Kaspersky Security Center 10 2f

Today, cyber security, cyber defense, information warfare andcyber warfare issues are among the most relevant topics both at thenational and international level. All the major states of the worldare facing cyber threats and trying to understand how cyberspacecould be used to increase power. Through an empirical, conceptual and theoretical approach, CyberConflict has been written by researchers and experts in the fieldsof cyber security, cyber defense and information warfare. It aimsto analyze the processes of information warfare and cyber warfarethrough historical, operational and strategic perspectives of cyberattack. It is original in its delivery because of itsmultidisciplinary approach within an international framework, withstudies dedicated to different states – Canada, Cuba, France,Greece, Italy, Japan, Singapore, Slovenia and South Africa –describing the state's application of information warfareprinciples both in terms of global development and"local" usage and examples. Contents 1. Canada's Cyber Security Policy: a Tortuous Path Towarda Cyber Security Strategy, Hugo Loiseau and Lina Lemay. 2. Cuba: Towards

an Active Cyber-defense, Daniel Ventre. 3. French Perspectives on Cyber-conflict, Daniel Ventre. 4. Digital Sparta: Information Operations and Cyber-warfare inGreece, Joseph Fitsanakis. 5. Moving Toward an Italian Cyber Defense and Security Strategy,Stefania Ducci. 6. Cyberspace in Japan's New Defense Strategy, DanielVentre. 7. Singapore's Encounter with Information Warfare: FilteringElectronic Globalization and Military Enhancements, AlanChong. 8. A Slovenian Perspective on Cyber Warfare, Gorazd Praprotnik,Iztok Podbregar, Igor Bernik and Bojan Ticar. 9. A South African Perspective on Information Warfare and CyberWarfare, Brett van Niekerk and Manoj Maharaj. 10. Conclusion, Daniel Ventre

This book constitutes the refereed proceedings of the 10th International Conference on Digital Forensics and Cyber Crime, ICDF2C 2018, held in New Orleans, LA, USA, in September 2018. The 11 reviewed full papers and 1 short paper were selected from 33 submissions and are grouped in topical sections on carving and data hiding, android, forensic readiness, hard drives and digital forensics, artefact correlation.

Advances in digital technologies have provided ample positive impacts to modern

society; however, in addition to such benefits, these innovations have inadvertently created a new venue for criminal activity to generate. Combating Violent Extremism and Radicalization in the Digital Era is an essential reference for the latest research on the utilization of online tools by terrorist organizations to communicate with and recruit potential extremists and examines effective countermeasures employed by law enforcement agencies to defend against such threats. Focusing on perspectives from the social and behavioral sciences, this book is a critical source for researchers, analysts, intelligence officers, and policy makers interested in preventive methods for online terrorist activities.

In 2011, the United States government declared a cyber attack as equal to an act of war, punishable with conventional military means. Cyber operations, cyber crime, and other forms of cyber activities directed by one state against another are now considered part of the normal relations range of combat and conflict, and the rising fear of cyber conflict has brought about a reorientation of military affairs. What is the reality of this threat? Is it actual or inflated, fear or

fact-based? Taking a bold stand against the mainstream wisdom, Valeriano and Maness argue that there is very little evidence that cyber war is, or is likely to become, a serious threat. Their claim is empirically grounded, involving a careful analysis of cyber incidents and disputes experienced by international states since 2001, and an examination of the processes leading to cyber conflict. As the authors convincingly show, cyber incidents are a little-used tactic, with low-level intensity and few to no long-term effects. As well, cyber incidents are motivated by the same dynamics that prompt regional conflicts. Based on this evidence, Valeriano and Maness lay out a set of policy recommendations for proper defense against cyber threats that is built on restraint and regionalism.

Interoperability, Safety and Security in IoT

The Hacker and the State

World at the Crossroads

Cyber Conflict

12th IFIP WG 11.10 International Conference, ICCIP 2018, Arlington, VA, USA, March 12-14, 2018, Revised Selected Papers

10th International EAI Conference, ICDF2C 2018, New Orleans, LA, USA, September

10–12, 2018, Proceedings

Cyber Attacks and the New Normal of Geopolitics

th This volume is an edition of the papers selected from the 12 FIRA RoboWorld C-gress, held in Incheon, Korea, August 16–18, 2009. The Federation of International Robosoccer Association (FIRA – www. fira. net) is a non-profit organization, which organizes robotic competitions and meetings around the globe annually. The RoboSoccer competitions started in 1996 and FIRA was - tablished on June 5, 1997. The Robot Soccer competitions are aimed at promoting the spirit of science and technology to the younger generation. The congress is a forum in which to share ideas and future directions of technologies, and to enlarge the human networks in robotics area. The objectives of the FIRA Cup and Congress are to explore the technical dev-opment and achievement in the field of robotics, and provide participants with a robot festival including technical presentations, robot soccer competitions and exhibits - der the theme "Where Theory and Practice Meet. " th Under the umbrella of the 12 FIRA RoboWorld Incheon Congress 2009, six int- national conferences were held for greater impact and scientific exchange: th • 6 International Conference

on Computational Intelligence, Robotics and Autonomous Systems (CIRAS) th • 5 International Symposium on Autonomous Minirobots for Research and Edutainment (AMiRE) • International Conference on Social Robotics (ICSR) • International Conference on Advanced Humanoid Robotics Research (ICAHRR) • International Conference on Entertainment Robotics (ICER) • International Robotics Education Forum (IREF) This volume consists of selected quality papers from the six conferences.

This book constitutes the proceedings of the 4th International Conference on Science of Cyber Security, SciSec 2022, held in Matsu, Japan in August 2022. The 36 full papers presented in this volume were carefully reviewed and selected from 88 submissions. The papers are organized in the following topical sections: blockchain and applications; cryptography and applications; network security; cyber-physical system; malware; mobile system security; system and web security; security in financial industry; social engineering and personalized security; privacy and anonymity.

The world was standing at the crossroads in 2015 as globalization propelled human beings into an increasingly integrated

community of common destiny. In the meantime, the world witnessed the strategic competition among major powers. This annual publication offers views, opinions and predictions on global political and security issues, and China's strategic choices by Chinese scholars. It covers almost all the significant issues that took place in the international security arena in 2015. Besides the relations among major powers, it studies the international community's fight against Islamic State (IS), the strategic situation in the Korean Peninsula, political situation in Myanmar, the Joint Comprehensive Plan of Action on the Iranian nuclear issue, free navigation in the South China Sea, China's Belt and Road Initiative and its grand diplomacy. This book argues that the strategic competition among major powers is heightening, and smaller countries as well as extremist forces like the IS are seeking strategic space by taking advantage of the conflicts among major powers. The book concludes that to address this major historic challenge in international politics, it is essential that some major powers drop the hostile stance towards each other and enhance partnership to foster international cooperation.

Transitional justice and diaspora studies are

interdisciplinary and expanding fields of study. Finding the right combination of mechanisms to forward transitional justice in post-conflict societies is an ongoing challenge for states and affected populations. Diasporas, as non-state actors with increased agency in homelands, host-lands, and other global locations, engage with their past from a distance, but their actions are little understood. Diaspora Mobilizations for Transitional Justice develops a novel framework to demonstrate how diasporas connect with local actors in transitional justice processes through a variety of mechanisms and their underlying analytical rationales—emotional, cognitive, symbolic/value-based, strategic, and networks-based. Mechanisms featured here are: thin sympathetic response and chosen trauma, fear and hope, contact and framing, cooperation and coalition-building, brokerage, patronage, and connective action, among others. The contributors discuss the role of diasporas in truth commissions, memorialization, recognition of genocides and other human rights atrocities, as well as their abilities to affect transitional justice from afar by holding particular attitudes, or upon return temporarily or for good. This book sheds light on how diasporas' contextual

embeddedness shapes their mobilization strategies, and features empirical evidence from Europe, United States and Canada, as well as from conflict and postconflict polities in the Balkans, Middle East, Eurasia and Latin America. It was originally published as a special issue of Ethnic and Racial Studies.

International Handbook of Media Literacy Education

10th International Conference, ATIS 2019, Thanjavur, India, November 22–24, 2019, Proceedings

Research in Attacks, Intrusions, and Defenses

Cyberspace in Peace and War, Second Edition

Constructing cybersecurity

Architectures, Countermeasures, and Challenges

The Evolving Character of Power and Coercion

The two-volume set LNCS 11944-11945 constitutes the proceedings of the 19th International Conference on Algorithms and Architectures for Parallel Processing, ICA3PP 2019, held in Melbourne, Australia, in December 2019. The 73 full and 29 short papers presented were carefully reviewed and selected from 251 submissions. The papers are organized in topical sections

on: Parallel and Distributed Architectures, Software Systems and Programming Models, Distributed and Parallel and Network-based Computing, Big Data and its Applications, Distributed and Parallel Algorithms, Applications of Distributed and Parallel Computing, Service Dependability and Security, IoT and CPS Computing, Performance Modelling and Evaluation.

A Futurist's Guide to Emergency Management provides interdisciplinary analysis on how particular sets of conditions may occur in the future by evaluating global trends, possible scenarios, emerging conditions, and various other elements of risk management. Firmly based in science, the book leverages historical data, current best practices, and scie

NOTE: The CISSP objectives this book covered were issued in 2018. For coverage of the most recent CISSP objectives effective in April 2021, please look for the latest edition of this guide: (ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide, 9th Edition (ISBN: 9781119786238). CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide, 8th Edition has been completely updated for the latest 2018 CISSP Body of

Knowledge. This bestselling Sybex study guide covers 100% of all exam objectives. You'll prepare for the exam smarter and faster with Sybex thanks to expert content, real-world examples, advice on passing each section of the exam, access to the Sybex online interactive learning environment, and much more. Reinforce what you've learned with key topic exam essentials and chapter review questions. Along with the book, you also get access to Sybex's superior online interactive learning environment that includes: Six unique 150 question practice exams to help you identify where you need to study more. Get more than 90 percent of the answers correct, and you're ready to take the certification exam. More than 700 Electronic Flashcards to reinforce your learning and give you last-minute test prep before the exam A searchable glossary in PDF to give you instant access to the key terms you need to know for the exam Coverage of all of the exam topics in the book means you'll be ready for: Security and Risk Management Asset Security Security Engineering Communication and Network Security Identity and Access Management Security Assessment and Testing Security Operations Software Development Security

This book constitutes the refereed proceedings of the 18th International Symposium on Research in Attacks, Intrusions and Defenses, RAID 2015, held in Kyoto, Japan, in November 2015. The 28 full papers were carefully reviewed and selected from 119 submissions. This symposium brings together leading researchers and practitioners from academia, government, and industry to discuss novel security problems, solutions, and technologies related to intrusion detection, attacks, and defenses.

18th International Symposium, RAID 2015, Kyoto, Japan,November 2-4, 2015. Proceedings

The Official (ISC)2 Guide to the SSCP CBK

SSC CHSL (10+2) Combined Higher Secondary Level Tier I 30 Practice Sets 2022

International Conference on Security and Privacy in Communication Networks

Socio-Technological Transformations and Political Fragmentation

19th International Conference, ICA3PP 2019, Melbourne, VIC, Australia, December 9–11, 2019, Proceedings, Part I

Trends and Applications in Software Engineering

This 2-volume set constitutes the thoroughly refereed post-conference

proceedings of the 10th International Conference on Security and Privacy in Communication Networks, SecureComm 2014, held in Beijing, China, in September 2014. The 27 regular and 17 short papers presented were carefully reviewed. It also presents 22 papers accepted for four workshops (ATCS, SSS, SLSS, DAPRO) in conjunction with the conference, 6 doctoral symposium papers and 8 poster papers. The papers are grouped in the following topics: security and privacy in wired, wireless, mobile, hybrid, sensor, ad hoc networks; network intrusion detection and prevention, firewalls, packet filters; malware, and distributed denial of service; communication privacy and anonymity; network and internet forensics techniques; public key infrastructures, key management, credential management; secure routing, naming/addressing, network management; security and privacy in pervasive and ubiquitous computing; security & privacy for emerging technologies: VoIP, peer-to-peer and overlay network systems; security & isolation in data center networks; security & isolation in software defined networking.

Modern society has become dependent on technology, allowing personal information

to be input and used across a variety of personal and professional systems. From banking to medical records to e-commerce, sensitive data has never before been at such a high risk of misuse. As such, organizations now have a greater responsibility than ever to ensure that their stakeholder data is secured, leading to the increased need for cybersecurity specialists and the development of more secure software and systems. To avoid issues such as hacking and create a safer online space, cybersecurity education is vital and not only for those seeking to make a career out of cybersecurity, but also for the general public who must become more aware of the information they are sharing and how they are using it. It is crucial people learn about cybersecurity in a comprehensive and accessible way in order to use the skills to better protect all data. The Research Anthology on Advancements in Cybersecurity Education discusses innovative concepts, theories, and developments for not only teaching cybersecurity, but also for driving awareness of efforts that can be achieved to further secure sensitive data. Providing information on a range of topics from cybersecurity education requirements, cyberspace security talents training

systems, and insider threats, it is ideal for educators, IT developers, education professionals, education administrators, researchers, security analysts, systems engineers, software security engineers, security professionals, policymakers, and students.

Kaspersky security center 10 step by step with pictures: installation, activation, tasks, policies. V1 in arabic.

This book constitutes the refereed proceedings of the 7th International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ACNS 2017, held in Warsaw, Poland, in August 2017. The 12 revised full papers, 13 revised short presentations, and 3 invited papers were carefully reviewed and selected from a total of 40 submissions. The papers are organized in topical sections on Critical Infrastructure Protection and Visualization; Security and Resilience of Network Systems; Adaptive Security; Anti-malware Techniques: Detection, Analysis, Prevention; Security of Emerging Technologies; Applied Cryptography; New Ideas and Paradigms for Security.

7th International Conference on Mathematical Methods, Models, and Architectures for Computer Network

Security, MMM-ACNS 2017, Warsaw, Poland, August 28-30, 2017, Proceedings
Proceedings of the 4th International Conference on Software Process Improvement CIMPS'2015
10th International ICST Conference, SecureComm 2014, Beijing, China, September 24-26, 2014, Revised Selected Papers, Part II
FIRA RoboWorld Congress 2009, Incheon, Korea, August 16-20, 2009. Proceedings
Kaspersky security center
Hacking, Trust and Fear Between Nations
Chapter 25. A Quick Perspective on the Current State in Cybersecurity

Threat actors, be they cyber criminals, terrorists, hacktivists or disgruntled employees, are employing sophisticated attack techniques and anti-forensics tools to cover their attacks and breach attempts. As emerging and hybrid technologies continue to influence daily business decisions, the proactive use of cyber forensics to better assess the risks that the exploitation of these technologies pose to enterprise-wide operations is rapidly becoming a strategic business objective. This book moves beyond the typical, technical approach to discussing cyber forensics processes and procedures. Instead, the authors examine how cyber forensics can be applied to identifying, collecting, and examining evidential data from emerging and hybrid technologies, while taking

steps to proactively manage the influence and impact, as well as the policy and governance aspects of these technologies and their effect on business operations. A world-class team of cyber forensics researchers, investigators, practitioners and law enforcement professionals have come together to provide the reader with insights and recommendations into the proactive application of cyber forensic methodologies and procedures to both protect data and to identify digital evidence related to the misuse of these data. This book is an essential guide for both the technical and non-technical executive, manager, attorney, auditor, and general practitioner who is seeking an authoritative source on how cyber forensics may be applied to both evidential data collection and to proactively managing today's and tomorrow's emerging and hybrid technologies. The book will also serve as a primary or supplemental text in both under- and post-graduate academic programs addressing information, operational and emerging technologies, cyber forensics, networks, cloud computing and cybersecurity.
The threat of cyberwar can feel very Hollywood: nuclear codes hacked, power plants melting down, cities burning. In reality, state-sponsored hacking is covert, insidious, and constant. It is also much harder to prevent. Ben Buchanan reveals the cyberwar that's already here, reshaping the global contest for geopolitical advantage.
This book defines the phenomenon of mHealth and its evolution, explaining why an

understanding of mHealth is critical for decision makers, entrepreneurs and policy analysts who are pivotal to developing products that meet the collaborative health information needs of consumers and providers in a competitive and rapidly-changing environment. The book examines trends in mHealth and discusses how mHealth technologies offer opportunities for innovators and entrepreneurs, those who often are industry first-movers with regard to technology advancement. It also explores the changing dynamics and relationships among physicians, patients, insurers, regulators, managers, administrators, caregivers and others involved in the delivery of health services. The primary focus is on the ways in which mHealth technologies are revising and reshaping healthcare delivery systems in the United States and globally and how those changes are expected to change the ways in which the business of healthcare is conducted. mHealth: Transforming Healthcare consists of nine chapters that addresses key content areas, including history (to the extent that dynamic technologies have a history), projection of immediate evolution and consistent issues associated with health technology, such as security and information privacy and government and industry regulation. A major point of discussion addressed is whether mHealth is a transient group of products and a passing patient encounter approach, or if it is the way much of our health care will be delivered in future years

with incremental evolution to achieve sustainable innovation of health technologies. Nowadays, cybersecurity makes headlines across the media and in companies, blogs, social networks, among other places. The Internet is a wild cyberspace, an arena for commercialization, consumerism, business, and leisure, to name a few activities. Networks, populations, and nations around the world, now interconnected through the Internet, rely on it for their daily lives. But some Internet users have learned to take advantage of vulnerable systems and of Internet technologies for their own good, sending out spam, phishing, data breaches, botnets, and other threats. An underground criminal network has emerged, creating complex malware kits for several purposes. "Hacktivism" has become a popular term with many supporters worldwide, but cyberwarfare is now on the rise, gaining more and more attention from nation-states. This chapter provides a quick overview of these topics, discussing them in a timely manner, referencing key events from the past while focusing on the present day.

Look Who's Watching

Power, expertise and the internet security industry

mHealth

The Challenge of BRIC Multinationals

Cyber Conflict in the International System

Examining Emerging and Hybrid Technologies

The Global Cyber-Vulnerability Report

Contemporary Digital Forensic Investigations of Cloud and Mobile Applications comprehensively discusses the implications of cloud (storage) services and mobile applications on digital forensic investigations. The book provides both digital forensic practitioners and researchers with an up-to-date and advanced knowledge of collecting and preserving electronic evidence from different types of cloud services, such as digital remnants of cloud applications accessed through mobile devices. This is the first book that covers the investigation of a wide range of cloud services. Dr. Kim-Kwang Raymond Choo and Dr. Ali Dehghantanha are leading researchers in cloud and mobile security and forensics, having organized research, led research, and been published widely in the field. Users will gain a deep overview of seminal research in the field while also identifying prospective future research topics and open challenges. Presents the most current, leading edge research on cloud and mobile application forensics, featuring a panel of top experts in the field Introduces the first book to provide an in-depth overview of the issues surrounding digital forensic investigations in cloud and associated mobile apps Covers key technical topics and provides readers with a complete understanding of the most current research findings Includes discussions on future research directions and challenges

Kaspersky security centerLulu Press, Inc

This book provides solid, state-of-the-art contributions from both scientists and practitioners working on botnet detection and analysis, including botnet economics. It presents original theoretical and empirical chapters dealing with both offensive and defensive aspects in this field. Chapters address fundamental theory, current trends and techniques for evading detection, as well as practical experiences concerning detection and defensive strategies for the botnet ecosystem, and include surveys, simulations, practical results, and case studies.

This PIBR volume examines a number of idiosyncratic elements in the internationalization strategies of BRIC MNEs and, in particular, in their relationship with home country policies.

Surveillance, Treachery and Trust Online

A Futurist's Guide to Emergency Management

Research Anthology on Advancements in Cybersecurity Education

Progress in Robotics

Cyber Forensics

Emerging Trends in ICT Security

Remote Instrumentation for eScience and Related Aspects

This updated and expanded edition of Cyberspace in Peace and War by Martin C. Libicki presents a comprehensive

understanding of cybersecurity, cyberwar, and cyber-terrorism. From basic concepts to advanced principles, Libicki examines the sources and consequences of system compromises, addresses strategic aspects of cyberwar, and defines cybersecurity in the context of military operations while highlighting unique aspects of the digital battleground and strategic uses of cyberwar. This new edition provides updated analysis on cyberespionage, including the enigmatic behavior of Russian actors, making this volume a timely and necessary addition to the cyber-practitioner's library. Cyberspace in Peace and War guides readers through the complexities of cybersecurity and cyberwar and challenges them to understand the topics in new ways. Libicki provides the technical and geopolitical foundations of cyberwar necessary to understand the policies, operations, and strategies required for safeguarding an increasingly online infrastructure.

Why do nations break into one another's most important computer networks? There is an obvious answer: to steal valuable information or to attack. But this isn't the full story. This book draws on often-overlooked documents leaked by Edward Snowden, real-world case studies of cyber operations, and policymaker perspectives to show that intruding into other countries' networks has enormous defensive value as well. Two nations, neither of which seeks to harm the other but neither

of which trusts the other, will often find it prudent to launch intrusions. This general problem, in which a nation's means of securing itself threatens the security of others and risks escalating tension, is a bedrock concept in international relations and is called the 'security dilemma'. This book shows not only that the security dilemma applies to cyber operations, but also that the particular characteristics of the digital domain mean that the effects are deeply pronounced. The cybersecurity dilemma is both a vital concern of modern statecraft and a means of accessibly understanding the essential components of cyber operations.
The fourth edition of the Official (ISC)2® Guide to the SSCP CBK® is a comprehensive resource providing an in-depth look at the seven domains of the SSCP Common Body of Knowledge (CBK). This latest edition provides an updated, detailed guide that is considered one of the best tools for candidates striving to become an SSCP. The book offers step-by-step guidance through each of SSCP's domains, including best practices and techniques used by the world's most experienced practitioners. Endorsed by (ISC)² and compiled and reviewed by SSCPs and subject matter experts, this book brings together a global, thorough perspective to not only prepare for the SSCP exam, but it also provides a reference that will serve you well into your career.
This book constitutes the refereed post-

conference proceedings of the International Conference on Safety and Security in Internet of Things , SaSeIoT 2016, which was collocated with InterIoT and took place in Paris, France, in October 2016. The 14 revised full papers were carefully reviewed and selected from 22 submissions and cover all aspects of the latest research findings in the area of Internet of Things (IoT).

Applications and Techniques in Information Security

Cyber Strategy

Computer Network Security

Transforming Healthcare

International Strategic Relations and China's National Security

The Cybersecurity Dilemma

Algorithms and Architectures for Parallel Processing

This book examines new and challenging political aspects of cyber security and presents it as an issue defined by socio-technological uncertainty and political fragmentation. Structured along two broad themes and providing empirical examples for how socio-technical changes and political responses interact, the first part of the book looks at the current use of cyber space in conflictual settings, while the second focuses on political responses by state and non-state actors in an environment defined by uncertainties. Within this, it highlights four key debates that encapsulate the complexities and paradoxes of cyber security politics from a Western perspective – how much political

influence states can achieve via cyber operations and what context factors condition the (limited) strategic utility of such operations; the role of emerging digital technologies and how the dynamics of the tech innovation process reinforce the fragmentation of the governance space; how states attempt to uphold stability in cyberspace and, more generally, in their strategic relations; and how the shared responsibility of state, economy, and society for cyber security continues to be re-negotiated in an increasingly trans-sectoral and transnational governance space. This book will be of much interest to students of cyber security, global governance, technology studies, and international relations.

This book will focus on new Remote Instrumentation aspects related to middleware architecture, high-speed networking, wireless Grid for acquisition devices and sensor networks, QoS provisioning for real-time control, measurement instrumentation and methodology. Moreover, it will provide knowledge about the automation of mechanisms oriented to accompanying processes that are usually performed by a human. Another important point of this book is focusing on the future trends concerning Remote Instrumentation systems development and actions related to standardization of remote instrumentation mechanisms.

Cyber-physical systems (CPS) have emerged as a unifying name for systems where cyber parts (i.e., the computing and communication parts) and physical parts are tightly integrated, both in design and during operation. Such systems use computations and

communication deeply embedded in and interacting with human physical processes as well as augmenting existing and adding new capabilities. As such, CPS is an integration of computation, networking, and physical processes. Embedded computers and networks monitor and control the physical processes, with feedback loops where physical processes affect computations and vice versa. The economic and societal potential of such systems is vastly greater than what has been realized, and major investments are being made worldwide to develop the technology. Artificial Intelligence Paradigms for Smart Cyber-Physical Systems focuses on the recent advances in Artificial intelligence-based approaches towards affecting secure cyber-physical systems. This book presents investigations on state-of-the-art research issues, applications, and achievements in the field of computational intelligence paradigms for CPS. Covering topics that include autonomous systems, access control, machine learning, and intrusion detection and prevention systems, this book is ideally designed for engineers, industry professionals, practitioners, scientists, managers, students, academicians, and researchers seeking current research on artificial intelligence and cyber-physical systems.

Constructing cybersecurity adopts a constructivist approach to cybersecurity and problematises the state of contemporary knowledge within this field. Setting out by providing a concise overview of such knowledge this book subsequently adopts Foucauldian positions on power and security to highlight assumptions and limitations found herein. What follows is a detailed

analysis of the discourse produced by various internet security companies demonstrating the important role that these security professionals play constituting and entrenching this knowledge by virtue of their specific epistemic authority. As a relatively new source within a broader security dispositif these security professionals have created relationships of mutual recognition and benefit with traditional political and security professionals.

Combating Violent Extremism and Radicalization in the Digital Era

Botnets

Diaspora Mobilizations for Transitional Justice

Competing National Perspectives

Science of Cyber Security

Cyber Security Politics

The Internet ecosystem is held together by a surprisingly intangible glue — trust. To meet its full potential, users need to trust that the Internet works reliably and efficiently when providing them with the information they are seeking, while also being secure, private and safe. When trust in the Internet wanes, the network's stock of "digital social capital" falls and users begin to alter their online behaviour. These often subtle changes in behaviour tend to be collectively highly maladaptive, hindering the economic, developmental and innovative potential of the globe-spanning network of networks. Look Who's Watching: Surveillance, Treachery and Trust Online confirms in vivid detail that the trust placed by users in the Internet is increasingly misplaced. Edward Snowden's revelations that the United States National Security Agency and other government agencies are spying on Internet users, the proliferation of

cybercrime and the growing commodification of user data and regulatory changes — which threaten to fragment the system — are all rapidly eroding the confidence users have in the Internet ecosystem. Based on a combination of illustrative anecdotal evidence and analysis of new survey data, Look Who's Watching clearly demonstrates why trust matters, how it is being eroded and how, with care and deliberate policy action, the essential glue of the Internet can be restored.

Some pundits claim cyber weaponry is the most important military innovation in decades, a transformative new technology that promises a paralyzing first-strike advantage difficult for opponents to deter. Yet, what is cyber strategy? How do actors use cyber capabilities to achieve a position of advantage against rival states? This book examines the emerging art of cyber strategy and its integration as part of a larger approach to coercion by states in the international system between 2000 and 2014. To this end, the book establishes a theoretical framework in the coercion literature for evaluating the efficacy of cyber operations. Cyber coercion represents the use of manipulation, denial, and punishment strategies in the digital frontier to achieve some strategic end. As a contemporary form of covert action and political warfare, cyber operations rarely produce concessions and tend to achieve only limited, signaling objectives. When cyber operations do produce concessions between rival states, they tend to be part of a larger integrated coercive strategy that combines network intrusions with other traditional forms of statecraft such as military threats, economic sanctions, and diplomacy. The books finds that cyber operations rarely produce concessions in isolation. They are additive instruments that complement traditional statecraft and coercive diplomacy. The book combines an analysis of cyber exchanges between rival states and broader event data on political, military, and economic interactions with case studies on the leading cyber powers: Russia, China, and the United

States. The authors investigate cyber strategies in their integrated and isolated contexts, demonstrating that they are useful for maximizing informational asymmetries and disruptions, and thus are important, but limited coercive tools. This empirical foundation allows the authors to explore how leading actors employ cyber strategy and the implications for international relations in the 21st century. While most military plans involving cyber attributes remain highly classified, the authors piece together strategies based on observations of attacks over time and through the policy discussion in unclassified space. The result will be the first broad evaluation of the efficacy of various strategic options in a digital world.
Understanding cybersecurity principles and practices is vital to all users of IT systems and services, and is particularly relevant in an organizational setting where the lack of security awareness and compliance amongst staff is the root cause of many incidents and breaches. If these are to be addressed, there needs to be adequate support and provision for related training and education in order to ensure that staff know what is expected of them and have the necessary skills to follow through. Cybersecurity Education for Awareness and Compliance explores frameworks and models for teaching cybersecurity literacy in order to deliver effective training and compliance to organizational staff so that they have a clear understanding of what security education is, the elements required to achieve it, and the means by which to link it to the wider goal of good security behavior. Split across four thematic sections (considering the needs of users, organizations, academia, and the profession, respectively), the chapters will collectively identify and address the multiple perspectives from which action is required. This book is ideally designed for IT consultants and specialist staff including chief information security officers, managers, trainers, and organizations.
The information infrastructure – comprising computers,

embedded devices, networks and software systems – is vital to operations in every sector: chemicals, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors, materials and waste, transportation systems, and water and wastewater systems. Global business and industry, governments, indeed society itself, cannot function if major components of the critical information infrastructure are degraded, disabled or destroyed. Critical Infrastructure Protection XII describes original research results and innovative applications in the interdisciplinary field of critical infrastructure protection. Also, it highlights the importance of weaving science, technology and policy in crafting sophisticated, yet practical, solutions that will help secure information, computer and network assets in the various critical infrastructure sectors. Areas of coverage include: Themes and Issues; Infrastructure Protection; Infrastructure Modeling and Simulation; Industrial Control Systems Security. This book is the twelfth volume in the annual series produced by the International Federation for Information Processing (IFIP) Working Group 11.10 on Critical Infrastructure Protection, an international community of scientists, engineers, practitioners and policy makers dedicated to advancing research, development and implementation efforts focused on infrastructure protection. The book contains a selection of fifteen edited papers from the Twelfth Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection, held at SRI International, Arlington, Virginia, USA in the spring of 2018. Critical Infrastructure Protection XII is an important resource for researchers, faculty members and graduate students, as well as for policy makers, practitioners and other individuals with interests in homeland security.

Contemporary Digital Forensic Investigations of Cloud and Mobile Applications
Critical Infrastructure Protection XII
Second International Conference, InterIoT 2016 and Third International Conference, SaSeIoT 2016, Paris, France, October 26-27, 2016, Revised Selected Papers
Artificial Intelligence Paradigms for Smart Cyber-Physical Systems
Cyber War versus Cyber Realities
(ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide
Cybersecurity Education for Awareness and Compliance

At the forefront in its field, this Handbook examines the theoretical, conceptual, pedagogical and methodological development of media literacy education and research around the world. Building on traditional media literacy frameworks in critical analysis, evaluation, and assessment, it incorporates new literacies emerging around connective technologies, mobile platforms, and social networks. A global perspective rather than a Western-centric point of view is explicitly highlighted, with contributors from all continents, to show the empirical research being done at the intersection of media, education, and engagement in daily life. Structured around five themes—Educational Interventions; Safeguarding/Data and Online Privacy; Engagement in Civic Life; Media, Creativity and Production; Digital Media Literacy—the volume as a whole emphasizes the competencies needed to engage in meaningful participation in digital culture.

This book constitutes the refereed proceedings of the 10th International Conference on Applications and Techniques in Information Security, ATIS 2019, held in

Tamil Nadul, India, in November 2019. The 22 full papers and 2 short papers presented in the volume were carefully reviewed and selected from 50 submissions. The papers are organized in the following topical sections: information security; network security; intrusion detection system; authentication and key management system; security centric applications.

This book contains a selection of papers from The 2015 International Conference on Software Process Improvement (CIMPS'15), held between the 28th and 30th of October in Mazatlán, Sinaloa, México. The CIMPS'15 is a global forum for researchers and practitioners that present and discuss the most recent innovations, trends, results, experiences and concerns in the several perspectives of Software Engineering with clear relationship but not limited to software processes, Security in Information and Communication Technology and Big Data Field. The main topics covered are: Organizational Models, Standards and Methodologies, Knowledge Management, Software Systems, Applications and Tools, Information and Communication Technologies and Processes in non-software domains (Mining, automotive, aerospace, business, health care, manufacturing, etc.) with a demonstrated relationship to software process challenges.

This is the first book that uses cyber-vulnerability data to explore the vulnerability of over four million machines per year, covering a two-year period as reported by Symantec. Analyzing more than 20 billion telemetry reports comprising malware and binary reputation reports, this book quantifies the cyber-vulnerability of 44 countries for which at least 500

hosts were monitored. Chapters explain the context for this data and its impact, along with explaining how the cyber-vulnerability is calculated. This book also contains a detailed summary of the cyber-vulnerability of dozens of nations according to the percentage of infected hosts and number of infections. It identifies relationships between piracy rates, GDP and other country indicators. The book contains detailed information about potential cyber-security policies that 44 countries have announced, as well as an analysis of gaps in cyber-security policies in general. The Global Cyber-Vulnerability Report targets researchers and professionals including government and military workers, policy-makers and law-makers working in cybersecurity or the web intelligence fields. Advanced-level students in computer science will also find this report valuable as a reference.

Digital Forensics and Cyber Crime

4th International Conference, SciSec 2022, Matsue, Japan, August 10–12, 2022, Revised Selected Papers