of the growing field of intelligence studies. The recent growth of interest in intelligence and security studies has led to an increased demand for popular depictions of intelligence and reference works to explain the architecture and underpinnings of intelligence activity. Divided into five comprehensive sections, this Companion provides a strong survey of the cutting-edge research in the field of intelligence studies: Part I: The evolution of intelligence studies; Part II: Abstract approaches to intelligence; Part III: Historical approaches to intelligence; Part IV: Systems of intelligence; Part V: Contemporary challenges. With a broad focus on the origins, practices and nature of intelligence, the book not only addresses classical issues, but also examines topics of recent interest in security studies. The overarching aim is to reveal the rich tapestry of intelligence studies in both a sophisticated and accessible way. This Companion will be essential reading for students of intelligence studies and strategic studies, and highly recommended for students of defence studies, foreign policy, Cold War studies, diplomacy and international relations in general.

"Written by a former CIA covert ops and intelligence expert, The Open-Source Everything Manifesto provides a roadmap for empowering the public to return to an informed, engaged democracy of, by, and for the people"--Provided by publisher.

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.

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

Open Source BI solutions have many advantages over traditional proprietary software, from offering lower initial costs to more flexible support and integration options; but, until now, there has been no comprehensive guide to the complete offerings of the OS BI market. Writing for IT managers and business analysts without bias toward any BI suite, industry insider Lyndsay Wise covers the benefits and challenges of all available open source BI systems and tools, enabling readers to identify the solutions and technologies that best meet their business needs. Wise compares and contrasts types of OS BI and proprietary tools on the market, including Pentaho, Jaspersoft, RapidMiner, SpagoBI, BIRT, and many more. Real-world case studies and project templates clarify the steps involved in implementing open source BI, saving new users the time and trouble of developing their own solutions from scratch. For business managers who are hard pressed to indentify the best BI solutions and software for their companies, this book provides a practical guide to evaluating the ROI of open source versus traditional BI deployments. The only book to provide complete coverage of all open source BI systems and tools specifically for business managers, without bias toward any OS BI suite A practical, step-by-step guide to implementing OS BI solutions that maximize ROI Comprehensive coverage of all open source systems and tools, including architectures, data integration, support, optimization, data mining,

data warehousing, and interoperability Case studies and project templates enable readers to evaluate the benefits and tradeoffs of all OS BI options without having to spend time developing their own solutions from scratch

This book explores how social media and its advances enables citizens to empower themselves during a crisis. The book addresses the key issues related to crises management and social media as the new platform to assist citizens and first responders dealing with multiple forms of crisis, from major terrorist attacks, larger scale public disorder, large-scale movement of people across borders, and natural disasters. The book is based on the results and knowledge gained during the European Commission ATHENA project which has been addressing critical issues in contemporary crisis management and social media and smart mobile communications. This book is authored by a mix of global contributors from across the landscape of academia, emergency response and experts in government policy and private industry. This title explores and explains that during a modern crisis, the public self-organizes into voluntary groups, adapt quickly to changing circumstances, emerge as leaders and experts and perform life-saving actions; and that they are increasingly reliant upon the use of new communications media to do it.

The second edition of Secret Intelligence: A Reader brings together key essays from the field of intelligence studies, blending classic works on concepts and approaches with more recent essays dealing with current issues and ongoing debates about the future of intelligence. Secret intelligence has never enjoyed a higher profile. The events of 9/11, the conflicts in Iraq and Afghanistan, the missing WMD controversy, public debates over prisoner interrogation, together with the revelations of figures such as Edward Snowden, recent cyber attacks and the rise of 'hybrid warfare' have all contributed to make this a ‘hot’ subject over the past two decades. Aiming to be more comprehensive than existing books, and to achieve truly international coverage of the field, this book provides key readings and supporting material for students and course convenors. It is divided into four main sections, each of which includes full summaries of each article, further reading suggestions and student questions: • The intelligence cycle • Intelligence, counter-terrorism and security • Ethics, accountability and secrecy • Intelligence and the new warfare This new edition contains essays by leading scholars in the field and will be essential reading for students of intelligence studies, strategic studies, international security and political science in general, and of interest to anyone wishing to understand the current relationship between intelligence and policy-making.

This book presents 12 essays that focus on the analysis of the problems prompted by cyber operations (COs). It clarifies and discusses the ethical and regulatory problems raised by the deployment of cyber capabilities by a state’s army to inflict disruption or damage to an adversary’s targets in or through cyberspace. Written by world-leading philosophers, ethicists, policy-makers, and law and military experts, the essays cover such topics as the conceptual novelty of COs and the ethical problems that this engenders; the applicability of existing conceptual and regulatory frameworks to COs deployed in case of conflicts; the definition of deterrence strategies involving COs; and the analysis of models to foster cooperation in managing cyber crises. Each essay is an invited contribution or a revised version of a paper originally presented at the workshop on Ethics and Policies for Cyber Warfare, organized by the NATO Cooperative Cyber Defence Centre of Excellence in collaboration with the University of Oxford. The volume endorses a multi-disciplinary approach, as such it offers a comprehensive overview of the ethical, legal, and policy problems posed by COs and of the different approaches and methods that can be used to solve them. It will appeal to a wide readership, including ethicists, philosophers, military experts, strategy planners, and law- and policy-makers.

The intelligence failures exposed by the events of 9/11 and the missing weapons of mass destruction in Iraq have made one thing perfectly clear: change is needed in how the U.S. intelligence community operates. Transforming U.S. Intelligence argues that transforming intelligence requires as much a look to the future as to the past and a focus more on the art and practice of intelligence rather than on its bureaucratic arrangements. In fact, while the recent restructuring, including the creation of the Department of Homeland Security, may solve some problems, it has also created new ones. The authors of this volume agree that transforming policies and practices will be the most effective way to tackle future challenges facing the nation's security. This volume's contributors, who have served in intelligence agencies, the Departments of State or Defense, and the staffs of congressional oversight committees, bring their experience as insiders to bear in thoughtful and thought-provoking essays that address what such an overhaul of the system will require. In the first section, contributors discuss twenty-first-century security challenges and how the intelligence community can successfully defend U.S. national interests. The second section focuses on new technologies and modified policies that can increase the effectiveness of intelligence gathering and analysis. Finally, contributors consider management procedures that ensure the implementation of enhanced capabilities in practice. Transforming U.S. Intelligence supports the mandate of the new director of national intelligence by offering both careful analysis of existing strengths and weaknesses in U.S. intelligence and specific recommendations on how to fix its problems without harming its strengths. These recommendations, based on intimate knowledge of the way U.S. intelligence actually works, include suggestions for the creative mixing of technologies with new missions to bring about the transformation of U.S. intelligence without incurring unnecessary harm or expense. The goal is the creation of an intelligence community that can rapidly respond to developments in international politics, such as the emergence of nimble terrorist networks while reconciling national security requirements with the rights and liberties of American citizens.

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.

2018 version of the OSINT Tools and Resources Handbook. This version is almost three times the size of the last public release in 2016. It reflects the changing intelligence needs of our clients in both the public and private sector, as well as the many areas we have been active in over the past two years.

This book explains how to take surreptitious photographs and record video of people and property in a safe and effective manner while producing excellent results. It is the most comprehensive text on clandestine photography available. It takes the reader through conventional as well as the most sophisticated clandestine photography methods in practice today, and it covers the use of all types of equipment ranging from off-the-shelf to the most high-tech equipment available. The ultra-long-range night vision photography methods discussed in this book were devised by the authors and only exist here. Readers will discover esoteric techniques for photographically recording recognizable human and vehicle plate images from distances of over a mile in both daylight and night conditions. Myriad methods for secretly photographing people and property under diverse and difficult conditions are presented. Readers will discover

innovative applications of combinations of old and new photographic-related technologies—some combined in unexpected ways that produce surprising results. It is written and extremely well illustrated in an easy to understand style for all photographers regardless of skill level. The book is appropriate for anyone in law enforcement, military operations, and private investigation. It will also benefit government surveillance specialists and those responsible for detecting and thwarting manual clandestine photography.

This book will serve as a reference guide for anyone that is responsible for the collection of online content. It is written in a hands-on style that encourages the reader to execute the tutorials as they go. The search techniques offered will inspire analysts to "think outside the box" when scouring the internet for personal information. Much of the content of this book has never been discussed in any publication. Always thinking like a hacker, the author has identified new ways to use various technologies for an unintended purpose. This book will improve anyone's online investigative skills. Among other techniques, you will learn how to locate: Hidden Social Network Content, Cell Phone Owner Information, Twitter GPS & Account Data, Hidden Photo GPS & Metadata, Deleted Websites & Posts, Website Owner Information, Alias Social Network Profiles, Additional User Accounts, Sensitive Documents & Photos, Live Streaming Social Content, IP Addresses of Users, Newspaper Archives & Scans, Social Content by Location, Private Email Addresses, Historical Satellite Imagery, Duplicate Copies of Photos, Local Personal Radio Frequencies, Compromised Email Information, Wireless Routers by Location, Hidden Mapping Applications, Complete Facebook Data, Free Investigative Software, Alternative Search Engines, Stolen Items for Sale, Unlisted Addresses, Unlisted Phone Numbers, Public Government Records, Document Metadata, Rental Vehicle Contracts, Online Criminal Activity.

Get rich. Wield incredible power. Get revenge. But avoid paradox, or get erased from the timestream so you never existed. Time travel offer endless possibilities and limitless dangers. What would you do if you could go back and relive your past? What if others could too? Who polices time? How do you win a time war? Four tales from a time war by veteran SF authors: Time’s Revenge Craig repeats the same day, getting ever closer to pulling off the perfect murder. He just wants to make a fortune, but who gave Craig this power and why is the killing so important to them? Time Trapped Librarian Irene has started traveling through time, but someone else controls her destinations. As history starts to unravel, can Irene prevent a terrible future she has already seen? The Comatose Man In his attempt to right an old wrong, Ross accidentally unleashes something far worse. Can the past fight an invasion from the future? The Terror Out of Time Dimitri-Laurent de Marigny is a criminal mastermind with a plan to finally realise his dream of immortality. But has de Marigny really understood the price that he – and the world – will pay? Bonus story - A Stitch in Time Time travel operative Art is on a simple mission to correct a previous mistake. But why is his partner behaving strangely, and are missions ever really simple?

Digital Forensics with Open Source Tools is the definitive book on investigating and analyzing computer systems and media using open source tools. The book is a technical procedural guide, and explains the use of open source tools on Mac, Linux and Windows systems as a platform for performing computer forensics. Both well-known and novel forensic methods are demonstrated using command-line and graphical open source computer forensic tools for examining a wide range of target systems and artifacts. Written by world-renowned forensic practitioners, this book uses the most current examination and analysis techniques in the field. It consists of 9 chapters that cover a range of topics such as the open source examination platform; disk and file system analysis; Windows systems and artifacts; Linux systems and artifacts; Mac OS X systems and artifacts; Internet artifacts; and automating analysis and extending capabilities. The book lends itself to use by students and those entering the field who do not have means to purchase new tools for different investigations. This book will appeal to forensic practitioners from areas including incident response teams and computer forensic investigators; forensic technicians from legal, audit, and consulting firms; and law enforcement agencies. Written by world-renowned forensic practitioners Details core concepts and techniques of forensic file system analysis Covers analysis of artifacts from the Windows, Mac, and Linux operating systems

The real power for security applications will come from the synergy of academic and commercial research focusing on the specific issue of security. Special constraints apply to this domain, which are not always taken into consideration by academic research, but are critical for successful security applications: large volumes: techniques must be able to handle huge amounts of data and perform 'on-line' computation; scalability: algorithms must have processing times that scale well with ever growing volumes; automation: the analysis process must be automated so that information extraction can 'run on its own'; ease of use: everyday citizens should be able to extract and assess the necessary information; and robustness: systems must be able to cope with data of poor quality (missing or erroneous data). The NATO Advanced Study Institute (ASI) on Mining Massive Data Sets for Security, held in Italy, September 2007, brought together around ninety participants to discuss these issues. This publication includes the most important contributions, but can of course not entirely reflect the lively interactions which allowed the participants to exchange their views and share their experience. The bridge between academic methods and industrial constraints is systematically discussed throughout. This volume will thus serve as a reference book for anyone interested in understanding the techniques for handling very large data sets and how to apply them in conjunction for solving security issues.

Air power for warfighting is a story that's been told many times. Air power for peacekeeping and UN enforcement is a story that desperately needs to be told. For the first-time, this volume covers the fascinating range of aerial peace functions. In rich detail it describes: aircraft transporting vital supplies to UN peacekeepers and massive amounts of humanitarian aid to war-affected populations; aircraft serving as the 'eyes in sky' to keep watch for the world organization; and combat aircraft enforcing the peace. Rich poignant case studies illuminate the past and present use of UN air power, pointing the way for the future. This book impressively fills the large gap in the current literature on peace operations, on the United Nations and on air power generally.

Despite a clear and compelling need for an intelligence-led approach to security, operational, and reputational risks, the subject of corporate security intelligence remains poorly understood. An effective intelligence process can directly support and positively impact operational activity and associated decision-making and can even be used to driv

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.

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 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.

This in-depth analysis shows how the high stakes contest surrounding open source information is forcing significant reform within the U.S. intelligence community, the homeland security sector, and among citizen activists. • Critique and commentary from intelligence officials and analysts regarding open source reforms within the intelligence community and homeland security sector • Three interrelated case studies through which post-9/11 U.S. intelligence reform is analyzed and critiqued • Examples of collateral, including official and unofficial photos, from the 2007 and 2008 Open Source Conferences sponsored by the Director of National Intelligence • A timeline of key open source developments, including the establishment of associated commissions and changes in organizational structures, policies, and cultures • Appendices containing excerpts of key open source legislation and policy documents • A bibliography of open source-related scholarship and commentary

Since the 9/11 terrorist attacks in the United States, serious concerns were raised on domestic and international security issues. Consequently, there has been considerable interest recently in technological strategies and resources to counter acts of terrorism. In this context, this book provides a state-of-the-art survey of the most recent advances in the field of counterterrorism and open source intelligence, demonstrating how various existing as well as novel tools and techniques can be applied in combating covert terrorist networks. A particular focus will be on future challenges of open source intelligence and perspectives on how to effectively operate in order to prevent terrorist activities.

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

Open Source Intelligence InvestigationFrom Strategy to ImplementationSpringer

Paradigms of AI Programming is the first text to teach advanced Common Lisp techniques in the context of building major AI systems. By reconstructing authentic, complex AI programs using state-of-the-art Common Lisp, the book teaches students and professionals how to build and debug robust practical programs, while demonstrating superior programming style and important AI concepts. The author strongly emphasizes the practical performance issues involved in writing real working programs of significant size. Chapters on troubleshooting and efficiency are included, along with a discussion of the fundamentals of object-oriented programming and a description of the main CLOS functions. This volume is an excellent text for a course on AI programming, a useful supplement for general AI courses and an indispensable reference for the professional programmer.

This important work identifies the problems of counter-drug intelligence and points toward a remedy for the failed anti-drug policies in the United States through the effective use of open source intelligence.

While Web 2.0 was about data, Web 3.0 is about knowledge and information. Scripting Intelligence: Web 3.0 Information Gathering and Processing offers the reader Ruby scripts for intelligent information management in a Web 3.0 environment—including information extraction from text, using Semantic Web technologies, information gathering (relational database metadata, web scraping, Wikipedia, Freebase), combining information from multiple sources, and strategies for publishing processed information. This book will be a valuable tool for anyone needing to gather, process, and publish web or database information across the modern web environment. Text processing recipes, including speech tagging and automatic summarization Gathering, visualizing, and publishing information from the Semantic Web Information gathering from traditional sources such as relational databases and web sites

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.

In the fast-paced world of international business, competitive intelligence is necessary for the daily survival of small firms and national economies alike. In Competitive Intelligence and Senior Management, veteran consultant Joseph H. A. M. Rodenberg argues that business leaders should devote more of their time and attention to seeking out and interpreting information about competitors. This instructive volume offers tools that will help senior managers to increase their firms’ competitiveness, carry out successful mergers and acquisitions, and avoid surprise attacks from corporate raiders and private equity firms.