User Guide Fireeye

Providing an invaluable introductory resource for students studying cyber warfare, this book highlights the evolution of cyber conflict in modern times through dozens of key primary source documents related to its development and implementation. This meticulously curated primary source collection is designed to offer a broad examination of key documents related to cyber warfare, covering the subject from multiple perspectives. The earliest documents date from the late 20th century, when the concept and possibility of cyber attacks became a reality, while the most recent documents are from 2019. Each document is accompanied by an introduction and analysis written by an expert in the field that provides the necessary context for readers to learn about the complexities of cyber warfare. The title's nearly 100 documents are drawn primarily but not exclusively from government sources and allow readers to understand how policy, strategy, doctrine, and tactics of cyber warfare are created and devised, particularly in the United States. Although the United States is the global leader in cyber capabilities and is largely driving the determination of norms within the cyber domain, the title additionally contains a small number of international documents. This invaluable work will serve as an excellent starting point for anyone seeking to understand the nature and character of international cyber warfare. Covers in detail one of the defining forms of conflict of the 21st century—cyber warfare will significantly impact virtually every American citizen over the next two decades Provides more than 90 primary source documents and matching analysis, allowing readers to investigate the underpinnings of cyber warfare Enables readers to see the development of different concepts of cyber warfare through its chronological organization Reflects the deep knowledge of an editor who is a noted expert in cyber warfare and has taught for the United States Air Force for more than a decade

Learn the key objectives and most crucial concepts covered by the Security+ Exam SY0-601 with this comprehensive and practical Deluxe Study Guide Covers 100% of exam objectives including threats, attacks, and vulnerabilities; technologies and tools; architecture and design; identity and access management; risk management; cryptography and PKI, and much more... Includes interactive online learning environment and study tools with: 4 custom practice exams 100 Electronic Flashcards Searchable key term glossary Plus 33 Online Security+ Practice Lab Modules Expert Security+ SY0-601 exam preparation--Now with 33 Online Lab Modules The Fifth edition of CompTIA Security+ Deluxe Study Guide offers invaluable preparation for Exam SY0-601. Written by expert authors, Mike Chapple and David Seidl, the book covers 100% of the exam objectives with clear and concise explanations. Discover how to handle threats, attacks, and vulnerabilities using industry-standard tools and technologies, while gaining and understanding the role of architecture and design. Spanning topics from everyday tasks like identity and access management to complex subjects such as risk management and cryptography, this study guide helps you consolidate your knowledge base in preparation for the Security+ exam. Illustrative examples show how these processes play out in real-world scenarios, allowing you to immediately translate essential concepts to on-the-job application. Coverage of 100% of all exam objectives in this Study Guide means you'll be ready for: Attacks, Threats, and Vulnerabilities Architecture and Design

Implementation Operations and Incident Response Governance, Risk, and Compliance Interactive learning environment Take your exam prep to the next level with Sybex's superior interactive online study tools. To access our learning environment, simply visit www.wiley.com/go/sybextestprep, register your book to receive your unique PIN, and instantly gain one year of FREE access after activation to: Interactive test bank with 4 bonus exams. Practice questions help you identify areas where further review is needed. 100 Electronic Flashcards to reinforce learning and last-minute prep before the exam. Comprehensive glossary in PDF format gives you instant access to the key terms so you are fully prepared. ABOUT THE PRACTICE LABS SECURITY+ LABS So you can practice with hands-on learning in a real environment, Sybex has bundled Practice Labs virtual labs that run from your browser. The registration code is included with the book and gives you 6 months unlimited access to Practice Labs CompTIA Security+ Exam SY0-601 Labs with 33 unique lab modules to practice your skills.

This volume presents the proceedings of the 3rd International Conference on Nanotechnologies and Biomedical Engineering which was held on September 23-26, 2015 in Chisinau, Republic of Moldova. ICNBME-2015 continues the series of International Conferences in the field of nanotechnologies and biomedical engineering. It aims at bringing together scientists and engineers dealing with fundamental and applied research for reporting on the latest theoretical developments and applications involved in the fields. Topics include Nanotechnologies and nanomaterials Plasmonics and metamaterials Bio-micro/nano technologies Biomaterials Biosensors and sensors systems Biomedical instrumentation Biomedical signal processing Biomedical imaging and image processing Molecular, cellular and tissue engineering Clinical engineering, health technology management and assessment; Health informatics, e-health and telemedicine Biomedical engineering education Nuclear and radiation safety and security Innovations and technology transfer

This book offers an introduction to Information Technology with regard to peace, conflict, and security research, a topic that it approaches from natural science, technical and computer science perspectives. Following an initial review of the fundamental roles of IT in connection with peace, conflict and security, the contributing authors address the rise of cyber conflicts via information warfare, cyber espionage, cyber defence and Darknets. The book subsequently explores recent examples of cyber warfare, including: • The Stuxnet attack on Iran’s uranium refining capability • The hacking of the German Federal Parliament’s internal communication system • The Wannacry malware campaign, which used software stolen from a US security agency to launch ransomware attacks worldwide The book then introduces readers to the concept of cyber peace, including a discussion of confidence and security-building measures. A section on Cyber Arms Control draws comparisons to global efforts to control chemical warfare, to reduce the risk of nuclear war, and to prevent the militarization of space. Additional topics include the security of critical information infrastructures, and cultural violence and peace in social media. The book concludes with an outlook on the future role of IT in peace and security. Information Technology for Peace and Security breaks new ground in a largely unexplored field of study, and offers a valuable asset for a broad readership including students, educators and working professionals in computer science, IT security, peace and conflict studies, and political science.

Develop a comprehensive plan for building a HIPAA-compliant security operations center, designed to detect and respond to an increasing number of healthcare data breaches and events. Using risk analysis, assessment, and management data combined with knowledge of cybersecurity program maturity, this book gives you the tools you need to operationalize threat intelligence, vulnerability management, security monitoring, and incident response processes to effectively meet the challenges presented by healthcare's current threats. Healthcare entities are bombarded with data. Threat intelligence feeds, news updates, and messages come rapidly and in many forms such as email, podcasts, and more. New vulnerabilities are found every day in applications, operating systems, and databases while older vulnerabilities remain exploitable. Add in the number of dashboards, alerts, and data points each information security tool provides and security teams find themselves swimming in oceans of data and unsure where to focus their energy. There is an urgent need to have a cohesive plan in place to cut through the noise and face these threats. Cybersecurity operations do not require expensive tools or large capital investments. There are ways to capture the necessary data. Teams protecting data and supporting HIPAA compliance can do this. All that's required is a plan—which author Eric Thompson provides in this book. What You Will Learn Know what threat intelligence is and how you can make it useful Understand how effective vulnerability management extends beyond the risk scores provided by vendors Develop continuous monitoring on a budget Ensure that incident response is appropriate Help healthcare organizations comply with HIPAA Who This Book Is For Cybersecurity, privacy, and compliance professionals working for organizations responsible for creating, maintaining, storing, and protecting patient information.

This book constitutes the thoroughly refereed proceedings of the 21st International Conference on Computer Networks, CN 2014, held in Brunów, Poland, in June 2014. The 34 revised full papers presented were carefully reviewed and selected for inclusion in the book. The papers in these proceedings cover the following topics: computer networks, tele informatics and communications, new technologies, queueing theory, innovative applications and networked and IT-related aspects of e-business.

The Arctic-Barents Region is facing numerous pressures from a variety of sources, including the effect of environmental changes and extractive industrial developments. The threats arising out of these pressures result in human security challenges. This book analyses the formation, and promotion, of societal security within the context of the Arctic-Barents Region. It applies the human security framework, which has increasingly gained currency at the UN level since 1994 (UNDP), as a tool to provide answers to many questions that face the Barents population today. The study explores human security dimensions such as environmental security, economic security, health, food, water, energy, communities, political security and digital security in order to assess the current challenges that the Barents population experiences today or may encounter in the future. In doing so, the book develops a comprehensive analysis of vulnerabilities, challenges and needs in the Barents Region and provides recommendations for new strategies to tackle insecurity and improve the wellbeing of both indigenous and local communities. This book will be a valuable tool for academics, policy-makers and students interested in environmental and human security, sustainable development, environmental studies and the Arctic and Barents Region in particular.

This book collects articles presented at the 13th International Conference on Information Technology- New Generations, April, 2016, in Las Vegas, NV USA. It includes over 100 chapters on critical areas of IT including Web Technology, Communications, Security, and Data Mining.

As protecting information becomes a rapidly growing concern for today's businesses, certifications in IT security have become highly desirable, even as the number of certifications has grown. Now you can set yourself apart with the Certified Ethical Hacker (CEH v10) certification. The CEH v10 Certified Ethical Hacker Study Guide offers a comprehensive overview of the CEH certification requirements using concise and easy-to-follow instruction. Chapters are organized by exam objective, with a handy section that maps each objective to its corresponding chapter, so you can keep track of your progress. The text provides thorough coverage of all topics, along with challenging chapter review questions and Exam Essentials, a key feature that identifies critical study areas. Subjects include intrusion detection, DDoS attacks, buffer overflows, virus creation, and more. This study guide goes beyond test prep, providing practical hands-on exercises to reinforce vital skills and real-world scenarios that put what you've learned into the context of actual job roles. Gain a unique certification that allows you to understand the mind of a hacker Expand your career opportunities with an IT certificate that satisfies the Department of Defense's 8570 Directive for Information Assurance positions Fully updated for the 2018 CEH v10 exam, including the latest developments in IT security Access the Sybex online learning center, with chapter review questions, full-length practice exams, hundreds of electronic flashcards, and a glossary of key terms Thanks to its clear organization, all-inclusive coverage, and practical instruction, the CEH v10 Certified Ethical Hacker Study Guide is an excellent resource for anyone who needs to understand the hacking process or anyone who wants to demonstrate their skills as a Certified Ethical Hacker.

Cyberwarfare: Information Operations in a Connected World puts students on the real-world battlefield of cyberspace! It reviews the role that cyberwarfare plays in modern military operations–operations in which it has become almost impossible to separate cyberwarfare from traditional warfare.

Ten Strategies of a World-Class Cyber Security Operations Center conveys MITRE's accumulated expertise on enterprise-grade computer network defense. It covers ten key qualities of leading Cyber Security Operations Centers (CSOCs), ranging from their structure and organization, to processes that best enable smooth operations, to approaches that extract maximum value from key CSOC technology investments. This book offers perspective and context for key decision points in structuring a CSOC, such as what capabilities to offer, how to architect large-scale data collection and analysis, and how to prepare the CSOC team for agile, threat-based response. If you manage, work in, or are standing up a CSOC, this book is for you. It is also available on MITRE's website, www.mitre.org.

CCNA Cybersecurity Operations Companion Guide is the official supplemental textbook for the Cisco Networking Academy CCNA Cybersecurity Operations course. The course emphasizes real-world practical application, while providing opportunities for you to gain the skills needed to successfully handle the tasks, duties, and responsibilities of an associate-level security analyst working in

a security operations center (SOC). The Companion Guide is designed as a portable desk reference to use anytime, anywhere to reinforce the material from the course and organize your time. The book's features help you focus on important concepts to succeed in this course: · Chapter Objectives—Review core concepts by answering the focus questions listed at the beginning of each chapter. · Key Terms—Refer to the lists of networking vocabulary introduced and highlighted in context in each chapter. · Glossary—Consult the comprehensive Glossary with more than 360 terms. · Summary of Activities and Labs—Maximize your study time with this complete list of all associated practice exercises at the end of each chapter. · Check Your Understanding—Evaluate your readiness with the end-of-chapter questions that match the style of questions you see in the online course quizzes. The answer key explains each answer. How To—Look for this icon to study the steps you need to learn to perform certain tasks. Interactive Activities—Reinforce your understanding of topics with dozens of exercises from the online course identified throughout the book with this icon. Packet Tracer Activities—Explore and visualize networking concepts using Packet Tracer. There are exercises interspersed throughout the chapters and provided in the accompanying Lab Manual book. Videos—Watch the videos embedded within the online course. Hands-on Labs—Develop critical thinking and complex problem-solving skills by completing the labs and activities included in the course and published in the separate Lab Manual.

- This is the latest practice test to pass the NSE6_FNC-8.5 Fortinet NSE 6 - FortiNAC 8.5 Exam. - It contains 30 Questions and Answers. - All the questions are 100% valid and stable. - You can reply on this practice test to pass the exam with a good mark and in the first attempt.

Through the rise of big data and the internet of things, terrorist organizations have been freed from geographic and logistical confines and now have more power than ever before to strike the average citizen directly at home. This, coupled with the inherently asymmetrical nature of cyberwarfare, which grants great advantage to the attacker, has created an unprecedented national security risk that both governments and their citizens are woefully ill-prepared to face. Examining cyber warfare and terrorism through a critical and academic perspective can lead to a better understanding of its foundations and implications. Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications 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. Highlighting a range of topics such as cyber threats, digital intelligence, and counterterrorism, this multi-volume book is ideally designed for law enforcement, government officials, lawmakers, security analysts, IT specialists, software developers, intelligence and security practitioners, students, educators, and researchers.

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.

The Internet of Things (IoT) is the notion that nearly everything we use, from gym shorts to streetlights, will soon be connected to the Internet; the Internet of Everything (IoE) encompasses not just objects, but the social connections, data, and processes that the IoT makes possible. Industry and financial analysts have predicted that the number of Internet-enabled devices will increase from 11 billion to upwards of 75 billion by 2020. Regardless of the number, the end result looks to be a mind-boggling explosion in Internet connected stuff. Yet, there has been relatively little attention paid to how we should go about regulating smart devices, and still less about how cybersecurity should be enhanced. Similarly, now that everything from refrigerators to stock exchanges can be connected to a ubiquitous Internet, how can we better safeguard privacy across networks and borders? Will security scale along with this increasingly crowded field? Or, will a combination of perverse incentives, increasing complexity, and new problems derail progress and exacerbate cyber insecurity? For all the press that such questions have received, the Internet of Everything remains a topic little understood or appreciated by the public. This volume demystifies our increasingly "smart" world, and unpacks many of the outstanding security, privacy, ethical, and policy challenges and opportunities represented by the IoE. Scott J. Shackelford provides real-world examples and straightforward discussion about how the IoE is impacting our lives, companies, and nations, and explain how it is increasingly shaping the international community in the twenty-first century. Are there any downsides of your phone being able to unlock your front door, start your car, and control your thermostat? Is your smart speaker always listening? How are other countries dealing with these issues? This book answers these questions, and more, along with offering practical guidance for how you can join the effort to help build an Internet of Everything that is as secure, private, efficient, and fun as possible.

Scrappy fifteen-year-old Dallas Marge and his older brother, Logan, strive to live a normal life, in the infamous city of kaspers, Starfall City. However, an unspoken truth between the two siblings leads Dallas to find a mysterious orb imprisoning a malevolent entity called Oryga, the tiger god, that curses him with an unimaginable power. Training under the supervision of the formerly villainous dragon kasper, Singuard, Dallas adapts to his newfound strength. Anxious to test himself, he disregards Singuard’s warnings about the dangerously ominous and superpowered criminal underworld and the kasper hunting militia, GAUNTLET, challenging them both as Starfall’s first-ever vigilante, Kirikon. However, the novice mask, alongside his friends, struggle to save Starfall from a sinister duo of otherworldly creatures when they target him for reasons unknown. Discover the truth behind the tigris orb as Kirikon blasts his way into action in this adventurous and gripping chapter of a brand new series, The Fire Eye Kronicles.

Learn the key objectives and most crucial concepts covered by the Security+ Exam SY0-601 with this comprehensive and

practical study guide The Eighth Edition of the CompTIA Security+ Study Guide Exam SY0-601 efficiently and comprehensively prepares you for the SY0-601 Exam. Accomplished authors and security experts Mike Chapple and David Seidl walk you through the fundamentals of crucial security topics, including the five domains covered by the SY0-601 Exam: Attacks, Threats, and Vulnerabilities Architecture and Design Implementation Operations and Incident Response Governance, Risk, and Compliance The study guide comes with the Sybex online, interactive learning environment that includes a pre-assessment test, hundreds of review questions, practice exams, flashcards, and a glossary of key terms. The book is written in a practical and straightforward manner, ensuring you can easily learn and retain the material. Perfect for everyone planning to take the SY0-601 Exam—as well as those who hope to secure a high-level certification like the CASP+, CISSP, or CISA—the study guide also belongs on the bookshelves of everyone who has ever wondered if the field of IT security is right for them. It’s a must-have reference!

Relations between the European Union (EU) and India have been growing in quantity and quality in the last two decades. Alongside the economic dimension, the political and security elements of the relationship have emerged as the most promising area for further collaboration between the two sides. This volume brings together analyses and recommendations on EU-India security relations in the fields of: (i) maritime security and freedom of navigation; (ii) cyber security and data protection; (iii) space policy and satellite navigation; (iv) defence cooperation. The chapters have been written by a select pan-European and Indian group of experts tasked by the Rome-based Istituto Affari Internazionali (IAI) and the Mumbai-based Gateway House (GH) in the framework of the EU-India Think Tank Twinning Initiative – a public diplomacy project aimed at connecting research institutions in Europe and India funded by the EU. The book provides the reader with original research and innovative insights into how to move forward EU-India relations. It will be essential reading for scholars and policy makers interested in the subject.

This book is a multi-disciplinary analysis of cyber warfare, featuring contributions by leading experts from a mixture of academic and professional backgrounds. Cyber warfare, meaning interstate cyber aggression, is an increasingly important emerging phenomenon in international relations, with state-orchestrated (or apparently state-orchestrated) computer network attacks occurring in Estonia (2007), Georgia (2008) and Iran (2010). This method of waging warfare – given its potential to, for example, make planes fall from the sky or cause nuclear power plants to melt down – has the capacity to be as devastating as any conventional means of conducting armed conflict. Every state in the world now has a cyber-defence programme and over 120 states also have a cyber-attack programme. While the amount of literature on cyber warfare is growing within disciplines, our understanding of the subject has been limited by a lack of cross-disciplinary engagement. In response, this book, drawn from the fields of computer science, military strategy, international law, political science and military ethics, provides a critical overview of cyber warfare for those approaching the topic from whatever angle. Chapters consider the emergence of the phenomena of cyber warfare in international affairs; what cyber-attacks are from a technological standpoint; the extent to which cyber-attacks can be attributed to state actors; the strategic value and danger posed by cyber conflict; the legal regulation of cyber-attacks, both as international uses of force and as part of an on-going armed conflict, and the ethical implications of cyber warfare. This book will

be of great interest to students of cyber warfare, cyber security, military ethics, international law, security studies and IR in general.
Cybersecurity has become a topic of concern over the past decade as private industry, public administration, commerce, and communication have gained a greater online presence. As many individual and organizational activities continue to evolve in the digital sphere, new vulnerabilities arise. Cybersecurity Policies and Strategies for Cyberwarfare Prevention serves as an integral publication on the latest legal and defensive measures being implemented to protect individuals, as well as organizations, from cyber threats. Examining online criminal networks and threats in both the public and private spheres, this book is a necessary addition to the reference collections of IT specialists, administrators, business managers, researchers, and students interested in uncovering new ways to thwart cyber breaches and protect sensitive digital information.
Computer security touches every part of our daily lives from our computers and connected devices to the wireless signals around us. Breaches have real and immediate financial, privacy, and safety consequences. This handbook has compiled advice from top professionals working in the real world about how to minimize the possibility of computer security breaches in your systems. Written for professionals and college students, it provides comprehensive best guidance about how to minimize hacking, fraud, human error, the effects of natural disasters, and more. This essential and highly-regarded reference maintains timeless lessons and is fully revised and updated with current information on security issues for social networks, cloud computing, virtualization, and more.
Jena is asked to guide a large group of hierophants into the dangerous mountains of Atlantis to perform a religious ceremony. Earthquakes are tearing the nation apart, and sending carnivorous reptiles into everyone’s kitchens, and this is an attempt to contact the earth elementals to begin a reversal. She has the usual wacky group of companions, and meets more along the way. The clock is ticking as other armies attempt to destroy the temple, and it’s a rough ride for all. A thorough exploration of this part of the continent, with its even more ancient ruins and underground caverns, Jena must turn from weapons to accomplish this with wit and humor
This book provides profound insights into industrial control system resilience, exploring fundamental and advanced topics and including practical examples and scenarios to support the theoretical approaches. It examines issues related to the safe operation of control systems, risk analysis and assessment, use of attack graphs to evaluate the resiliency of control systems, preventive maintenance, and malware detection and analysis. The book also discusses sensor networks and Internet of Things devices. Moreover, it covers timely responses to malicious attacks and hazardous situations, helping readers select the best approaches to handle such unwanted situations. The book is essential reading for engineers, researchers, and specialists addressing security and safety issues related to the implementation of modern industrial control systems. It is also a valuable resource for students interested in this area.
Learn how to identify vulnerabilities within computer networks and implement countermeasures that mitigate risks and damage with Whitman/Mattord's PRINCIPLES OF INCIDENT RESPONSE & DISASTER RECOVERY, 3rd Edition. This edition offers the knowledge you

need to help organizations prepare for and avert system interruptions and natural disasters. Comprehensive coverage addresses information security and IT in contingency planning today. Updated content focuses on incident response and disaster recovery. You examine the complexities of organizational readiness from an IT and business perspective with emphasis on management practices and policy requirements. You review industry's best practices for minimizing downtime in emergencies and curbing losses during and after system service interruptions. This edition includes the latest NIST knowledge, expanded coverage of security information and event management (SIEM) and unified threat management, and more explanation of cloud-based systems and Web-accessible tools to prepare you for success. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Use the methodology in this study guide to design, manage, and operate a balanced enterprise cybersecurity program that is pragmatic and realistic in the face of resource constraints and other real-world limitations. This guide is an instructional companion to the book Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats. The study guide will help you understand the book’s ideas and put them to work. The guide can be used for self-study or in the classroom. Enterprise cybersecurity is about implementing a cyberdefense program that will succeed in defending against real-world attacks. While we often know what should be done, the resources to do it often are not sufficient. The reality is that the Cybersecurity Conundrum—what the defenders request, what the frameworks specify, and what the budget allows versus what the attackers exploit—gets in the way of what needs to be done. Cyberattacks in the headlines affecting millions of people show that this conundrum fails more often than we would prefer. Cybersecurity professionals want to implement more than what control frameworks specify, and more than what the budget allows. Ironically, another challenge is that even when defenders get everything that they want, clever attackers are extremely effective at finding and exploiting the gaps in those defenses, regardless of their comprehensiveness. Therefore, the cybersecurity challenge is to spend the available budget on the right protections, so that real-world attacks can be thwarted without breaking the bank. People involved in or interested in successful enterprise cybersecurity can use this study guide to gain insight into a comprehensive framework for coordinating an entire enterprise cyberdefense program. What You’ll Learn Know the methodology of targeted attacks and why they succeed Master the cybersecurity risk management process Understand why cybersecurity capabilities are the foundation of effective cyberdefenses Organize a cybersecurity program's policy, people, budget, technology, and assessment Assess and score a cybersecurity program Report cybersecurity program status against compliance and regulatory frameworks Use the operational processes and supporting information systems of a successful cybersecurity program Create a data-driven and objectively managed cybersecurity program Discover how cybersecurity is evolving and will continue to evolve over the next decade Who This Book Is For Those involved in or interested in successful enterprise cybersecurity (e.g., business professionals, IT professionals, cybersecurity professionals, and students). This guide can be used in a self-study mode. The book can be used by students to facilitate note-taking in the classroom and by Instructors to develop classroom presentations based on the contents of the original book, Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats.

Eons ago, the Conclave of Sensi chose Cera as a laboratory for creating consciousness. True, the work was experimental, but it had been successful long before the rebellion that threatened to destroy the planet. Led by the High Priestess Khyan and her first apostle, Rhee, ten members of the Khyan Circle of Fostering decide upon a desperate plan for survival. Escaping a fiery destruction is only the beginning. The bizarre world that appears beneath them demands new risks. They must become something far different than what they have been. High up in the Fourth Valley of the White Mountains in this strange new homeland, the repulsive upright ones await their destiny. They have lived here

for ages past, but they aren't prepared for life in the future. Symbolic features in Legend of the Fire Eye promise to give it a niche in the "New Myth" now being written. At the same time, it will fit well on the traditional fantasy bookshelf.

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).

The Oxford Handbook of Cyber Security presents forty-eight chapters examining the technological, economic, commercial, and strategic aspects of cyber security, including studies at the international, regional, amd national level.

Cyber security has become a topic of concern over the past decade as private industry, public administration, commerce, and communication have gained a greater online presence. As many individual and organizational activities continue to evolve in the digital sphere, new vulnerabilities arise. Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications contains a compendium of the latest academic material on new methodologies and applications in the areas of digital security and threats. Including innovative studies on cloud security, online threat protection, and cryptography, this multi-volume book is an ideal source for IT specialists, administrators, researchers, and students interested in uncovering new ways to thwart cyber breaches and protect sensitive digital information.

The United States is at a crossroads. Despite a defense budget that dwarfs that of any of the nation's rivals, the marginal return on this investment has decreased dramatically since the end of World War II. Why? Why have America's rivals, despite inferior resources, increasingly set the terms of international competition? How might America's leaders reconsider the application of power to ensure a favorable place on an increasingly crowded global stage? By tracing the geographic and historical development of four global actors--Russia, Iran, China, and the United States--Phillip T. Lohaus illuminates four equally distinct approaches to competition outside of warfare. He argues that while America's actions may have birthed information as a currency of power, the nation's failure to fully grasp the implications of this transition has created critical opportunities for its rivals to increase their power at the expense of the United States. The American way of competition, rooted in a scientific understanding of warfare, may impede effectiveness in the amorphous and unscientific landscape of twenty-first-century competition. From Rome to Britain, complacency has contributed to the downfall of many empires. Yet the slow bleed of American power may still be stanched by an approach to competition that emphasizes subtlety, diffusion, and ubiquity. America has developed and used these tools in the past--its very survival may hinge on returning to them. Power and Complacency defines the differing perspectives of America's international conflicts and offers possible solutions for reformulating its superpower strengths.

The availability of very large data sets and the increase in computing power to process them has led to a renewed intensity in corporate and governmental use of Artificial Intelligence (AI) technologies. This groundbreaking book, the first devoted entirely to the growing presence of AI in the legal profession, responds to the necessity of building up a discipline that due to its novelty requires the pooling of knowledge and experiences of well-respected experts in the AI field, taking into account the impact of AI on the law and legal practice. Essays by internationally known expert authors introduce the essentials of AI in a straightforward and intelligible style, offering jurists as many practical examples and business cases as possible so that they are able to understand the real application of this technology and its impact on their jobs and lives. Elements of the analysis include the following: crucial terms: natural language processing, machine learning and deep learning; regulations in force in major jurisdictions; ethical and social issues; labour and employment issues, including the impact that robots have on employment; prediction of outcome in the legal field (judicial proceedings, patent granting, etc.); massive analysis of documents and

identification of patterns from which to derive conclusions; AI and taxation; issues of competition and intellectual property; liability and responsibility of intelligent systems; AI and cybersecurity; AI and data protection; impact on state tax revenues; use of autonomous killer robots in the military; challenges related to privacy; the need to embrace transparency and sustainability; pressure brought by clients on prices; minority languages and AI; danger that the existing gap between large and small businesses will further increase; how to avoid algorithmic biases when AI decides; AI application to due diligence; AI and non-disclosure agreements; and the role of chatbots. Interviews with pioneers in the field are included, so readers get insights into the issues that people are dealing with in day-to-day actualities. Whether conceiving AI as a transformative technology of the labour market and training or an economic and business sector in need of legal advice, this introduction to AI will help practitioners in tax law, labour law, competition law and intellectual property law understand what AI is, what it serves, what is the state of the art and the potential of this technology, how they can benefit from its advantages and what are the risks it presents. As the global economy continues to suffer the repercussions of a framework that was previously fundamentally self-regulatory, policymakers will recognize the urgent need to formulate rules to properly manage the future of AI.

This best-selling guide provides a complete, practical, up-to-date introduction to network and computer security. SECURITY+ GUIDE TO NETWORK SECURITY FUNDAMENTALS, Fifth Edition, maps to the new CompTIA Security+ SY0-401 Certification Exam, providing thorough coverage of all domain objectives to help readers prepare for professional certification and career success. The text covers the essentials of network security, including compliance and operational security; threats and vulnerabilities; application, data, and host security; access control and identity management; and cryptography. The extensively updated Fifth Edition features a new structure based on major domains, a new chapter dedicated to mobile device security, expanded coverage of attacks and defenses, and new and updated information reflecting recent developments and emerging trends in information security, such as virtualization. New hands-on and case activities help readers review and apply what they have learned, and end-of-chapter exercises direct readers to the Information Security Community Site for additional activities and a wealth of learning resources, including blogs, videos , and current news and information relevant to the information security field. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Develop the advanced cybersecurity knowledge and skills for success on the latest CompTIA Cybersecurity Analyst certification exam (CySA+ CS0-002) with Ciampa's COMPTIA CYSA+ GUIDE TO CYBERSECURITY ANALYST (CS0-002), 2nd Edition. Updated, stair-stepped content builds on material you've previously mastered as you learn to analyze and interpret threat intelligence data, identify and address both external and internal vulnerabilities and respond effectively to cyber incidents. Each module opens with an actual, recent cybersecurity event that provides context for the information that follows. Quick review questions help test your understanding as you progress through content that completely maps to the latest CySA+ CS0-002 certification. New case projects and updates illustrate actual on-the-job tasks and procedures, including controls, monitoring, incident response and compliance, to further prepare you to meet the challenges in cybersecurity today. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

The implementation of wireless sensor networks has wide-ranging applications for monitoring various physical and environmental settings. However, certain limitations with these technologies must be addressed in order to effectively utilize them. The Handbook of Research on Advanced Wireless Sensor Network Applications, Protocols, and Architectures is a pivotal reference source for the latest research on recent innovations and developments in the field of wireless sensors. Examining the advantages and challenges presented by the application of these networks in various areas, this book is ideally designed for academics, researchers, students, and IT developers.

Competitors are contesting the rules of the international system and U.S. leadership and their approaches lie in the “gray zone.” The United States needs a concrete and actionable campaign plan is needed to deal with this challenge.

This book constitutes the refereed proceedings of the International Symposium on Security in Computing and Communications, SSCC 2015, held in Kochi, India, in August 2015. The 36 revised full papers presented together with 13 short papers were carefully reviewed and selected from 157 submissions. The papers are organized in topical sections on security in cloud computing; authentication and access control systems; cryptography and steganography; system and network security; application security.

Cyber Warfare: A Documentary and Reference GuideABC-CLIO

Cyberwars in the Middle East argues that hacking is a form of online political disruption whose influence flows vertically in two directions (top-bottom or bottom-up) or horizontally. These hacking activities are performed along three political dimensions: international, regional, and local. Author Ahmed Al-Rawi argues that political hacking is an aggressive and militant form of public communication employed by tech-savvy individuals, regardless of their affiliations, in order to influence politics and policies. Kenneth Waltz’s structural realism theory is linked to this argument as it provides a relevant framework to explain why nation-states employ cyber tools against each other. On the one hand, nation-states as well as their affiliated hacking groups like cyber warriors employ hacking as offensive and defensive tools in connection to the cyber activity or inactivity of other nation-states, such as the role of Russian Trolls disseminating disinformation on social media during the US 2016 presidential election. This is regarded as a horizontal flow of political disruption. Sometimes, nation-states, like the UAE, Saudi Arabia, and Bahrain, use hacking and surveillance tactics as a vertical flow (top-bottom) form of online political disruption by targeting their own citizens due to their oppositional or activists’ political views. On the other hand, regular hackers who are often politically independent practice a form of bottom-top political disruption to address issues related to the internal politics of their respective nation-states such as the case of a number of Iraqi, Saudi, and Algerian hackers. In some cases, other hackers target ordinary citizens to express opposition to their political or ideological views which is regarded as a horizontal form of online political disruption. This book is the first of its kind to shine a light on many ways that governments and hackers are perpetrating cyber attacks in the Middle East and beyond, and to show the ripple effect of these attacks.