9th International Conference On Cyber Warfare And Security

Information modeling and knowledge bases have become an important area of academic and industry research in the 21st century, addressing complexities of modeling that reach beyond the traditional borders of information systems and academic computer science research. This book presents 32 reviewed, selected and updated papers delivered at the 29th International Conference on Information Modeling and Knowledge Bases (EJC2019), held in Lappeenranta, Finland, from 3 to 7 June 2019. In addition, two papers based on the keynote presentations and one paper edited from the discussion of the panel session are included in the book. The conference provided a forum to exchange scientific results and experience, and attracted academics and practitioners working with information and knowledge. The papers cover a wide range of topics, ranging from knowledge discovery through conceptual and linguistic modeling, knowledge and information modeling and discovery, cross-cultural communication and social computing, environmental modeling and engineering, and multimedia data modeling and systems to complex scientific problem-solving. The conference presentation sessions: Learning and Linguistics; Systems and Processes; Data and Knowledge Representation; Models and Interface; Formalizations and Reasoning; Models and Modeling; Machine Learning; Models and Programming; Environment and Predictions; and Emotion Modeling and Social Networks reflect the main

themes of the conference. The book also includes 2 extended publications of keynote addresses: 'Philosophical Foundations of Conceptual Modeling' and ?Sustainable Solid Waste Management using Life Cycle Modeling for Environmental Impact Assessment', as well as additional material covering the discussion and findings of the panel session. Providing an overview of current research in the field, the book will be of interest to all those working with information systems, information modeling and knowledge bases.

This book constitutes the refereed proceedings of the 9th International Conference on Digital Forensics and Cyber Crime, ICDF2C 2017, held in Prague, Czech Republic, in October 2017. The 18 full papers were selected from 50 submissions and are grouped in topical sections on malware and botnet, deanonymization, digital forensics tools, cybercrime investigation and digital forensics triage, digital forensics tools testing and validation, hacking

Annotation International cooperation and international relations with regards to cyberspace Technical challenges and requirements Conflict in cyberspace Regulations and standards virtualisation.

Wireless communication and sensor networks would form the backbone to create pervasive and ubiquitous environments that would have profound influence on the society and thus are important to the society. The wireless communication technologies and wireless sensor networks would encompass a wide range of domains such as HW devices such as motes, sensors and associated instrumentation, actuators, transmitters,

receivers, antennas, etc., sensor network aspects such as topologies, routing algorithms, integration of heterogeneous network elements and topologies, designing RF devices and systems for energy efficiency and reliability etc. These sensor networks would provide opportunity to continuously and in a distributed manner monitor the environment and generate the necessary warnings and actions. However most of the developments have been demonstrated only in controlled and laboratory environments. So we are yet to see those powerful, ubiquitous applications for the benefit of the society. The conference and consequentially the proceedings would provide opportunity to the researchers to interact with other researchers and share their researches covering all the above areas. The proceedings of the conference thus covers the research work of different authors in the area of wireless sensor networks, wireless communications, devices, tools and techniques for WSN, and applications of wireless sensor networks. This book is beneficial for those researchers who are working in the area of wireless sensor networks, wireless communication, and developing applications of Wireless sensor networks. This book gathers papers presented at the 9th International Conference on Computer Engineering and Networks (CENet2019), held in Changsha, China, on October 18–20, 2019. It examines innovations in the fields of computer engineering and networking and explores important, state-of-the-art developments in areas such as Information Security, Information Hiding and Cryptography, Cyber Security, and Intelligent

Computing and Applications. The book also covers emerging topics in computer engineering and networking, along with their applications, discusses how to improve productivity by using the latest advanced technologies, and examines innovation in the fields of computer engineering and networking, particularly in intelligent computing and security.

CyberSA 2015 is an international referred conference dedicated to the advancement of the principles, methods and applications of situational awareness on Cyber Systems, Business Information Systems (BIS), Computer Network Defence (CND), Computer Physical Systems (CPS) and Internet of Things (IoTs)

This book features selected research papers presented at the First International Conference on Computing, Communications, and Cyber-Security (IC4S 2019), organized by Northwest Group of Institutions, Punjab, India, Southern Federal University, Russia, and IAC Educational Trust, India along with KEC, Ghaziabad and ITS, College Ghaziabad as an academic partner and held on 12–13 October 2019. It includes innovative work from researchers, leading innovators and professionals in the area of communication and network technologies, advanced computing technologies, data analytics and intelligent learning, the latest electrical and electronics trends, and security and privacy issues.

These proceedings represent the work of contributors to the 16th International Conference on Cyber Warfare and Security (ICCWS 2021), hosted by joint collaboration of Tennessee Tech Cybersecurity Education, Research and Outreach Center (CEROC), Computer Science

department and the Oak Ridge National Laboratory, Tennessee on 25-26 February 2021. The Conference Co-Chairs are Dr. Juan Lopez Jr, Oak Ridge National Laboratory, Tennessee, and Dr. Ambareen Siraj, Tennessee Tech's Cybersecurity Education, Research and Outreach Center (CEROC), and the Program Chair is Dr. Kalyan Perumalla, from Oak Ridge National Laboratory, Tennessee.

The scope of this conference includes the latest research on computer science, computer networks, information systems and general topic information technology

ACM IEEE ICCPS is the premier single track conference for reporting advances in all CPS aspects, including theory, tools, applications, systems, test beds and field deployments

The 11thInternational Conference on Cyber Warfare and Security (ICCWS 2016) is being held at Boston University, Boston, USA on the 17-18th March 2016. The Conference Chair is Dr Tanya Zlateva and the Programme Chair is Professor Virginia Greiman, both from Boston University. ICCWS is a recognised Cyber Security event on the International research conferences calendar and provides a valuable platform for individuals to present their research findings, display their work in progress and discuss conceptual and empirical advances in the area of Cyber Warfare and Cyber Security. It provides an important opportunity for researchers and managers to come together with peers to share their experiences of using the varied and expanding range of Cyberwar and Cyber Security research available to them. The keynote speakers for the

conference are Daryl Haegley from the Department of Defense (DoD), who will address the topic Control Systems Networks...What's in Your Building? and Neal Ziring from the National Security Agency who will be providing some insight to the issue of Is Security Achievable? A Practical Perspective. ICCWS received 125 abstract submissions this year. After the double blind, peer review process there are 43 Academic Research Papers 8 PhD papers Research papers, 7 Masters and 1 work-in-progress papers published in these Conference Proceedings. These papers represent work from around the world, including: Australia, Canada, China, Czech Republic, District of Columbia, Finland, France, Israel, Japan, Lebanon, Netherlands, Pakistan, Russian Federation, Saudi Arabia, South Africa, Turkey, United Arab Emirates, UK, USA. These proceedings represent the work of researchers participating in the 13th International Conference on Cyber Warfare and Security (ICCWS 2018) which is being hosted this year by the National Defense University in Washington DC, USA on 8-9 March 2018. This book presents refereed proceedings of the Second International Conference on Advances in Cyber Security, ACeS 2020, held in Penang, Malaysia, in September 2020. Due to the COVID-19 pandemic the conference was held online. The 46 full papers and 1 short paper were carefully reviewed and selected from 132 submissions. The papers are organized in topical sections on internet of things, industry 4.0 and blockchain, and cryptology; digital forensics and surveillance, botnet and malware, and intrusion

detection/prevention; ambient cloud and edge computing, wireless and cellular communication; governance, social media, mobile and web, data privacy, data policy and fake news. .

Cyber weapons and the possibility of cyber conflict—including interference in foreign political campaigns, industrial sabotage, attacks on infrastructure, and combined military campaigns—require policymakers, scholars, and citizens to rethink twenty-first-century warfare. Yet because cyber capabilities are so new and continually developing, there is little agreement about how they will be deployed, how effective they can be, and how they can be managed. Written by leading scholars, the fourteen case studies in this volume will help policymakers, scholars, and students make sense of contemporary cyber conflict through historical analogies to past military-technological problems. The chapters are divided into three groups. The first—What Are Cyber Weapons Like?—examines the characteristics of cyber capabilities and how their use for intelligence gathering, signaling, and precision striking compares with earlier technologies for such missions. The second section—What Might Cyber Wars Be Like?—explores how lessons from several wars since the early nineteenth century, including the World Wars, could apply—or not—to cyber conflict in the twenty-first century. The final section—What Is Preventing and/or Managing Cyber Conflict Like?—offers lessons from past cases of managing threatening actors and technologies.

International cooperation and international relations with regards to cyberspace Technical challenges and

requirements Conflict in cyberspace Regulations and standards virtualisation

There is little doubt that cyber-space has become the battle space for confrontations. However, to conduct cyber operations, a new armory of weapons needs to be employed. No matter how many, or how sophisticated an aggressor's kinetic weapons are, they are useless in cyber-space. This book looks at the milieu of the cyber weapons industry, as well as the belligerents who use cyber weapons. It discusses what distinguishes these hardware devices and software programs from computer science in general. It does this by focusing on specific aspects of the topic—contextual issues of why cyber-space is the new battleground, defensive cyber weapons, offensive cyber weapons, dual-use weapons, and the implications these weapons systems have for practice. Contrary to popular opinion, the use of cyber weapons is not limited to nation states; though this is where the bulk of news reporting focuses. The reality is that there isn't a sector of the political-economy that is immune to cyber skirmishes. So, this book looks at cyber weapons not only by national security agencies and the military, but also by law enforcement, and the business sector—the latter includes administrations termed non-government organisations (NGOs). This book offers study material suitable for a wide-ranging audience—students, professionals, researchers, policy officers, and ICT specialists.

This book presents the proceedings of the International Conference on Cyber-Physical Systems and Control (CPS&C'2019), held in Peter the Great St. Petersburg

Polytechnic University, which is celebrating its 120th anniversary in 2019. The CPS&C'2019 was dedicated to the 35th anniversary of the partnership between Peter the Great St. Petersburg Polytechnic University and Leibniz University of Hannover. Cyber-physical systems (CPSs) are a new generation of control systems and techniques that help promote prospective interdisciplinary research. A wide range of theories and methodologies are currently being investigated and developed in this area to tackle various complex and challenging problems. Accordingly, CPSs represent a scientific and engineering discipline that is set to make an impact on future systems of industrial and social scale that are characterized by the deep integration of real-time processing, sensing, and actuation into logical and physical heterogeneous domains. The CPS&C'2019 brought together researchers and practitioners from all over the world and to discuss cross-cutting fundamental scientific and engineering principles that underline the integration of cyber and physical elements across all application fields. The participants represented research institutions and universities from Austria, Belgium, Bulgaria, China, Finland, Germany, the Netherlands, Russia, Syria, Ukraine, the USA, and Vietnam. These proceedings include 75 papers arranged into five sections, namely keynote papers, fundamentals, applications, technologies, and education and social aspects.

This book constitutes the proceedings of the Second International Conference on Science of Cyber Security, SciSec 2019, held in Nanjing, China, in August 2019.

The 20 full papers and 8 short papers presented in this volume were carefully reviewed and selected from 62 submissions. These papers cover the following subjects: Artificial Intelligence for Cybersecurity, Machine Learning for Cybersecurity, and Mechanisms for Solving Actual Cybersecurity Problems (e.g., Blockchain, Attack and Defense; Encryptions with Cybersecurity Applications).

This book reports on the latest research and developments in the field of cybersecurity, giving a special emphasis on personal security and new methods for reducing human error and increasing cyber awareness, and innovative solutions for increasing the security of advanced Information Technology (IT) infrastructures. It covers a wealth of topics, including methods for human training, novel Cyber-Physical and Process-Control Systems, social, economic and behavioral aspects of the cyberspace, issues concerning the cyber security index, security metrics for enterprises, risk evaluation, and many others. Based on the AHFE 2016 International Conference on Human Factors in Cybersecurity, held on July 27-31, 2016, in Walt Disney World®, Florida, USA, this book not only presents innovative cybersecurity technologies, but also discusses emerging threats, current gaps in the available systems and future challenges that may be coped with through the help of human factors research.

Conferences Proceedings of 20th European

Conference on Cyber Warfare and Security
Cyber norms and other ways to regulate responsible state behavior in cyberspace is a fast-moving political and diplomatic field. The academic study of these processes is varied and interdisciplinary, but much of the literature has been organized according to discipline. Seeking to cross disciplinary boundaries, this timely book brings together researchers in fields ranging from international law, international relations, and political science to business studies and philosophy to explore the theme of responsible state behavior in cyberspace. . Divided into three parts, Governing Cyberspace first looks at current debates in and about international law and diplomacy in cyberspace. How does international law regulate state behaviour and what are its limits? How do cyber superpowers like China and Russia shape their foreign policy in relation to cyberspace? The second focuses on power and governance. What is the role for international organisations like NATO or for substate actors like intelligence agencies? How do they adapt to the realities of cyberspace and digital conflict? How does the classic balance of power play out in cyberspace and how do different states position themselves? The third part takes a critical look at multistakeholder and corporate diplomacy. How do global tech companies shape their role as norm entrepreneurs in cyberspace, and how do their cyber diplomatic

efforts relate to their corporate identity?

This book constitutes the refereed proceedings of the 9th International Conference on Model and Data Engineering, MEDI 2019, held in Toulouse, France, in October 2019. The 11 full papers and 7 short papers presented in this book were carefully reviewed and selected from 41 submissions. The papers cover broad research areas on both theoretical, systems and practical aspects. Some papers include mining complex databases, concurrent systems, machine learning, swarm optimization, query processing, semantic web, graph databases, formal methods, model-driven engineering, blockchain, cyber physical systems, IoT applications, and smart systems.

With the increased use of technology in modern society, high volumes of multimedia information exists. It is important for businesses, organizations, and individuals to understand how to optimize this data and new methods are emerging for more efficient information management and retrieval. Information Retrieval and Management: Concepts, Methodologies, Tools, and Applications is an innovative reference source for the latest academic material in the field of information and communication technologies and explores how complex information systems interact with and affect one another. Highlighting a range of topics such as knowledge discovery, semantic web, and information

resources management, this multi-volume book is ideally designed for researchers, developers, managers, strategic planners, and advanced-level students.

International health security (IHS) is a broad and highly heterogeneous area. Within this general context, IHS encompasses subdomains that potentially influence (and more specifically endanger) the well-being and wellness of humans. The general umbrella of IHS includes, but is not limited to, natural disasters, emerging infectious diseases (EID) and pandemics, rapid urbanization, social determinants of health, population growth, systemic racism and discrimination, environmental matters, civilian violence and warfare, various forms of terrorism, misuse of antibiotics, and the misuse of social media. The need for this expanded definition of health security stems from the realization that topics such as EID; food, water, and pharmaceutical supply chain safety; medical and health information cybersecurity; and bioterrorism, although important within the overall realm of health security, are not only able to actively modulate the wellness and health of human populations, but also tend to do so in a synergistic fashion. This inaugural tome of a multi-volume collection, Contemporary Developments and Perspectives in International Health Security, introduces many of the topics directly relevant to modern IHS theory and practice.

This first volume provides a solid foundation for future installments of this important and relevant book series.

These Proceedings are the work of researchers contributing to the 10th International Conference on Cyber Warfare and Security ICCWS 2015, co hosted this year by the University of Venda and The Council for Scientific and Industrial Research. The conference is being held at the Kruger National Park, South Africa on the 24 25 March 2015. The Conference Chair is Dr Jannie Zaaiman from the University of Venda, South Africa, and the Programme Chair is Dr Louise Leenen from the Council for Scientific and Industrial Research, South Africa.

This book constitutes selected and revised papers from the First International Conference on Cybersecurity in Emerging Digital Era, ICCEDE 2020, held in Greater Noida, India, in October 2020. Due to the COVID-19 pandemic the conference was held online. The 9 full papers and 2 short papers presented in this volume were thoroughly reviewed and selected from 193 submissions. The papers are organized in topical sections on ?cyber security issues and challenges in emerging digital era; security resilience in contemporary applications.

The proceeding is a collection of research papers presented, at the 9th International Conference on Robotics, Vision, Signal Processing & Power Applications (ROVISP 2016), by researchers, scientists, engineers, academicians as well as industrial professionals from all around the globe to present their research results and development activities for oral or

poster presentations. The topics of interest are as follows but are not limited to: • Robotics, Control, Mechatronics and Automation • Vision, Image, and Signal Processing • Artificial Intelligence and Computer Applications • Electronic Design and Applications • Telecommunication Systems and Applications • Power System and Industrial Applications • Engineering Education

These proceedings represent the work of researchers participating in the 15th European Conference on Cyber Warfare and Security (ECCWS 2016) which is being hosted this year by the Universitat der Bundeswehr, Munich, Germany on the 7-8 July 2016. ECCWS is a recognised event on the International research conferences calendar and provides a valuable plat-form for individuals to present their research findings, display their work in progress and discuss conceptual and empirical advances in the area of Cyberwar and Cyber Security. It provides an important opportunity for researchers and managers to come together with peers to share their experiences of using the varied and ex-panding range of Cyberwar and Cyber Security research available to them. With an initial submission of 110 abstracts, after the double blind, peer review process there are 37 Academic research papers and 11 PhD research papers, 1 Master's research paper, 2 Work In Progress papers and 2 non-academic papers published in these Conference Proceedings. These papers come from many different coun-tries including Austria, Belgium, Canada, Czech Republic, Finland, France, Germany, Greece, Hungary, Ireland, Kenya, Luxembourg, Netherlands, Norway, Portugal, Romania,

Russia, Slovenia, South Africa, Sweden, Turkey, UK and USA. This is not only highlighting the international character of the conference, but is also promising very interesting discussions based on the broad treasure trove of experience of our community and partici-pants." 2021 9th International Conference on Cyber and IT Service Management (CITSM)