Open Source Intelligence Methods And Tools

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 and private enterprises. The downside is that this increased level of complexity and vulnerability presents a daunting challenge for enterprise and personal security. Internet Searches for Vetting, Investigations, and Open-Source Intelligence provides an understanding of the implications of the activities and data documented by individuals on the Internet. It delineates a much-needed framework for the responsible collection and use 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 leverage the capabilities of networked systems on the Internet and find critically important data to complete an up-to-date picture of people, employees, 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 problems encountered in Internet searching practice and information usage, from internal and external threats. The book is a valuable resource on how to utilize open-source, online sources to gather important information and screen and vet employees, prospective employees, corporate partners, and vendors.

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.

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 supply our search tools, virtual environments, and investigation techniques. We have seen this protocol fail us when services shut down, websites disappear, and custom resources are dismantled due to outside pressures. This book aims to correct our dilemma. We will take control of our investigative resources and 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.

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.

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.

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.

An ethical introduction to social engineering, an attack technique that leverages psychology, deception, and publicly available information to breach the defenses of a human target in order to gain access to an asset. Social engineering is key to the effectiveness of any computer security professional. Practical Social Engineering teaches you how to leverage human psychology and publicly available information to attack a target. The book includes sections on how to evade detection, spear phish, generate reports, and protect victims to ensure their well-being. You'll learn how to collect information about a target and how to exploit that information to make your attacks more effective. You'll also learn how to defend yourself or your workplace against social engineering attacks. Case studies throughout offer poignant examples such as how the author was able to piece together the details of a person's life simply by gathering details from an overheard restaurant conversation. Gray walks you through the sometimes difficult decision making process that every ethical social engineer must go through when implementing a phishing engagement including how to decide whether to do things manually or use automated tools; even how to set up your web server and build other technical tools necessary to succeed.

THE SUNDAY TIMES BESTSELLER 'John le Carré demystified the intelligence services; Higgins has demystified intelligence gathering itself' Financial Times 'Uplifting . . . Riveting . . . What will fire people through these pages, gripped, is the focused, and extraordinary, investigations that Bellingcat runs . . . Each runs as if the concluding chapter of a Holmesian whodunit' Telegraph 'We Are Bellingcat is Higgins's gripping account of how he reinvented reporting for the internet age . . . A manifesto for optimism in a dark age' Luke Harding, Observer How did a collective of self-taught internet sleuths end up solving some of the biggest crimes of our time? Bellingcat, the home-grown investigative unit, is redefining the way we think about news, politics and the digital future. Here, their founder – a high-school dropout on a kitchen laptop – tells the story of how they created a whole new category of information-gathering, galvanising citizen journalists across the globe to expose war crimes and pick apart disinformation, using just their computers. From the downing of Malaysia Flight 17 over the Ukraine to the sourcing of weapons in the Syrian Civil War and the identification of the Salisbury poisoners, We Are Bellingcat digs deep into some of Bellingcat's most successful investigations. It explores the most cutting-edge tools for analysing data, from virtual-reality software that can build photorealistic 3D models of a crime scene, to apps that can identify exactly what time of day a photograph was taken. In our age of uncertain truths, Bellingcat is what the world needs right now – an intelligence agency by the people, for the people.

Intelligence Methods and Systems Advancements for Knowledge-Based Business
Ransomware Revealed
The Oxford Handbook of National Security Intelligence
Open Source Intelligence Techniques
Extreme Privacy
Internet Searches for Vetting, Investigations, and Open-Source Intelligence
Defining Second Generation Open Source Intelligence (Osint) for the Defense Enterprise
Red Team + OSINT + Blue Team Reference
Open Source Intelligence and Cyber Crime
Automating Open Source Intelligence
Mathematical-Statistical Models and Qualitative Theories for Economic and Social Sciences
Open Source Intelligence Methods and Tools

Know how to mitigate and handle ransomware attacks via the essential cybersecurity training in this book so you can stop attacks before they happen. Learn the types of ransomware, distribution methods, internal structure, families (variants), defense strategies, recovery methods, and legal issues related to reporting ransomware incidents to authorities and other affected parties. This book also teaches you how to develop a ransomware incident response plan to minimize ransomware damage and recover normal operations quickly. Ransomware is a category of malware that can encrypt your computer and mobile device files until you pay a ransom to unlock them. Ransomware attacks are considered the most prevalent cybersecurity threats today—the number of new ransomware variants has grown 30-fold since 2015 and they currently account for roughly 40% of all spam messages. Attacks have increased in occurrence from one every 40 seconds to one every 14 seconds. Government and private corporations are targets. Despite the security controls set by organizations to protect their digital assets, ransomware is still dominating the world of security and will continue to do so in the future. Ransomware Revealed discusses the steps to follow if a ransomware infection occurs, such as how to pay the ransom through anonymous payment methods, perform a backup and restore your affected files, and search online to find a decryption tool to unlock (decrypt) your files for free. Mitigation steps are discussed in depth for both endpoint devices and network systems. What You Will Learn Be aware of how ransomware infects your system Comprehend ransomware components in simple terms Recognize the different types of ransomware families Identify the attack vectors employed by ransomware to infect computer systems Know how to prevent ransomware attacks from successfully comprising your system and network (i.e., mitigation strategies) Know what to do if a successful ransomware infection takes place Understand how to pay the ransom as well as the pros and cons of paying Set up a ransomware response plan to recover from such attacks Who This Book Is For Those who do not specialize in the cybersecurity field (but have adequate IT skills) and want to fully understand the anatomy of ransomware threats. Although most of the book's content will be understood by ordinary computer users, it will also prove useful for experienced IT users aiming to understand the ins and outs of ransomware threats without diving deep into the technical jargon of the internal structure of ransomware.

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 edited book provides an insight into the new approaches, challenges and opportunities that characterise open source intelligence (OSINT) at the beginning of the twenty-first century. It does so by considering the impacts of OSINT on three important contemporary security issues: nuclear proliferation, humanitarian crises and terrorism.

This book covers the developing field of open source research and discusses how to use social media, satellite imagery, big data analytics, and user-generated content to strengthen human rights research and investigations. The topics are presented in an accessible format through extensive use of images and data visualization (éditeur).

This edited volume takes a fresh look at the subject of open source intelligence (OSINT), exploring both the opportunities and the challenges that this emergent area offers at the beginning of the twenty-first century. In particular, it explores the new methodologies and approaches that technological advances have engendered, while at the same time considering the risks associated with the pervasive nature of the Internet. Drawing on a diverse range of experience and expertise, the book begins with a number of chapters devoted to exploring the uses and value of OSINT in a general sense, identifying patterns, trends and key areas of debate. The focus of the book then turns to the role and influence of OSINT in three key areas of international security – nuclear proliferation; humanitarian crises; and terrorism. The book offers a timely discussion on the merits and failings of OSINT and provides readers with an insight into the latest and most original research being conducted in this area.

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

If you are an expert Perl programmer interested in penetration testing or information security, this guide is designed for you. However, it will also be helpful for you even if you have little or no Linux shell experience.

This book presents a broad spectrum of problems related to statistics, mathematics, teaching, social science, and economics as well as a range of tools and techniques that can be used to solve these problems. It is the result of a scientific collaboration between experts in the field of economic and social systems from the University of Defence in Brno (Czech Republic), G. d'Annunzio University of Chieti-Pescara (Italy), Pablo de Olavid eUniversity of Sevilla (Spain), and Ovidius University in Constanţa, (Romania). The studies included were selected using a peer-review process and reflect heterogeneity and complexity of economic and social phenomena. They and present interesting empirical research from around the globe and from several research fields, such as statistics, decision making, mathematics, complexity, psychology, sociology and economics. The volume is divided into two parts. The first part, "Recent trends in mathematical and statistical models for economic and social sciences", collects papers on quantitative matters, which propose mathematical and statistical models for social sciences, economics, finance, and business administration. The second part, "Recent trends in qualitative theories for economic and social sciences", includes papers on qualitative matters, which discuss social, economic, and teaching issues. It is an ideal reference work for all those researchers interested in recent quantitative and qualitative tools. Covering a wide range of topics, it appeals in equal measure to mathematicians, statisticians, sociologists, philosophers, and specialists in the fields of communication, social and political sciences.

Hunting Cyber Criminals
Practical Social Engineering

The Encyclopaedia Britannica
Social Media Analytics
The Five Disciplines of Intelligence Collection
Applying Methods of Scientific Inquiry Into Intelligence, Security, and Counterterrorism
The Tao Of Spycraft
An Intelligence Agency for the People
A Practical Guide to Online Intelligence
Using Open Source Information for Human Rights Investigation, Documentation, and Accountability
Transparency, Truth, and Trust

"No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." Did you know that these twenty-six words are responsible for much of America's multibillion-dollar online industry? What we can and cannot write, say, and do online is based on just one law—a law that protects online services from lawsuits based on user content. Jeff Kosseff exposes the workings of Section 230 of the Communications Decency Act, which has lived mostly in the shadows since its enshrinement in 1996. Because many segments of American society now exist largely online, Kosseff argues that we need to understand and pay attention to what Section 230 really means and how it affects what we like, share, and comment upon every day. The Twenty-Six Words That Created the Internet tells the story of the institutions that flourished as a result of this powerful statute. It introduces us to those who created the law, those who advocated for it, and those involved in some of the most prominent cases decided under the law. Kosseff assesses the law that has facilitated freedom of online speech, trolling, and much more. His keen eye for the law, combined with his background as an award-winning journalist, demystifies a statute that affects all our lives –for good and for ill. While Section 230 may be imperfect and in need of refinement, Kosseff maintains that it is necessary to foster free speech and innovation. For filings from many of the cases discussed in the book and updates about Section 230, visit jeffkosseff.com

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.

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

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.

The book explains how openly available information is undervalued by the intelligence community and how analysts can use of this huge amount of information.

Completely Rewritten Sixth Edition Sheds New Light on Open Source Intelligence Collection and Analysis Author Michael Bazzell has been well known 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 twenty-five chapters of specialized websites, software solutions, and creative search techniques. Over 250 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 greatly improve anyone's online investigative skills. Among other techniques, you will learn how to locate: Hidden Social Network Content Cell Phone Subscriber Information Deleted Websites & Posts Missing Facebook Profile Data Full Twitter Account Data Alias Social Network Profiles Free Investigative Software Useful Browser Extensions Alternative Search Engine Results Website Owner Information Photo GPS & Metadata Live Streaming Social Content Social Content by Location IP Addresses of Users Additional User Accounts Sensitive Documents & Photos Private Email Addresses Duplicate Video Posts Mobile App Network Data Unlisted Addresses &#s Public Government Records Document Metadata Rental Vehicle Contracts Online Criminal Activity Personal Radio Communications Compromised Email Information Automated Collection Solutions Linux Investigative Programs Dark Web Content (Tor) Restricted YouTube Content Hidden Website Details Vehicle Registration Details

Provides an unclassified reference handbook which explains the categories of intelligence threat, provides an overview of worldwide threats in each category, and identifies available resources for obtaining threat information. Contents: intelligence collection activities and disciplines (computer intrusion, etc.); adversary foreign intelligence operations (Russian, Chinese, Cuban, North Korean and Romanian); terrorist intelligence operations; economic collections directed against the U.S. (industrial espionage); open source collection; the changing threat and OPSEC programs.

This book has been considered by academicians and scholars of great significance and value to literature. This forms a part of the knowledge base for future generations. So that the book is never forgotten we have represented this book in a print format as the same form as it was originally first published. Hence any marks or annotations seen are left intentionally to preserve its true nature.

We Are Bellingcat
Python for Data Analysis
The Tao of Open Source Intelligence
A Dictionary Of Arts, Sciences, Literature And General Information (Volume Xx) Ode To Payment Of Members
Operator Handbook
Resources for Searching and Analyzing Online Information
Hacking Web Intelligence
A Beginner's Guide to Protecting and Recovering from Ransomware Attacks
Digital Witness
Critical Infrastructure Security and Resilience
A Hacker's Guide to Online Intelligence Gathering Tools and Techniques
The Twenty-Six Words That Created the Internet

The Operator Handbook takes three disciplines (Red Team, OSINT, Blue Team) and combines them into one complete reference guide. The book contains 123 individual cheat sheet references for many of the most frequently used tools and techniques by practitioners. Over 400 pages of content to assist the most seasoned cybersecurity veteran or someone just getting started in the career field. The goal of combining all disciplines into one book was to remove the artificial barriers that only certain knowledge exists within a "Team". The reality is today's complex digital landscape demands some level of knowledge in all areas. The "Operator" culture should mean a well-rounded team member no matter the "Team" you represent. All cybersecurity practitioners are Operators. The Blue Team should observe and understand Red Team tactics, Red Team should continually push collaboration with the Blue Team, and OSINT should continually work to peel back evidence of evil doers scattered across disparate data sources. In the spirit of having no separation, each reference is listed in alphabetical order. Not only does this remove those team separated notions, but it also aids in faster lookup. We've all had the same experience where we knew there was an "NMAP Cheat Sheet" but did it fall under Networking, Windows, or Tools? In the Operator Handbook it begins with "N" so flip to the N's section. Also almost every topic is covered in "How to exploit X" and "How to defend X" perspectives. Tools and topics covered: Cloud (AWS, Azure, GCP), Windows, macOS, Linux, Android, iOS, DevOps (Docker, Kubernetes), OSINT, Ports, Forensics, Malware Resources, Defender tools, Attacker tools, OSINT tools, and various other supporting tools (Vim, iptables, nftables, etc...). This handbook was truly meant to be a single source for the most common tool and techniques an Operator can encounter while on the job. Search Copy Paste L33t.

Open source intelligence (OSINT) and web reconnaissance are rich topics for infosec professionals looking for the best ways to sift through the abundance of information widely available online. In many cases, the first stage of any security assessment—that is, reconnaissance—is not given enough attention by security professionals, hackers, and penetration testers. Often, the information openly present is as critical as the confidential data. Hacking Web Intelligence shows you how to dig into the Web and uncover the information many don't even know exists. The book takes a holistic approach that is not only about using tools to find information online but also how to link all the information and transform it into presentable and actionable intelligence. You will also learn how to secure your information online to prevent it being discovered by these reconnaissance methods. Hacking Web Intelligence is an in-depth technical reference covering the methods and techniques you need to unearth open source information from the Internet and utilize it for the purpose of targeted attack during a security assessment. This book will introduce you to many new and leading-edge reconnaissance, information gathering, and open source intelligence methods and techniques, including metadata extraction tools, advanced search engines, advanced browsers, power searching methods, online anonymity tools such as TOR and i2p, OSINT tools such as Maltego, Shodan, Creepy, SearchDiggity, Recon-ng, Social Network Analysis (SNA), Darkweb/Deepweb, data visualization, and much more. Provides a holistic approach to OSINT and Web recon, showing you how to fit all the data together into actionable intelligence Focuses on hands-on tools such as TOR, i2p, Maltego, Shodan, Creepy, SearchDiggity, Recon-ng, FOCA, EXIF, Metagoofil, MAT, and many more Covers key technical topics such as metadata searching, advanced browsers and power searching, online anonymity, Darkweb / Deepweb, Social Network Analysis (SNA), and how to manage, analyze, and visualize the data you gather Includes hands-on technical examples and case studies, as well as a Python chapter that shows you how to create your own information-gathering tools and modify existing APIs

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.

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 field of artificial intelligence (AI) and the law is on the cusp of a revolution that began with text analytic programs like IBM's Watson and Debater and the open-source information management architectures on which they are based. Today, new legal applications are beginning to appear and this book - designed to explain computational processes to non-programmers - describes how they will change the practice of law, specifically by connecting computational models of legal reasoning directly with legal text, generating arguments for and against particular outcomes, predicting outcomes and explaining these predictions with reasons that legal professionals will be able to evaluate for themselves. These legal applications will support conceptual legal information retrieval and allow cognitive computing, enabling a collaboration between humans and computers in which each does what it can do best. Anyone interested in how AI is changing the practice of law should read this illuminating work.

The present book includes extended and revised versions of papers presented during the 2018 International Computer Symposium (ICS 2018), held in Yunlin, Republic of China (Taiwan), on December 20-22, 2018. The 86 papers presented were carefully reviewed and selected from 263 submissions from 11 countries. The variety of the topics include machine learning, sensor devices and platforms, sensor networks, robotics, embedded systems, networks, operating systems, software system structures, database design and models, multimedia and multimodal retrieval, object detection, image processing, image compression, mobile and wireless security.

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.

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

Theories, Methods, Tools and Technologies
Open Source Intelligence in the Twenty-First Century
23rd International Computer Symposium, ICS 2018, Yunlin, Taiwan, December 20–22, 2018, Revised Selected Papers
Artificial Intelligence and Legal Analytics
Open Source Intelligence Investigation
Open Source Intelligence in a Networked World
Open Source Intelligence and Web Reconnaissance Concepts and Techniques

Open Source Intelligence Tools and Resources Handbook
Data Wrangling with Pandas, NumPy, and IPython
Advanced Criminal Investigations and Intelligence Operations
Penetration Testing with Perl
Intelligence Theory And Practice In Traditional China

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.
Knowledge is power: In today's era of knowledge-based economies, constantly changing business environments, severe competition, and globalization, gaining the knowledge edge will greatly empower an organization to stay on the cutting edge. Intelligence Methods and Systems Advancements for Knowledge-Based Business examines state-of-the-art research in decision sciences and business intelligence, and the applications of knowledge-based business with information systems. This comprehensive volume will provide researchers, academics, and business professionals with the research and inspiration they need to strengthen and empower their businesses in today's world.
But The Tao of Spycraft is more than an examination of military tactics; it also provides a thorough overview of the history of spies in China, emphasizing their early development, ruthless employment, and dramatic success in subverting famous generals, dooming states to extinction, and facilitating the rise of the first imperial dynasty known as the Ch'in.
"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.
This book presents the latest trends in attacks and protection methods of Critical Infrastructures. It describes original research models and applied solutions for protecting major emerging threats in Critical Infrastructures and their underlying networks. It presents a number of emerging endeavors, from newly adopted technical expertise in industrial security to efficient modeling and implementation of attacks and relevant security measures in industrial control systems; including advancements in hardware and services security, interdependency networks, risk analysis, and control systems security along with their underlying protocols. Novel attacks against Critical Infrastructures (CI) demand novel security solutions. Simply adding more of what is done already (e.g. more thorough risk assessments, more expensive Intrusion Prevention/Detection Systems, more efficient firewalls, etc.) is simply not enough against threats and attacks that seem to have evolved beyond modern analyses and protection methods. The knowledge presented here will help Critical Infrastructure authorities, security officers, Industrial Control Systems (ICS) personnel and relevant researchers to (i) get acquainted with advancements in the field, (ii) integrate security research into their industrial or research work, (iii) evolve current practices in modeling and analyzing Critical Infrastructures, and (iv) moderate potential crises and emergencies influencing or emerging from Critical Infrastructures.
Get complete instructions for manipulating, processing, cleaning, and crunching datasets in Python. Updated for Python 3.6, the second edition of this hands-on guide is packed with practical case studies that show you how to solve a broad set of data analysis problems effectively. You'll learn the latest versions of pandas, NumPy, IPython, and Jupyter in the process. Written by Wes McKinney, the creator of the Python pandas project, this book is a practical, modern introduction to data science tools in Python. It's ideal for analysts new to Python and for Python programmers new to data science and scientific computing. Data files and related material are available on GitHub. Use the IPython shell and Jupyter notebook for exploratory computing Learn basic and advanced features in NumPy (Numerical Python) Get started with data analysis tools in the pandas library Use flexible tools to load, clean, transform, merge, and reshape data Create informative visualizations with matplotlib Apply the pandas groupby facility to slice, dice, and summarize datasets Analyze and manipulate regular and irregular time series data Learn how to solve real-world data analysis problems with thorough, detailed examples
Tradecraft is a term used within the intelligence community to describe the methods, practices, and techniques used in espionage and clandestine investigations. Whether the practitioner is a covert agent for the government or an identity thief and con man, the methods, practices, tactics, and techniques are often the same and sometimes learned from the same sources. Advanced Criminal Investigations and Intelligence Operations: Tradecraft Methods, Practices, Tactics, and Techniques reveals how intelligence officers and investigators conduct their tradecraft. You'll learn how to plan an operation, how to build an identity and cover story for deep cover operations, and how to detect those who have created false identities for illegal purposes. You'll also get insight into the technical aspects of intelligence (the INTs), counterintelligence, and criminal investigations, and legal considerations for conducting intelligence investigations. Topics include: A discussion of black bag operational planning HUMINT (human intelligence)—the gathering of information from human sources DAME (defenses against methods of entry), forced entry into buildings, safes and combination locks, and automobile locks PSYOPS (psychological operations) and the use of social networks ELINT (electronic intelligence) and SIGINT (signals intelligence)—electronic interception of intelligence, bugs, wiretaps, and other communications interceptions EMINT (emanations intelligence), which concerns the emanation of data, signals, or other intelligence from C4I systems IMINT (imagery intelligence), involving any intelligence gathered using images Intelligence files and analytical methods Based upon the author's training and experience over more than three decades as a law enforcement investigator and military officer, as well as research conducted as an attorney and in academia, the book provides you with an insider perspective on sensitive covert and overt operations and sources. Supplemented with roughly 140 illustrations and photos, this collection of special skills and reference materials is essential to the professional investigator and intelligence operative.

New Trends in Computer Technologies and Applications
What it Takes to Disappear in America
Intelligence Threat Handbook
The Open-Source Everything Manifesto
Handbook of Intelligence Studies
New Approaches and Opportunities
Algorithms for OSINT
From Strategy to Implementation
Tradecraft Methods, Practices, Tactics, and Techniques