Algorithms For Osint

The book explains how openly available information is undervalued by the intelligence community and how analysts can use of this huge amount of 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
Psychopharmacology is the study of drugs used to treat psychiatric disorders. This textbook looks at the use of clinical algorithms in relation to clinical psychopharmacology, especially the nature and current use of algorithms, and their future potential for the medical community.
A riveting account of espionage for the digital age, from one of America's leading intelligence experts Spying has never been more ubiquitous—or less understood. The world is drowning in spy movies, TV shows, and novels, but universities offer more courses on rock and roll than on the CIA and there are more congressional experts on powdered milk than espionage. This crisis in intelligence education is distorting public opinion, fueling conspiracy theories, and hurting intelligence policy. In Spies, Lies, and Algorithms, Amy Zegart separates fact from fiction as she offers an engaging and enlightening account of the past, present, and future of American espionage as it faces a revolution driven by digital technology. Drawing on decades of research and hundreds of interviews with intelligence officials, Zegart provides a history of U.S. espionage, from George Washington's Revolutionary War spies to today's spy satellites; examines how fictional spies are influencing real officials; gives an overview of intelligence basics and life inside America's intelligence agencies; explains the deadly cognitive biases that can mislead analysts; and explores the vexed issues of traitors, covert action, and congressional oversight. Most of all, Zegart describes how technology is empowering new enemies and opportunities, and creating powerful new players, such as private citizens who are successfully tracking nuclear threats using little more than Google Earth. And she shows why cyberspace is, in many ways, the ultimate cloak-and-dagger battleground, where nefarious actors employ deception, subterfuge, and advanced technology for theft, espionage, and information warfare. A fascinating and revealing account of espionage for the digital age, Spies, Lies, and Algorithms is essential reading for anyone who wants to understand the reality of spying today.
These proceedings represent the work of contributors to the 16th International Conference on Cyber Warfare and Security (ICCWS 2021), hosted by joint collaboration of Tennessee Tech Cybersecurity Education, Research and Outreach Center (CEROC), Computer Science department and the Oak Ridge National Laboratory, Tennessee on 25-26 February 2021. The Conference Co-Chairs are Dr. Juan Lopez Jr, Oak Ridge National Laboratory, Tennessee, and Dr. Ambareen Siraj, Tennessee Tech's Cybersecurity Education, Research and Outreach Center (CEROC), and the Program Chair is Dr. Kalyan Perumalla, from Oak Ridge National Laboratory, Tennessee.
Learn how to apply modern AI to create powerful cybersecurity solutions for malware, pentesting, social engineering, data privacy, and intrusion detection Key Features Manage data of varying complexity to protect your system using the Python ecosystem Apply ML to pentesting, malware, data privacy, intrusion detection system(IDS) and social engineering Automate your daily workflow by addressing various security challenges using the recipes covered in the book Book Description Organizations today face a major threat in terms of cybersecurity, from malicious URLs to credential reuse, and having robust security systems can make all the difference. With this book, you'll learn how to use Python libraries such as TensorFlow and scikit-learn to implement the latest artificial intelligence (AI) techniques and handle challenges faced by cybersecurity researchers. You'll begin by exploring various machine learning (ML) techniques and tips for setting up a secure lab environment. Next, you'll implement key ML algorithms such as clustering, gradient boosting, random forest, and XGBoost. The book will guide you through constructing classifiers and features for malware, which you'll train and test on real samples. As you progress, you'll build self-learning, reliant systems to handle cybersecurity tasks such as identifying malicious URLs, spam email detection, intrusion detection, network protection, and tracking user and process behavior. Later, you'll apply generative adversarial networks (GANs) and autoencoders to advanced security tasks. Finally, you'll delve into secure and private AI to protect the privacy rights of consumers using your ML models. By the end of this book, you'll have the skills you need to tackle real-world problems faced in the cybersecurity domain using a recipe-based approach. What you will learn Learn how to build malware classifiers to detect suspicious activities Apply ML to generate custom malware to pentest your security Use ML algorithms with complex datasets to implement cybersecurity concepts Create neural networks to identify fake videos and images Secure your organization from one of the most popular threats – insider threats Defend against zero-day threats by constructing an anomaly detection system Detect web vulnerabilities effectively by combining Metasploit and ML Understand how to train a model without exposing the training data Who this book is for This book is for cybersecurity professionals and security researchers who are looking to implement the latest machine learning techniques to boost computer security, and gain insights into securing an organization using red and blue team ML. This recipe-based book will also be useful for data scientists and machine learning developers who want to experiment with smart techniques in the cybersecurity domain. Working knowledge of Python programming and familiarity with cybersecurity fundamentals will help you get the most out of this book.
If you're interested in using social media as an investigative tool, Introduction to Social Media Investigation will show you how! Social networks and social media, like Facebook, Twitter, and Foursquare, are some of the most popular services on the Web, with hundreds of millions of users. The public information that people share on these sites can be valuable for anyone interested in investigating people of interest through open, public sources. Social media as an investigative device is in its infancy and not well understood. This book presents an overview of social media and discusses special skills and techniques to use when conducting investigations. The book features hands-on tutorials and case studies and offers additional data-gathering techniques. Presents an overview of social media sites, information types, privacy policies, and other general issues relevant to investigating individuals online Discusses the special skills and techniques needed when conducting investigations using social media Includes hands-on tutorials and case studies using Facebook, LinkedIn, Twitter, and other social media sites using proven investigative techniques Shows how to gather additional data using advanced techniques such as crowdsourcing, data mining, and network analysis
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.

Proceedings, IMPA, Rio de Janeiro, Brazil, October 20-23, 1998
Internet of Things, Threats, Landscape, and Countermeasures
ECCWS 2014
Algorithms for Osint
A Practical Guide to Online Intelligence
Under the Rose
Hunting Cyber Criminals
Open Source Intelligence Methods and Tools
Human Interaction, Emerging Technologies and Future Systems V
Proceedings of the 5th International Virtual Conference on Human Interaction and Emerging Technologies, IHIET 2021, August 27–29, 2021 and the 6th IHIET: Future Systems (IHIET-FS 2021), October 28–30, 2021, France
Innovative Advanced Materials for Energy Storage and Beyond
Open Source Intelligence Investigation
Spies, Lies, and Algorithms

Discover how conservation can be made more effective through strengthening links between science research, policy and practice. This title is also available as Open Access on Cambridge Core.
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 b 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 in-depth analysis shows how the high stakes contest surrounding open source information is forcing significant reform within the U.S. intelligence community, the homeland security sector, and among citizen activists. • Critique and commentary from intelligence officials and analysts regarding open source reforms within the intelligence community and homeland security sector • Three interrelated case studies through which post-9/11 U.S. intelligence reform is analyzed and critiqued • Examples of collateral, including official and unofficial photos, from the 2007 and 2008 Open Source Conferences sponsored by the Director of National Intelligence • A timeline of key open source developments, including the establishment of associated commissions and changes in organizational structures, policies, and cultures • Appendices containing excerpts of key open source legislation and policy documents • A bibliography of open source-related scholarship and commentary
Cybercrime remains a growing challenge in terms of security and privacy practices. Working together, deep learning and cyber security experts have recently made significant advances in the fields of intrusion detection, malicious code analysis and forensic identification. This book addresses questions of how deep learning methods can be used to advance cyber security objectives, including detection, modeling, monitoring and analysis of as well as defense against various threats to sensitive data and security systems. Filling an important gap between deep learning and cyber security communities, it discusses top covering a wide range of modern and practical deep learning techniques, frameworks and development tools to enable readers to engage with the cutting-edge research across various aspects of cyber security. The book focuses on mature and proven techniques, and provides ample examples to help readers grasp the key points.
Can machine learning techniques solve our computer security problems and finally put an end to the cat-and-mouse game between attackers and defenders? Or is this hope merely hype? Now you can dive into the science and answer this question for yourself! With this practical guide, you'll explore ways to apply machine learning to security issues such as intrusion detection, malware classification, and network analysis. Machine learning and security specialists Clarence Chio and David Freeman provide a framework for discussing the marriage of these two fields, as well as a toolkit of machine-learning algorithms that you can apply to an array of security problems. This book is ideal for security engineers and data scientists alike. Learn how machine learning has contributed to the success of modern spam filters Quickly detect anomalies, including breaches, fraud, and impending system failure Conduct malware analysis by extracting useful information from computer binaries Uncover attackers within the network by finding patterns inside datasets Examine how attackers exploit consumer-facing websites and app functionality Translate your machine learning algorithms from the lab to production Understand the threat attackers pose to machine learning solutions
At the beginning of the 21st century, new forms and dynamics of interplay are constituted at the interfaces of media, art and politics. Current challenges in society and ecology, like climate, surveillance, virtualization of the global financial markets, are characterized by hybrid and subtle technologies. They are ubiquitous, turn out to be increasingly complex and act invasively. New media art utilizes its broad range of expression in order to tackle the most urgent topics through multi-sensorial, participatory, and activist approaches. This volume shows how media artists address, with a political lens, the core of these developments critically and productively. With contributions by Elisa Arca, Andrés Burbano, Derek Curry, Yael Eylat Van Essen, Mathias Fuchs, Jennifer Gradecki, Sabine Himmelsbach, Ingrid Hoelzl, Katja Kwastek, José-Carlos Mariátegui, Gerald Nestler, Randall Packer, Viola Rühse, Chris Salter.
Powerful, Flexible Tools for a Data-Driven World As the data deluge continues in today's world, the need to master data mining, predictive analytics, and business analytics has never been greater. These techniques and tools provide unprecedented insights into data, enabling better decision making and forecasting, and ultimately the solution of increasingly complex problems. Learn from the Creators of the RapidMiner Software Written by leaders in the data mining community, including the developers of the RapidMiner software, RapidMiner: Data Mining Use Cases and Business Analytics Applications provides an in-depth introduction to the application of data mining and business analytics techniques and tools in scientific research, medicine, industry, commerce, and diverse other sectors. It presents the most powerful and flexible open source software solutions: RapidMiner and RapidAnalytics. The software and their extensions can be freely downloaded at www.RapidMiner.com. Understand Each Stage of the Data Mining Process The book and software tools cover all relevant steps of the data mining process, from data loading, transformation, integration, aggregation, and visualization to automated feature selection, automated parameter and process optimization, and integration with other tools, such as R packages or your IT infrastructure via web services. The book and software also extensively discuss the analysis of unstructured data, including text and image mining. Easily Implement Analytics Approaches Using RapidMiner and RapidAnalytics Each chapter describes an application, how to approach it with data mining methods, and how to implement it with RapidMiner and RapidAnalytics. These application-oriented chapters give you not only the necessary analytics to solve problems and tasks, but also reproducible, step-by-step descriptions of using RapidMiner and RapidAnalytics. The case studies serve as blueprints for your own data mining applications, enabling you to effectively solve similar problems.
Machine learning algorithms and artificial intelligence influence many aspects of life today. This report identifies some of their shortcomings and associated policy risks and examines some approaches for combating these problems.

Introduction to Social Media Investigation
An Intelligence Agency for the People
Over 80 recipes on how to implement machine learning algorithms for building security systems using Python
Open Source Information and the Reshaping of U.S. Intelligence
Open Source Intelligence in a Networked World
Synthesis, Characterization and Applications
Publications Combined: Studies In Open Source Intelligence (OSINT) And Information
Security Informatics
Strategies in Contemporary New Media Art
A Clandestine Tradecraft Manual
16th International Conference on Cyber Warfare and Security
Conservation Research, Policy and Practice
The History and Future of American Intelligence

Essential reading for cybersecurity professionals, security analysts, policy experts, decision-makers, activists, and law enforcement! During the Arab Spring movements, the world witnessed the power of social media to dramatically shape events. Now this timely book shows government decision-makers, security analysts, and activists how to use the social world to improve security locally, nationally, and globally--and cost-effectively. Authored by two technology/behavior/security professionals, Using Social Media for Global Security offers pages of instruction and detail on cutting-edge social media technologies, analyzing social media data, and building crowdsourcing platforms. The book teaches how to collect social media data and analyze it to map the social networks of terrorists and sex traffickers, and forecast attacks and famines. You will learn how to coalesce communities through social media to help catch murderers, coordinate disaster relief, and collect intelligence about drug smuggling from hard-to-reach areas. Also highlighting dramatic case studies drawn from the headlines, this crucial book is a must-read. Illustrates linguistic, correlative, and network analysis of OSINT Examines using crowdsourcing technologies to work and engage with populations globally to solve security problems Explores how to ethically deal with social media data without compromising people's rights to privacy and freedom of expression Shows activists fighting against oppressive regimes how they can protect their identities online If you're responsible for maintaining local, national or global security, you'll want to read Using Social Media for Global Security.
Internet of Things (IoT) is an ecosystem comprised of heterogeneous connected devices that communicate to deliver capabilities making our living, cities, transport, energy, and other areas more intelligent. This book delves into the different cyber-security domains and their challenges due to the massive amount and the heterogeneity of devices. This book introduces readers to the inherent concepts of IoT. It offers case studies showing how IoT counteracts the cyber-security concerns for domains. It provides suggestions on how to mitigate cyber threats by compiling a catalogue of threats that currently comprise the contemporary threat landscape. It then examines different security measures that can be applied to system installations or operational environment and discusses how these measures may alter the threat exploitability level and/or the level of the technical impact. Professionals, graduate students, researchers, academicians, and institutions that are interested in acquiring knowledge in the areas of IoT and cyber-security, will find this book of interest.
This highly informative and carefully presented book covers the most recent advances as well as comprehensive reviews addressing novel and state-of-the-art topics from active researchers in innovative advanced materials and hybrid materials, concerning not only their synthesis, preparation, and characterization but especially focusing on the applications of such materials with outstanding performance.
The intended audience of this book are those who are called to work in oppressive regions of the world; particularly, journalists, missionaries, and liberators who find themselves in an asymmetric fight. The content inside does not derive from any one nation or organization's methods, but a culmination of many. It pulls from governmental, criminal, and militant techniques without regard to nationality. Topics of study include: creating covers, counter-surveillance, establishing caches, planning and executing urban, rural, and vehicular meetings, planning ratlines, and appropriate use of technology to augment clandestine communications.
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
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.
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.

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.

Internet Searches for Vetting, Investigations, and Open-Source Intelligence
ECCWS2014-Proceedings of the 13th European Conference on Cyber warefare and Security
Machine Learning for Cybersecurity Cookbook
Resources for Searching and Analyzing Online Information
The Black Box Society
We Are Bellingcat
Counterterrorism and Open Source Intelligence
Defining Second Generation Open Source Intelligence (Osint) for the Defense Enterprise
Retracing Political Dimensions
Open Source Intelligence and Web Reconnaissance Concepts and Techniques
The Risks of Bias and Errors in Artificial Intelligence
Aviation Systems
Machine Learning and Security

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

This book gathers the proceedings of the 2018 International Conference on Digital Science (DSIC'18), held in Budva, Montenegro, on October 19 – 21, 2018. DSIC'18 was an international forum for researchers and practitioners to present and discuss the latest innovations, trends, results, experiences and concerns in Digital Science. The main goal of the Conference was to efficiently disseminate original findings in the natural and social sciences, art & the humanities. The contributions address the following topics: Digital Agriculture & Food Technology Digital Art & Humanities Digital Economics Digital Education Digital Engineering Digital Environmental Sciences Digital Finance, Business & Banking Digital Health Care, Hospitals & Rehabilitation Digital Media Digital Medicine, Pharma & Public Health Digital Public Administration Digital Technology & Applied Sciences Digital Virtual Reality

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

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.

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.

Ten Strategies of a World-Class Cyber Security Operations Center conveys MITRE's accumulated expertise on enterprise-grade computer network defense. It covers ten key qualities of leading Cyber Security Operations Centers (CSOCs), ranging from their structure and organization, to processes that best enable smooth operations, to approaches that extract maximum value from key CSOC technology investments. This book offers perspective and context for key decision points in structuring a CSOC, such as what capabilities to offer, how to architect large-scale data collection and analysis, and how to prepare the CSOC team for agile, threat-based response. If you manage, work in, or are standing up a CSOC, this book is for you. It is also available on MITRE's website, www.mitre.org.

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.

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.

Cyber-Security Threats, Actors, and Dynamic Mitigation
Management of the Integrated Aviation Value Chain
The Secret Algorithms That Control Money and Information
Data Mining Use Cases and Business Analytics Applications
Deep Learning Applications for Cyber Security
An Intelligence in Our Image
Textbook of Treatment Algorithms in Psychopharmacology
SIBGRAPI '98. International Symposium on Computer Graphics, Image Processing, and Vision
Digital Science
RapidMiner
No More Secrets: Open Source Information and the Reshaping of U.S. Intelligence
Automating Open Source Intelligence
Using Social Media for Global Security

Intelligence and Security Informatics (ISI) is defined as the study of the development and use of advanced information systems and technologies for national, international, and societal security-related applications. With the rise of global terrorism, the field has been given an increasing amount of attention from academic researchers, law enforcement, intelligent experts, information technology consultants and practitioners. SECURITY INFORMATICS is global in scope and perspective. Leading experts will be invited as contributing authors from the US, UK, Denmark, Israel, Singapore, Hong Kong, Taiwan, Europe, etc. It is the first systematic, archival volume treatment of the field and will cover the very latest advances in ISI research and practice. It is organized in four major subject areas: (1) Information and Systems Security, (2) Information Sharing and Analysis in Security Informatics, (3) Infrastructure Protection and Emergency Responses, and (4) National Security and Terrorism Informatics.

This volume on computer graphics is aimed at researchers, professors, practitioners, students, and other computing professionals.

Every day, corporations are connecting the dots about our personal behavior—silently scrutinizing clues left behind by our work habits and Internet use. But who connects the dots about what firms are doing with all this information? Frank Pasquale exposes how powerful interests abuse secrecy for profit and explains ways to rein them in.

Cyber-Security Threats, Actors, and Dynamic Mitigation provides both a technical and state-of-the-art perspective as well as a systematic overview of the recent advances in different facets of cyber-security. It covers the methodologies for modeling attack strategies used by threat actors targeting devices, systems, and networks such as smart homes, critical infrastructures, and industrial IoT. With a comprehensive review of the threat landscape, the book explores both common and sophisticated threats to systems and networks. Tools and methodologies are presented for precise modeling of attack strategies, which can be used both proactively in risk management and reactively in intrusion prevention and response systems. Several contemporary techniques are offered ranging from reconnaissance and penetration testing to malware detection, analysis, and mitigation. Advanced machine learning-based approaches are also included in the area of anomaly-based detection, that are capable of detecting attacks relying on zero-day vulnerabilities and exploits. Academics, researchers, and professionals in cyber-security who want an in-depth look at the contemporary aspects of the field will find this book of interest. Those wanting a unique reference for various cyber-security threats and how they are detected, analyzed, and mitigated will reach for this book often.

Algorithms for OSINT
Ten Strategies of a World-Class Cybersecurity Operations Center
Protecting Systems with Data and Algorithms
Theories, Methods, Tools and Technologies
Red Team + OSINT + Blue Team Reference
Operator Handbook
Hacking Web Intelligence
A Hands-on Approach
Critical Infrastructure Security and Resilience
Open Source Intelligence Techniques
From Strategy to Implementation
A Hacker's Guide to Online Intelligence Gathering Tools and Techniques