# Open Source Intelligence Techniques

**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**

**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.**

**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.**

**'If you're thinking about trying mindfulness, this is the perfect introduction....I'm grateful to Andy for helping me on this journey.' BILL GATES 'It's kind of genius' EMMA WATSON Feeling stressed about Christmas/Brexit/everthing? Try this... Demystifying meditation for the modern world: an accessible and practical route to improved health, happiness and well being, in as little as 10 minutes. Andy Puddicombe, founder of the celebrated Headspace, is on a mission: to get people to take 10 minutes out of their day to sit in the now. Here he shares his simple to learn, but highly effective techniques of meditation. * Rest an anxious, busy mind * Find greater ease when faced with difficult emotions, thoughts, circumstances * Improve focus and concentration * Sleep better * Achieve new levels of calm and fulfilment. The benefits of mindfulness and meditation are well documented and here Andy brings this ancient practice into the modern world, tailor made for the most time starved among us. First published as Get Some Headspace, this reissue shows you how just 10 minutes of mediation per day can bring about life changing results.**

**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.**

**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**

**Python is fast becoming the programming language of choice for hackers, reverse engineers, and software testers because it's easy to write quickly, and it has the low-level support and libraries that make hackers happy. But until now, there has been no real manual on how to use Python for a variety of hacking tasks. You had to dig through forum posts and man pages, endlessly tweaking your own code to get everything working. Not anymore. Gray Hat Python explains the concepts behind hacking tools and techniques like debuggers, trojans, fuzzers, and emulators. But author Justin Seitz goes beyond theory, showing you how to harness existing Python-based security tools—and how to build your own when the pre-built ones won't cut it. You'll learn how to: –Automate tedious reversing and security tasks –Design and program your own debugger –Learn how to fuzz Windows drivers and create powerful fuzzers from scratch –Have fun with code and library injection, soft and hard hooking techniques, and other software trickery –Sniff secure traffic out of an encrypted web browser session –Use PyDBG, Immunity Debugger, Sulley, IDAPython, PyEMU, and more The world's best hackers are using Python to do their handiwork. Shouldn't you?**

**Completely rewritten 7th edition contains over 550 pages and 30 chapters! It is time to look at OSINT in a different way. For many years, and within the previous six 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. The new OSINT professional must be self-sustaining and possess their own tools and resources. You will become a more proficient subject matter expert who will be armed with the knowledge and readiness to articulate the sources of your findings. Aside from eleven brand new chapters, hundreds of pages have been updated to keep your OSINT investigative methods fresh. Furthermore, an entire new section featuring Methodology, Workflow, Documentation, and Ethics provides a clear game plan for your next active investigation. All-new custom search tools, report templates, and detailed documents are included via download. Today, we start over.**

**Open Source Intelligence Gathering - DELUXE, FULL COLOR EDITION: How the FBI, Media, and Public Used OSINT to Identify the January 6, 2021 Capitol Rioters**
**Practical Threat Intelligence and Data-Driven Threat Hunting**
**Red Team + OSINT + Blue Team Reference**
**A hands-on guide to threat hunting with the ATT&CK™ Framework and open source tools**
**Cyber Warfare**
**Theories, Methods, Tools and Technologies**
**A Practical Guide to Online Intelligence**
**Extreme Privacy**
**Open Source Intelligence and Web Reconnaissance Concepts and Techniques**
**Open Source Intelligence Tools and Resources Handbook**
**How to Find Out Anything**
**Open Source Intelligence Techniques**

***"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.***

***Fifth Edition Sheds New Light on Open Source Intelligence Collection and Analysis.Author Michael Bazzell has been well known and respected in government circles for his ability to locate personal information about any target through Open Source Intelligence (OSINT). In this book, he shares his methods in great detail. Each step of his process is explained throughout sixteen chapters of specialized websites, application programming interfaces, and software solutions. Based on his live and online video training at IntelTechniques.com, 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 improve anyone's online investigative skills. Among other techniques, you will learn how to locate: Hidden Social Network ContentCell Phone Subscriber InformationDeleted Websites & PostsMissing Facebook Profile DataFull Twitter Account DataAlias Social Network ProfilesFree Investigative SoftwareUseful Browser ExtensionsAlternative Search Engine ResultsWebsite Owner InformationPhoto GPS & MetadataLive Streaming Social ContentSocial Content by LocationIP Addresses of UsersAdditional User AccountsSensitive Documents & PhotosPrivate Email AddressesDuplicate Video PostsMobile App Network DataUnlisted Addresses & #sPublic Government RecordsDocument MetadataRental Vehicle ContractsOnline Criminal ActivityPersonal Radio CommunicationsCompromised Email InformationWireless Routers by LocationHidden Mapping ApplicationsDark Web Content (Tor)Restricted YouTube ContentHidden Website DetailsVehicle Registration Details***

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

***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.***

***Vibrantly illustrated, NOWHERE TO HIDE: Open Source Intelligence Gathering provides practical insight into the investigative tools and open source intelligence gathering (commonly known as "OSINT") used by law enforcement, the media, and the general public to identify individuals involved in the events of January 6, 2021, at the U.S. Capitol Building in Washington, DC. NOWHERE TO HIDE retraces the FBI's investigative techniques - some using cutting-edge technology and others using old fashioned, knocking-on-doors detective work - used to pursue the hundreds of thousands of leads received from the general public. NOWHERE TO HIDE is filled with real world case studies, specific resources and practical "how to" guides to equip both beginner and seasoned OSINT investigators with the right tools for their OSINT toolboxes. This insightful volume includes 36 case studies that follow the FBI's investigations of individual persons of interest, including the tactics, techniques, and procedures used by law enforcement, the media, and public sleuths to track down, identify, and - most importantly - verify the identities of suspected rioters. Learn how the FBI sifted through hundreds of thousands of leads, false positives, dead ends, as well as numerous unexpected leads to perform their investigations. NOWHERE TO HIDE provides vivid context around the events of January 6, 2021, at the U.S. Capitol Building in Washington, DC, which left five people - one police officer and four protestors - dead by the end of the assault. Effective OSINT research requires a combination of technical knowledge to find the Who, What, When, Where, and How threads of data and information as well as taking into account our unpredictable human nature that sometimes leads us to do the things we do (the Why). OSINT is both science and art. NOWEHERE TO HIDE provides practical, actionable information to help both novice and expert investigators, researchers, advocates, and journalists navigate and penetrate OSINT resources to find the information and evidence they seek. Daniel Farber Huang is author of "Practical Cyber Security for Extremely Busy People" and a consultant to a wide range of organizations on cyber and strategy issues. He has worked closely with numerous federal, state, and local law enforcement agencies across the U.S. on providing solutions to their mobile technology requirements. He has focused on providing hardware and software solutions to federal field agents, investigators, the police, and other authorities to support them in performing their duties. He is a strategic consultant helping a wide range of companies in different industries reduce risks at all levels of their organizations, including their cyber security. Daniel is also a documentary photographer and freelance journalist.***

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

***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.***

***Be like Bond. James Bond. MI6 Spy Skills for Civilians shows readers how to master the skills of an agent in Her Majesty's Secret Service in order to protect themselves, be sneakier and handle any situation - even if it involves escaping from a hostile foreign country. Inside they'll find dozens of real secret agent skills and tips detailed and explained, often with helpful illustrations to clarify how they're done. Sections covered include: Surveillance Safe Travel Tips Dead Letter Boxes Brush Contacts Self Defense Innocuous and Natural Weapons Intelligence Gathering Subterfuge Covert Methods of Entry Insertion and Extraction Techniques And More! Readers will find more than 100 tips and techniques in all, detailed by Red Riley, a former SAS and MI6 operative. It's invaluable information formerly available only to a select few - and now it's available to readers, too! Includes a foreword by Ian Sharp, action director of the James Bond film Goldeneye.***

***From Strategy to Implementation***
***The Tao of Open Source Intelligence***
***Python Programming for Hackers and Reverse Engineers***
***The Great Mental Models: General Thinking Concepts***
***The Oxford Handbook of National Security Intelligence***
***Open Source Intelligence Methods and Tools***
***Counterterrorism and Open Source Intelligence***
***Techniques, Tactics and Tools for Security Practitioners***
***Defining Second Generation Open Source Intelligence (Osint) for the Defense Enterprise***
***Resources for Searching and Analyzing Online Information (le)***
***Open Source Intelligence in a Networked World***
***A Hacker's Guide to Online Intelligence Gathering Tools and Techniques***

Are you ready to learn everything you need to know about sourcing and recruitment? Then you've found the right book! Whether you are already working in recruitment, new to the industry, or just hoping to begin your career as a recruiter, there are essential strategies used by successful recruiters that will help you accelerate your career. Of course, no one is born knowing these things; they come from years of experience in the field. That's exactly what this book is: years of practical, real-world experience distilled into one comprehensive guide to succeeding in your recruiting career in the digital era. This book is designed to help recruiters gain a broad understanding of the industry while expanding and deepening the knowledge of more senior professionals. Whether you belong in the first category or the second, this book will help you take your career to the next level. This comprehensive recruitment and sourcing guide is divided into two parts. The first part focuses entirely on sourcing strategies. You'll learn new and creative ways to source and find great candidates, as well as how to uncover their contact details and approach them in a respectful and effective manner. And much more! The second part deals with recruitment. You'll learn how to excel in recruitment marketing, candidate engagement, recruitment analytics, candidate engagement, cold-calling, and efficiently manage many other essential aspects of your role. Both sections work together to create a comprehensive guide to excelling in every aspect of your recruitment career! The author, Jan Tegze, is an experienced recruiter with extensive talent acquisition expertise and demonstrated success in start-ups and fast-growth environments. In this book, he shares the most successful methods, tips, and strategies that he has learned, tested and implemented throughout his career, with the hope of providing the inspiration and guidance you need to develop into a top-performing recruiter and sourcer. Do you want to learn more about sourcing and recruiting? Do you want to gain a greater understanding of the recruitment business? Do you want to expand your knowledge and become a top-performing recruiter? Do you want to launch a career in the recruitment industry? Do you want to learn the strategies used by the most successful recruiters in the business? If you have answered "YES" to these questions, start reading this book NOW!

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.

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 ( é diteur).

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 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 old saying goes, "To the man with a hammer, everything looks like a nail." But anyone who has done any kind of project knows a hammer often isn't enough. The more tools you have at your disposal, the more likely you'll use the right tool for the job - and get it done right. The same is true when it comes to your thinking. The quality of your outcomes depends on the mental models in your head. And most people are going through life with little more than a hammer. Until now. The Great Mental Models: General Thinking Concepts is the first book in The Great Mental Models series designed to upgrade your thinking with the best, most useful and powerful tools so you always have the right one on hand. This volume details nine of the most versatile, all-purpose mental models you can use right away to improve your decision making, productivity, and how clearly you see the world. You will discover what forces govern the universe and how to focus your efforts so you can harness them to your advantage, rather than fight with them or worse yet- ignore them. Upgrade your mental toolbox and get the first volume today. AUTHOR BIOGRAPHY Farnam Street (FS) is one of the world's fastest growing websites, dedicated to helping our readers master the best of what other people have already figured out. We curate, examine and explore the timeless ideas and mental models that history's brightest minds have used to live lives of purpose. Our readers include students, teachers, CEOs, coaches, athletes, artists, leaders, followers, politicians and more. They're not defined by gender, age, income, or politics but rather by a shared passion for avoiding problems, making better decisions, and lifelong learning. AUTHOR HOME Ottawa, Ontario, Canada

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 Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information, he shares his methods in great detail. Each step of his process is explained throughout twenty-four 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 ContentCell Phone Subscriber InformationDeleted Websites & PostsMissing Facebook Profile DataFull Twitter Account DataAlias Social Network ProfilesFree Investigative SoftwareUseful Browser ExtensionsAlternative Search Engine ResultsWebsite Owner InformationPhoto GPS & MetadataLive Streaming Social ContentSocial Content by LocationIP Addresses of UsersAdditional User AccountsSensitive Documents & PhotosPrivate Email AddressesDuplicate Video PostsMobile App Network DataUnlisted Addresses & #sPublic Government RecordsDocument MetadataRental Vehicle ContractsOnline Criminal ActivityPersonal Radio CommunicationsCompromised Email InformationAutomated Collection SolutionsLinux Investigative ProgramsDark Web Content (Tor)Restricted YouTube ContentHidden Website DetailsVehicle Registration Details

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.

What it Takes to Disappear in America
We Are Bellingcat
Gray Hat Python
Automating Open Source Intelligence
Full Stack Recruiter
Using Open Source Information for Human Rights Investigation, Documentation, and Accountability

Social Engineering
Applying Methods of Scientific Inquiry Into Intelligence, Security, and Counterterrorism
Critical Infrastructure Security and Resilience
From Extreme Google Searches to Scouring Government Documents, a Guide to Uncovering Anything About Everyone and Everything
Get Some Headspace

*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.*

*Harden the human firewall against the most current threats Social Engineering: The Science of Human Hacking reveals the craftier side of the hacker's repertoire—why hack into something when you could just ask for access? Undetectable by firewalls and antivirus software, social engineering relies on human fault to gain access to sensitive spaces; in this book, renowned expert Christopher Hadnagy explains the most commonly-used techniques that fool even the most robust security personnel, and shows you how these techniques have been used in the past. The way that we make decisions as humans affects everything from our emotions to our security. Hackers, since the beginning of time, have figured out ways to exploit that decision making process and get you to take an action not in your best interest. This new Second Edition has been updated with the most current methods used by sharing stories, examples, and scientific study behind how those decisions are exploited. Networks and systems can be hacked, but they can also be protected; when the "system" in question is a human being, there is no software to fall back on, no hardware upgrade, no code that can lock information down indefinitely. Human nature and emotion is the secret weapon of the malicious social engineering, and this book shows you how to recognize, predict, and prevent this type of manipulation by taking you inside the social engineer's bag of tricks. Examine the most common social engineering tricks used to gain access Discover which popular techniques generally don't work in the real world Examine how our understanding of the science behind emotions and decisions can be used by social engineers Learn how social engineering factors into some of the biggest recent headlines Learn how to use these skills as a professional social engineer and secure your company Adopt effective counter-measures to keep hackers at bay By working from the social engineer's playbook, you gain the advantage of foresight that can help you protect yourself and others from even their best efforts. Social Engineering gives you the inside information you need to mount an unshakeable defense.*

*In How to Find Out Anything, master researcher Don MacLeod explains how to find what you're looking for quickly, efficiently, and accurately—and how to avoid the most common mistakes of the Google Age. Not your average research book, How to Find Out Anything shows you how to unveil nearly anything about anyone. From top CEO's salaries to police records, you'll learn little-known tricks for discovering the exact information you're looking for. You'll learn: •How to really tap the power of Google, and why Google is the best place to start a search, but never the best place to finish it. •The scoop on vast, yet little-known online resources that search engines cannot scour, such as refdesk.com, ipl.org, the University of Michigan Documents Center, and Project Gutenberg, among many others. •How to access free government resources (and put your tax dollars to good use). •How to find experts and other people with special knowledge. •How to dig up seemingly confidential information on people and businesses, from public and private companies to non-profits and international companies. Whether researching for a term paper or digging up dirt on an ex, the advice in this book arms you with the sleuthing skills to tackle any mystery.*

*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.*

*When a meteorite lands in Surrey, the locals don't know what to make of it. But as Martians emerge and begin killing bystanders, it quickly becomes clear—England is under attack. Armed soldiers converge on the scene to ward off the invaders, but meanwhile, more Martian cylinders land on Earth, bringing reinforcements. As war breaks out across England, the locals must fight for their lives, but life on Earth will never be the same. This is an unabridged version of one of the first fictional accounts of extraterrestrial invasion. H. G. Wells's military science fiction novel was first published in book form in 1898, and is considered a classic of English literature.*

*Cyber Warfare Techniques, Tactics and Tools for Security Practitioners provides a comprehensive look at how and why digital warfare is waged. This book explores the participants, battlefields, and the tools and techniques used during today's digital conflicts. The concepts discussed will give students of information security a better idea of how cyber conflicts are carried out now, how they will change in the future, and how to detect and defend against espionage, hacktivism, insider threats and non-state actors such as organized criminals and terrorists. Every one of our systems is under attack from multiple vectors - our defenses must be ready all the time and our alert systems must detect the threats every time. This book provides concrete examples and real-world guidance on how to identify and defend a network against malicious attacks. It considers relevant technical and factual information from an insider's point of view, as well as the ethics, laws and consequences of cyber war and how computer criminal law may change as a result. Starting with a definition of cyber warfare, the book's 15 chapters discuss the following topics: the cyberspace battlefield; cyber doctrine; cyber warriors; logical, physical, and psychological weapons; computer network exploitation; computer network attack and defense; non-state actors in computer network operations; legal system impacts; ethics in cyber warfare; cyberspace challenges; and the future of cyber war. This book is a valuable resource to those involved in cyber warfare activities, including policymakers, penetration testers, security professionals, network and systems administrators, and college instructors. The information provided on cyber tactics and attacks can also be used to assist in developing improved and more efficient procedures and technical defenses. Managers will find the text useful in improving the overall risk management strategies for their organizations. Provides concrete examples and real-world guidance on how to identify and defend your network against malicious attacks Dives deeply into relevant technical and factual information from an insider's point of view Details the ethics, laws and consequences of cyber war and how computer criminal law may change as a result*

*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*

*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.*

*Resources for Searching and Analyzing Online Information (LEIU)*
*Algorithms for OSINT*
*Hacking Web Intelligence*
*Resources for Searching and Analyzing Online Information*
*The Science of Human Hacking*
*An Intelligence Agency for the People*
*MI6 Spy Skills for Civilians*
*Blood Brothers*
*Open Source Intelligence Investigation*
*Internet Searches for Vetting, Investigations, and Open-Source Intelligence*
*The Secret History of the Sackler Dynasty*
*The Five Disciplines of Intelligence Collection*

*'A real-life thriller, a page-turner, a deeply shocking dissection of avarice and calculated callousness. We knew some of this story; it turns out we didn't know the half of it. Exhaustively researched and written with grace and gravity, Empire of Pain unpeels a most terrible American scandal. You feel almost guilty for enjoying it so much.' Melanie Reid, The Times The gripping and shocking story of three generations of the Sackler family and their roles in the stories of Valium and Oxycontin, by the prize-winning, bestselling author of Say Nothing. The Sackler name adorns the walls of many storied institutions – Harvard; the Metropolitan Museum of Art; Oxford; the Louvre. They are one of the richest families in the world, known for their lavish donations in the arts and the sciences. The source of the family fortune was vague, however, until it emerged that the Sacklers were responsible for making and marketing Oxycontin, a blockbuster painkiller that was a catalyst for the opioid crisis-an international epidemic of drug addiction which has killed nearly half a million people. In this masterpiece of narrative reporting and writing, Patrick Radden Keefe exhaustively documents the jaw-dropping and ferociously compelling reality. Empire of Pain is the story of a dynasty: a parable of 21st century greed.*

*A Liverpudlian West Side Story, Blood Brothers is the story of twin brothers separated at birth because their mother cannot afford to keep them both. One of them is given away to wealthy Mrs Lyons and they grow up as friends in ignorance of their fraternity until the inevitable quarrel unleashes a blood-bath. Blood Brothers was first performed at the Liverpool Playhouse in 1983 and subsequently transferred to the Lyric Theatre, London. It was revived in the West End in 1988 for a long-running production and opened on Broadway in 1993.*

*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.*

*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.*

*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.*

*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.*

*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.*

*Penetration Testing with Perl*
*The War of the Worlds*
*Digital Witness*
*Social Media Analytics*
*Operator Handbook*
*Empire of Pain*
*Nowhere to Hide*
*The Ultimate Edition*
*Hunting Cyber Criminals*
*A former British agent reveals how to live like a spy - smarter, sneakier and ready for anything*
*Open Source Intelligence and Cyber Crime*