Istr Volume 22 Symantec

Real-Time Sensor Networks and Systems for the Industrial IoT
Cybersecurity – Attack and Defense Strategies
Shaping the Digital Enterprise
Faster Disaster Recovery
Атлас профессий будущего
Artificial Intelligence and Digital Diplomacy
Buying your Self on the Internet
Information Security
Security and Privacy in Communication Networks
Security in Computer and Information Sciences
Service-Oriented Computing
Malware Analysis Using Artificial Intelligence and Deep Learning
Mass Communication in India, Fifth Edition
Managed Software Evolution
Trends and Innovations in Information Systems and Technologies
Proceedings of the International Conference on Computing and Communication Systems

Cyber Security
India's National Security
Applied Learning Algorithms for Intelligent IoT
Security and Privacy in Cyber-Physical Systems
ICT and Society
World Internet Development Report 2017
Information and Communication Technology for Sustainable Development
Machine Intelligence and Big Data Analytics for Cybersecurity Applications
The Aerospace Supply Chain and Cyber Security
Cybercrimes et enjeux technologiques - Contexte et perspectives
Data Exfiltration Threats and Prevention Techniques
Neural Information Processing
Threat Mitigation and Detection of Cyber Warfare and Terrorism Activities
Broadband Communications, Networks, and Systems
Secure IT Systems
Cybersecurity in China
Cybersecurity Awareness Among Students and Faculty
Cyber Arms
Cyber Technological Paradigms and Threat Landscape in India
The Art of Cyberwarfare

Information Security
Advances in Computer Communication and Computational Sciences
Hacking Wireless Access Points

BURCH JAMARCUS

Real-Time Sensor Networks and Systems for the Industrial IoT Springer Nature
This book contains the latest research work presented at the International Conference on Computing and Communication Systems (I3CS 2020) held at North-Eastern Hill University (NEHU), Shillong, India. The book presents original research results, new ideas and practical development experiences which concentrate on both theory and practices. It includes papers from all areas of information technology, computer science, electronics and communication engineering written by researchers, scientists, engineers and scholar students and experts from India and abroad.
Cybersecurity – Attack and Defense Strategies Springer
This book constitutes the refereed proceedings on the 23rd Nordic Conference on Secure IT Systems, NordSec 2018, held in Oslo, Norway, in November 2018. The 29 full papers presented in this volume were carefully reviewed and selected from 81 submissions. They are organized in

topical sections named: privacy; cryptography; network and cloud security; cyber security and malware; and security for software and software development.

Shaping the Digital Enterprise John Wiley & Sons

This volume discusses digital diplomacy and artificial intelligence within the context of global governance and international security. Rapid digitalization has changed the way international actors interact, offering new opportunities for international and bilateral cooperation and reinforcing the role of the emergent actors within global governance. New phenomena linked to digitalization and artificial intelligence are emerging and this volume brings a multidisciplinary, mixed-methods approach to studying them. Written by globally recognized experts, each chapter presents a case study covering an emerging topic such as: international regulation of the web and digital diplomacy, the interplay of artificial intelligence and cyber diplomacy, social media and artificial intelligence as tools for digital diplomacy, the malicious use of artificial intelligence, cyber security, and data sovereignty. Incorporating both theory and practice, quantitative and qualitative analysis, this volume will be of interest to graduate students and researchers in international relations, diplomacy, security studies, and artificial intelligence, as well as

diplomats and policymakers looking to understand the implications of digitalization and artificial intelligence in their fields.
Faster Disaster Recovery
John Wiley & Sons
Malgré l'impact qu'a eu l'informatisation de la société sur le crime, les connaissances sur le cybercrime n'abondent pas. Ce livre se veut une contribution à la synthèse des connaissances sur différents cybercrimes, notamment par l'examen des enjeux qu'ils soulèvent. Il étudie de façon approfondie quatorze phénomènes liés aux cybercrimes, allant des pratiques policières sur les médias sociaux à l'exploitation sexuelle des enfants sur Internet, en passant par la cyberintimidation, le piratage, les fraudes et l'utilisation des nouvelles technologies à des fins de propagande. Selon le sujet, les chapitres adoptent l'une de deux structures : les chapitres de type synthèse proposent une analyse des dernières connaissances criminologiques, sociologiques, juridiques et technologiques relatives à un cybercrime donné tandis que les chapitres de type nouvelle recherche présentent les résultats d'une recherche récente. Dans tous les cas, les expériences professionnelles et universitaires des auteurs, à l'instar de la diversité de leur provenance géographique au sein de la Francophonie (Canada, Suisse, France), viennent enrichir le contenu. Cet ouvrage, qui s'adresse aussi bien à l'étudiant, au

chercheur ou à l'intervenant du milieu de la justice qu'au citoyen, peut se lire d'une couverture à l'autre ou un chapitre - voire une section - à la fois.
Атлас профессий будущего Springer Nature
This book includes key insights that reflect ‘Advances in Computer and Computational Sciences’ from upcoming researchers and leading academics around the globe. It gathers high-quality, peer-reviewed papers presented at the International Conference on Computer, Communication and Computational Sciences (IC4S 2018), which was held on 20-21 October, 2018 in Bangkok. The book covers a broad range of topics, including intelligent hardware and software design, advanced communications, intelligent computing techniques, intelligent image processing, and web and informatics. Its goal is to familiarize readers from the computer industry and academia with the latest advances in next-generation computer and communication technology, which they can subsequently integrate into real-world applications.
Artificial Intelligence and Digital Diplomacy Springer
Technology provides numerous opportunities for positive developments in modern society; however, these venues inevitably increase vulnerability to threats in online environments. Addressing issues of

security in the cyber realm is increasingly relevant and critical to society. Threat Mitigation and Detection of Cyber Warfare and Terrorism Activities is a comprehensive reference source for the latest scholarly perspectives on countermeasures and related methods to enhance security and protection against criminal activities online. Highlighting a range of topics relevant to secure computing, such as parameter tampering, surveillance and control, and digital protests, this book is ideally designed for academics, researchers, graduate students, professionals, and practitioners actively involved in the expanding field of cyber security.
Jaico Publishing House
This book constitutes the refereed proceedings of the 11th IFIP TC 9 International Conference on Human Choice and Computers, HCC11 2014, held in Turku, Finland, in July/August 2014. The 29 revised full papers presented were carefully reviewed and selected from numerous submissions. The papers are based on both academic research and the professional experience of information technologists working in the field. They have been organized in the following topical sections: society, social responsibility, ethics and ICT; the history of computing and its meaning for the future; peace, war, cyber-security and ICT; and health, care, well-being and ICT.
Buying your Self on the Internet Springer
This book will raise

awareness on emerging challenges of AIempowered cyber arms used in weapon systems and stockpiled in the global cyber arms race. Based on real life events, it provides a comprehensive analysis of cyber offensive and defensive landscape, analyses the cyber arms evolution from prank malicious codes into lethal weapons of mass destruction, reveals the scale of cyber offensive conflicts, explores cyber warfare mutation, warns about cyber arms race escalation and use of Artificial Intelligence (AI) for military purposes. It provides an expert insight into the current and future malicious and destructive use of the evolved cyber arms, AI and robotics, with emphasis on cyber threats to CBRNe and critical infrastructure. The book highlights international efforts in regulating the cyber environment, reviews the best practices of the leading cyber powers and their controversial approaches, recommends responsible state behaviour. It also proposes information security and cyber defence solutions and provides definitions for selected conflicting cyber terms. The disruptive potential of cyber tools merging with military weapons is examined from the technical point of view, as well as legal, ethical, and political perspectives.

Information Security

Springer

This open access book constitutes the thoroughly refereed proceedings of

the First International ISCIS Security Workshop 2018, Euro-CYBERSEC 2018, held in London, UK, in February 2018. The 12 full papers presented together with an overview paper were carefully reviewed and selected from 31 submissions. Security of distributed interconnected systems, software systems, and the Internet of Things has become a crucial aspect of the performance of computer systems. The papers deal with these issues, with a specific focus on societally critical systems such as health informatics systems, the Internet of Things, energy systems, digital cities, digital economy, mobile networks, and the underlying physical and network infrastructures.

Security and Privacy in Communication Networks Springer Nature

The Aerospace Supply Chain and Cyber Security - Challenges Ahead looks at the current state of commercial aviation and cyber security, how information technology and its attractiveness to cyber attacks is affecting it, and the way supply chains have become a vital part of the industry's cyber-security strategy. More than ever before, commercial aviation relies on information and communications technology. Some examples of this include the use of e-tickets by passengers, electronic flight bags by pilots, wireless web access in flight, not to mention the thousands of sensors throughout the aircraft constantly gathering and sharing data with the

crew on the ground. The same way technology opens the doors for speed, efficiency and convenience, it also offers the unintended opportunity for malicious cyber attacks, with threat agents becoming bolder and choosing any possible apertures to breach security. Supply chains are now being seriously targeted as a pathway to the vital core of organizations around the world. Written in a direct and informative way, The Aerospace Supply Chain and Cyber Security - Challenges Ahead discusses the importance of deeply mapping one's supply chain to identify risky suppliers or potential disruptions, developing supplier monitoring programs to identify critical suppliers, and identifying alternative sources for IT/ICT products or components, to name a few of the necessary actions to be taken by the industry. The Aerospace Supply Chain and Cyber Security - Challenges Ahead also discusses the standardization of communications platforms and its pitfalls, the invisible costs associated with cyber attacks, how to identify vulnerabilities of the supply chain, and what future scenarios are likely to play out in this arena. For those interested in the many aspects of cyber security, The Aerospace Supply Chain and Cyber Security - Challenges Ahead is a must-read.

Security in Computer and Information Sciences John Wiley & Sons

The last two years have witnessed deterioration in

the global security situation characterised by increasing tensions among major powers. The threat perceptions of the US, China and Russia vis-à-vis each other have sharpened. There is stiff competition among them to dominate the strategic space in different parts of the world. This has led them to formulate national security strategies which are more assertive, aggressive and competitive. There is lack of consensus in resolution of conflicts in Afghanistan and Syria. There is no concerted effort in meeting the challenge of the Islamic State. It is in this fractured security environment that India has been making special efforts to project itself as a leading power commensurate with its economic and military potential. This fifteenth volume of India's National Security Annual Review undertakes an incisive analysis of India's endeavours to maximise its gains with respect to its strategic partners. The volume also focuses on the new dynamism that India has injected in its relations with countries in the Middle East and the Asia Pacific. India's threat perceptions in its extended security zone, critical aspects of its strategic preparedness and complex issues regarding its internal security have been thoroughly examined. With contributions from experts from the fields of diplomacy, academia and civil and military services, the book will be one of the most dependable sources of analyses for scholars of international relations,

foreign policy, defence and strategic studies, and political science, and practitioners alike.

Service-Oriented Computing Springer

A practical guide to understanding and analyzing cyber attacks by advanced attackers, such as nation states. Cyber attacks are no longer the domain of petty criminals. Today, companies find themselves targeted by sophisticated nation state attackers armed with the resources to craft scarily effective campaigns. This book is a detailed guide to understanding the major players in these cyber wars, the techniques they use, and the process of analyzing their advanced attacks. Whether you're an individual researcher or part of a team within a Security Operations Center (SoC), you'll learn to approach, track, and attribute attacks to these advanced actors. The first part of the book is an overview of actual cyber attacks conducted by nation-state actors and other advanced organizations. It explores the geopolitical context in which the attacks took place, the patterns found in the attackers' techniques, and the supporting evidence analysts used to attribute such attacks. Dive into the mechanisms of: North Korea's series of cyber attacks against financial institutions, which resulted in billions of dollars stolen The world of targeted ransomware attacks, which have leveraged nation state tactics to cripple entire corporate enterprises with ransomware Recent cyber

attacks aimed at disrupting or influencing national elections globally The book's second part walks through how defenders can track and attribute future attacks. You'll be provided with the tools, methods, and analytical guidance required to dissect and research each stage of an attack campaign. Here, Jon DiMaggio demonstrates some of the real techniques he has employed to uncover crucial information about the 2021 Colonial Pipeline attacks, among many other advanced threats. He now offers his experience to train the next generation of expert analysts.

Malware Analysis Using Artificial Intelligence and Deep Learning Springer Nature

This open access book presents the outcomes of the "Design for Future – Managed Software Evolution" priority program 1593, which was launched by the German Research Foundation ("Deutsche Forschungsgemeinschaft (DFG)") to develop new approaches to software engineering with a specific focus on long-lived software systems. The different lifecycles of software and hardware platforms lead to interoperability problems in such systems. Instead of separating the development, adaptation and evolution of software and its platforms, as well as aspects like operation, monitoring and maintenance, they should all be integrated into one overarching process. Accordingly, the book is split into three major

parts, the first of which includes an introduction to the nature of software evolution, followed by an overview of the specific challenges and a general introduction to the case studies used in the project. The second part of the book consists of the main chapters on knowledge carrying software, and cover tacit knowledge in software evolution, continuous design decision support, model-based round-trip engineering for software product lines, performance analysis strategies, maintaining security in software evolution, learning from evolution for evolution, and formal verification of evolutionary changes. In turn, the last part of the book presents key findings and spin-offs. The individual chapters there describe various case studies, along with their benefits, deliverables and the respective lessons learned. An overview of future research topics rounds out the coverage. The book was mainly written for scientific researchers and advanced professionals with an academic background. They will benefit from its comprehensive treatment of various topics related to problems that are now gaining in importance, given the higher costs for maintenance and evolution in comparison to the initial development, and the fact that today, most software is not developed from scratch, but as part of a continuum of former and future releases.

Mass Communication in India, Fifth Edition

Springer

The Art of CyberwarfareNo Starch Press
Managed Software Evolution Springer
This book vividly illustrates all the promising and potential machine learning (ML) and deep learning (DL) algorithms through a host of real-world and real-time business use cases. Machines and devices can be empowered to self-learn and exhibit intelligent behavior. Also, Big Data combined with real-time and runtime data can lead to personalized, prognostic, predictive, and prescriptive insights. This book examines the following topics: Cognitive machines and devices Cyber physical systems (CPS) The Internet of Things (IoT) and industrial use cases Industry 4.0 for smarter manufacturing Predictive and prescriptive insights for smarter systems Machine vision and intelligence Natural interfaces K-means clustering algorithm Support vector machine (SVM) algorithm A priori algorithms Linear and logistic regression Applied Learning Algorithms for Intelligent IoT clearly articulates ML and DL algorithms that can be used to unearth predictive and prescriptive insights out of Big Data. Transforming raw data into information and relevant knowledge is gaining prominence with the availability of data processing and mining, analytics algorithms, platforms, frameworks, and other accelerators discussed in the book. Now, with the emergence of machine learning

algorithms, the field of data analytics is bound to reach new heights. This book will serve as a comprehensive guide for AI researchers, faculty members, and IT professionals. Every chapter will discuss one ML algorithm, its origin, challenges, and benefits, as well as a sample industry use case for explaining the algorithm in detail. The book's detailed and deeper dive into ML and DL algorithms using a practical use case can foster innovative research.

Trends and Innovations in Information Systems and Technologies

Presses internationales Polytechnique

Hacking Wireless Access Points: Cracking, Tracking, and Signal Jacking provides readers with a deeper understanding of the hacking threats that exist with mobile phones, laptops, routers, and navigation systems. In addition, applications for Bluetooth and near field communication (NFC) technology continue to multiply, with athletic shoes, heart rate monitors, fitness sensors, cameras, printers, headsets, fitness trackers, household appliances, and the number and types of wireless devices all continuing to increase dramatically. The book demonstrates a variety of ways that these vulnerabilities can be—and have been—exploited, and how the unfortunate consequences of such exploitations can be mitigated through the responsible use of technology. Explains how the wireless access points

in common, everyday devices can expose us to hacks and threats Teaches how wireless access points can be hacked, also providing the techniques necessary to protect and defend data Presents concrete examples and real-world guidance on how to protect against wireless access point attacks Proceedings of the International Conference on Computing and Communication Systems Springer This book is focused on the use of deep learning (DL) and artificial intelligence (AI) as tools to advance the fields of malware detection and analysis. The individual chapters of the book deal with a wide variety of state-of-the-art AI and DL techniques, which are applied to a number of challenging malware-related problems. DL and AI based approaches to malware detection and analysis are largely data driven and hence minimal expert domain knowledge of malware is needed. This book fills a gap between the emerging fields of DL/AI and malware analysis. It covers a broad range of modern and practical DL and AI techniques, including frameworks and development tools enabling the audience to innovate with cutting-edge research advancements in a multitude of malware (and closely related) use cases. **Cyber Security** Springer This book gathers selected papers presented at the 2020 World Conference on Information Systems and Technologies

(WorldCIST'20), held in Budva, Montenegro, from April 7 to 10, 2020. WorldCIST provides a global forum for researchers and practitioners to present and discuss recent results and innovations, current trends, professional experiences with and challenges regarding various aspects of modern information systems and technologies. The main topics covered are A) Information and Knowledge Management; B) Organizational Models and Information Systems; C) Software and Systems Modeling; D) Software Systems, Architectures, Applications and Tools; E) Multimedia Systems and Applications; F) Computer Networks, Mobility and Pervasive Systems; G) Intelligent and Decision Support Systems; H) Big Data Analytics and Applications; I) Human–Computer Interaction; J) Ethics, Computers & Security; K) Health Informatics; L) Information Technologies in Education; M) Information Technologies in Radiocommunications; and N) Technologies for Biomedical Applications.

India's National Security Edinburgh University Press

This book examines the rise of the direct-to-consumer genetic testing industry (DTC) and its use of 'wrap' contracts. It uses the example of DTC to show the challenges that disruptive technologies pose for societies and for regulation. It also uses the wrap contracts of DTC companies to explore broader issues with online contracting.

Applied Learning

Algorithms for Intelligent IoT Springer Nature
The Industrial Internet of Things (Industrial IoT—IIoT) has emerged as the core construct behind the various cyber-physical systems constituting a principal dimension of the fourth Industrial Revolution. While initially born as the concept behind specific industrial applications of generic IoT technologies, for the optimization of operational efficiency in automation and control, it quickly enabled the achievement of the total convergence of Operational (OT) and Information Technologies (IT). The IIoT has now surpassed the traditional borders of automation and control functions in the process and manufacturing industry, shifting towards a wider domain of functions and industries, embraced under the dominant global initiatives and architectural frameworks of Industry 4.0 (or Industrie 4.0) in Germany, Industrial Internet in the US, Society 5.0 in Japan, and Made-in-China 2025 in China. As real-time embedded systems are quickly achieving ubiquity in everyday life and in industrial environments, and many processes already depend on real-time cyber-physical systems and embedded sensors, the integration of IoT with cognitive computing and real-time data exchange is essential for real-time analytics and realization of digital twins in smart environments and services under the various frameworks' provisions. In this context, real-time sensor networks

and systems for the Industrial IoT encompass multiple technologies and raise significant design, optimization, integration and exploitation challenges. The ten articles in this Special Issue describe advances in real-time sensor networks and systems that are significant enablers of the Industrial IoT paradigm. In the relevant landscape, the domain of wireless networking technologies is centrally positioned, as expected.