Cyber Risks I Mia

MARISA HUERTA

Detecting and Mitigating Robotic Cyber Security Risks John Wiley & Sons
This book constitutes the proceedings of the 7th International Workshop on Graphical Models for Security, GramSec 2020, which took place on June 22, 2020. The workshop was planned to take place in Boston, MA, USA but changed to a virtual format due to the COVID-19 pandemic. The 7 full and 3 short papers presented in this volume were carefully reviewed and selected from 14 submissions. The papers were organized in topical sections named: attack trees; attacks and risks modelling and visualization; and models for reasoning about security.

How to Think about Homeland Security Oxford University Press
The Maidan Revolution in Ukraine created an opportunity for change and reforms in a system that had resisted them for 25 years. This report examines Ukraine’s security sector—assessing what different institutions need to do and where gaps exist—and offers recommendations for the reform of Ukraine’s security and defense institutions that meet Ukraine’s security needs and align with Euro-Atlantic standards and approaches.
Maritime Autonomous Surface Ships (MASS) - Regulation, Technology, and Policy Bloomsbury Publishing
To cope with the competitive worldwide marketplace, organizations rely on business intelligence to an increasing extent. Cyber security is an inevitable practice to protect the entire business sector and its customer. This book presents the significance and application of cyber security for safeguarding organizations, individuals’ personal information, and government. The book provides both practical and managerial implications of cyber security that also supports business intelligence and discusses the latest innovations in cyber security. It offers a roadmap to master degree students and PhD researchers for cyber security analysis in order to minimize the cyber security risk and protect customers from cyber-attack. The book also introduces the most advanced and novel machine learning techniques including, but not limited to, Support Vector Machine, Neural Networks, Extreme Learning Machine, Ensemble Learning, and Deep Learning Approaches, with a goal to apply those to cyber risk management

datasets. It will also leverage real-world financial instances to practise business product modelling and data analysis. The contents of this book will be useful for a wide audience who are involved in managing network systems, data security, data forecasting, cyber risk modelling, fraudulent credit risk detection, portfolio management, and data regulatory bodies. It will be particularly beneficial to academics as well as practitioners who are looking to protect their IT system, and reduce data breaches and cyber-attack vulnerabilities.

Accounting for U.S. POW/MIA's in Southeast Asia Rand Corporation

This collection of essays critically evaluates the legal framework necessary for the use of autonomous ships in international waters. The work is divided into three parts: Part 1 evaluates how far national shipping regulation, and the public international law background that lies behind it, may need modification and updating to accommodate the use of autonomous ships on international voyages. Part 2 deals with private law and insurance issues such as collision and pollution liability, salvage, limitation of liability and allocation of risk between carrier and cargo interests. Part 3 analyses international convention regimes dealing with maritime safety and other matters, arguing for specific changes in the existing conventions such as SOLAS and MARPOL, which would provide the international framework that is necessary for putting autonomous ships into commercial use. The book also takes the view that amendment of international conventions is important in the case of liability issues, arguing that leaving such matters to national law, particularly issues concerning product liability, could not only restrict or hinder the availability of liability insurance but also hamper the development of technology in this field. Written by internationally-known experts in their respective areas, the book offers a holistic approach to the debate on autonomous ships and makes a timely and important contribution to the literature.

Proceedings of the 5th International Conference on Water Resources (ICWR) – Volume 1 Springer Nature

This book constitutes the refereed proceedings of the 21th International Conference on Information and Communications Security, ICICS 2019, held in Beijing, China, in December 2019. The 47 revised full papers were carefully selected from 199 submissions. The papers are organized in topics on malware analysis and detection, IoT and CPS security enterprise network security, software security, system security, authentication, applied cryptograph internet security, machine learning security, machine learning privacy, Web security, steganography and steganalysis.

AI Applications in Cyber Security and Communication Networks Wolters Kluwer Italia

In "Dead Line - A Technological Dystopia" readers are taken on a thrilling journey through the world of cyber warfare, corruption, and moral dilemmas. The story opens with Professor Kurt Pellmann's harrowing experience of being trapped and tortured for information by the ruthless Agent Waltz from World Corp.'s Network Police. As Pellmann struggles to endure the relentless interrogation, he recalls his former student, Frederickson, whose loyalty is tested when he's asked to extract information from Pellmann. As the narrative unfolds, readers are introduced to Mia Seiert, a skilled cybersecurity expert. Her personal life is burdened by her mother's deteriorating health due to dementia induced by a tumor. Some day, she receives a mysterious message from her former professor, Pellmann. He reveals critical information about her aborted research on quantum encryption, linking it to staged terror attacks and corporate corruption. Mia's sense of purpose is reignited as she receives a flash drive containing the algorithm she developed years ago, leading her to uncover the truth about World Corp.'s sinister intentions. As Mia embarks on her investigation, the story explores her struggles with her past, relationships, and the pervasive influence of World Corp. The intricate web of power dynamics in the digital world becomes apparent as Mia faces mounting frustration and dead ends in her quest for evidence. Despite the isolation and pressure, Mia remains steadfast in her determination to expose the truth. The narrative takes a dark turn when Mia's investigation draws unwanted attention. The book's gripping plot and compelling characters draw readers into a world of secrets, betrayals, and the pursuit of justice. The story delves into the lengths people will go to protect the truth, the sacrifices made for the greater good, and the power of unity in the face of oppression.

Cyber Smart Taylor & Francis

When most of Eastern Europe was struggling with dictatorships of one kind or another, the Democratic Republic of Georgia (1918-1921) established a constitution, a parliamentary system with national elections, an active opposition, and a free press. Like the Democratic Republic of Georgia in 1918, its successors emerged after 1991 from a bankrupt empire, and faced, yet again, the task of establishing a new economic, political and social system from scratch. In both 1918 and 1991, Georgia was confronted with a hostile Russia and followed a pro-Western and pro-democratic course. The top regional experts in this book explore the domestic and external parallels between the Georgian post-colonial governments of the early twentieth and twenty-first centuries. How did the inexperienced Georgian leaders in both eras deal with the challenge of secessionism, what were their state building strategies, and what did democracy mean to them? What did their electoral systems look like, why were their economic strategies so different, and how did they negotiate with the international community neighbouring threats. These are the central challenges of transitional governments around the world today. Georgia’s experience over one hundred years suggests that both history and contemporary political analysis offer the best (and most interesting) explanation of the often ambivalent outcomes.

The Rules of Security IGI Global

This book demystifies and explains a subject that affects every one of us in our private lives and at work. Security is a practical discipline concerned with safeguarding lives, property, information, wealth, reputations, and social wellbeing. It is the basis of civilised society. People, businesses, and nations cannot thrive in its absence, whereas the right kind of security frees us to live fulfilling lives. But deciding what is needed, and then making it happen, is not easy. The threats to our security are complex and continually evolving, as criminals, hackers, terrorists, and hostile foreign states continually find new ways of staying one step ahead of us, their potential victims. At the same time, we are continually creating new vulnerabilities as we adopt new technologies and new ways of working. Those who do not understand the fundamentals of security, risk, and resilience open themselves, and those around them, to avoidable dangers, needless anxieties, and unnecessary costs. Inadequate security may leave them exposed to intolerable risks, while the wrong kind of security is expensive, intrusive, and ineffective. In his essential new book, world-leading security expert Paul Martin sets out the ten most important guiding principles of protective security and resilience. Clearly expressed in the form of simple but powerful rules of thumb, their purpose is to help solve complicated problems for which there are

no textbook solutions. The rules offer a powerful toolkit, designed to work in many different situations, including the cyber domain. When we are faced with novel problems requiring complex decisions, it is easy to focus on the wrong things. These rules remind us what really matters. The psychological and behavioural aspects of security are key themes throughout the book. People lie at the heart of security. The criminals, terrorists, and hackers are social animals with complex emotions and psychological predispositions. So too are the victims of those attackers and the security practitioners who strive to protect us. The human dimension is therefore crucial to understanding security. The Rules of Security will help anyone with an interest in their own security and that of their home, family, business, or society. It will be indispensable to those in positions of responsibility, allowing them to understand how best to protect their organisation, people, and assets. It assumes no expert technical knowledge and explains the ideas in clear and simple terms. It will appeal to anyone with an interest in security. If you read only one book about security, it should be this one.

Decision and Game Theory for Security epubli

This timely book offers up-to-date information for both researchers and decision makers regarding five core areas of Middle Eastern institutional and cultural context and its role in shaping business's strategies and practices in the region. The book is structured around four broad themes of: a) impact of corporate social responsibility and its reporting on different outcome variables related to performance, b) organizational change strategies, c) market entry strategies for the Middle East, and d) mergers and acquisitions in the MENA region. The analysis reveals the state of socio-cultural, historical and economic forces that shape business operations and management practices and processes in the region. It also highlights the research work undertaken by scholars along the above-mentioned themes over the last many decades in different Middle Eastern countries, what have been the dominant ideologies of the nations along with their institutional attributes, which have dictated the dominant management approaches in the region. The contributions included in the book also offer guidance for future research. The volume will appeal to researchers, scholars and students interested in business and management and corporate social responsibility. The chapters in this book were originally published as a special issue of International Studies of Management & Organization.

Security Sector Reform in Ukraine Routledge

In May 2021, Jim Gosler, known as the Godfather and commander of US agencies' cyber offensive capability, said, ''Either the Intelligence Community (IC) would grow and adapt, or the Internet would eat us alive.'' Mr Gosler was speaking at his retirement only several months before the terrorist attacks of 9/11. He possibly did not realise the catalyst or the tsunami that he and his tens of thousands of US IC offensive website operatives had created and commenced. Over the last two decades, what Mr Gosler and his army of Internet keyboard warriors created would become the modus operandi for every faceless, nameless, state-sponsored or individual cybercriminal to replicate against an unwary, ill-protected, and ignorant group of executives and security professionals who knew little to nothing about the clandestine methods of infiltration and weaponisation of the Internet that the US and UK agencies led, all in the name of security. This book covers many cyber and ransomware attacks and events, including how we have gotten to the point of massive digital utilisation, particularly during the global lockdown and COVID-19 pandemic, to online spending that will see twice the monetary amount lost to cybercrime than what is spent online. There is little to no attribution, and with the IC themselves suffering cyberattacks, they are all blamed on being sophisticated ones, of course. We are witnessing the undermining of our entire way of life, our economies, and even our liberties. The IC has lots to answer for and unequivocally created the disastrous situation we are currently in. They currently have little to no answer. We need—no, we must demand—change. That change must start by ensuring the Internet and all connections to it are secure and no longer allow easy access and exfiltration for both the ICs and cybercriminals.

Project SAVE Springer Nature

This fifth volume in the series comprises ten contributions written by an expert team of academics and practitioners. Collectively they analyse and expound many of the contemporary legal issues and debates in the law and practice of marine insurance. The new volume is not to be considered as a "new edition" superseding the earlier volumes. To the contrary, it extends on the previous coverage and contributes to the expanding coverage of the series. It achieves this by introducing new topics for analysis and by noting significant developments in themes considered in earlier volumes, thereby providing a useful tool for keeping abreast of an ever developing body of judicial law. This volume tackles topics such as the impact of the Insurance Act 2015 on remedies and the pre-contractual duty of insurers, as well as a contribution from Professor Wilhelmsen on the state ship arrest as a peril under the Nordic Marine Insurance Plan and London terms. It explores the impact of Brexit on jurisdiction in marine insurance whilst also dedicating time to the comparison of US and English law relating to the duties of brokers, and analyses the "but for" test in marine insurance as well as historical development of the law relating to fraudulent claims. Alongside many other important topics, this book meticulously examines Direct and Third-Party claims against P & I Insurers, Passenger liabilities and class actions, Seaworthiness and the operation of the MIA 1906 s.39 post Insurance Act 2015 and the insuring of autonomous and remote-controlled vessels. This book is essential reading for maritime lawyers, brokers and insurance market practitioners, academics, and companies associated with the marine insurance markets worldwide.

Ecological Security □□□□

As cyberspace continues to rapidly expand, its infrastructure is now an in- gral part of the world's economy and social structure. Given this increasing int- connectivity and interdependence, what progress has been made in developing an ecosystem of safety and security? This study is the second phase of an initial - tempt to survey and catalog the multitude of emerging organizations promoting global initiatives to secure cyberspace. The authors provide a breakdown and analysis of organizations by type, - cluding international, regional, private-public, and non-governmental organi- tions. Concluding with a discussion of the progress made in recent years, the study explores current trends regarding the effectiveness and scope of coverage provided by these organizations and addresses several questions concerning the overall state of international cyber security. The authors would like to thank Mr. Anthony Rutkowski for generously p- viding his time, guidance, and support. The authors would also like to thank the International Telecommunication Union (ITU) Telecommunication Development Sector (ITU-D) and the United States National Science Foundation (NSF Grant R3772) for partially supporting the research conducted in this study. In addition, the authors would like to thank the Georgia Institute of Technology's

Center for International Strategy, Technology, and Policy (CISTP) for assistance in hosting the Cyber Security Organization Catalog, and the Georgia Tech Information Se- rity Center (GTISC) for cooperation and promotion of this study. Table of Contents 1 The International Landscape of Cyber Security . . . . . 1 2 A Brief History of Global Responses to Cyber Threats . . . . . *Maritime Organisation, Management and Liability* Springer Nature
In today’s digital transformation environments, a rigorous cybersecurity approach to effective risk management — including contingency planning, outlining immediate actions, preparing post-breach responses — is central to defending organizations’ interconnected computer systems, networks, and infrastructure resources from malicious cyber-attacks. Specifically, cybersecurity technologies, processes, and practices need to be generalized and applied to intrusion detection and prevention measures. This entails analyzing profiles of cyber-attackers and building cyber-attack models for behavior simulation that can effectively counter such attacks. This comprehensive volume aims to cover all essential aspects of cybersecurity in digital transformation and to provide a framework for considering the many objectives and requirements involved. In addition to introducing theoretical foundations, the work also offers practical techniques for defending against malicious cybercriminals. Topics and features: Explores cybersecurity’s impact on the dynamics of interconnected, complex cyber- and physical systems, infrastructure resources, and networks Provides numerous examples of applications and best practices Considers methods that organizations can use to assess their cybersecurity awareness and/or strategy Describes anomaly intrusion detection, a key tool in thwarting both malware and theft (whether by insiders or external parties) of corporate data Addresses cyber-attacker profiles, cyber-attack models and simulation, cybersecurity ontology, access-control mechanisms, and policies for handling ransomware attacks Discusses the NIST Cybersecurity Framework, MITRE Adversarial Tactics, Techniques and Common Knowledge, CIS Critical Security Controls, and the ISA/IEC 62442 Cybersecurity Standard Gathering all the relevant information, this practical guide is eminently suitable as a self-study resource for engineers, scientists, computer scientists, and chief information officers. Further, with its many examples of best practices, it can serve as an excellent text for graduate-level courses and research into cybersecurity. Dietmar P. F. Möller, a retired full professor, is affiliated with the Institute for Mathematics at Clausthal University of Technology, Germany. He was an author of several other Springer titles, including Guide to Automotive Connectivity and Cybersecurity.
Securing Next-Generation Connected Healthcare Systems Walter de Gruyter GmbH & Co KG
The General Data Protection Regulation is the latest, and one of the most stringent, regulations regarding Data Protection to be passed into law by the European Union. Fundamentally, it aims to protect the Rights and Freedoms of all the individuals included under its terms; ultimately the privacy and security of all our personal data. This requirement for protection extends globally, to all organisations, public and private, wherever personal data is held, processed, or transmitted concerning any EU citizen. Cyber Security is at the core of data protection and there is a heavy emphasis on the application of encryption and state of the art technology within the articles of the GDPR. This is considered to be a primary method in achieving compliance with the law. Understanding the overall use and scope of Cyber Security principles and tools allows for greater efficiency and more cost effective management of Information systems.GDPR and Cyber Security for Business Information Systems is designed to present specific and practical information on the key areas of compliance to the GDPR relevant to Business Information Systems in a global context.
Cybersecurity Risk Management Springer Nature
This book outlines risk management theory systematically and comprehensively while distinguishing it from academic fields such as insurance theory. In addition, the book builds a risk financing theory that is independent of insurance theory. Until now, risk management (RM) theory has been discussed while the framework of the theory has remained unclear. However, this book, unlike previous books of this type, provides risk management theory after presenting a framework for it. Enterprise risk management (ERM) is seen differently depending on one’s position. For accountants, it is a means for internal control to prevent accounting fraud, whereas for financial institutions, it quantifies the risk that administrators can take to meet supervisory standards. Therefore, most of the ERM outlines are written to suit the intended uses or topics, with no systematic RM overviews. This book discusses a systematic RM theory linked to the framework of it, unlike previous books that were written according to topic. After the Enron scandal in December 2001 and WorldCom accounting fraud in June 2002, several laws were enacted or revised throughout the world, such as the SOX Act(Sarbanes-Oxley Act) in the United States and the Financial Instruments and Exchange Law and Companies Act in Japan. In this process, the COSO(Committee of Sponsoring Organizations of Treadway Commission) published their ERM framework, while the ISO (International Organization for Standardization) published their RM framework. The author believes that the competition between these frameworks was an opportunity to systematize RM theory and greatly develop it as an independent discipline from insurance. On the other hand, the Great East Japan Earthquake that occurred on March 11, 2011, caused enormous losses. Also, because pandemics and cyber risks are increasing, businesses must have a comprehensive and systematic ERM for these risks associated with their business activities
Artificial Intelligence and Autonomous Shipping Springer Science & Business Media
Risk detection and cyber security play a vital role in the use and success of contemporary computing. By utilizing the latest technological advances, more effective prevention techniques can be developed to protect against cyber threats. Detecting and Mitigating Robotic Cyber Security Risks is an essential reference publication for the latest research on new methodologies and applications in the areas of robotic and digital security. Featuring extensive coverage on a broad range of topics, such as authentication techniques, cloud security, and mobile robotics, this book is ideally designed for students, researchers, scientists, and engineers seeking current research on methods, models, and implementations of optimized security in digital contexts.
Cyber insurance: strategia, gestione e governance Springer Nature
CYBER INSURANCE: STRATEGIA, GESTIONE E GOVERNANCE è una guida nella comprensione e nella gestione del rischio cyber, contribuendo a costruire un ambiente digitale più sicuro e resiliente. Dopo aver analizzato la letteratura scientifica di riferimento sulla cyber

insurance, nonché la storia e l’evoluzione delle pratiche di assicurazione contro le minacce informatiche, il libro propone delle riflessioni sulla tecnologia e il cyber risk, esaminando le principali minacce e rischi. Successivamente, il volume esplora in dettaglio gli aspetti legali, etici e regolatori della cyber insurance, fornendo un'analisi approfondita delle normative vigenti e delle questioni etiche connesse alla gestione del rischio informatico. Viene, poi, presentata una disamina tecnico-pratica del mercato dell’assicurazione informatica, analizzando l'offerta, la domanda e le dinamiche in corso. Un capitolo significativo è dedicato all’ampia tematica delle tecnologie emergenti e degli impatti sulla cyber insurance, evidenziando come le nuove tecnologie stiano trasformando il panorama del rischio informatico e la gestione delle polizze assicurative. Vengono, inoltre, presentati i modelli di misurazione del rischio attualmente in uso per la cyber insurance, offrendo una panoramica delle metodologie e degli strumenti impiegati per valutare e quantificare il rischio cyber. A seguire, gli autori propongono una disamina dei sinistri cyber, illustrando alcune peculiarità e casi reali. Il manuale termina con una panoramica sul futuro della cyber insurance, proponendo conclusioni, tendenze, sfide e opportunità per i lettori che si stanno avvicinando al tema o per coloro che già si occupano professionalmente di questa materia.

Critical Information Infrastructure Protection and Resilience in the ICT Sector Bloomsbury Publishing

Securing Next-Generation Connected Healthcare Systems focuses on the crucial aspects of IoT security in a connected environment, which will not only benefit from cutting-edge methodological approaches but also assist in the rapid scalability and improvement of these systems. This book shows how to utilize technologies like blockchain and its integration with IoT for communication, data security, and trust management. This book will introduce the security aspect of next generation technologies for healthcare, covering a wide range of security and computing methodologies. Researchers, data scientists, students, and professionals interested in the application of artificial intelligence in healthcare management, data security of connected healthcare systems and related fields, specifically on data intensive secured systems and computing environments will finds this to be a welcomed resource. - Covers the latest next generation connected healthcare technologies using parallel computing - Presents all the security aspects in next-generation technologies for healthcare - Utilizes technologies such as blockchain and its integration with IoT for communication, data security, and trust management - Discusses privacy and security issues and challenges in data intensive cloud computing environment - Dives into the concept of parallel and distributed computing technologies and their applications in the real world

Information and Communications Security Cambridge University Press

The Armed Conflict Survey is the annual review of the political, military and humanitarian dimensions of all active conflicts from the International Institute for Strategic Studies. It offers in-depth analysis of the drivers, dynamics and outlook of 34 current armed conflicts along with detailed information on conflict parties and more than 60 full-colour maps and infographics. The Armed Conflict Survey is an essential resource for those involved in security, foreign and humanitarian policymaking, and an indispensable handbook for anyone conducting serious analysis of armed conflict. Key features · Essays on global trends in armed conflict, with a focus on the changing nature of third-party intervention, the long aftermath of armed conflicts, and economic migration and forced displacement in a COVID-19 world. · Overviews of key events and political and military developments from January 2020–February 2021 for each conflict. · Strategic analysis of national and regional drivers and conflict outlooks. · Regional analyses with unique insights into the geopolitical and geo-economic threads linking conflicts across regions and globally. · Expanded information on conflict parties. · The Armed Conflict Global Relevance Indicator (ACGRI), an IISS proprietary indicator that combines measures of incidence and human impact with geopolitical impact to assess the global salience of armed conflicts. · Analysis of the humanitarian, social and economic impact of conflicts. · Conflict-specific trends, strategic implications and prospects for peace. · More than 60 full-colour maps, tables and infographics highlighting key conflict developments and data. · Key statistics on violent events, fatalities, military power, geopolitical salience, refugees and internally displaced persons. · The 2021 Chart of Armed Conflict, presenting information on conflict start dates, typologies and relevant refugee flows, as well as providing a visual overview of each conflict’s geopolitical relevance, looking at 2020 UN Security Council resolutions, multilateral missions and the involvement of third-party countries.

Graphical Models for Security Routledge

Climate change is increasingly recognised as a security issue. Yet this recognition belies contestation over what security means and whose security is viewed as threatened. Different accounts – here defined as discourses – of security range from those focused on national sovereignty to those emphasising the vulnerability of human populations. This book examines the ethical assumptions and implications of these 'climate security' discourses, ultimately making a case for moving beyond the protection of human institutions and collectives. Drawing on insights from political ecology, feminism and critical theory, Matt McDonald suggests the need to focus on the resilience of ecosystems themselves when approaching the climate-security relationship, orienting towards the most vulnerable across time, space and species. The book outlines the ethical assumptions and contours of ecological security before exploring how it might find purchase in contemporary political contexts. A shift in this direction could not be more urgent, given the current climate crisis.

Related with Cyber Risks I Mia:

• Science Notebook Matter Properties And Changes Answers : click here