# Open Source Intelligence In A Networked World Bloomsbury Intelligence Studies

Presents students with an anthology of published articles from diverse sources as well as contributions to the study of intelligence. This collection includes perspectives from the history of warfare, views on the evolution of US intelligence, and studies on the balance between the need for information-gathering and the values of a democracy.

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.

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.

Open Source Intelligence TechniquesResources for Searching and Analyzing Online InformationCreatespace Independent Publishing Platform

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.

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

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

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

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.

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 amount of publicly and often freely available information is staggering. Yet, the intelligence community still continues to collect and use information in the same manner as during WWII, when the OSS set out to learn as much as possible about Nazi Germany and Imperial Japan by scrutinizing encyclopedias, guide books, and short-wave radio. Today, the supply of information is greater than any possible demand, and anyone can

provide information. In effect, intelligence analysts are drowning in information. The book explains how to navigate this rising flood and make best use of these new, rich sources of information. Written by a pioneer in the field, it explores the potential uses of digitized data and the impact of the new means of creating and transmitting data, recommending to the intelligence community new ways of collecting and processing information. This comprehensive overview of the world of open source intelligence will appeal not only to practitioners and students of intelligence, but also to anyone interested in communication and the challenges posed by the information age."--Bloomsbury Publishing.
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

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.

Whats the best design framework for Open-source intelligence organization now that, in a post industrial-age if the top-down, command and control model is no longer relevant? Have all basic functions of Open-source intelligence been defined? Which Open-source intelligence goals are the most important? What may be the consequences for the performance of an organization if all stakeholders are not consulted regarding Open-source intelligence? Is maximizing Open-source intelligence protection the same as minimizing Open-source intelligence loss? This premium Open-source intelligence self-assessment will make you the assured Open-source intelligence domain authority by revealing just what you need to know to be fluent and ready for any Open-source intelligence challenge. How do I reduce the effort in the Open-source intelligence work to be done to get problems solved? How can I ensure that plans of action include every Open-source intelligence task and that every Open-source intelligence outcome is in place? How will I save time investigating strategic and tactical options and ensuring Open-source intelligence costs are low? How can I deliver tailored Open-source intelligence advice instantly with structured going-forward plans? There's no better guide through these mind-expanding questions than acclaimed best-selling author Gerard Blokdyk. Blokdyk ensures all Open-source intelligence essentials are covered, from every angle: the Open-source

intelligence self-assessment shows succinctly and clearly that what needs to be clarified to organize the required activities and processes so that Open-source intelligence outcomes are achieved. Contains extensive criteria grounded in past and current successful projects and activities by experienced Open-source intelligence practitioners. Their mastery, combined with the easy elegance of the self-assessment, provides its superior value to you in knowing how to ensure the outcome of any efforts in Open-source intelligence are maximized with professional results. Your purchase includes access details to the Open-source intelligence self-assessment dashboard download which gives you your dynamically prioritized projects-ready tool and shows you exactly what to do next. Your exclusive instant access details can be found in your book. You will receive the following contents with New and Updated specific criteria: - The latest quick edition of the book in PDF - The latest complete edition of the book in PDF, which criteria correspond to the criteria in... - The Self-Assessment Excel Dashboard, and... - Example pre-filled Self-Assessment Excel Dashboard to get familiar with results generation ...plus an extra, special, resource that helps you with project managing. INCLUDES LIFETIME SELF ASSESSMENT UPDATES Every self assessment comes with Lifetime Updates and Lifetime Free Updated Books. Lifetime Updates is an industry-first feature which allows you to receive verified self assessment updates, ensuring you always have the most accurate information at your fingertips.

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

The Tao of Open Source Intelligence provides a

comprehensive guide to OSINT (Open Source Intelligence) techniques, for the investigator: It catalogues and explains the tools and investigative approaches that are required when conducting research within the surface, deep and dark webs. It explains how to scrutinize criminal activity without compromising your anonymity and your investigation. It examines the relevance of cyber geography and how to get around its limitations. It describes useful add-ons for common search engines, as well as considering metasearch engines (including Dogpile, Zuula, PolyMeta, iSeek, Cluuz, and Carrot2) that collate search data from single-source intelligence platforms such as Google. It considers deep-web social media platforms and platform-specific search tools, detailing such concepts as concept mapping, entity extraction tools, and specialist search syntax.

Open source intelligence (OSINT) is one of many intelligence disciplines used in the all-source analysis process. Although limited national and tactical level exploitation of open sources has been successful in the past, intelligence staffs and commands directly supporting joint force commanders at the operational level often neglect to fully consider and incorporate OSINT into their efforts. The reasons are numerous, ranging from biases favoring classified intelligence to futility in attempting to manage an ever-increasing volume of open source material. There are, however, many compelling reasons for pursuing and exploiting OSINT at the operational level. Easier and faster access to information via electronic databases and networks, alternatives offered by the private sector, the ability to share OSINT with coalition partners and civilian organizations, and its applicability in operations other than war make it a significant asset. Operational intelligence staffs and commands must recognize. the increasing importance of OSINT and shift their collection and exploitation paradigms accordingly. Changes

are warranted to take advantage of OSINT within Unified and Specified command intelligence programs, within theater joint intelligence centers, and within joint task force intelligence organizations. Likewise, joint intelligence doctrine must be revised to give OSINT greater legitimacy as a primary intelligence discipline.

Fourth Edition (Traditional Chinese Translation) 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 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 Hidden Personal Videos Duplicate Copies of Photos Personal Radio Communications Compromised Email Information Wireless Routers by Location Hidden Mapping Applications Complete Facebook Data Free Investigative Software Alternative Search Engines Mobile App Network Data Unlisted Addresses Unlisted Phone Numbers Useful Browser Extensions Public Government Records Document Metadata Rental Vehicle Contracts Online Criminal Activity

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 book explains how openly available information is undervalued by the intelligence community and how

analysts can use of this huge amount of information. Traditionally, intelligence has been distinguished from all other forms of information working by its secrecy. Secret intelligence is about the acquisition of information from entities that do not wish that information to be acquired and, ideally, never know that it has. However, the transformation in information and communication technology (ICT) over the last two decades challenges this conventionally held perception of intelligence in one critical aspect: that information can increasingly be acquired legally in the public domain- 'open source intelligence'(OSINT). The intelligence community has recognised this phenomenon by formally creating discrete open source exploitation systems within extant intelligence institutions. Indeed, the exploitation of open source of information is reckoned by many intelligence practitioners to constitute 80 percent or more of final intelligence product. Yet, the resource committed to, and status of, open source exploitation belies that figure. This research derives a model of the high order factors describing the operational contribution of open source exploitation to the broader intelligence function: context; utility; cross-check; communication; focus; surge; and analysis. Such a model is useful in three related ways: first, in determining appropriate tasking for the intelligence function as a whole; second, as a basis for optimum intelligence resource allocation; and third, as defining objectives for specifically open source policy and doctrine. Additionally, the research details core capabilities, resources, and political arguments necessary for successful open source exploitation.

Significant drivers shape the contemporary context in which nation-state intelligence functions operate: globalisation; risk society; and changing societal expectation. The contemporary transformation in ICT percolates each of them. Understanding this context is crucial to the intelligence community. Implicitly, these drivers shape intelligence, and the relationship intelligence manages between knowledge and power within politics, in order to optimise decision-making. Because open source exploitation obtains from this context, it is better placed than closed to understand it. Thus, at a contextual level, this thesis further argues that the potential knowledge derived from open source exploitation not only has a unique contribution by comparison to closed, but that it can also usefully direct power towards determination of the appropriate objectives upon which any decisions should be made at all.

This report describes the evolution of open source intelligence, defines open source information and the intelligence cycle, and parallels with other intelligence disciplines, along with methods used and challenges of using off-the-shelf technology.

The research scenario in advanced systems for protecting critical infrastructures and for deeply networked information tools highlights a growing link between security issues and the need for intelligent processing abilities in the area of information s- tems. To face the ever-evolving nature of cyber-threats, monitoring systems must have adaptive capabilities for continuous adjustment and timely, effective response to

modifications in the environment. Moreover, the risks of improper access pose the need for advanced identification methods, including protocols to enforce comput- security policies and biometry-related technologies for physical authentication. C- putational Intelligence methods offer a wide variety of approaches that can be fruitful in those areas, and can play a crucial role in the adaptive process by their ability to learn empirically and adapt a system's behaviour accordingly. The International Workshop on Computational Intelligence for Security in Inf- mation Systems (CISIS) proposes a meeting ground to the various communities - volved in building intelligent systems for security, namely: information security, data mining, adaptive learning methods and soft computing among others. The main goal is to allow experts and researchers to assess the benefits of learning methods in the data-mining area for information-security applications. The Workshop offers the opportunity to interact with the leading industries actively involved in the critical area of security, and have a picture of the current solutions adopted in practical domains. This volume of Advances in Soft Computing contains accepted papers presented at CISIS'08, which was held in Genova, Italy, on October 23rd–24th, 2008.

Do you enjoy the reconnaissance part of a penetration testing? Want to discover issues on your network, assets or applications proactively? Would you like to learn some new OSINT based recon tools and techniques? Follow the rabbit hole and find exploitable critical vulnerabilities in the Panama Papers law firm and politics both American and international

including Trump and the DNC. Analyse network and email configurations for entry points and exploits with FOCA, Maltego, Nmap/ZenMap, and Spiderfoot. Learn how to use advanced searches, alternative search engines that don't respect robots.txt., intel tools, and leak databases. Open source intelligence gathering (OSINT) and web-based reconnaissance is an important part of penetration testing and proactive defense. The more connected we are, the more information is held about everything. Yummy, juicy information for both a penetration tester or a malicious actor. Learning what sources of are available to start your search is an important first step in learning about reconnaissance and how the information could be utilized or resold. Both issues you or your client need to know. All of the tools and techniques in this book can be ninjafied with Python, Ruby or PowerShell. Initially, this book began as a presentation at the Cyber Senate Industrial Control Cybersecurity Nuclear Summit in Warrington, UK 2016. Originally, I intended to use some of the same techniques to target a nuclear power plant or someone in a nuclear regulatory capacity. After submitting my original talk idea. Daesh, otherwise known as ISIS, began publicly threatening the European nuclear industry. Due to the threats, we decided it wasn't in anyone's best interest to give a how to target nuclear installations and changed the target instead to the law firm behind the Panama Papers fiasco. The project expanded to include additional targets with mostly a political slant. 2016 was a very tumultuous year in politics. Brexit, Trump, and the rise of the interesting politics and coups in Turkey, Netherlands, Germany, Russia, Bulgaria and the Philippines. It's a lot more fun to learn about a topic in an empowering way. Also, only politicians like politicians. They make a fun target. Learning a new technique is easier when it's fun. I chose targets and case studies which gave me a happy hacker smile.

Owing to the recent transitions in the Czech Republic, the Czech military must satisfy a large set of new requirements. One way the military intelligence can become more effective and can conserve resources is by increasing the efficiency of open-source intelligence (OSINT), which plays an important part in intelligence gathering in the age of information. When using OSINT effectively, the military intelligence can elevate its responsiveness to different types of crises and can also properly allocate its limited resources into areas, in which covert collection in unavoidable. This thesis combines modern knowledge-management theory with current issues in military intelligence, creating a base for designing a future OSINT system in the Czech military. First, the thesis introduces recent U.S. research in knowledge management and examines the current intelligence issues. Then the thesis examines the Czech military intelligence environment in the framework of the national security and defense policy and also analyzes the actual use of OSINT in the Military Intelligence Service, following the four stages of the knowledge system and process design. Finally, the thesis outlines the main aspects of the future OSINT knowledge-management system and recommends further research and development.

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

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

Are procedures in place governing the criminal intelligence units use of special funds? Did units get intelligence based on priority? Is there an articulated collection plan for the Intelligence Unit? How will source reliability and information validity be evaluated? Will machines surpass human intelligence? Defining, designing, creating, and implementing a process to solve a challenge or meet an objective is the most valuable role... In EVERY group, company, organization and department. Unless you are talking a one-time, single-use project, there should be a process. Whether that process is managed and implemented by humans, AI, or a combination of the two, it needs to be designed by someone with a complex enough perspective to ask the right questions. Someone capable of asking the right questions and step back and say, 'What are we really trying to accomplish here? And is there a different way to look at it?' This Self-Assessment empowers people to do just that - whether their title is entrepreneur, manager, consultant, (Vice-)President, CxO

etc... - they are the people who rule the future. They are the person who asks the right questions to make Open Source Intelligence investments work better. This Open Source Intelligence All-Inclusive Self-Assessment enables You to be that person. All the tools you need to an in-depth Open Source Intelligence Self-Assessment. Featuring 989 new and updated case-based questions, organized into seven core areas of process design, this Self-Assessment will help you identify areas in which Open Source Intelligence improvements can be made. In using the questions you will be better able to: - diagnose Open Source Intelligence projects, initiatives, organizations, businesses and processes using accepted diagnostic standards and practices - implement evidence-based best practice strategies aligned with overall goals - integrate recent advances in Open Source Intelligence and process design strategies into practice according to best practice guidelines Using a Self-Assessment tool known as the Open Source Intelligence Scorecard, you will develop a clear picture of which Open Source Intelligence areas need attention. Your purchase includes access details to the Open Source Intelligence self-assessment dashboard download which gives you your dynamically prioritized projects-ready tool and shows your organization exactly what to do next. You will receive the following contents with New and Updated specific criteria: - The latest quick edition of the book in PDF - The latest complete edition of the book in PDF, which criteria correspond to the criteria in... - The Self-Assessment Excel Dashboard - Example pre-filled Self-Assessment Excel Dashboard to get familiar with results generation - In-depth and specific Open Source Intelligence Checklists - Project management checklists and templates to assist with implementation INCLUDES LIFETIME SELF ASSESSMENT UPDATES Every self assessment comes with Lifetime

Updates and Lifetime Free Updated Books. Lifetime Updates is an industry-first feature which allows you to receive verified self assessment updates, ensuring you always have the most accurate information at your fingertips.

Open source information (OSINT) is derived from newspapers, journals, radio and television, and the Internet. Intelligence analysts have long used such information to supplement classified data, but systematically collecting open source information has not been a priority of the U.S. Intelligence Community (IC). In recent years, given changes in the international environment, there have been calls, from Congress and the 9/11 Commission among others, for a more intense and focused investment in open source collection and analysis. However, some still emphasize that the primary business of intelligence continues to be obtaining and analyzing secrets.