Virginia Cybersecurity Education Conference

ICCWS 2023 18th International Conference on Cyber Warfare and Security
No Ordinary Moment
Learning Spaces
Information Security Education for Cyber Resilience
Information Security Education for a Global Digital Society
Introduction to the Cyber Ranges
HCI for Cybersecurity, Privacy and Trust
Creative Approaches to Technology-Enhanced Learning for the Workplace and Higher Education
16th International Conference on Cyber Warfare and Security
Countering Cyber Sabotage
Advances in Human Factors in Cybersecurity
ICCSM2015-3rd International Conference on Cloud Security and Management
Cybersecurity Issues in Emerging Technologies
ECCWS 2023 22nd European Conference on Cyber Warfare and Security
ECCWS2015-Proceedings of the 14th European Conference on Cyber Warfare and Security 2015
Iccws 2015 - The Proceedings of the 10th International Conference on Cyber Warfare and Security
Confidential Information Sources
11th International Conference on Cyber Warfare and Security
International Joint Conference 15th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2022) 13th International Conference on EUropean Transnational Education (ICEUTE 2022)
The Shadow War
ICIW2012-Proceedings of the 7th International Conference on Information Warfare and Security
Hiding Behind the Keyboard
Official (ISC)2® Guide to the CISSP®-ISSEP® CBK®
ICCWS 2020 15th International Conference on Cyber Warfare and Security
Congressional Record
New Threats and Countermeasures in Digital Crime and Cyber Terrorism
ICCWS 2019 14th International Conference on Cyber Warfare and Security
Cyber Security Engineering
Professionalizing the Nation's Cybersecurity Workforce?
Cybersecurity Law
Foundational Practices of Online Writing Instruction
Advances in Cybersecurity Management
The Twenty-Six Words That Created the Internet
Computer Security
The Cybersecurity Workforce of Tomorrow
Information Security Education – Towards a Cybersecure Society
Network Security Attacks and Countermeasures

CRISTINA KENNY

ICCWS 2023 18th International Conference on Cyber Warfare and Security Academic Conferences and publishing limited
In 2022, Virginia Tech will celebrate its 150th anniversary. What started as a fledgling school to promote agricultural, mechanical, and military education grew into a comprehensive research university with a global land grant mission. As part of the upcoming celebrations, "Virginia Tech: 150 Years in 150 Images" will provide a unique look at the history of Virginia Polytechnic Institute & State University from its late nineteenth century origins up to the present day. The book includes 150 unique or rare photographs and other items from the Special Collections and University Archives at Virginia Tech. These iconic and less familiar historic photographs celebrate the milestones and lesser-known achievements of the past 150 years and point to the bright future of Virginia Tech.
No Ordinary Moment Parlor Press LLC
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.
Learning Spaces Springer
Professionalizing the Nation's Cybersecurity Workforce? Criteria for Decision-Making considers approaches to increasing the professionalization of the nation's cybersecurity workforce. This report examines workforce requirements for cybersecurity and the segments and job functions in which professionalization is most needed; the role of assessment tools, certification, licensing, and other means for assessing and enhancing professionalization; and emerging approaches, such as performance-based measures. It also examines requirements for the federal (military and civilian) workforce, the private sector, and state and local government. The report focuses on three essential elements: (1) understanding the context for cybersecurity workforce development, (2) considering the relative advantages, disadvantages, and approaches to professionalizing the nation's cybersecurity workforce, and (3) setting forth criteria that can be used to identify which, if any, specialty areas may require professionalization and set forth criteria for evaluating different approaches and tools for professionalization. Professionalizing the Nation's Cybersecurity Workforce? Criteria for Decision-Making characterizes the current landscape for cybersecurity workforce development and sets forth criteria that the federal agencies participating in the National Initiative for Cybersecurity Education□as well as organizations that employ cybersecurity workers□could use to identify which specialty areas may require professionalization and to evaluate different approaches and tools for professionalization.
Information Security Education for Cyber Resilience Academic Conferences and publishing limited
Introduction to the Cyber Ranges provides a comprehensive, integrative, easy-to-comprehend overview of different aspects involved in the cybersecurity arena. It expands on various concepts like cyber situational awareness, simulation and emulation environments, and cybersecurity exercises. It also focuses on detailed analysis and the comparison of various existing cyber ranges in military, academic, and commercial sectors. It highlights every crucial aspect necessary for developing a deeper insight about the working of the cyber ranges, their architectural design, and their need in the market. It conveys how cyber ranges are complex and effective tools in dealing with advanced cyber threats and attacks. Enhancing the network defenses, resilience, and efficiency of different components of critical infrastructures is the principal objective of cyber ranges. Cyber ranges provide simulations of possible cyberattacks and training on how to thwart such attacks. They are widely used in urban enterprise sectors because they present a sturdy and secure setting for hands-on cyber skills training, advanced cybersecurity education, security testing/training, and certification. Features: A comprehensive guide to understanding the complexities involved with cyber ranges and other cybersecurity aspects Substantial theoretical knowhow on cyber ranges, their architectural design, along with case studies of existing cyber ranges in leading urban sectors like military, academic, and commercial Elucidates the defensive technologies used by various cyber ranges in enhancing the security setups of private and government organizations Information organized in an accessible format for students (in engineering, computer science, and information management), professionals, researchers, and scientists working in the fields of IT, cybersecurity, distributed systems, and computer networks
Information Security Education for a Global Digital Society IGI Global
This book constitutes the refereed proceedings of the 11th IFIP WG 11.8 World Conference on Information Security Education, WISE 11, held at the 24th IFIP World Computer Congress, WCC 2018, in Poznan, Poland, in September 2018. The 11 revised papers presented were carefully reviewed and selected from 25 submissions. They focus on cybersecurity and are organized in the following topical sections: information security learning techniques; information security training and awareness; and information security courses and curricula.
Introduction to the Cyber Ranges Academic Conferences Limited
Based on news reports, you might think there's a major cybersecurity threat every four to five months. In reality, there's a cybersecurity attack happening every minute of every day. Today, we live our lives—and conduct our business—online. Our data is in the cloud and in our pockets on our smartphones, shuttled over public Wi-Fi and company networks. To keep it safe, we rely on passwords and encryption and private servers, IT departments and best practices. But as you read this, there is a 70 percent chance that your data is compromised . . . you just don't know it yet. Cybersecurity attacks have increased exponentially, but because they're stealthy and often invisible, many underplay, ignore, or simply don't realize the danger. By the time they discover a breach,

most individuals and businesses have been compromised for over three years. Instead of waiting until a problem surfaces, avoiding a data disaster means acting now to prevent one. In Cyber Crisis, Eric Cole gives readers a clear-eyed picture of the information war raging in cyberspace. Drawing on 30 years of experience—as a professional hacker for the CIA, as the Obama administration's cybersecurity commissioner, and as a consultant to clients around the globe from Bill Gates to Lockheed Martin and McAfee—Cole offers practical, actionable advice that even those with little technical background can implement, including steps to take on a daily, weekly, and monthly basis to protect their businesses and themselves. No matter who you are or where you work, cybersecurity should be a top priority. The information infrastructure we rely on in every sector of our lives—in healthcare and finance, for governments and private citizens—is both critical and vulnerable, and sooner or later, you or your company will be a target. This book is your guide to understanding the threat and putting together a proactive plan to minimize exposure and damage, and ensure the security of your business, your family, and your future

HCI for Cybersecurity, Privacy and Trust Syngress

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.

Creative Approaches to Technology-Enhanced Learning for the Workplace and Higher Education Academic Conferences Limited

This book constitutes the refereed proceedings of the 14th IFIP WG 11.8 World Conference on Information Security Education, WISE 14, held virtually in June 2021. The 8 papers presented together with a special chapter showcasing the history of WISE and two workshop papers were carefully reviewed and selected from 19 submissions. The papers are organized in the following topical sections: a roadmap for building resilience; innovation in curricula; teaching methods and tools; and end-user security.

16th International Conference on Cyber Warfare and Security IGI Global

Complete proceedings of the 14th European Conference on Cyber Warfare and Security Hatfield UK Published by Academic Conferences and Publishing International Limited

Countering Cyber Sabotage Elsevier

Cyber Security Engineering is the definitive modern reference and tutorial on the full range of capabilities associated with modern cyber security engineering. Pioneering software assurance experts Dr. Nancy R. Mead and Dr. Carol C. Woody bring together comprehensive best practices for building software systems that exhibit superior operational security, and for considering security throughout your full system development and acquisition lifecycles. Drawing on their pioneering work at the Software Engineering Institute (SEI) and Carnegie Mellon University, Mead and Woody introduce seven core principles of software assurance, and show how to apply them coherently and systematically. Using these principles, they help you prioritize the wide range of possible security actions available to you, and justify the required investments. Cyber Security Engineering guides you through risk analysis, planning to manage secure software development, building organizational models, identifying required and missing competencies, and defining and structuring metrics. Mead and Woody address important topics, including the use of standards, engineering security requirements for acquiring COTS software, applying DevOps, analyzing malware to anticipate future vulnerabilities, and planning ongoing improvements. This book will be valuable to wide audiences of practitioners and managers with responsibility for systems, software, or quality engineering, reliability, security, acquisition, or operations. Whatever your role, it can help you reduce operational problems, eliminate excessive patching, and deliver software that is more resilient and secure.

Advances in Human Factors in Cybersecurity Syngress

Foundational Practices in Online Writing Instruction addresses administrators' and instructors' questions for developing online writing programs and courses. Written by experts in the field, this book uniquely attends to issues of inclusive and accessible online writing instruction in technology-enhanced settings, as well as teaching with mobile technologies and multimodal compositions.

ICCSM2015-3rd International Conference on Cloud Security and Management Academic Conferences Limited

The Cybersecurity Workforce of Tomorrow discusses the current requirements of the cybersecurity worker and analyses the ways in which these roles may change in the future as attacks from hackers, criminals and enemy states become increasingly sophisticated.

Cybersecurity Issues in Emerging Technologies Cornell University Press

This book constitutes the refereed proceedings of the 10th IFIP WG 11.8 World Conference on Security Education, WISE 10, held in Rome, Italy, in May 2017. The 14 revised papers presented were carefully reviewed and selected from 31 submissions. They represent a cross section of applicable research as well as case studies in security education and are organized in the following topical sections: information security education; teaching information security; information security awareness and culture; and training information security professionals..

ECCWS 2023 22nd European Conference on Cyber Warfare and Security Emerald Group Publishing

This book concentrates on a wide range of advances related to IT cybersecurity management. The topics covered in this book include, among others, management techniques in security, IT risk

management, the impact of technologies and techniques on security management, regulatory techniques and issues, surveillance technologies, security policies, security for protocol management, location management, GOS management, resource management, channel management, and mobility management. The authors also discuss digital contents copyright protection, system security management, network security management, security management in network equipment, storage area networks (SAN) management, information security management, government security policy, web penetration testing, security operations, and vulnerabilities management. The authors introduce the concepts, techniques, methods, approaches and trends needed by cybersecurity management specialists and educators for keeping current their cybersecurity management knowledge. Further, they provide a glimpse of future directions where cybersecurity management techniques, policies, applications, and theories are headed. The book is a rich collection of carefully selected and reviewed manuscripts written by diverse cybersecurity management experts in the listed fields and edited by prominent cybersecurity management researchers and specialists.

ECCWS2015-Proceedings of the 14th European Conference on Cyber Warfare and Security 2015 Springer Nature

Are we losing a war few of us realize we’re fighting? Jim Sciutto, CNN’s Chief National Security Correspondent, reveals the invisible fronts that make up 21st century warfare, from disinformation campaigns to advanced satellite weapons. Poisoned dissidents. Election interference. Armed invasions. International treaties thrown into chaos. Secret military buildups. Hackers and viruses. Weapons deployed in space. China and Russia (and Iran and North Korea) spark news stories by carrying out bold acts of aggression and violating international laws and norms. Isn’t this just bad actors acting badly? That kind of thinking is outdated and dangerous. Emboldened by their successes, these countries are, in fact, waging a brazen, global war on the US and the West. This is a new Cold War, which will not be won by those who fail to realize they are fighting it. The enemies of the West understand that while they are unlikely to win a shooting war, they have another path to victory. And what we see as our greatest strengths—open societies, military innovation, dominance of technology on Earth and in space, longstanding leadership in global institutions—these countries are undermining or turning into weaknesses. In The Shadow War, CNN anchor and chief national security correspondent Jim Sciutto provides us with a revealing and at times disturbing guide to this new international conflict. This Shadow War is already the greatest threat to America’s national security, even though most Americans know little or nothing about it. With on-the-ground reporting from Ukraine to the South China Sea, from a sub under the Arctic to unprecedented access to America’s Space Command, Sciutto draws on his deep knowledge, high-level contacts, and personal experience as a journalist and diplomat to paint the most comprehensive and vivid picture of a nation targeted by a new and disturbing brand of warfare. Thankfully, America is adapting and fighting back. In The Shadow War, Sciutto introduces readers to the dizzying array of soldiers, sailors, submariners and their commanders, space engineers, computer scientists, civilians, and senior intelligence officials who are on the front lines of this new kind of forever war. Intensive and disturbing, this invaluable and important work opens our eyes and makes clear that the war of the future is already here.

Iccws 2015 - The Proceedings of the 10th International Conference on Cyber Warfare and Security National Academies Press

This book constitutes the proceedings of the Second International Conference on HCI for Cybersecurity, Privacy and Trust, HCI-CPT 2020, held as part of the 22nd International Conference, HCI International 2020, which took place in Copenhagen, Denmark, in July 2020. The total of 1439 papers and 238 posters included in the 37 HCII 2020 proceedings volumes was carefully reviewed and selected from 6326 submissions. HCI-CPT 2020 includes a total of 45 regular papers; they were organized in topical sections named: human factors in cybersecurity; privacy and trust; usable security approaches. As a result of the Danish Government's announcement, dated April21, 2020, to ban all large events (above 500 participants) until September 1, 2020, the HCII 2020 conference was held virtually.

Confidential Information Sources Springer Nature

"No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." Did you know that these twenty-six words are responsible for much of America's multibillion-dollar online industry? What we can and cannot write, say, and do online is based on just one law—a law that protects online services from lawsuits based on user content. Jeff Kosseff exposes the workings of Section 230 of the Communications Decency Act, which has lived mostly in the shadows since its enshrinement in 1996. Because many segments of American society now exist largely online, Kosseff argues that we need to understand and pay attention to what Section 230 really means and how it affects what we like, share, and comment upon every day. The Twenty-Six Words That Created the Internet tells the story of the institutions that flourished as a result of this powerful statute. It introduces us to those who created the law, those who advocated for it, and those involved in some of the most prominent cases decided under the law. Kosseff assesses the law that has facilitated freedom of online speech, trolling, and much more. His keen eye for the law, combined with his background as an award-winning journalist, demystifies a statute that affects all our lives –for good and for ill. While Section 230 may be imperfect and in need of refinement, Kosseff maintains that it is necessary to foster free speech and innovation. For filings from many of the cases discussed in the book and updates about Section 230, visit jeffkosseff.com

11th International Conference on Cyber Warfare and Security Academic Conferences Limited

Digital Forensics Trial Graphics: Teaching the Jury Through Effective Use of Visuals helps digital forensic practitioners explain complex technical material to laypeople (i.e., juries, judges, etc.). The book includes professional quality illustrations of technology that help anyone understand the complex concepts behind the science. Users will find invaluable information on theory and best practices along with guidance on how to design and deliver successful explanations. Helps users learn skills for the effective presentation of digital forensic evidence via graphics in a trial setting to laypeople such as juries and judges Presents the principles of visual learning and graphic design as a foundation for developing effective visuals Demonstrates the best practices of slide design to develop effective visuals for presentation of evidence Professionally developed graphics, designed specifically for digital forensics, that you can use at trial Downloadable graphics available at: http://booksite.elsevier.com/9780128034835

International Joint Conference 15th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2022) 13th International Conference on EUropean Transnational Education (ICEUTE 2022) Academic Conferences and publishing limited
ICCWS 2020 15th International Conference on Cyber Warfare and SecurityAcademic Conferences and publishing limitedThe Cybersecurity Workforce of TomorrowEmerald Group Publishing
Springer Nature
Our world is increasingly driven by sophisticated networks of advanced computing technology, and the basic operation of everyday society is becoming increasingly vulnerable to those networks' shortcomings. The implementation and upkeep of a strong network defense is a substantial challenge, beset not only by economic disincentives, but also by an inherent logistical bias that grants advantage to attackers. Network Security Attacks and Countermeasures discusses the security and optimization of computer networks for use in a variety of disciplines and fields. Touching on such matters as mobile and VPN security, IP spoofing, and intrusion detection, this edited collection emboldens the efforts of researchers, academics, and network administrators working in both the public and private sectors. This edited compilation includes chapters covering topics such as attacks and countermeasures, mobile wireless networking, intrusion detection systems, next-generation firewalls, and more.