Open Source Intelligence Reader

This new edition, which is being reissued in a more artistic format and with many additional illustrations, updates the original text and adds a chapter showing what progress has been made in the ecological management of landscapes over the past decade."--BOOK JACKET.

The role of intelligence in US government operations has changed dramatically and is now more critical than ever to domestic security and foreign policy. This authoritative and highly researched book written by Jeffrey T. Richelson provides a detailed overview of America's vast intelligence empire, from its organizations and operations to its management structure. Drawing from a multitude of sources, including hundreds of official documents, The US Intelligence Community allows students to understand the full scope of intelligence organizations and activities, and gives valuable support to policymakers and military operations. The seventh edition has been fully revised to include a new chapter on the major issues confronting the intelligence community, including secrecy and leaks, domestic spying, and congressional oversight, as well as revamped chapters on signals intelligence and cyber collection, geospatial intelligence, and open sources. The inclusion of more maps, tables and photos, as well as electronic briefing books on the book's Web site, makes The US Intelligence Community an even more valuable and engaging resource for students.

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.

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.

Avoid Pitfalls and Maximize ROI

A National Security Strategy for a New Century

Peacekeeping Intelligence

Open Source Intelligence Techniques

Cloak & Gown

Transparency, Truth, and Trust

Practical Threat Intelligence and Data-Driven Threat Hunting

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: chan needed in how the U.S. intelligence community operates. Transforming U.S. Intelligence argues that transforming intelligence requires as much a look 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 volume agree that transforming policies and practices will be the most effective way to tackle future challenges facing the nation's security. This volume contributors, who have served in intelligence agencies, the Departments of State or Defense, and the staffs of congressional oversight committees, bri 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 fir section, contributors discuss twenty-first-century security challenges and how the intelligence community can successfully defend U.S. national interes The second section focuses on new technologies and modified policies that can increase the effectiveness of intelligence gathering and analysis. Final 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. intellige and specific recommendations on how to fix its problems without harming its strengths. These recommendations, based on intimate knowledge of the w 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 righ and liberties of American citizens.

Get to grips with cyber threat intelligence and data-driven threat hunting while exploring expert tips and techniques Key FeaturesSet up an environmen centralize all data in an Elasticsearch, Logstash, and Kibana (ELK) server that enables threat huntingCarry out atomic hunts to start the threat hunting process and understand the environmentPerform advanced hunting using MITRE ATT&CK Evals emulations and Mordor datasetsBook Description Th hunting (TH) provides cybersecurity analysts and enterprises with the opportunity to proactively defend themselves by getting ahead of threats before t can cause major damage to their business. This book is not only an introduction for those who don't know much about the cyber threat intelligence (CT and TH world, but also a guide for those with more advanced knowledge of other cybersecurity fields who are looking to implement a TH program from scratch. You will start by exploring what threat intelligence is and how it can be used to detect and prevent cyber threats. As you progress, you'll learn to collect data, along with understanding it by developing data models. The book will also show you how to set up an environment for TH using open source tools. Later, you will focus on how to plan a hunt with practical examples, before going on to explore the MITRE ATT&CK framework. By the en this book, you'll have the skills you need to be able to carry out effective hunts in your own environment. What you will learnUnderstand what CTI is, its key concepts, and how it is useful for preventing threats and protecting your organizationExplore the different stages of the TH processModel the data collected and understand how to document the findingsSimulate threat actor activity in a lab environmentUse the information collected to detect breach and validate the results of your queriesUse documentation and strategies to communicate processes to senior management and the wider businessWh book is for If you are looking to start out in the cyber intelligence and threat hunting domains and want to know more about how to implement a threat hunting division with open-source tools, then this cyber threat intelligence book is for you.

It is time to look at OSINT in a different way. For many years, and within the previous editions of this book, we have relied on external resources to sup our search tools, virtual environments, and investigation techniques. We have seen this protocol fail us when services shut down, websites disappear, custom resources are dismantled due to outside pressures. This book aims to correct our dilemma. We will take control of our investigative resources a become self-reliant. There will be no more need for online search tools; we will make and host our own locally. We will no longer seek pre-built virtual machines; we will create and configure our own. This book puts the power back in your hands.

Over 1,600 total pages ... CONTENTS: AN OPEN SOURCE APPROACH TO SOCIAL MEDIA DATA GATHERING Open Source Intelligence – Doctrin 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 Securit (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

Sharing the Secrets

A Reader

The Open-Source Everything Manifesto
Open Source Intelligence and the War on Drugs
We Are Bellingcat
Ethics and Policies for Cyber Operations
Handbook of Intelligence Studies

div This original and persuasive book examines the moral and religious revival led by the Church of England before and after the Glorious Revolution, and shows how that revival laid the groundwork for a burgeoning civil society in Britain. After outlining the Church of England's key role in the increase of voluntary, charitable, and religious societies, Brent Sirota examines how these groups drove the modernization of Britain through such activities as settling immigrants throughout the empire, founding charity schools, distributing devotional literature, and evangelizing and educating merchants, seamen, and slaves throughout the British empire—all leading to what has been termed the “age of benevolence.”/DIV

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.

"This textbook is PROACTIVE. It is about starting over. It is the complete guide that I would give to any new client in an extreme situation. It leaves nothing out and provides explicit details of every step I take to make someone completely disappear, including document templates and a chronological order of events. The information shared in this book is based on real experiences with my actual clients, and is unlike any content ever released in my other books. " -- publisher.

What the world lacks right now—especially the United States, where every form of organization from government to banks to labor unions has betrayed the public trust—is integrity. Also lacking is public intelligence in the sense of decision-support: knowing what one needs to know in order to make honest decisions for the good of all, rather than corrupt decisions for the good of the few. The Open-Source Everything Manifesto is a distillation of author, strategist, analyst, and reformer Robert David Steele life's work: the transition from top-down secret command and control to a world of bottom-up, consensual, collective decision-making as a means to solve the major crises facing our world today. The book is intended to be a catalyst for citizen dialog and deliberation, and for inspiring the continued evolution of a nation in which all citizens realize our shared aspiration of direct democracy—informed participatory democracy. Open-Source Everything is a cultural and philosophical concept that is essential to creating a prosperous world at peace, a world that

works for one hundred percent of humanity. The future of intelligence is not secret, not federal, and not expensive. It is about transparency, truth, and trust among our local to global collective. Only "open" is scalable. As we strive to recover from the closed world corruption and secrecy that has enabled massive fraud within governments, banks, corporations, and even non-profits and universities, this timely book is a manifesto for liberation—not just open technology, but open everything.

Hunting Cyber Criminals

From Strategy to Implementation

Application of Social Media in Crisis Management

Life 3.0

Advanced Sciences and Technologies for Security Applications

A Search for Environmental Harmony

Down the Rabbit Hole an Osint Journey

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.

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

Today's digital economy is uniquely dependent on the Internet, yet few users or decision makers have more than a

rudimentary understanding of the myriad of online risks that threaten us. Cyber crime is one of the main threats to the integrity and availability of data and systems. From insiders to complex external attacks and industrial worms, modern business faces unprecedented challenges; and while cyber security and digital intelligence are the necessary responses to this challenge, they are understood by only a tiny minority. In his second book on high-tech risks, Mark Johnson goes far beyond enumerating past cases and summarising legal or regulatory requirements. He describes in plain, non-technical language how cyber crime has evolved and the nature of the very latest threats. He confronts issues that are not addressed by codified rules and practice guidelines, supporting this with over 30 valuable illustrations and tables. Written for the non-technical layman and the high tech risk manager alike, the book also explores countermeasures, penetration testing, best practice principles, cyber conflict and future challenges. A discussion of Web 2.0 risks delves into the very real questions facing policy makers, along with the pros and cons of open source data. In a chapter on Digital Intelligence readers are provided with an exhaustive guide to practical, effective and ethical online investigations. Cyber Crime, Security and Digital Intelligence is an important work of great relevance in today's interconnected world and one that nobody with an interest in either risk or technology should be without.

Algorithms for OSINT

Open Source Information and the Reshaping of U.S. Intelligence

Advances in Data Mining, Search, Social Networks and Text Mining, and Their Applications to Security

A NATO Cooperative Cyber Defence Centre of Excellence Initiative

Using Open Source Platforms for Business Intelligence

Open Source Intelligence Gathering for Penetration Testing

Preparing American Intelligence for the Twenty-first Century

Open Source Intelligence InvestigationFrom Strategy to ImplementationSpringer

Do you enjoy the reconnaissance part of a penetration testing? Want to discover issues on your network, assets or applications proactively? Would you like to learn some new OSINT based recon tools and techniques? Follow the rabbit hole and find exploitable critical vulnerabilities in the Panama Papers law firm and politics both American and international including Trump and the DNC. Analyse network and email configurations for entry points and exploits with FOCA, Maltego, Nmap/ZenMap, and Spiderfoot. Learn how to use advanced searches, alternative search engines that don't respect robots.txt., intel tools, and leak databases. Open source intelligence gathering (OSINT) and web-based reconnaissance is an important part of penetration testing and proactive defense. The more connected we are, the more information is held about everything. Yummy, juicy information for both a penetration tester or a malicious actor. Learning what sources of are available to start your search is an important first step in learning about reconnaissance and how the information could be utilized or resold. Both issues you or your client need to know. All of the tools and techniques in this book can be ninjafied with Python, Ruby or PowerShell. Initially, this book began as a presentation at the Cyber Senate Industrial Control Cybersecurity Nuclear Summit in Warrington, UK 2016. Originally, I intended to use some of the same techniques to target a

nuclear power plant or someone in a nuclear regulatory capacity. After submitting my original talk idea. Daesh, otherwise known as ISIS, began publicly threatening the European nuclear industry. Due to the threats, we decided it wasn't in anyone's best interest to give a how to target nuclear installations and changed the target instead to the law firm behind the Panama Papers fiasco. The project expanded to include additional targets with mostly a political slant. 2016 was a very tumultuous year in politics. Brexit, Trump, and the rise of the interesting politics and coups in Turkey, Netherlands, Germany, Russia, Bulgaria and the Philippines. It's a lot more fun to learn about a topic in an empowering way. Also, only politicians like politicians. They make a fun target. Learning a new technique is easier when it's fun. I chose targets and case studies which gave me a happy hacker smile.

Based on interviews with more than 200 former OSS and CIA agents and recently declassified OSS files, this is an investigation into the role of a great university and the relationship between social and academic elites and Intelligence.

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.

Cyber Crime, Security and Digital Intelligence

Secret Intelligence

Toward a Sociology of Algorithms

Extreme Privacy

The Christian Monitors

Early Detection and Response in Disease Outbreak Crises

Transforming U.S. Intelligence

New York Times Best Seller How will Artificial Intelligence affect crime, war, justice, jobs, society and our very sense of being human? The rise of AI has the potential to transform our future more than any other technology—and there's nobody better qualified or situated to explore that future than Max Tegmark, an MIT professor who's helped mainstream research on how to keep AI beneficial. How can we grow our prosperity through automation without leaving people lacking income or purpose? What career advice should we give today's kids? How can we make future AI systems more robust, so that they do what we want without crashing, malfunctioning or getting hacked? Should we fear an arms race in lethal autonomous weapons? Will machines eventually outsmart us at all tasks, replacing humans on the job market and perhaps altogether? Will AI help life flourish like never before or give us more power than we can handle? What sort of future do you want? This book empowers you to join what may be the most important conversation of our time. It doesn't shy away from the full range of viewpoints or from the most controversial issues—from

superintelligence to meaning, consciousness and the ultimate physical limits on life in the cosmos.
INTERNATIONAL BESTSELLER “Fascinating ... A powerful, exhortatory call to arms.”-New York Times Book Review “A David-and-Goliath story for the digital age ... Thrilling.”-Foreign Policy The page-turning inside story of the global team wielding the internet to fight for facts and combat autocracy-revealing the extraordinary ability of ordinary people to hold the powerful to account. In 2018, Russian exile Sergei Skripal and his daughter were nearly killed in an audacious poisoning attempt in Salisbury, England. Soon, the identity of one of the suspects was revealed: he was a Russian spy. This huge investigative coup wasn't pulled off by an intelligence agency or a traditional news outlet. Instead, the scoop came from Bellingcat, the open-source investigative team that is redefining the way we think about news, politics, and the digital future. We Are Bellingcat tells the inspiring story of how a college dropout pioneered a new category of reporting and galvanized citizen journalists-working together from their computer screens around the globe-to crack major cases, at a time when fact-based journalism is under assault from authoritarian forces. Founder Eliot Higgins introduces readers to the tools Bellingcat investigators use, tools available to anyone, from software that helps you pinpoint the location of an image, to an app that can nail down the time that photo was taken. This book digs deep into some of Bellingcat's most important investigations-the downing of flight MH17 over Ukraine, Assad's use of chemical weapons in Syria, the identities of alt-right protestors in Charlottesville-with the drama and gripping detail of a spy novel.
Some extraordinary rats come to the aid of a mouse family in this Newbery Medal Award–winning classic by notable children’s author Robert C. O’Brien. Mrs. Frisby, a widowed mouse with four small children, is faced with a terrible problem. She must move her family to their summer quarters immediately, or face almost certain death. But her youngest son, Timothy, lies ill with pneumonia and must not be moved. Fortunately, she encounters the rats of NIMH, an extraordinary breed of highly intelligent creatures, who come up with a brilliant solution to her dilemma. And Mrs. Frisby in turn renders them a great service.
We commonly think of society as made of and by humans, but with the proliferation of machine learning and AI technologies, this is clearly no longer the case. Billions of automated systems tacitly contribute to the social construction of reality by drawing algorithmic distinctions between the visible and the invisible, the relevant and the irrelevant, the likely and the unlikely – on and beyond platforms. Drawing on the work of Pierre Bourdieu, this book develops an original sociology of algorithms as social agents, actively participating in social life. Through a wide range of examples, Massimo Airoldi shows how society shapes algorithmic code, and how this culture in the code guides the practical behaviour of the code in the culture, shaping society in turn. The ‘machine habitus’ is the generative mechanism at work throughout myriads of feedback loops linking humans with artificial social agents, in the context of digital infrastructures and pre-digital social structures. Machine Habitus will be of great interest to students and scholars in sociology, media and cultural studies, science and technology studies and information technology, and to anyone interested in the growing

role of algorithms and AI in our social and cultural life.
Routledge Companion to Intelligence Studies
Scholars in the Secret War, 1939-1961
Being Human in the Age of Artificial Intelligence
Global Crime, Online Sleuths, and the Bold Future of News
Machine Habitus
The Church of England and the Age of Benevolence, 1680-1730
A Practical Guide to Online Intelligence

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.

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.

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 associate 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

"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.
Internet-Based Intelligence in Public Health Emergencies
Open Source Intelligence Investigation
Publications Combined: Studies In Open Source Intelligence (OSINT) And Information
No More Secrets
Mining Massive Data Sets for Security
Fixing the Spy Machine
Defining Second Generation Open Source Intelligence (Osint) for the Defense Enterprise

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.

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.
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.
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.
The U.S. Intelligence Community
Automating Open Source Intelligence
Reader 2.0 ; Executive Overviews, Asymmetric Warfare, Information Peacekeeping, Command Capabilities
What it Takes to Disappear in America
Emerging Concepts for the Future
Open Source Intelligence Methods and Tools
Social Capital
SCOTT (copy 1): From the John Holmes Library 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.

Social capital is a principal concept across the social sciences and has readily entered into mainstream discourse. In short, it is popular. However, this popularity has taken its toll. Social capital suffers from a lack of consensus because of the varied ways it is measured, defined, and deployed by different researchers. It has been put to work in ways that stretch and confuse its conceptual value, blurring the lines between networks, trust, civic engagement, and any type of collaborative action. This clear and concise volume presents the diverse theoretical approaches of scholars from Marx, Coleman, and Bourdieu to Putnam, Fukuyama, and Lin, carefully analyzing their commonalities and differences. Joonmo Son categorizes this wealth of work according to whether its focus is on the necessary preconditions for social capital, its structural basis, or its production. He distinguishes between individual and collective social capital (from shared resources of a personal network to pooled assets of a whole society), and interrogates the practical impact social capital has had in various policy areas (from health to economic development). Social Capital will be of immense value to readers across the social sciences and practitioners in relevant fields seeking to understand this mercurial concept.

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.

Redesigning the American Lawn

A hands-on guide to threat hunting with the ATT&CK™ Framework and open source tools

Mrs. Frisby and the Rats of Nimh

Altlaw, Co-Occurrence Networks, Commercial Intelligence, Dan Butler (Civil Servant), Digitalglobe, Eliot

A. Jardines, Factiv

A Hacker's Guide to Online Intelligence Gathering Tools and Techniques

The Tao of Open Source Intelligence

Resources for Searching and Analyzing Online Information

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

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 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.

Open Source Intelligence Tools and Resources Handbook

Open Source Intelligence