Challenging Online Propaganda and Disinformation in the 21st Century

Disinformation has recently become a salient issue, not just for researchers but for the media, politicians, and the general public as well. Changing circumstances are a challenge for system and societal resilience; disinformation is also a challenge for governments, civil society, and individuals. Thus, this book focuses on the post-truth era and the online environment, which has changed both the ways and forms in which disinformation is presented and spread. The volume is dedicated to the complex processes of understanding the mechanisms and effects of online propaganda and disinformation, its detection and reactions to it in the European context. It focuses on questions and dilemmas from political science, security studies, IT, and law disciplines with the aim to protect society and build resilience against online propaganda and disinformation in the post-truth era.
Essential for anyone who works with technology in the field, E-DISCOVERY is a hands-on, how-to training guide that provides students with comprehensive coverage of the technology used in e-discovery in civil and criminal cases. From discovery identification to collection, processing, review, production, and trial presentation, this practical text covers everything your students need to know about e-discovery, including the Federal Rules of Civil Procedure, Federal Rules of Criminal Procedure, and Federal Rules of Evidence. Throughout the text, students will have the opportunity to work with e-discovery tools such as Discovery Attender, computer forensics tools such as AccessData's Forensics ToolKit, as well as popular processing and review platforms such as iConect, Concordance, and iPro. An interactive courtroom tutorial and use of Trial Director are included to complete the litigation cycle. Multiple tools are discussed for each phase, giving your students a good selection of potential resources for each task. Finally, real-life examples are woven throughout the text, revealing little talked-about potential pitfalls, as well as best practice and cost management suggestions. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.
Chapter "Predictive Policing in 2025: A Scenario" is available open access under a Creative Commons Attribution 4.0 International License via link.springer.com.

Convenience Triangle in White-Collar Crime

Master the tools and techniques of mobile forensic investigations Conduct mobile forensic investigations that are legal, ethical, and highly effective using the detailed information contained in this practical guide. Mobile Forensic Investigations: A Guide to Evidence Collection, Analysis, and Presentation, Second Edition fully explains the latest tools and methods along with features, examples, and real-world case studies. Find out how to assemble a mobile forensics lab, collect prosecutable evidence, uncover hidden files, and lock down the chain of custody. This comprehensive resource shows not only how to collect and analyze mobile device data but also how to accurately document your investigations to deliver court-ready documents. • Legally seize mobile devices, USB drives, SD cards, and SIM cards • Uncover sensitive data through both physical and logical techniques • Properly package, document, transport, and store evidence • Work with free, open source, and commercial forensic software • Perform a deep dive analysis of iOS, Android, and Windows Phone file systems • Extract evidence from application, cache, and user storage files • Extract and analyze data from IoT devices, drones, wearables, and infotainment systems • Build SQLite queries and Python scripts for mobile device file interrogation • Prepare reports that will hold up to judicial and defense scrutiny

Proceedings of New York University Annual Institute on Federal Taxation

Financial Forensics Body of Knowledge

Cyber Crime and Cyber Terrorism Investigator’s Handbook is a vital tool in the arsenal of today’s computer programmers, students, and investigators. As computer networks become ubiquitous throughout the world, cyber crime, cyber terrorism, and cyber war have become some of the most concerning topics in today’s security landscape. News stories about Stuxnet and PRISM have brought these activities into the public eye, and serve to show just how effective, controversial, and worrying these tactics can become. Cyber Crime and Cyber Terrorism Investigator’s Handbook describes and analyzes many of the motivations, tools, and tactics behind cyber attacks and the defenses against them. With this book, you will learn about the technological and logistic framework of cyber crime, as well as the social and legal backgrounds of its prosecution and investigation. Whether you are a law enforcement professional, an IT specialist, a researcher, or a student, you will find valuable insight into the world of cyber crime and cyber warfare. Edited by experts in computer security, cyber investigations, and counter-terrorism, and with contributions from computer researchers, legal experts, and law enforcement professionals, Cyber Crime and Cyber Terrorism Investigator’s Handbook will serve as your best reference to the modern world of cyber crime. Written by experts in cyber crime, digital investigations, and counter-terrorism Learn the motivations, tools, and tactics used by cyber-attackers, computer security professionals, and investigators Keep up to date on current national and international law regarding cyber crime and cyber terrorism See just how significant cyber crime has become, and how important cyber law enforcement is in the modern world

Policing in the Era of AI and Smart Societies

In this book, the editors explain how students enrolled in two digital forensic courses at their institution are exposed to experiential learning opportunities, where the students acquire the knowledge and skills of the subject-matter while also learning how to adapt to the ever-changing digital forensic landscape.
Digital forensics is a topic of increasing importance as our society becomes “smarter” with more of the “things” around us being internet- and inter-connected (e.g., Internet of Things (IoT) and smart home devices); thus, the increasing likelihood that we will need to acquire data from these things in a forensically sound manner. This book is of interest to both digital forensic educators and digital forensic practitioners, as well as students seeking to learn about digital forensics.

Cybercrime and Digital Forensics

Security threats are a significant problem for information technology companies today. This book focuses on how to mitigate these threats by using security standards and provides ways to address associated problems faced by engineers caused by ambiguities in the standards. The security standards are analysed, fundamental concepts of the security standards presented, and the relations to the elementary concepts of security requirements engineering (SRE) methods explored. Using this knowledge, engineers can build customised methods that support the establishment of security standards. Standards such as Common Criteria or ISO 27001 are explored and several extensions are provided to well-known SRE methods such as Si*, CORAS, and UML4PF to support the establishment of these security standards. Through careful analysis of the activities demanded by the standards, for example the activities to establish an Information Security Management System (ISMS) in compliance with the ISO 27001 standard, methods are proposed which incorporate existing security requirement approaches and patterns. Understanding Pattern and Security Requirements engineering methods is important for software engineers, security analysts and other professionals that are tasked with establishing a security standard, as well as researchers who aim to investigate the problems with establishing security standards. The examples and explanations in this book are designed to be understandable by all these readers.
investigations.

E-Discovery: An Introduction to Digital Evidence

The SADFE International Workshop is intended to further the advancement of computer forensic engineering by promoting innovative and leading-edge systematic approaches to cyber crime investigation. The workshop brings together top digital forensic researchers, advanced tool/product builders, and expert law enforcement from around the world for information exchange and R&D collaboration. In addition to advanced digital evidence discovery, gathering and correlation, SADFE recognizes the value of solid digital forensic engineering processes based on both technical and legal grounds. SADFE further recognizes the need of advanced forensic-enabled and proactive monitoring/response technologies. SADFE 2005 addresses broad-based, innovative digital forensic engineering technology, practical experience and process areas.

Photoshop CS3 for Forensics Professionals

ISDF 2009, the First International Conference on Information Security and Digital Forensics, was held at City University London during September 7-8, 2009. The conference was organized as a meeting point for leading national and international experts of information security and digital forensics. The conference was rewarding in many ways; ISDF 2009 was an exciting and vibrant event, with 4 keynote talks, 25 invited talks and 18 full-paper presentations and those attending had the opportunity to meet and talk with many distinguished people who are responsible for shaping the area of information security. This conference was organized as part of two major research projects funded by the UK Engineering and Physical Sciences Research Council in the areas of Security and Digital Forensics. I would like to thank all the people who contributed to the technical program. The most apparent of these are the Indian delegates who all accepted our invite to give presentations at this conference. Less apparent perhaps is the terrific work of the members of the Technical Program Committee, especially in reviewing the papers, which is a critical and time-consuming task. I would like to thank Raj Rajarajan (City University London) for making the idea of the ISDF 2009 conference a reality with his hard work. Last but not least, I would like to thank all the authors who submitted papers, making the conference possible, and the authors of accepted papers for their cooperation. Dasun Weerasinghe

CCSP (ISC)2 Certified Cloud Security Professional Official Study Guide

Digital forensics deals with the acquisition, preservation, examination, analysis and presentation of electronic evidence. Computer networks, cloud computing, smartphones, embedded devices and the Internet of Things have expanded the role of digital forensics beyond traditional computer crime investigations. Practically every crime now involves some aspect of digital evidence; digital forensics provides the techniques and tools to articulate this evidence in legal proceedings. Digital forensics also has myriad intelligence applications; furthermore, it has a vital role in cyber security -- investigations of security breaches yield valuable information that can be used to design more secure and resilient systems. Advances in Digital Forensics XVI describes original research results and innovative applications in the discipline of digital forensics. In addition, it highlights some of the major technical and legal issues related to digital evidence and electronic crime investigations. The areas of coverage include: themes and issues, forensic techniques, filesystem forensics, cloud forensics, social media forensics, multimedia forensics, and novel applications. This book is the sixteenth volume in the annual series produced by the International Federation for Information Processing (IFIP) Working Group 11.9 on Digital Forensics, an international community of scientists, engineers and practitioners dedicated to advancing the state of the art of research and practice in digital forensics. The book contains a
A selection of sixteen edited papers from the Sixteenth Annual IFIP WG 11.9 International Conference on Digital Forensics, held in New Delhi, India, in the winter of 2020. Advances in Digital Forensics XVI is an important resource for researchers, faculty members and graduate students, as well as for practitioners and individuals engaged in research and development efforts for the law enforcement and intelligence communities.

Digital Forensics, Investigation, and Response

Threat actors, be they cyber criminals, terrorists, hacktivists or disgruntled employees, are employing sophisticated attack techniques and anti-forensics tools to cover their attacks and breach attempts. As emerging and hybrid technologies continue to influence daily business decisions, the proactive use of cyber forensics to better assess the risks that the exploitation of these technologies pose to enterprise-wide operations is rapidly becoming a strategic business objective. This book moves beyond the typical, technical approach to discussing cyber forensics processes and procedures. Instead, the authors examine how cyber forensics can be applied to identifying, collecting, and examining evidential data from emerging and hybrid technologies, while taking steps to proactively manage the influence and impact, as well as the policy and governance aspects of these technologies and their effect on business operations. A world-class team of cyber forensics researchers, investigators, practitioners and law enforcement professionals have come together to provide the reader with insights and recommendations into the proactive application of cyber forensic methodologies and procedures to both protect data and to identify digital evidence related to the misuse of these data. This book is an essential guide for both the technical and non-technical executive, manager, attorney, auditor, and general practitioner who is seeking an authoritative source on how cyber forensics may be applied to both evidential data collection and to proactively managing today's and tomorrow's emerging and hybrid technologies. The book will also serve as a primary or supplemental text in both under- and post-graduate academic programs addressing information, operational and emerging technologies, cyber forensics, networks, cloud computing and cybersecurity.

Recent Trends in Data Science and Soft Computing

This volume offers a general overview on the handling and regulating electronic evidence in Europe, presenting a standard for the exchange process. Chapters explore the nature of electronic evidence and readers will learn of the challenges involved in upholding the necessary standards and maintaining the integrity of information. Challenges particularly occur when European Union member states collaborate and evidence is exchanged, as may be the case when solving a cybercrime. One such challenge is that the variety of possible evidences is so wide that potentially anything may become the evidence of a crime. Moreover, the introduction and the extensive use of information and communications technology (ICT) has generated new forms of crimes or new ways of perpetrating them, as well as a new type of evidence. Contributing authors examine the legal framework in place in various EU member states when dealing with electronic evidence, with prominence given to data protection and privacy issues. Readers may learn about the state of the art tools and standards utilized for treating and exchanging evidence, and existing platforms and environments run by different Law Enforcement Agencies (LEAs) at local and central level. Readers will also discover the operational point of view of LEAs when dealing with electronic evidence, and their requirements and expectations for the future. Finally, readers may consider a proposal for realizing a unique legal framework for governing in a uniform and aligned way the treatment and cross border exchange of electronic evidence in Europe. The use, collection and exchange of electronic evidence in the European Union context and the rules, practises, operational guidelines, standards and tools utilized by LEAs, judges, Public prosecutors and other relevant stakeholders are all covered in this comprehensive work. It will appeal to researchers in both law and computer science, as well as those with an interest in privacy, digital forensics, electronic...
This is the first digital forensics book that covers the complete lifecycle of digital evidence and the chain of custody. This comprehensive handbook includes international procedures, best practices, compliance, and a companion web site with downloadable forms. Written by world-renowned digital forensics experts, this book is a must for any digital forensics lab. It provides anyone who handles digital evidence with a guide to proper procedure throughout the chain of custody—from incident response through analysis in the lab. A step-by-step guide to designing, building and using a digital forensics lab.

Handling and Exchanging Electronic Evidence Across Europe

An understanding of how digital forensics integrates with the overall response to cybersecurity incidents is a must for all organizations. This book offers concrete and detailed guidance on how to conduct the full spectrum of incident response and digital forensic activities.

Cyber Forensics

The 'convenience triangle' is the dynamic relationship between motive, opportunity, and willingness to commit a crime, which culminates in the illegal acts which constitute white-collar crime. This book aims to discuss the role of the 'convenience triangle' in white-collar crime, how it affects the perpetration of these crimes, the impact of this on detection and prevention and the effects of the punitive measures taken against white-collar criminals.
Digital Forensics and Forensic Investigations: Breakthroughs in Research and Practice

This book will present the most advanced research on forensic archaeology presented during the annual European meetings in the last 3 years. Thanks to the broad nature of the chapters presented, this book will show not only different approaches and different crime scenes around Europe, but also how every single European law enforcement has faced forensic investigations. This book shows forensic archaeology as practiced in this legal context, emerging and solidifying in many European countries, differing in some respects because of differences in legal systems but ultimately sharing common grounds. Differently from similar books, this will be not only a collection of research and case studies in which forensic practitioners demonstrate the extent and complexity of the various aspects of forensic archaeology, but also it will show the necessity of co-operation as a condition for any work in forensic archaeology among scientists of different disciplines and law enforcers.

Information Security and Digital Forensics

This fully updated study guide covers every topic on the current version of the CompTIA Security+ exam. Get complete coverage of all objectives included on the CompTIA Security+ exam SY0-601 from this comprehensive resource. Written by a team of leading information security experts, this authoritative guide fully addresses the skills required to perform essential security functions and to secure hardware, systems, and software. You’ll find learning objectives at the beginning of each chapter, exam tips, practice exam questions, and in-depth explanations. Designed to help you pass the exam with ease, this definitive volume also serves as an essential on-the-job reference. Covers all exam domains, including: Threats, Attacks, and Vulnerabilities; Architecture and Design; Implementation; Operations and Incident Response; Governance, Risk, and Compliance. Online content includes: 250 practice exam questions; Test engine that provides full-length practice exams and customizable quizzes by chapter or by exam domain.

Advances in Digital Forensics XVI

Further Issues and Serious Fraud Instances

The definitive text for students of digital forensics, as well as professionals looking to deepen their understanding of an increasingly critical field. Written by faculty members and associates of the world-renowned Norwegian Information Security Laboratory (NisLab) at the Norwegian University of Science and Technology (NTNU), this textbook takes a scientific approach to digital forensics ideally suited for university courses in digital forensics and information security. Each chapter was written by an accomplished expert in his or her field, many of them with extensive experience in law enforcement and industry. The author team comprises experts in digital forensics, cybercrime law, information security and related areas. Digital forensics is a key competency in meeting the growing risks of cybercrime, as well as for criminal investigation generally. Considering the astonishing pace at which new information technology – and new ways of exploiting information technology – is brought on line, researchers and practitioners regularly face new technical challenges, forcing them to continuously upgrade their investigatory skills. Designed to prepare the next generation to rise to those challenges, the material contained in Digital Forensics has been tested and refined by use in both graduate and undergraduate programs and subjected to formal evaluations for more than ten years. Encompasses all aspects of the field, including methodological, scientific, technical and legal matters. Based on the latest research, it provides novel insights for students, including an informed look at the future of digital forensics. Includes test questions from actual exam sets, multiple choice questions suitable for online use and numerous...
Digital Forensics Processing and Procedures

The onlyoffice.beeznest.com

Visuals, illustrations, and case example images. Features real-world examples and scenarios, including court cases and technical problems, as well as a rich library of academic references and references to online media. Digital Forensics is an excellent introductory text for programs in computer science and computer engineering and for master degree programs in military and police education. It is also a valuable reference for legal practitioners, police officers, investigators, and forensic practitioners seeking to gain a deeper understanding of digital forensics and cybercrime.

Cybersecurity: The Essential Body of Knowledge

Implementing Digital Forensic Readiness: From Reactive to Proactive Process, Second Edition presents the optimal way for digital forensic and IT security professionals to implement a proactive approach to digital forensics. The book details how digital forensic processes can align strategically with business operations and an already existing information and data security program. Detailing proper collection, preservation, storage, and presentation of digital evidence, the procedures outlined illustrate how digital evidence can be an essential tool in mitigating risk and reducing the impact of both internal and external, digital incidents, disputes, and crimes. By utilizing a digital forensic readiness approach and stance, a company's preparedness and ability to take action quickly and respond as needed. In addition, this approach enhances the ability to gather evidence, as well as the relevance, reliability, and credibility of any such evidence. New chapters to this edition include Chapter 4 on Code of Ethics and Standards, Chapter 5 on Digital Forensics as a Business, and Chapter 10 on Establishing Legal Admissibility. This book offers best practices to professionals on enhancing their digital forensic program, or how to start and develop one the right way for effective forensic readiness in any corporate or enterprise setting.

Intelligent Multimedia Analysis for Security Applications

As computer and internet technologies continue to advance at a fast pace, the rate of cybercrimes is increasing. Crimes employing mobile devices, data embedding/mining systems, computers, network communications, or any malware impose a huge threat to data security, while cyberbullying, cyberstalking, child pornography, and trafficking crimes are made easier through the anonymity of the internet. New developments in digital forensics tools and an understanding of current criminal activities can greatly assist in minimizing attacks on individuals, organizations, and society as a whole. Digital Forensics and Forensic Investigations: Breakthroughs in Research and Practice addresses current challenges and issues emerging in cyber forensics and new investigative tools and methods that can be adopted and implemented to address these issues and counter security breaches within various organizations. It also examines a variety of topics such as advanced techniques for forensic developments in computer and communication-link environments and legal perspectives including procedures for cyber investigations, standards, and policies. Highlighting a range of topics such as cybercrime, threat detection, and forensic science, this publication is an ideal reference source for security analysts, law enforcement, lawmakers, government officials, IT professionals, researchers, practitioners, academicians, and students currently investigating the up-and-coming aspects surrounding network security, computer science, and security engineering.

CyberForensics
Encyclopedia of Cybercrime

CYBERSECURITY: THE ESSENTIAL BODY OF KNOWLEDGE provides a comprehensive, trustworthy framework of practices for assuring information security. This book is organized to help readers understand how the various roles and functions within cybersecurity practice can be combined and leveraged to produce a secure organization. In this unique book, concepts are not presented as stagnant theory; instead, the content is interwoven in a real world adventure story that runs throughout. In the story, a fictional company experiences numerous pitfalls of cyber security and the reader is immersed in the everyday practice of securing the company through various characters’ efforts. This approach grabs learners’ attention and assists them in visualizing the application of the content to real-world issues that they will face in their professional life. Derived from the Department of Homeland Security’s Essential Body of Knowledge (EBK) for IT Security, this book is an indispensable resource dedicated to understanding the framework, roles, and competencies involved with information security.

Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Advances in Digital Forensics II

Digital Forensics, Investigation, and Response, Fourth Edition examines the fundamentals of system forensics, addresses the tools, techniques, and methods used to perform computer forensics and investigation, and explores incident and intrusion response.

First International Workshop on Systematic Approaches to Digital Forensic Engineering

The definitive, must-have guide for the forensic accounting professional Financial Forensics Body of Knowledge is the unique, innovative, and definitive guide and technical reference work for the financial forensics and/or forensic accounting professional, including nearly 300 forensic tools, techniques, methods and methodologies apply to virtually all civil, criminal and dispute matters. Many of the tools have never before been published. It defines the profession: “The Art & Science of Investigating People & Money.” It defines Forensic Operators: “financial forensics-capable personnel possess unique and specific skills, knowledge, experience, education, training, and integrity to function in the financial forensics discipline.” It defines why: “If you understand financial forensics you understand fraud, but not vice versa” by applying financial forensics to all aspects of the financial community. It contains a book-within-a-book Companion Section for financial valuation and litigation specialists. It defines foundational financial forensics/forensic accounting methodologies: FAIM, Forensic Accounting Investigation Methodology, ICE/SCORE, CICO, APD, forensic lexicology, and others. It contains a Reader Lookup Table that permits everyone in the financial community to immediately focus on the pertinent issues.

Pattern and Security Requirements

Cyber Crime and Cyber Terrorism Investigator’s Handbook

This is one of the very few books focused on analysis of multimedia data and newly emerging multimedia applications with an emphasis on security. The main objective of this project was to assemble as much research coverage as possible related to the field by defining the latest innovative technologies and providing the most comprehensive list of research references. The book includes sixteen chapters highlighting current concepts, issues and emerging technologies. Distinguished scholars from many prominent research institutions around the world contribute to the book. The book

10 / 12
covers various aspects, including not only some fundamental knowledge and the latest key techniques, but also typical applications and open issues. Topics covered include dangerous or abnormal event detection, interaction recognition, person identification based on multiple traits, audiovisual biometric person authentication and liveness verification, emerging biometric technologies, sensitive information filtering for teleradiology, detection of nakedness in images, audio forensics, steganalysis, media content tracking authentication and illegal distributor identification through watermarking and content-based copy detection. We believe that the comprehensive coverage of diverse disciplines in the field of intelligent multimedia analysis for security applications will contribute to a better understanding of all topics, research, and discoveries in this emerging and evolving field and that the included contributions will be instrumental in the expansion of the corresponding body of knowledge, making this book a reference source of information. It is our sincere hope that this publication and its great amount of information and research will assist our research colleagues, faculty members and students, and organization decision makers in enhancing their understanding for the concepts, issues, problems, trends, challenges and opportunities related to this research field. Perhaps this book will even inspire its readers to contribute to the current discoveries in this immense field.

Crime Scene Photography

There are today no more compelling sets of crime and security threats facing nations, communities, organizations, groups, families and individuals than those encompassed by cybercrime. For over fifty years crime enabled by computing and telecommunications technologies have increasingly threatened societies as they have become reliant on information systems for sustaining modernized living. Cybercrime is not a new phenomenon, rather an evolving one with respect to adoption of information technology (IT) for abusive and criminal purposes. Further, by virtue of the myriad ways in which IT is abused, it represents a technological shift in the nature of crime rather than a new form of criminal behavior. In other words, the nature of crime and its impacts on society are changing to the extent computers and other forms of IT are used for illicit purposes. Understanding the subject, then, is imperative to combating it and to addressing it at various levels. This work is the first comprehensive encyclopedia to address cybercrime. Topical articles address all key areas of concern and specifically those having to with: terminology, definitions and social constructs of crime; national infrastructure security vulnerabilities and capabilities; types of attacks to computers and information systems; computer abusers and cybercriminals; criminological, sociological, psychological and technological theoretical underpinnings of cybercrime; social and economic impacts of crime enabled with information technology (IT) inclusive of harms experienced by victims of cybercrimes and computer abuse; emerging and controversial issues such as online pornography, the computer hacking subculture and potential negative effects of electronic gaming and so-called computer addiction; bodies and specific examples of U.S. federal laws and regulations that help to prevent cybercrimes; examples and perspectives of law enforcement, regulatory and professional member associations concerned about cybercrime and its impacts; and computer forensics as well as general investigation/prosecution of high tech crimes and attendant challenges within the United States and internationally.

CompTIA Security+ All-in-One Exam Guide, Sixth Edition (Exam SY0-601)

This book offers a comprehensive and integrative introduction to cybercrime. It provides an authoritative synthesis of the disparate literature on the various types of cybercrime, the global investigation and detection of cybercrime and the role of digital information, and the wider role of technology as a facilitator for social relationships between deviants and criminals. It includes coverage of: key theoretical and methodological perspectives; computer hacking and malicious software; digital piracy and intellectual theft; economic crime and online fraud; pornography and online sex crime; cyber-bullying and cyber-stalking; cyber-terrorism and extremism; digital forensic investigation and its legal implications; and computer forensics as well as general investigation/prosecution of high tech crimes and attendant challenges within the United States and internationally.
context around the world; the law enforcement response to cybercrime transnationally; cybercrime policy and legislation across the globe. The new edition features two new chapters, the first looking at the law enforcement response to cybercrime and the second offering an extended discussion of online child pornography and sexual exploitation. This book includes lively and engaging features, such as discussion questions, boxed examples of unique events and key figures in offending, quotes from interviews with active offenders, and a full glossary of terms. This new edition includes QR codes throughout to connect directly with relevant websites. It is supplemented by a companion website that includes further exercises for students and instructor resources. This text is essential reading for courses on cybercrime, cyber-deviancy, digital forensics, cybercrime investigation, and the sociology of technology.

This book presents the proceedings of the 3rd International Conference of Reliable Information and Communication Technology 2018 (IRICT 2018), which was held in Kuala Lumpur, Malaysia, on July 23–24, 2018. The main theme of the conference was "Data Science, AI and IoT Trends for the Fourth Industrial Revolution." A total of 158 papers were submitted to the conference, of which 103 were accepted and considered for publication in this book. Several hot research topics are covered, including Advances in Data Science and Big Data Analytics, Artificial Intelligence and Soft Computing, Business Intelligence, Internet of Things (IoT) Technologies and Applications, Intelligent Communication Systems, Advances in Computer Vision, Health Informatics, Reliable Cloud Computing Environments, Recent Trends in Knowledge Management, Security Issues in the Cyber World, and Advances in Information Systems Research, Theories and Methods.