Iccws2016

This OECD Recommendation and its Companion Document provide guidance for all stakeholders on the economic and social prosperity dimensions of digital security risk.

Wherever grapevines are cultivated this book will be welcome because it fills longstanding need for a clear, concise treatment of modern viticulture. The chapters on vine structure, vine physiology, the grape flower and berry set, development and composition of grapes, and means of improving grape quality add to our knowledge of the vine and its functions. The text is designed to enable those concerned with either vine or fruit problems to arrive at considered diagnoses.

????? ??????????? ????? ????? ?????? ??? ??????????? ?????? ? ????? ???????? ???????????? ????????? ???????????. ????????? ????????? ???? ???????? ?? ????????????, ????????????? ?? ???????????? ??????? ???????????? ? ??????, ???, ???????, ??????, ?????????, ???????, ??????? ???????? ??? ???? ???????????? ?? ??????? ? ????????? ??????. ? ????????? ???????????? ??? ????? ???????????? ?????? 2010-? ?????, ????????????? ?????????????? ???????, ??? ? ????????? ???????????? ?????? 2020 ????, ???????????? ?????? ???????????? ???????? ???????????? ??????? ?????????????? ?????? ?????????? ?????? ?? ???????????? ? ???????????? ???????.??? ??????????, ?????????????, ???????????? ? ????? ???????????? ????????????????? ? ?????????????????? PR.

With the increased dependence on digital and internet technologies, cyber security has come to be regarded as a national security issue, and the number of countries with a published cyber security strategy continues to rise. But these national cyber security strategies often run the risk of failing to address all the cyber security requirements of the many institutions within a given country, and the complex nature of the stakeholders involved and the networks formed by them means that the problem requires an interdisciplinary approach. This book presents papers from the NATO Advanced Research Workshop (ARW) entitled "A Framework for a Military Cyber Defense Strategy", held in Norfolk, Virginia, USA, in April 2016. The workshop focused on key priority areas for cyber defense along with NATO's cyber defense policy implementation and brought together experts with an eclectic mix of backgrounds and specialties from a group of NATO member states and partner countries. The participants considered not only the technical implications of cyber security efforts, but also the legal, strategic, educational and organizational aspects, and the book reflects this wide view of the field and its intricacies, highlighting the complexity of cyber security and the many challenges it presents. This overview of cyber security offers state-of-the-art approaches from a multidisciplinary standpoint, and will be of interest to all those working in the field.

A landmark in Australian wine publishing. Superbly crafted and uncompromisingly presented, this limited-edition collectors' item of original photographs and words lives the story of one of the world's most celebrated wines.

This book constitutes the refereed proceedings of the 9th International Symposium on Engineering Secure Software and Systems, ESSoS 2017, held in Bonn, Germany in July 2017. The 12 full papers presented together with 3 short papers were carefully reviewed and selected from 32 submissions. The goal of this symposium is to bring together researchers and practitioners to advance the states of the art and practice in secure software engineering.

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.

Red Wine Technology is a solutions-based approach on the challenges associated with red wine production. It focuses on the technology and biotechnology of red wines, and is ideal for anyone who needs a quick reference on novel ways to increase and improve overall red wine production and innovation. The book provides emerging trends in modern enology, including molecular tools for wine quality and analysis. It includes sections on new ways of maceration extraction, alternative microorganisms for alcoholic fermentation, and malolactic fermentation. Recent studies and technological advancements to improve grape maturity and production are also presented, along with tactics to control PH level. This book is an essential resource for wine producers, researchers, practitioners, technologists and students. Winner of the OIV Award 2019 (Category: Enology), International Organization of Vine and Wine Provides innovative technologies to

improve maceration and color/tannin extraction, which influences color stability due to the formation of pyranoanthocyanins and polymeric pigments Contains deep evaluations of barrel ageing as well as new alternatives such as microoxigenation, chips, and biological ageing on lees Explores emerging biotechnologies for red wine fermentation including the use of non-Saccharomyces yeasts and yeast-bacteria coinoculations, which have effects in wine aroma and sensory quality, and also control spoilage microorganisms

The United States is increasingly dependent on information and information technology for both civilian and military purposes, as are many other nations. Although there is a substantial literature on the potential impact of a cyberattack on the societal infrastructure of the United States, little has been written about the use of cyberattack as an instrument of U.S. policy. Cyberattacks--actions intended to damage adversary computer systems or networks--can be used for a variety of military purposes. But they also have application to certain missions of the intelligence community, such as covert action. They may be useful for certain domestic law enforcement purposes, and some analysts believe that they might be useful for certain private sector entities who are themselves under cyberattack. This report considers all of these applications from an integrated perspective that ties together technology, policy, legal, and ethical issues. Focusing on the use of cyberattack as an instrument of U.S. national policy, Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities explores important characteristics of cyberattack. It describes the current international and domestic legal structure as it might apply to cyberattack, and considers analogies to other domains of conflict to develop relevant insights. Of special interest to the military, intelligence, law enforcement, and homeland security communities, this report is also an essential point of departure for nongovernmental researchers interested in this rarely discussed topic.

This volume covers a wide spectrum of issues relating to economic and political development enabled by information and communication technology (ICT). Showcasing contributions from researchers, industry leaders and policymakers, this Handbook provides a comprehensive overview of the challenges and opportunities created by technological innovations that are profoundly affecting the dynamics of economic growth, promotion of democratic principles, and the protection of individual, national, and regional rights. Of particular interest is the influence of ICT on the generation and dissemination of knowledge, which, in turn, empowers citizens and accelerates change across all strata of society. Each essay features literature reviews and key references; definition of critical terms and concepts, case examples; implications for practice, policy and theory; and discussion of future directions. Representing such fields as management, political science, economics, law, psychology and education, the authors cover such timely topics as health care, energy and environmental policy, banking and finance, disaster recovery, investment in research and development, homeland security and diplomacy in the context of ICT and its economic, political and social impact.

In this monograph, the authors state that Russia planned the war against Georgia in August 2008 aiming for the annexation of Abkhazia, weakening the Saakashvili regime, and prevention of NATO enlargement. According to them, while Russia won the campaign, it also exposed its own military as badly needing reform. The war also demonstrated weaknesses of the NATO and the European Union security systems.

Uncover hidden patterns of data and respond withcountermeasures Security professionals need all the tools at their disposal toincrease their visibility in order to prevent security breaches andattacks. This careful guide explores two of the most powerful data analysis and visualization. You'll soon understand how toharness and wield data, from collection and storage to managementand analysis as well as visualization and presentation. Using ahands-on approach with real-world examples, this book shows you howto gather feedback, measure the effectiveness of your securitymethods, and make better decisions. Everything in this book will have practical application forinformation security professionals. Helps IT and security professionals understand and use data, sothey can thwart attacks and understand and visualizevulnerabilities in their networks Includes more than a dozen real-world examples and hands-onexercises that demonstrate how to analyze security data andintelligence and translate that information into visualizationsthat make plain how to prevent attacks Covers topics such as how to acquire and prepare security data,use simple statistical methods to detect malware, predict roguebehavior, correlate security events, and more Written by a team of well-known experts in the field ofsecurity and data analysis Lock down your networks, prevent hacks, and thwart malware byimproving visibility into the environment, all through the power ofdata and Security Using Data Analysis, Visualization, andDashboards.

This book introduces fundamental concepts of cyber resilience, drawing expertise from academia, industry, and government. Resilience is defined as the ability to recover from or easily adjust to shocks and stresses. Unlike the concept of security - which is often and incorrectly conflated with resilience -- resilience refers to the system's ability to recover or regenerate its performance after an unexpected impact produces a degradation in its performance. A clear understanding of

distinction between security, risk and resilience is important for developing appropriate management of cyber threats. The book presents insightful discussion of the most current technical issues in cyber resilience, along with relevant methods and procedures. Practical aspects of current cyber resilience practices and techniques are described as they are now, and as they are likely to remain in the near term. The bulk of the material is presented in the book in a way that is easily accessible to non-specialists. Logical, consistent, and continuous discourse covering all key topics relevant to the field will be of use as teaching material as well as source of emerging scholarship in the field. A typical chapter provides introductory, tutorial-like material, detailed examples, in-depth elaboration of a selected technical approach, and a concise summary of key ideas.

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.

As internet technologies continue to advance, new types and methods of data and security breaches threaten national security. These potential breaches allow for information theft and can provide footholds for terrorist and criminal organizations. Developments in Information Security and Cybernetic Wars is an essential research publication that covers cyberwarfare and terrorism globally through a wide range of security-related areas. Featuring topics such as crisis management, information security, and governance, this book is geared toward practitioners, academicians, government officials, military professionals, and industry professionals.

This book constitutes the refereed proceedings of the 5th Conference on AElectronic Governance and Open Society: Challenges in Eurasia, EGOSE 2018, held in St. Petersburg, Russia, in November 2018. The 36 revised full papers were carefully reviewed and selected from 98 submissions. The papers are organized in topical sections on smart city infrastructure, policy; digital privacy, rights,security;data science, machine learning, algorithms, computational linguistics; digital public administration, economy, policy; digital services, values, inclusion; digital democracy, participation, security, communities, social media, activism; social media discourse analysis; digital data, policy modeling; digital government, administration, communication.

This book brings a high level of fluidity to analytics and addresses recent trends, innovative ideas, challenges and cognitive computing solutions in big data and the Internet of Things (IoT). It explores domain knowledge, data science reasoning and cognitive methods in the context of the IoT, extending current data science approaches by incorporating insights from experts as well as a notion of artificial intelligence, and performing inferences on the knowledge The book provides a comprehensive overview of the constituent paradigms underlying cognitive computing methods, which illustrate the increased focus on big data in IoT problems as they evolve. It includes novel, in-depth fundamental research contributions from a methodological/application in data science accomplishing sustainable solution for the future perspective. Mainly focusing on the design of the best cognitive embedded data science technologies to process and analyze the large amount of data collected through the IoT, and aid better decision making, the book discusses adapting decision-making approaches under cognitive computing paradigms to demonstrate how the proposed procedures as well as big data and IoT problems can be handled in practice. This book is a valuable resource for scientists, professionals, researchers, and academicians dealing with the new challenges and advances in the specific areas of cognitive computing and data science approaches.

This book constitutes the refereed proceedings of the 12th IFIP TC 9 International Conference on Human Choice and Computers, HCC12 2016, held in Salford, UK, in September 2016. The 26 revised full papers presented were carefully reviewed and selected from 34 submissions. The papers deal with the constantly evolving intimate relationship between humans and technology. They focus on three main themes: ethics, communications, and futures.

Engineering Secure Software and Systems
A Multidisciplinary Perspective
Analysis, Visualization and Dashboards
Cognitive Computing for Big Data Systems Over IoT
ICMLG 2017 5th International Conference on Management Leadership and Governance
The Practice of Enterprise Modeling
ICEL2016-Proceedings of the 11th International Conference on e- Learning
Lessons and Implications
ICIE 2016 Proceedings of the 4th International Conference on Innovation and Entrepreneurship
9th IFIP WG 8.1. Working Conference, PoEM 2016, Sk ö vde, Sweden, November 8-10, 2016, Proceedings
Red Wine Technology
OECD Recommendation and Companion Document
5th International Conference, EGOSE 2018, St. Petersburg, Russia, November 14-16, 2018, Revised Selected Papers

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.

A precise and exhaustive description of different types of malware from three different points of view, namely the theoretical fundamentals of computer virology, algorithmic and practical aspects of viruses and their potential applications to various areas.

"A vintner's blend of science, history, travel, and tantalizing drink recommendations." --Amy Stewart, author of The Drunken Botanist In search of a mysterious wine he once tasted in a hotel room minibar, journalist Kevin Begos travels along the original wine routes—from the Caucasus Mountains, where wine grapes were first domesticated eight thousand years ago, crossing the

Mediterranean to Europe, and then America—and unearths a whole world of forgotten grapes, each with distinctive tastes and aromas. We meet the scientists who are decoding the DNA of wine grapes, and the historians who are searching for ancient vineyards and the flavors cultivated there. Begos discovers wines that go far beyond the bottles of Chardonnay and Merlot found in most stores and restaurants, and he offers suggestions for wines that are at once ancient and new.

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."

Offering compelling practical and legal reasons why de-identification should be one of the main approaches to protecting patients' privacy, the Guide to the De-Identification of Personal Health Information outlines a proven, risk-based methodology for the de-identification of sensitive health information. It situates and contextualizes this risk-based methodology and provides a general overview of its steps. The book supplies a detailed case for why de-identification is important as well as best practices to help you pin point when it is necessary to apply de-identification in the disclosure of personal health information. It also: Outlines practical methods for de-identification Describes how to measure re-identification risk Explains how to reduce the risk of re-identification Includes proofs and supporting reference material Focuses only on transformations proven to work on health information—rather than covering all possible approaches, whether they work in practice or not Rated the top systems and software engineering scholar worldwide by The Journal of Systems and Software, Dr. El Emam is one of only a handful of individuals worldwide qualified to de-identify personal health information for secondary use under the HIPAA Privacy Rule Statistical Standard. In this book Dr. El Emam explains how we can make health data more accessible—while protecting patients' privacy and complying with current regulations.

These proceedings represent the work of contributors to the 19th European Conference on Cyber Warfare and Security (ECCWS 2020), supported by University of Chester, UK on 25-26 June 2020. The Conference Co-chairs are Dr Thaddeus Eze and Dr Lee Speakman, both from University of Chester and the Programme Chair is Dr Cyril Onwubiko from IEEE and Director, Cyber Security Intelligence at Research Series Limited. ECCWS is a well-established event on the academic research calendar and now in its 19th year the key aim remains the opportunity for participants to share ideas and meet. The conference was due to be held at University of Chester, UK, but due to the global Covid-19 pandemic it was moved online to be held as a virtual event. The scope of papers will ensure an interesting conference. The subjects covered illustrate the wide range of topics that fall into this important and ever-growing area of research.

ECCWS 2020 20th European Conference on Cyber Warfare and Security
ECCWS2016-Proceedings fo the 15th European Conference on Cyber Warfare and Security "
Computer Viruses: from theory to applications
Cyber Resilience of Systems and Networks
Guide to the De-Identification of Personal Health Information
ICCWS 2019
Digital Security Risk Management for Economic and Social Prosperity OECD Recommendation and Companion Document
ICCWS 2019 14th International Conference on Cyber Warfare and Security
The Ethics of Cybersecurity
ICCWS 2018 13th International Conference on Cyber Warfare and Security
11th International Conference on Cyber Warfare and Security
A Year in the Life of Grange
European Conference on Games Based Learning (ECGBL 2007)

This volume constitutes the proceedings of the 9th IFIP WG 8.1 Conference on the Practice of Enterprise Modeling held in November 2016 in Skövde, Sweden. The PoEM conference series started in 2008 and aims to provide a forum sharing knowledge and experiences between the academic community and practitioners from industry and the public sector. The 18 full papers and 9 short papers accepted were carefully reviewed and selected from 54 submissions and cover topics related to information systems development, enterprise modeling, requirements engineering, and process management. In

addition, the keynote by Robert Winter on “Establishing 'Architectural Thinking' in Organizations” is also included in this volume.
This two volume set (CCIS 858 and CCIS 859) constitutes the refereed proceedings of the Third International Conference on Digital Transformation and Global Society, DTGS 2018, held in St. Petersburg, Russia, in May/June 2018. The 75 revised full papers and the one short paper presented in the two volumes were carefully reviewed and selected from 222 submissions. The papers are organized in topical sections on e-polity: smart governance and e-participation, politics and activism in the cyberspace, law and regulation; e-city: smart cities and urban planning; e-economy: IT and new markets; e-society: social informatics, digital divides; e-communication: discussions and perceptions on the social media; e-humanities: arts and culture; International Workshop on Internet Psychology; International Workshop on Computational Linguistics.
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.
Space-critical infrastructures represent an interdependent system of systems consisting of workforce, environment, facilities, and multidirectional interactions. These are essential for the maintenance of vital societal functions such as health, safety, security, mobility, and the economic and social well-being of people, and their destruction or disruption would have a significant impact on society as a whole. In all, 79 nations and government consortia currently operate satellites, with 11 countries operating 22 launch sites. Despite creating new challenges, this multi-actor environment offers opportunities for international cooperation, but making the most of these opportunities requires a holistic approach to space-critical infrastructure, away from strictly defined space technologies and towards understanding the resilience of complex systems and how they are intertwined in reality. This book presents papers from the NATO Advanced Research Workshop (ARW), entitled Critical Space Infrastructure: From Vulnerabilities and Threats to Resilience, held in Norfolk, Virginia, USA from 21-22 May 2019. The ARW brought together representatives from academia, industry, and international organizations in an effort to deepen scientific and technological understanding of space-critical infrastructures and explore the implications for national and international space security and resilience. It examined space as a critical infrastructure from a multidisciplinary perspective in accordance with NATO’s Strategic Concept. The 29 chapters in the book are divided into six sections covering space infrastructure: governance; cybersecurity; risk, resiliency and complexity; emerging technologies such as block chain, artificial intelligence and quantum computing; application domains; and national approaches and applications.