Online Library Hacking Ethical On Papers Ieee 2013

If you ally craving such a referred **Hacking Ethical On Papers Ieee 2013** book that will come up with the money for you worth, acquire the unquestionably best seller from us currently from several preferred authors. If you desire to funny books, lots of novels, tale, jokes, and more fictions collections are in addition to launched, from best seller to one of the most current released.

You may not be perplexed to enjoy every ebook collections Hacking Ethical On Papers Ieee 2013 that we will no question offer. It is not a propos the costs. Its roughly what you infatuation currently. This Hacking Ethical On Papers Ieee 2013, as one of the most effective sellers here will categorically be accompanied by the best options to review.

KEY=HACKING - RICH WELLS

PROCEEDINGS OF INTERNATIONAL ETHICAL HACKING CONFERENCE 2018

EHACON 2018, KOLKATA, INDIA

Springer **This book discusses the implications of new technologies for a secured society. As such, it reflects the main focus of the International Conference on Ethical Hacking, eHaCon 2018, which is essentially in evaluating the security of computer systems using penetration testing techniques. Showcasing the most outstanding research papers presented at the conference, the book shares new findings on computer network attacks and defenses, commercial security solutions, and hands-on, real-world security experience. The respective sections include network security, ethical hacking, cryptography, digital forensics, cloud security, information security, mobile communications security, and cyber security.**

PROCEEDINGS OF INTERNATIONAL ETHICAL HACKING CONFERENCE 2019

EHACON 2019, KOLKATA, INDIA

Springer Nature **This book gathers the peer-reviewed proceedings of the International Ethical Hacking Conference, eHaCON 2019, the second international conference of its kind, which was held in Kolkata, India, in August 2019.**

Bringing together the most outstanding research papers presented at the conference, the book shares new findings on computer network attacks and defenses, commercial security solutions, and hands-on, real-world security lessons learned. The respective sections include network security, ethical hacking, cryptography, digital forensics, cloud security, information security, mobile communications security, and cyber security.

CYBER-ASSURANCE FOR THE INTERNET OF THINGS

John Wiley & Sons **Presents an Cyber-Assurance approach to the Internet of Things (IoT) This book discusses the cyber-assurance needs of the IoT environment, highlighting key information assurance (IA) IoT issues and identifying the associated security implications. Through contributions from cyber-assurance, IA, information security and IoT industry practitioners and experts, the text covers fundamental and advanced concepts necessary to grasp current IA issues, challenges, and solutions for the IoT. The future trends in IoT infrastructures, architectures and applications are also examined. Other topics discussed include the IA protection of IoT systems and information being stored, processed or transmitted from unauthorized access or modification of machine-2-machine (M2M) devices, radio-frequency identification (RFID) networks, wireless sensor networks, smart grids, and supervisory control and data acquisition (SCADA) systems. The book also discusses IA measures necessary to detect, protect, and defend IoT information and networks/systems to ensure their availability, integrity, authentication, confidentially, and non-repudiation. Discusses current research and emerging trends in IA theory, applications, architecture and information security in the IoT based on theoretical aspects and studies of practical applications Aids readers in understanding how to design and build cyber-assurance into the IoT Exposes engineers and designers to new strategies and emerging standards, and promotes active development of cyber-assurance Covers challenging issues as well as potential solutions, encouraging discussion and debate amongst those in the field Cyber-Assurance for the Internet of Things is written for researchers and professionals working in the field of wireless technologies, information security architecture, and security system design. This book will also serve as a reference for professors and students involved in IA and IoT networking. Tyson T. Brooks is an Adjunct Professor in the School of Information Studies at Syracuse University; he also works with the Center for Information and Systems Assurance and Trust (CISAT) at Syracuse University, and is an information security technologist and science-practitioner. Dr. Brooks is the founder/Editor-in-Chief of the International Journal of Internet of Things and Cyber-Assurance, an associate editor for the Journal of Enterprise Architecture, the International Journal of Cloud Computing and Services Science, and the International Journal of Information and Network Security.**

ETHICAL HACKING TECHNIQUES AND COUNTERMEASURES FOR CYBERCRIME PREVENTION

IGI Global **As personal data continues to be shared and used in all aspects of society, the protection of this information has become paramount. While cybersecurity should protect individuals from cyber-threats, it also should be eliminating any and all vulnerabilities. The use of hacking to prevent cybercrime and contribute new countermeasures towards protecting computers, servers, networks, web applications, mobile devices, and stored data from black hat attackers who have malicious intent, as well as to stop against unauthorized access instead of using hacking in the traditional sense to launch attacks on these devices, can contribute emerging and advanced solutions against cybercrime. Ethical Hacking Techniques and Countermeasures for Cybercrime Prevention is a comprehensive text that discusses and defines ethical hacking, including the skills and concept of ethical hacking, and studies the countermeasures to prevent and stop cybercrimes, cyberterrorism, cybertheft, identity theft, and computer-related crimes. It broadens the understanding of cybersecurity by providing the necessary tools and skills to combat cybercrime. Some specific topics include top cyber investigation trends, data security of consumer devices, phases of hacking attacks, and stenography for secure image transmission. This book is relevant for ethical hackers, cybersecurity analysts, computer forensic experts, government officials, practitioners, researchers, academicians, and students interested in the latest techniques for preventing and combatting cybercrime.**

SECURITY SOLUTIONS FOR HYPERCONNECTIVITY AND THE INTERNET OF THINGS

IGI Global **The Internet of Things describes a world in which smart technologies enable objects with a network to communicate with each other and interface with humans effortlessly. This connected world of convenience and technology does not come without its drawbacks, as interconnectivity implies hackability. Security Solutions for Hyperconnectivity and the Internet of Things offers insights from cutting-edge research about the strategies and techniques that can be implemented to protect against cyber-attacks. Calling for revolutionary protection strategies to reassess security, this book is an essential resource for programmers, engineers, business professionals, researchers, and advanced students in relevant fields.**

THE CHANGING SCOPE OF TECHNOETHICS IN CONTEMPORARY SOCIETY

IGI Global **In the modern era each new innovation poses its own special ethical dilemma. How can human society adapt to these new forms of expression, commerce, government, citizenship, and learning while holding onto its ethical and**

moral principles? The Changing Scope of Technoethics in Contemporary Society is a critical scholarly resource that examines the existing intellectual platform within the field of technoethics. Featuring coverage on a broad range of topics such as ethical perspectives on internet safety, technoscience, and ethical hacking communication, this book is geared towards academicians, researchers, and students seeking current research on domains of technoethics.

ADVANCED INFORMATION SYSTEMS ENGINEERING WORKSHOPS

CAISE 2016 INTERNATIONAL WORKSHOPS, LJUBLJANA, SLOVENIA, JUNE 13-17, 2016, PROCEEDINGS

Springer **This book constitutes the thoroughly refereed proceedings of five international workshops held in Ljubljana, Slovenia, in conjunction with the 28th International Conference on Advanced Information Systems Engineering, CAiSE 2016, in June 2016. The 16 full and 9 short papers were carefully selected from 51 submissions. The associated workshops were the Third International Workshop on Advances in Services DEsign based on the Notion of CApabiliy (ASDENCA) co-arranged with the First International Workshop on Business Model Dynamics and Information Systems Engineering (BumDISE), the Fourth International Workshop on Cognitive Aspects of Information Systems Engineering (COGNISE), the First International Workshop on Energy-awareness and Big Data Management in Information Systems (EnBIS), the Second International Workshop on Enterprise Modeling (EM), and the Sixth International Workshop on Information Systems Security Engineering (WISSE).**

ETHICAL DIMENSIONS OF COMMERCIAL AND DIY NEUROTECHNOLOGIES

Academic Press **Ethical Dimensions of Commercial and DIY Neurotechnologies Volume Three, the latest release in the Developments in Neuroethics and Bioethics series, highlights new advances in the field, with this new volume presenting interesting chapters on timely topics surrounding neuroethics and bioethics. Each chapter is written by an international board of authors.**

HCI CHALLENGES AND PRIVACY PRESERVATION IN BIG DATA SECURITY

IGI Global **Privacy protection within large databases can be a challenge. By examining the current problems and challenges this domain is facing, more efficient strategies can be established to safeguard personal information against invasive pressures. HCI Challenges and Privacy Preservation in Big Data Security is an informative scholarly**

publication that discusses how human-computer interaction impacts privacy and security in almost all sectors of modern life. Featuring relevant topics such as large scale security data, threat detection, big data encryption, and identity management, this reference source is ideal for academicians, researchers, advanced-level students, and engineers that are interested in staying current on the advancements and drawbacks of human-computer interaction within the world of big data.

COMPUTATIONAL INTELLIGENT SECURITY IN WIRELESS COMMUNICATIONS

CRC Press **Wireless network security research is multidisciplinary in nature, including data analysis, economics, mathematics, forensics, information technology, and computer science. This text covers cutting-edge research in computational intelligence systems from diverse fields on the complex subject of wireless communication security. It discusses important topics including computational intelligence in wireless network and communications, artificial intelligence and wireless communication security, security risk scenarios in communications, security/resilience metrics and their measurements, data analytics of cyber-crimes, modeling of wireless communication security risks, advances in cyber threats and computer crimes, adaptive and learning techniques for secure estimation and control, decision support systems, fault tolerance and diagnosis, cloud forensics and information systems, and intelligent information retrieval. The book- Discusses computational algorithms for system modeling and optimization in security perspective. Focuses on error prediction and fault diagnosis through intelligent information retrieval via wireless technologies. Explores a group of practical research problems where security experts can help develop new data-driven methodologies. Covers application on artificial intelligence and wireless communication security risk perspective The text is primarily written for senior undergraduate, graduate students, and researchers in the fields of electrical engineering, electronics and communication engineering, and computer engineering. The text comprehensively discusses wide range of wireless communication techniques with emerging computational intelligent trends, to help readers understand the role of wireless technologies in applications touching various spheres of human life with the help of hesitant fuzzy sets based computational modeling. It will be a valuable resource for senior undergraduate, graduate students, and researchers in the fields of electrical engineering, electronics and communication engineering, and computer engineering.**

PRIVACY AND IDENTITY MANAGEMENT. BETWEEN DATA PROTECTION AND SECURITY

16TH IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 INTERNATIONAL SUMMER SCHOOL, PRIVACY AND IDENTITY 2021, VIRTUAL EVENT, AUGUST 16–20, 2021, REVISED SELECTED PAPERS

Springer Nature

DIGITAL FINGERPRINTING

Springer **This is the first book on digital fingerprinting that comprehensively covers the major areas of study in a range of information security areas including authentication schemes, intrusion detection, forensic analysis and more. Available techniques for assurance are limited and authentication schemes are potentially vulnerable to the theft of digital tokens or secrets. Intrusion detection can be thwarted by spoofing or impersonating devices, and forensic analysis is incapable of demonstrably tying a particular device to specific digital evidence. This book presents an innovative and effective approach that addresses these concerns. This book introduces the origins and scientific underpinnings of digital fingerprinting. It also proposes a unified framework for digital fingerprinting, evaluates methodologies and includes examples and case studies. The last chapter of this book covers the future directions of digital fingerprinting. This book is designed for practitioners and researchers working in the security field and military. Advanced-level students focused on computer science and engineering will find this book beneficial as secondary textbook or reference.**

NATIONAL SECURITY: BREAKTHROUGHS IN RESEARCH AND PRACTICE

BREAKTHROUGHS IN RESEARCH AND PRACTICE

IGI Global **The tactical organization and protection of resources is a vital component for any governmental entity. Effectively managing national security through various networks ensures the highest level of protection and defense for citizens and classified information. National Security: Breakthroughs in Research and Practice is an authoritative resource for the latest research on the multiple dimensions of national security, including the political, physical, economic, ecological, and computational dimensions. Highlighting a range of pertinent topics such as data breaches, surveillance, and threat detection, this publication is an ideal reference source for government officials, law**

enforcement, professionals, researchers, IT professionals, academicians, and graduate-level students seeking current research on the various aspects of national security.

PRIVACY AND IDENTITY MANAGEMENT

15TH IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 INTERNATIONAL SUMMER SCHOOL, MARIBOR, SLOVENIA, SEPTEMBER 21–23, 2020, REVISED SELECTED PAPERS

Springer Nature **This book contains selected papers presented at the 15th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School on Privacy and Identity Management, held in Maribor, Slovenia, in September 2020.* The 13 full papers included in this volume were carefully reviewed and selected from 21 submissions. Also included is a summary paper of a tutorial. As in previous years, one of the goals of the IFIP Summer School was to encourage the publication of thorough research papers by students and emerging scholars. The papers combine interdisciplinary approaches to bring together a host of perspectives, such as technical, legal, regulatory, socio-economic, social or societal, political, ethical, anthropological, philosophical, or psychological perspectives. *The summer school was held virtually.**

METHODS, IMPLEMENTATION, AND APPLICATION OF CYBER SECURITY INTELLIGENCE AND ANALYTICS

IGI Global **Cyber security is a key focus in the modern world as more private information is stored and saved online. In order to ensure vital information is protected from various cyber threats, it is essential to develop a thorough understanding of technologies that can address cyber security challenges. Artificial intelligence has been recognized as an important technology that can be employed successfully in the cyber security sector. Due to this, further study on the potential uses of artificial intelligence is required. Methods, Implementation, and Application of Cyber Security Intelligence and Analytics discusses critical artificial intelligence technologies that are utilized in cyber security and considers various cyber security issues and their optimal solutions supported by artificial intelligence. Covering a range of topics such as malware, smart grid, data breachers, and machine learning, this major reference work is ideal for security analysts, cyber security specialists, data analysts, security professionals, computer scientists, government officials, researchers, scholars, academicians, practitioners, instructors, and students.**

WIRELESS AND MOBILE DEVICE SECURITY

Jones & Bartlett Learning **Written by an industry expert, Wireless and Mobile Device Security explores the evolution of wired networks to wireless networking and its impact on the corporate world.**

ICCWS 2019 14TH INTERNATIONAL CONFERENCE ON CYBER WARFARE AND SECURITY

ICCWS 2019

Academic Conferences and publishing limited

EMERGING METHODS IN PREDICTIVE ANALYTICS: RISK MANAGEMENT AND DECISION-MAKING

RISK MANAGEMENT AND DECISION-MAKING

IGI Global **Decision making tools are essential for the successful outcome of any organization. Recent advances in predictive analytics have aided in identifying particular points of leverage where critical decisions can be made. Emerging Methods in Predictive Analytics: Risk Management and Decision Making provides an interdisciplinary approach to predictive analytics; bringing together the fields of business, statistics, and information technology for effective decision making. Managers, business professionals, and decision makers in diverse fields will find the applications and cases presented in this text essential in providing new avenues for risk assessment, management, and predicting the future outcomes of their decisions.**

ETHICS AND POLICIES FOR CYBER OPERATIONS

A NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE INITIATIVE

Springer **This book presents 12 essays that focus on the analysis of the problems prompted by cyber operations (COs). It clarifies and discusses the ethical and regulatory problems raised by the deployment of cyber capabilities by a state’s army to inflict disruption or damage to an adversary’s targets in or through cyberspace. Written by world-leading philosophers, ethicists, policy-makers, and law and military experts, the essays cover such topics as the conceptual novelty of COs and the ethical problems that this engenders; the applicability of existing conceptual and**

regulatory frameworks to COs deployed in case of conflicts; the definition of deterrence strategies involving COs; and the analysis of models to foster cooperation in managing cyber crises. Each essay is an invited contribution or a revised version of a paper originally presented at the workshop on Ethics and Policies for Cyber Warfare, organized by the NATO Cooperative Cyber Defence Centre of Excellence in collaboration with the University of Oxford. The volume endorses a multi-disciplinary approach, as such it offers a comprehensive overview of the ethical, legal, and policy problems posed by COs and of the different approaches and methods that can be used to solve them. It will appeal to a wide readership, including ethicists, philosophers, military experts, strategy planners, and law- and policy-makers.

PROMOTING GLOBAL LITERACY SKILLS THROUGH TECHNOLOGY-INFUSED TEACHING AND LEARNING

IGI Global **The increasing internationalization of today’s classrooms calls for learning institutions to prepare students for success in an interdependent and technologically-advanced world. Faculty who are competent in multiple 21st century skills are best equipped to engage students in curricula that are relevant, transformative, and engaging across content areas and cultures. Promoting Global Literacy Skills through Technology-Infused Teaching and Learning examines the function and role of globalization in 21st century teaching and learning, especially in light of technology integration and the need to prepare and empower global educators and global citizens respectively. Covering topics that range from social networking in linguistics to software used in engineering curricula, this premier reference work will be relevant to academicians, researchers, students, librarians, practitioners, professionals, and engineers.**

ENGINEERING ETHICS FOR A GLOBALIZED WORLD

Springer **This volume identifies, discusses and addresses the wide array of ethical issues that have emerged for engineers due to the rise of a global economy. To date, there has been no systematic treatment of the particular challenges globalization poses for engineering ethics standards and education. This volume concentrates on precisely this challenge. Scholars and practitioners from diverse national and professional backgrounds discuss the ethical issues emerging from the inherent symbiotic relationship between the engineering profession and globalization. Through their discussions a deeper and more complete understanding of the precise ways in which globalization impacts the formulation and justification of ethical standards in engineering as well as the curriculum and pedagogy of engineering ethics education emerges. The world today is witnessing an unprecedented demand for engineers and other science and technology professionals with advanced degrees due to both the off-shoring of western jobs and the**

rapid development of non-Western countries. The current flow of technology and professionals is from the West to the rest of the world. Professional practices followed by Western (or Western-trained) engineers are often based on presuppositions which can be in fundamental disagreement with the viewpoints of non-Westerners. A successful engineering solution cannot be simply technically sound, but also must account for cultural, social and religious constraints. For these reasons, existing Western standards cannot simply be exported to other countries. Divided into two parts, Part I of the volume provides an overview of particular dimensions of globalization and the criteria that an adequate engineering ethics framework must satisfy in a globalized world. Part II of the volume considers pedagogical challenges and aims in engineering ethics education that is global in character.

CYBERSECURITY POLICIES AND STRATEGIES FOR CYBERWARFARE PREVENTION

IGI Global **Cybersecurity has become a topic of concern over the past decade as private industry, public administration, commerce, and communication have gained a greater online presence. As many individual and organizational activities continue to evolve in the digital sphere, new vulnerabilities arise. Cybersecurity Policies and Strategies for Cyberwarfare Prevention serves as an integral publication on the latest legal and defensive measures being implemented to protect individuals, as well as organizations, from cyber threats. Examining online criminal networks and threats in both the public and private spheres, this book is a necessary addition to the reference collections of IT specialists, administrators, business managers, researchers, and students interested in uncovering new ways to thwart cyber breaches and protect sensitive digital information.**

SECURITY STANDARDISATION RESEARCH

6TH INTERNATIONAL CONFERENCE, SSR 2020, LONDON, UK, NOVEMBER 30 – DECEMBER 1, 2020, PROCEEDINGS

Springer Nature **This book constitutes the refereed proceedings of the 6th International Conference on Security Standardisation Research, SSR 2020, held in London, UK, in November 2020.* The papers cover a range of topics in the field of security standardisation research, including cryptographic evaluation, standards development, analysis with formal methods, potential future areas of standardisation, and improving existing standards. * The conference was held virtually due to the COVID-19 pandemic.**

HEALTHIER LIVES, DIGITALLY ENABLED

SELECTED PAPERS FROM THE DIGITAL HEALTH INSTITUTE SUMMIT 2020

IOS Press **Disruption often drives innovation, and 2020 was certainly an extraordinary year for all health professionals. Not only did it stretch individual providers and healthcare systems to their limits, it highlighted the urgent and rapid need to mobilize digital health technology, as well as pressure-testing digital health in ways and under timeframes not previously imagined. Many saw the rapid deployment and uptake of telehealth services, partly out of necessity to maintain continuity of care, but also to ensure that those who needed healthcare were still able to access it no matter what their situation or location. This book presents 17 selected papers from the Australian Health Informatics Conference (HIC 2020) – Healthier Lives, Digitally Enabled, held online from 5 – 25 November 2020. This annual conference usually marks the coming together of the nation's digital health community to discuss, share and showcase current and future initiatives that support the progression of digital health, but in 2020, it took the form of satellite events, culminating with an online Digital Health Institute Summit. The papers presented here reflect highly topical themes across various areas and disciplines, including: digital health in the care of the elderly, mental health, COVID-19, public health, and workforce. Familiar topics, such as wearables, mobile health and remote monitoring, interoperability, and data privacy are also covered, as well as telehealth, automation, bots, and other AI applications. The book will be of interest to all health professionals, especially those working in the fields of digital health informatics and telemedicine.**

FOUNDATIONS OF INFORMATION ETHICS

American Library Association **Foreword by Robert Hauptman As discussions about the roles played by information in economic, political, and social arenas continue to evolve, the need for an intellectual primer on information ethics that also functions as a solid working casebook for LIS students and professionals has never been more urgent. This text, written by a stellar group of ethics scholars and contributors from around the globe, expertly fills that need. Organized into twelve chapters, making it ideal for use by instructors, this volume from editors Burgess and Knox thoroughly covers principles and concepts in information ethics, as well as the history of ethics in the information professions; examines human rights, information access, privacy, discourse, intellectual property, censorship, data and cybersecurity ethics, intercultural information ethics, and global digital citizenship and responsibility; synthesizes the**

philosophical underpinnings of these key subjects with abundant primary source material to provide historical context along with timely and relevant case studies; features contributions from John M. Budd, Paul T. Jaeger, Rachel Fischer, Margaret Zimmerman, Kathrine A. Henderson, Peter Darch, Michael Zimmer, and Masooda Bashir, among others; and offers a special concluding chapter by Amelia Gibson that explores emerging issues in information ethics, including discussions ranging from the ethics of social media and social movements to AI decision making. This important survey will be a key text for LIS students and an essential reference work for practitioners.

SECURITY IN COMPUTING AND COMMUNICATIONS

6TH INTERNATIONAL SYMPOSIUM, SSCC 2018, BANGALORE, INDIA, SEPTEMBER 19–22, 2018, REVISED SELECTED PAPERS

Springer **This book constitutes the refereed proceedings of the 6th International Symposium on Security in Computing and Communications, SSCC 2018, held in Bangalore, India, in September 2018. The 34 revised full papers and 12 revised short papers presented were carefully reviewed and selected from 94 submissions. The papers cover wide research fields including cryptography, database and storage security, human and societal aspects of security and privacy.**

ADVANCES IN DIGITAL FORENSICS XVII

17TH IFIP WG 11.9 INTERNATIONAL CONFERENCE, VIRTUAL EVENT, FEBRUARY 1–2, 2021, REVISED SELECTED PAPERS

Springer Nature **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 XVII 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 seventeenth 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 selection of thirteen edited papers from the Seventeenth Annual IFIP WG 11.9 International Conference on Digital Forensics, held virtually in the winter of 2021. Advances in Digital Forensics XVII 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.

THE ETHICS OF CYBERSECURITY

Springer Nature **This open access book provides the first comprehensive collection of papers that provide an integrative view on cybersecurity. It discusses theories, problems and solutions on the relevant ethical issues involved. This work is sorely needed in a world where cybersecurity has become indispensable to protect trust and confidence in the digital infrastructure whilst respecting fundamental values like equality, fairness, freedom, or privacy. The book has a strong practical focus as it includes case studies outlining ethical issues in cybersecurity and presenting guidelines and other measures to tackle those issues. It is thus not only relevant for academics but also for practitioners in cybersecurity such as providers of security software, governmental CERTs or Chief Security Officers in companies.**

ICONISTECH-1 2019

SELECTED PAPERS FROM THE 1ST INTERNATIONAL CONFERENCE ON ISLAM, SCIENCE AND TECHNOLOGY, ICONISTECH-1 2019, 11-12 JULY 2019, BANDUNG, INDONESIA

European Alliance for Innovation **The first International Conference of Islam, Science, and Technology (ICONISTECH) 2019 is an annual event to bring researchers, academics, experts, and professionals in Science and Technology related to Industrial Revolution 4.0. In 2020, this event was held on July, 11-12th 2019 at Grand Tjokro, Bandung, Indonesia. The conference from any kind of stakeholders related to Mathematics and Its Application, Chemistry, Life Science, Physics, Applied Sciences, Agrotechnology, Computer Science, Electrical Engineering, Information Technology, Ethics in science and technology, Integrated Islam to Science and Technology. Each contributed paper was refereed before being** accepted for publication. The double-blind peer-reviewed was used in the paper selection.

SOCIO-TECHNICAL ASPECTS IN SECURITY AND TRUST

9TH INTERNATIONAL WORKSHOP, STAST 2019, LUXEMBOURG CITY, LUXEMBOURG, SEPTEMBER 26, 2019, REVISED SELECTED PAPERS

Springer Nature **The open access volume LNCS 11739 constitutes the proceedings of the 9th International Workshop on Socio-Technical Aspects in Security, STAST 2019, held in Luxembourg, in September 2019. The total of 9 full papers together with 1 short paper was carefully reviewed and selected from 28 submissions. The papers were organized in topical sections named as follows: Methods for Socio-Technical Systems focused on instruments, frameworks and re ections on research methodology and also System Security considered security analyses and attacks on security systems. Finally, Privacy Control incorporated works on privacy protection and control as well as human factors in relation to these topics.**

CONFLICT IN CYBER SPACE

THEORETICAL, STRATEGIC AND LEGAL PESPECTIVES

Routledge **Adopting a multidisciplinary perspective, this book explores the key challenges associated with the proliferation of cyber capabilities. Over the past two decades, a new man-made domain of conflict has materialized. Alongside armed conflict in the domains of land, sea, air, and space, hostilities between different types of political actors are now taking place in cyberspace. This volume addresses the challenges posed by cyberspace hostility from theoretical, political, strategic and legal perspectives. In doing so, and in contrast to current literature, cyber-security is analysed through a multidimensional lens, as opposed to being treated solely as a military or criminal issues, for example. The individual chapters map out the different scholarly and political positions associated with various key aspects of cyber conflict and seek to answer the following questions: do existing theories provide sufficient answers to the current challenges posed by conflict in cyberspace, and, if not, could alternative approaches be developed?; how do states and non-state actors make use of cyber-weapons when pursuing strategic and political aims?; and, how does the advent of conflict in cyberspace challenge our established legal framework? By asking important strategic questions on the theoretical, strategic, ethical and legal implications and challenges of the proliferation of cyber**

warfare capabilities, the book seeks to stimulate research into an area that has hitherto been neglected. This book will be of much interest to students of cyber-conflict and cyber-warfare, war and conflict studies, international relations, and security studies.

HACKING EUROPE

FROM COMPUTER CULTURES TO DEMOSCENES

Springer **Hacking Europe traces the user practices of chopping games in Warsaw, hacking software in Athens, creating chaos in Hamburg, producing demos in Turku, and partying with computing in Zagreb and Amsterdam. Focusing on several European countries at the end of the Cold War, the book shows the digital development was not an exclusively American affair. Local hacker communities appropriated the computer and forged new cultures around it like the hackers in Yugoslavia, Poland and Finland, who showed off their tricks and creating distinct “demoscenes.” Together the essays reflect a diverse palette of cultural practices by which European users domesticated computer technologies. Each chapter explores the mediating actors instrumental in introducing and spreading the cultures of computing around Europe. More generally, the “ludological” element--the role of mischief, humor, and play--discussed here as crucial for analysis of hacker culture, opens new vistas for the study of the history of technology.**

DEVELOPING NEXT-GENERATION COUNTERMEASURES FOR HOMELAND SECURITY THREAT PREVENTION

IGI Global **In the modern world, natural disasters are becoming more commonplace, unmanned systems are becoming the norm, and terrorism and espionage are increasingly taking place online. All of these threats have made it necessary for governments and organizations to steel themselves against these threats in innovative ways. Developing Next-Generation Countermeasures for Homeland Security Threat Prevention provides relevant theoretical frameworks and empirical research outlining potential threats while exploring their appropriate countermeasures. This relevant publication takes a broad perspective, from network security, surveillance, reconnaissance, and physical security, all topics are considered with equal weight. Ideal for policy makers, IT professionals, engineers, NGO operators, and graduate students, this book provides an in-depth look into the threats facing modern society and the methods to avoid them.**

CRITICAL INFORMATION INFRASTRUCTURES SECURITY

13TH INTERNATIONAL CONFERENCE, CRITIS 2018, KAUNAS, LITHUANIA, SEPTEMBER 24-26, 2018, REVISED SELECTED PAPERS

Springer **This book constitutes revised selected papers from the 13th International Conference on Critical Information Infrastructures Security, CRITIS 2018, held in Kaunas, Lithuania, in September 2018.The 16 full papers and 3 short papers presented were carefully reviewed and selected from 61 submissions. They are grouped in the following topical sections: advanced analysis of critical energy systems, strengthening urban resilience, securing internet of things and industrial control systems, need and tool sets for industrial control system security, and advancements in governance and resilience of critical infrastructures.**

HEALTHCARE ETHICS AND TRAINING: CONCEPTS, METHODOLOGIES, TOOLS, AND APPLICATIONS

CONCEPTS, METHODOLOGIES, TOOLS, AND APPLICATIONS

IGI Global **The application of proper ethical systems and education programs is a vital concern in the medical industry. When healthcare professionals are held to the highest moral and training standards, patient care is improved. Healthcare Ethics and Training: Concepts, Methodologies, Tools, and Applications is a comprehensive source of academic research material on methods and techniques for implementing ethical standards and effective education initiatives in clinical settings. Highlighting pivotal perspectives on topics such as e-health, organizational behavior, and patient rights, this multi-volume work is ideally designed for practitioners, upper-level students, professionals, researchers, and academics interested in the latest developments within the healthcare industry.**

CYBERSECURITY ETHICS

AN INTRODUCTION

Routledge **This new textbook offers an accessible introduction to the topic of cybersecurity ethics. The book is split into three parts. Part I provides an introduction to the field of ethics, philosophy and philosophy of science, three ethical frameworks – virtue ethics, utilitarian ethics and communitarian ethics – and the notion of ethical hacking. Part II**

applies these frameworks to particular issues within the field of cybersecurity, including privacy rights, intellectual property and piracy, surveillance, and cyberethics in relation to military affairs. The third part concludes by exploring current codes of ethics used in cybersecurity. The overall aims of the book are to: provide ethical frameworks to aid decision making; present the key ethical issues in relation to computer security; highlight the connection between values and beliefs and the professional code of ethics. The textbook also includes three different features to aid students: 'Going Deeper' provides background information on key individuals and concepts; 'Critical Issues' features contemporary case studies; and 'Applications' examine specific technologies or practices which raise ethical issues. The book will be of much interest to students of cybersecurity, cyberethics, hacking, surveillance studies, ethics and information science.

ETHICS AND CYBER WARFARE

THE QUEST FOR RESPONSIBLE SECURITY IN THE AGE OF DIGITAL WARFARE

Oxford University Press **From North Korea's recent attacks on Sony to perpetual news reports of successful hackings and criminal theft, cyber conflict has emerged as a major topic of public concern. Yet even as attacks on military, civilian, and commercial targets have escalated, there is not yet a clear set of ethical guidelines that apply to cyber warfare. Indeed, like terrorism, cyber warfare is commonly believed to be a war without rules. Given the prevalence cyber warfare, developing a practical moral code for this new form of conflict is more important than ever. In Ethics and Cyber Warfare, internationally-respected ethicist George Lucas delves into the confounding realm of cyber conflict. Comparing "state-sponsored hacktivism" to the transformative impact of "irregular warfare" in conventional armed conflict, Lucas offers a critique of legal approaches to governance, and outlines a new approach to ethics and "just war" reasoning. Lucas draws upon the political philosophies of Alasdair MacIntyre, John Rawls, and Jürgen Habermas to provide a framework for understanding these newly-emerging standards for cyber conflict, and ultimately presents a professional code of ethics for a new generation of "cyber warriors." Lucas concludes with a discussion of whether preemptive self-defense efforts - such as the massive government surveillance programs revealed by Edward Snowden - can ever be justified, addressing controversial topics such as privacy, anonymity, and public trust. Well-reasoned and timely, Ethics and Cyber Warfare is a must-read for anyone with an interest in philosophy, ethics, or cybercrime.**

HANDBOOK OF MULTIMEDIA INFORMATION SECURITY: TECHNIQUES AND APPLICATIONS

Springer **This handbook is organized under three major parts. The first part of this handbook deals with multimedia security for emerging applications. The chapters include basic concepts of multimedia tools and applications, biological and behavioral biometrics, effective multimedia encryption and secure watermarking techniques for emerging applications, an adaptive face identification approach for android mobile devices, and multimedia using chaotic and perceptual hashing function. The second part of this handbook focuses on multimedia processing for various potential applications. The chapter includes a detail survey of image processing based automated glaucoma detection techniques and role of de-noising, recent study of dictionary learning based image reconstruction techniques for analyzing the big medical data, brief introduction of quantum image processing and it applications, a segmentation-less efficient Alzheimer detection approach, object recognition, image enhancements and de-noising techniques for emerging applications, improved performance of image compression approach, and automated detection of eye related diseases using digital image processing. The third part of this handbook introduces multimedia applications. The chapter includes the extensive survey on the role of multimedia in medicine and multimedia forensics classification, a finger based authentication system for e-health security, analysis of recently developed deep learning techniques for emotion and activity recognition. Further, the book introduce a case study on change of ECG according to time for user identification, role of multimedia in big data, cloud computing, the Internet of things (IoT) and blockchain environment in detail for real life applications. This handbook targets researchers, policy makers, programmers and industry professionals in creating new knowledge for developing efficient techniques/framework for multimedia applications. Advanced level students studying computer science, specifically security and multimedia will find this book useful as a reference.**

CHALLENGES IN THE IOT AND SMART ENVIRONMENTS

A PRACTITIONERS' GUIDE TO SECURITY, ETHICS AND CRIMINAL THREATS

Springer Nature

SMART CITIES CYBERSECURITY AND PRIVACY

Elsevier **Smart Cities Cybersecurity and Privacy examines the latest research developments and their outcomes for safe,**

secure, and trusting smart cities residents. Smart cities improve the quality of life of citizens in their energy and water usage, healthcare, environmental impact, transportation needs, and many other critical city services. Recent advances in hardware and software, have fueled the rapid growth and deployment of ubiquitous connectivity between a city's physical and cyber components. This connectivity however also opens up many security vulnerabilities that must be mitigated. Smart Cities Cybersecurity and Privacy helps researchers, engineers, and city planners develop adaptive, robust, scalable, and reliable security and privacy smart city applications that can mitigate the negative implications associated with cyber-attacks and potential privacy invasion. It provides insights into networking and security architectures, designs, and models for the secure operation of smart city applications. Consolidates in one place state-of-the-art academic and industry research Provides a holistic and systematic framework for design, evaluating, and deploying the latest security solutions for smart cities Improves understanding and collaboration among all smart city stakeholders to develop more secure smart city architectures