Aviation Crisis Management In Europe Enisa

If you ally craving such a referred **Aviation Crisis Management In Europe Enisa** ebook that will find the money for you worth, acquire the utterly best seller from us currently from several preferred authors. If you want to funny books, lots of novels, tale, jokes, and more fictions collections are next launched, from best seller to one of the most current released.

You may not be perplexed to enjoy every book collections Aviation Crisis Management In Europe Enisa that we will very offer. It is not nearly the costs. Its roughly what you dependence currently. This Aviation Crisis Management In Europe Enisa , as one of the most energetic sellers here will extremely be accompanied by the best options to review.

Current and Emerging Trends in Cyber Operations - Frederic Lemieux 2015-08-27
This book explores current and emerging trends in policy, strategy, and practice related to cyber operations conducted by states and non-state actors. The book examines in depth the nature and dynamics of conflicts in the cyberspace, the geopolitics of cyber conflicts, defence strategy and practice, cyber intelligence and information security.
Striking Back - Lucas Kello 2022-09-02
Conflict in the last century was defined by the horrific potential of physical and especially nuclear war. Now we are in a new technological era--a world of more subtle, yet no less grave, threats, an environment in which various actors can deeply penetrate vital infrastructures and instigate diplomatic and military crises. Today, computer code is the weapon of choice. Can anything be done beyond shoring up our defenses in a state of permanent insecurity? Lucas Kello delves into recent history to reveal the failures of the present policy in preventing and punishing cyberattacks and other forms of technological aggression. Drawing upon case studies and interviews, Kello develops a bold new solution--a coordinated retaliation strategy that justly and effectively responds to attacks and deters further antagonism. This book provides an approachable yet nuanced exploration of national security and survival in the twenty-first century.
Cybersecurity Best Practices - Michael Bartsch 2018-07-20
Das Thema Cybersecurity ist so aktuell wie nie, denn im Cyberspace lassen sich nur schwer Grenzen in Bezug auf den Zugang zu Informationen, Daten und Redefreiheit setzen. Kriminelle nutzen die Lücken oft zu ihrem Vorteil aus. Die Vielzahl der IT-Systeme, ihre unterschiedlichen Nutzungsarten und ihre Innovations- und Lebenszyklen haben zu hohen Sicherheitsrisiken für Unternehmen und staatliche Einrichtungen geführt. Diese Risiken werden sich auch langfristig nicht so einfach aus der Welt schaffen lassen. Daher müssen Institutionen Strategien und Lösungen zu ihrem Selbstschutz entwickeln. Dieses Buch beschreibt Lösungsansätze und Best Practices aus den unterschiedlichsten Bereichen, die nachweislich zu einer höheren Resilienz gegenüber Cyberangriffen führen. Weltweit renommierte IT-Sicherheitsexperten berichten in 40 Beiträgen, wie sich staatliche Institutionen, unter anderem das Militär (Cyber Defence), Behörden, internationale Organisationen und Unternehmen besser gegen Cyberangriffe schützen und nachhaltige Schutzstrategien entwickeln können. Die Autoren widmen sich den Gründen und Zielen, die ihren jeweiligen Strategien zugrunde liegen, sie berichten, wie Unternehmen auf konkrete Cyberattacken reagiert haben und wie einzelne staatliche Institutionen angesichts nationaler Cyberstrategien agieren. In weiteren Kapiteln zeigen Wissenschaftler auf, was bei der Abwehr von Cyber-Attacken bereits heute möglich ist, welche Entwicklungen in Arbeit sind und wie diese in Zukunft eingesetzt werden können, um die Cyber-Sicherheit zu erhöhen. Im letzten Kapitel berichten Hersteller, Anwenderunternehmen und Dienstleister welche Best Practices sie in ihren Unternehmen eingeführt haben und wie andere Unternehmen ihrem Beispiel folgen können. Das Buch richtet sich an IT-Verantwortliche und -Sicherheitsbeauftragte in Unternehmen und anderen Organisationen, aber auch an Studierende in den verschiedenen IT-Studiengängen.
Intelligence Security in the European Union - Artur Gruszczak 2016-08-05
This book investigates the emergence of an EU strategic intelligence community as a complex multi-dimensional networked construction. It examines the constitution, structure and performance of EU intelligence arrangements as part of security policies of the European Union. Intelligence security has become a remarkable feature of the European integration processes. This study assess the ability of EU Member States, as well as relevant institutions and agencies, to develop effective, legitimate and accountable institutions and mechanisms for collection, transmission, processing and exchange of intelligence. In this regard, synergy is a key indicator that validates the ability to create the European strategic intelligence community in the EU's legal and institutional framework. This groundbreaking project constructs a comprehensive model of the intelligence community as a distorted epistemic community tailored to singularities of EU security policies and systemic arrangements provided by EU institutions and agencies.
National cyber security : framework manual - Alexander Klimburg 2012
"What, exactly, is 'National Cyber Security'? The rise of cyberspace as a field of human endeavour is probably nothing less than one of the most significant developments in world history. Cyberspace already directly impacts every facet of human existence including economic, social, cultural and political developments, and the rate of change is not likely to stop anytime soon. However, the socio-political answers to the questions posed by the rise of cyberspace often significantly lag behind the rate of technological change. One of the fields most challenged by this development is that of 'national security'. The National Cyber Security Framework Manual provides detailed background information and in-depth theoretical frameworks to help the reader understand the various facets of National Cyber Security, according to different levels of public policy formulation. The four levels of government--political, strategic, operational and tactical/technical--each have their own perspectives on National Cyber Security, and each is addressed in individual sections within the Manual. Additionally, the Manual gives examples of relevant institutions in National Cyber Security, from top-level policy coordination bodies down to cyber crisis management structures and similar institutions."--Page 4 of cover.
Yearbook of European Law 2009 - Piet Eeckhout 2010-02-25
Now in its 28th year, the Yearbook of European Law is one of the most highly respected periodicals in the field. Featuring extended essays from leading scholars and practitioners, the Yearbook has become essential reading for all involved in European legal research and practice. This year's issue includes a special symposium on the recent Kadi case in the European Court of Justice, with contributions by Giorgio Gaja, Christian Tomuschat, Enzo Cannizzaro, Riccardo Pavoni and Martin Scheinin.
Research Anthology on Reliability and Safety in Aviation Systems, Spacecraft, and Air Transport - Management Association, Information Resources 2020-09-24
As with other transportation methods, safety issues in aircraft can result in a total loss of life. Recently, the air transport industry has come under immense scrutiny after several deaths occurred due to aircraft design and airlines that allowed improperly inspected aircraft to fly. Spacecraft too have found errors in system software that could lead to catastrophic failure. It is imperative that the aviation and aerospace industries continue to revise and refine safety protocols from the construction and design of aircraft, to secure and improve aviation systems, and to test and inspect aircraft. The Research Anthology on Reliability and Safety in Aviation Systems, Spacecraft, and Air Transport is a vital reference source that examines the latest scholarly material on the use of adaptive and assistive technologies in aviation to establish clear guidelines for the design and implementation of such technologies to better serve the needs of both military and civilian pilots. It also covers new information technology use in aviation systems to streamline the cybersecurity, decision making, planning, and design processes within the aviation industry. Highlighting a range of topics such as air navigation systems, computer simulation, and airline operations, this multi-volume book is ideally designed for pilots, scientists, engineers, aviation operators, air traffic controllers, air crash investigators, teachers, academicians, researchers, and students.
The European Union and Global Politics - Richard Youngs 2021-03-31
This accessible new textbook situates the European Union in a

Downloaded from wyoelks.org on by guest

dramatically changed world order. Resisting a more traditional and abstract introduction to the institutions, structures and policy making processes of the EU, this innovative new text cuts through the jargon to demonstrate how hard the EU must work to retain its international influence. Taking into account the latest empirical developments, including the spread of war and violence in the East with Ukraine and the ongoing turbulent politics of North Africa and the Middle East, Richard Youngs – an expert in the field – introduces us to how the EU has been forced to act differently. The book is unique in offering an outside-in conceptual framework that inverts the way that the EU external action is studied and understood. It unpacks the different international challenges the EU has faced in recent years, including the weakening of global order, the need for more protective security, geo-economic competition, climate change and conflicts to its east and south. In each case the book examines how the EU has responded and how its core international identity has changed as a result, assessing whether the Union still retains strong global influence. This book is the ideal companion for students taking modules on the European Union's foreign policy, global politics, and for students of European Union Politics more broadly at both undergraduate and postgraduate levels.

The EU Security Continuum - Alistair J.K. Shepherd 2021-09-06

This book examines how internal and external security are blurring at the EU level, and the implications this has for EU security governance and the EU as a security actor. The EU claims that 'internal and external security are inseparable' and requires a more integrated approach. This book critically assesses this claim in relation to the threats facing the EU, its responses to them, and the practical and normative implications for EU security governance and actorness. It sets out a novel conceptual framework – the EU security continuum - to examine the ways and extent to which internal and external security are blurring along three axes: geographic, bureaucratic, and functional. This is done through an analysis of four key security issues, regional conflict, terrorism, organised crime, and cybersecurity. The book demonstrates that, to varying degrees, these security threats and/or responses do transcend boundaries. However, institutional turf wars and capability silos hamper the EU's integrated approach and, therefore, its management of transboundary security threats. Yet, the EU's pursuit of an integrated approach is reframing its claimed normative distinctiveness toward a more practical one, based on a transnational and multidimensional approach. Such a rearticulation, if implemented, would make the EU a genuinely transboundary security actor, properly structured and equipped to tackle the 21st century's internal-external security continuum. This book will be of much interest to students of European Security, EU politics, and international relations.

ECCWS 2021 20th European Conference on Cyber Warfare and Security - Dr Thaddeus Eze 2021-06-24

Conferences Proceedings of 20th European Conference on Cyber Warfare and Security

EU Counterterrorism Policy - Oldrich Bures 2016-04-22

Although there is a vast body of literature covering the ongoing debates concerning the novelty and gravity of the contemporary terrorist threat, as well as the most appropriate response to it, few authors have thus far analysed the complex set of counterterrorism measures that both the individual Member States and the European Union (EU) have attempted to develop. This volume offers a critical analysis of the measures the European Union has taken to combat terrorism and how, in a number of key areas, EU counterterrorism policy is more of a paper tiger than an effective counterterrorism device. Several legal EU counterterrorism instruments have not been properly implemented at the national level and questions have been raised regarding their effectiveness, appropriateness, and proportionality. The capabilities of EU agencies in the area of counterterrorism remain rather weak and the EU Counterterrorism Coordinator does not have any real powers apart from persuasion. However, this does not mean that EU level action cannot offer any value-added in the fight against terrorism. There are several areas where the EU can provide genuine value-added in the fight against terrorism due to the transnational nature of the contemporary terrorist threat and the nature of a borderless Europe.

European Agencies - Madalina Busuioc 2013-02-28

European agencies have been created at a rapid pace in recent years in a multitude of highly pertinent and sensitive fields ranging from pharmaceuticals and aviation safety to chemicals or financial supervision. This agency phenomenon shows no signs of relenting, and the trend in recent years is towards the delegation of ever-broader powers. These bodies, meant to operate at arm's length from political control, have real power and their opinions and decisions can have a direct impact on individuals, regulators, and member states. Given the powers wielded by the agencies, who is responsible for holding these non-majoritarian actors to account? Is the growing concern surrounding agency accountability 'much ado about nothing' or are we faced with the threat of a powerful and unaccountable bureaucracy? These are precisely the questions that this book seeks to answer. It thus addresses one of the most relevant topics in current European governance: the accountability of European agencies. Scholars have increasingly called attention to the risk of placing too much power in the hands of such agencies, which operate at arm's length from traditional controls and cannot easily be held accountable for their actions. Although this is a major issue of concern, systematic empirical research into the topic is lacking. This book addresses empirically whether, and if so on what counts, agency accountability is problematic. It examines how the accountability system of European agencies operates at both the de jure as well as the de facto level, through an examination of legal provisions, relevant case law as well as policy documents and extensive interview material. Reflecting on these findings, the book also offers important theoretical insights for our understanding and study of accountability in a complex regulatory regime such as the EU context. The book follows a multi-disciplinary approach and is at the cutting edge of law and public administration.

Rewired - Ryan Ellis 2019-04-25

Examines the governance challenges of cybersecurity through twelve, real-world case studies Through twelve detailed case studies, this superb collection provides an overview of the ways in which government officials and corporate leaders across the globe are responding to the challenges of cybersecurity. Drawing perspectives from industry, government, and academia, the book incisively analyzes the actual issues, and provides a guide to the continually evolving cybersecurity ecosystem. It charts the role that corporations, policymakers, and technologists are playing in defining the contours of our digital world. Rewired: Cybersecurity Governance places great emphasis on the interconnection of law, policy, and technology in cyberspace. It examines some of the competing organizational efforts and institutions that are attempting to secure cyberspace and considers the broader implications of the in-place and unfolding efforts—tracing how different notions of cybersecurity are deployed and built into stable routines and practices. Ultimately, the book explores the core tensions that sit at the center of cybersecurity efforts, highlighting the ways in which debates about cybersecurity are often inevitably about much more. Introduces the legal and policy dimensions of cybersecurity Collects contributions from an international collection of scholars and practitioners Provides a detailed "map" of the emerging cybersecurity ecosystem, covering the role that corporations, policymakers, and technologists play Uses accessible case studies to provide a non-technical description of key terms and technologies Rewired: Cybersecurity Governance is an excellent guide for all policymakers, corporate leaders, academics, students, and IT professionals responding to and engaging with ongoing cybersecurity challenges.

Disaster Management: Enabling Resilience - Anthony Masys 2014-11-03

The present work will discuss relevant theoretical frameworks and applications pertaining to enabling resilience within the risk, crisis and disaster management domain. The contributions to this book focus on resilience thinking along 4 broad themes: Urban Domain; Cyber Domain; Organizational/Social domain; and Socio-ecological domain. This book would serve as a valuable reference for courses on risk, crisis and disaster management, international development, social innovation and resilience. This will be of particular interest to those working in the risk, crisis and disaster management domain as it will provide valuable insights into enabling resilience. This book will be well positioned to inform disaster management professionals, policy makers and academics on strategies and perspectives regarding disaster resilience.

Information and Cyber Security - Hein Venter 2020-03-07

This book constitutes the refereed proceedings of the 18th International Conference on Information Security, ISSA 2019, held in Johannesburg, South Africa, in August 2019. The 12 revised full papers presented were carefully reviewed and selected from 35 submissions. The papers are dealing with topics such as authentication; access control; digital (cyber) forensics; cyber security; mobile and wireless security; privacy-preserving protocols; authorization; trust frameworks; security requirements; formal security models; malware and its mitigation; intrusion detection systems; social engineering; operating systems security; browser security; denial-of-service attacks; vulnerability management; file system security; firewalls; Web protocol security;

Downloaded from wyoelks.org on by guest

digital rights management; distributed systems security.
Cyberwar and Information Warfare - Daniel Ventre 2012-12-27
Integrating empirical, conceptual, and theoretical approaches, thisbook presents the thinking of researchers and experts in the fieldsof cybersecurity, cyberdefense, and information warfare. The aim of this book is to analyze the processes of informationwarfare and cyberwarfare through the historical, operational andstrategic perspectives of cyberattacks. Cyberwar and Information Warfare is of extreme use to experts insecurity studies and intelligence studies, defense universities,ministries of defense and security, and anyone studying politicalsciences, international relations, geopolitics, informationtechnologies, etc.
European Union Agencies as Global Actors - Florin Coman-Kund 2018-05-01
This book examines a largely unexplored dimension of the European agencies, namely their role in EU external relations and on the international plane. International cooperation has become a salient feature of EU agencies triggering important legal questions regarding the scope and limits of their international dimension, the nature and effects of their international cooperation instruments, their status within the EU and on the global level, and leading potentially to tensions between EU law and international law. This book fills the existing knowledge gap by scrutinizing the international cooperation legal framework and practice of EU agencies, including their mandate, tasks and instruments, together with their legal status as actors with a global dimension. It sets out a general legal-analytical framework which combines legal parameters from EU and international law to assess EU agencies as global actors, and examines in detail three case studies on carefully selected agencies to shed light on the complexities of EU agencies' daily international cooperation.
After the Tsunami - 2005
The earthquake and tsunami of 26 December 2004 devastated coastal communities in 12 countries in the Indian Ocean region, with Aceh Province, Sumatra, Indonesia the hardest hit. This report sets out the findings of the UNEP Asian Tsunami Disaster Task Force, set up to help national environmental authorities in the affected countries with their assessment and response to the environmental impact of the disaster. It summarises the interim findings from ongoing assessments in Indonesia, the Maldives, the Seychelles, Somalia, Sri Lanka, Thailand and Yemen, including evidence of environmental concerns that require immediate action. The short term clean-up programme must be coupled with policy development and strengthened institutions, and the recovery agenda will require the clean-up of contamination hotspots, and rehabilitation of critical livelihoods and ecosystems.
The European Union as Crisis Manager - Arjen Boin 2013-08-08
This book provides a unique and comprehensive overview of the European Union's many crisis management capacities and explains their origins.
Enterprise Level Security 2 - Kevin E. Foltz 2020-09-11
Enterprise Level Security 2: Advanced Topics in an Uncertain World follows on from the authors' first book on Enterprise Level Security (ELS), which covered the basic concepts of ELS and the discoveries made during the first eight years of its development. This book follows on from this to give a discussion of advanced topics and solutions, derived from 16 years of research, pilots, and operational trials in putting an enterprise system together. The chapters cover specific advanced topics derived from painful mistakes and numerous revisions of processes. This book covers many of the topics omitted from the first book including multi-factor authentication, cloud key management, enterprise change management, entity veracity, homomorphic computing, device management, mobile ad hoc, big data, mediation, and several other topics. The ELS model of enterprise security is endorsed by the Secretary of the Air Force for Air Force computing systems and is a candidate for DoD systems under the Joint Information Environment Program. The book is intended for enterprise IT architecture developers, application developers, and IT security professionals. This is a unique approach to end-to-end security and fills a niche in the market.
Risks in Technological Systems - Göran Grimvall 2009-10-24
"Risks in Technological Systems" is an interdisciplinary university textbook and a book for the educated reader on the risks of today's society. In order to understand and analyze risks associated with the engineering systems on which modern society relies, other concerns have to be addressed, besides technical aspects. In contrast to many academic textbooks dealing with technological risks, this book has a unique interdisciplinary character that presents technological risks in their own context. Twenty-four scientists have come together to present their views on risks in technological systems. Their scientific disciplines cover not only engineering, economics and medicine, but also history, psychology, literature and philosophy. Taken together these contributions provide a broad, but accurate, interdisciplinary introduction to a field of increasing global interest, as well as rich opportunities to achieve in-depth knowledge of the subject.
The Institutions of the European Union - Dermot Hodson 2022
In a time of disruption and rapid change, the European Union's institutions have endured. In The Institutions of the European Union, a team of expert contributors and editors explain everything you need to know about the functions, powers, and composition of these important organizations as they contend with the changing dynamics of European integration. It is the most comprehensive guide to understanding how the institutions of the EU provide political direction, govern policies, and integrate contrasting interests within the EU. New to this Edition: Fully updated to cover the institutional changes prompted by Brexit, Covid-19, and many other issues facing the EU. A new introductory chapter presents the idea of EU institutional politics and explores its different dimensions. Explores the urgent challenges of creating more diverse and inclusive EU institutions. New discussion questions help you reflect critically and engage with the content to take your learning further. Professor Uwe Puetter of Europa-Universität Flensburg, and Sabine Saurugger of Science Po Grenoble-UGA, join Dermot Hodson as editors. Book jacket.
The External Dimension of the European Union's Critical Infrastructure Protection Programme - Alessandro Lazari 2022-06-27
External Dimension of the European Union's Critical Infrastructure Protection Programme: From Neighboring Frameworks to Transatlantic Cooperation provides the basis, methodological framework, and first comprehensive analysis of the current state of the external dimension European Programme for Critical Infrastructure Protection. The challenges at the EU level are multidimension insofar as identifying, designating and protecting critical infrastructures with the ultimate goal of harmonizing different national policies of the Member States and creating the identity of the European Union in this arena. Modern society has become so reliant on various sectors of critical infrastructure—energy, telecommunications, transport, finance, ICT, and public services—that any disruption may lead to serious failures that impact individuals, society, and the economy. The importance of critical infrastructures grows with the industrial development of global and national communities; their interdependence and resiliency is increasingly important given security threats including terrorism, natural disaster, climate change and pandemic outbreak In the area of Critical Infrastructure Protection and Resilience, the European Union is constantly committed to setting the objectives for the Member States. At the same time, the European Commission promotes the importance of a common approach to Critical Infrastructure Protection (CIP), and ensure cooperation beyond the borders of the Union, while also cooperating with neighboring countries, including those soon willing to join the European Union. This book has been structured and written to contribute to current critical infrastructures, resilience policy development and discussions about regional and international cooperation. It serves as a reference for those countries willing to initiate cooperation and that therefore demand deeper knowledge on the security cultures and frameworks of their potential partners. Features: Provides an unprecedented analysis of the national frameworks of 14 neighboring countries of the EU, plus the United States and Canada Overcomes the language barriers to provide an overall picture of the state of play of the countries considered Outlines the shaping of national critical infrastructure protection frameworks to understanding the importance of service stability and continuity Presents guidelines to building a comprehensive and flexible normative framework Addresses the strategic and operational importance of international co-operation on critical infrastructure including efforts in CIP education and training Provides insight to institutions and decision-makers on existing policies and ways to improve the European security agenda The book explains and advocates for establishing stronger, more resilient systems to preserve functionalities at the local, national, and international levels. Security, industry, and policy experts—both practitioners and policy decision-makers—looking for answers will find the solutions they seek within this book.
Cybersecurity - Federico Bergamasco 2020-07-09
Cybersecurity Key Legal Considerations for the Aviation and Space Sectors Federico Bergamasco, Roberto Cassar, Rada Popova & Benjamyn

Downloaded from wyoelks.org on by guest

I. Scott As the aviation and space sectors become ever more connected to cyberspace and reliant on related technology, they become more vulnerable to potential cyberattacks. As a result, cybersecurity is a growing concern that all stakeholders in both sectors must consider. In this forward-looking book, which is the first comprehensive analysis of the relevant facets of cybersecurity in the aviation and space sectors, the authors explore the vast spectrum of relevant international and European Union (EU) law, with specific attention to associated risks, existing legal provisions and the potential development of new rules. Beginning with an overview of the different types of malicious cyber operations, the book proceeds to set the terminological landscape relevant to its core theme. It takes a top-down approach by first analysing general international and EU law related to cybersecurity, then moving to the more specific aspects of the aviation and space sectors, including telecommunications. Finally, the salient features of these analyses are combined with the practical realities in the relevant industries, giving due regard to legal and regulatory initiatives, industry standards and best practices. The broad range of issues and topics covered includes the following and more: whether the various facets of the international law on conflict apply in cyberspace and to cyberattacks; substantial policy and regulatory developments taking place at the EU level, including the activities of its relevant institutions, bodies and entities; jurisdiction and attributability issues relevant to cybersecurity in the aviation and space sectors; vulnerability of space systems, including large constellations, to malicious cyber activities and electromagnetic interference; various challenges for critical infrastructure resulting from, e.g., its interdependency, cross-border nature, public-private ownership and dual civil-military uses; safety and security in international air transportation, with special attention to the Chicago Convention and its Annexes; aviation liability and compensation in cases of cyberattacks, and insurance coverage against cyber risks; review of malicious relevant actors, malicious cyber operations, the typical life cycle of a cyberattack and industry responses. This book clearly responds to the need to elaborate adequate legal rules for ensuring that the multiple inlets for malicious cyber operations and the management of cybersecurity risks are addressed appropriately. It will be welcomed by all parties involved with aviation and space law and policy, including lawyers, governments, regulators, academics, manufacturers, operators, airports, and international governmental and non-governmental organisations.

Crisis Management in the European Union - Stefan Olsson 2009-07-06

In less than a decade, Europe has witnessed a series of large-scale natural disasters and two major terrorist attacks. Growing concern about the trans-national effects of these incidents has caused the EU Member States to seek more multilateral cooperation. As a result, a system of common arrangements for handling large-scale emergencies or disasters has emerged, which, due to its quick and ad-hoc development, may seem almost impenetrable to newcomers to the field. This book seeks to provide a much-needed overview of disaster and crisis management systems in the EU. It provides a basic understanding of how EU policy has evolved, the EU's mandate, and above all, a concise and hands-on description of the most central crisis management arrangements. Written by some of Europe's main experts and consultants in the field, this book represents a unique and comprehensive source of information for everyone involved or interested in the European Union crisis management system. "This book will quickly become an indispensable resource for two groups: Practitioners will enjoy its accessible and comprehensive style. Academics curious about this emerging field will turn to it for an introductory overview. As someone who closely studies this field, I find the book engaging, detailed, and accurate, and I read every line with great interest. The authors are to be commended for the quality of research that went into this work." Mark Rhinard, Senior Research Fellow at the Swedish Institute of International Affairs (UI)

An Investigation into the Detection and Mitigation of Denial of Service (DoS) Attacks - S.V. Raghavan 2011-09-29

Around the globe, nations face the problem of protecting their Critical Information Infrastructure, normally referred to as Cyber Space. In this monograph, we capture FIVE different aspects of the problem; High speed packet capture, Protection through authentication, Technology Transition, Test Bed Simulation, and Policy and Legal Environment. The monograph is the outcome of over three years of cooperation between India and Australia.

Aviation in the Digital Age - Ruwantissa Abeyratne 2020-06-25

All of the topics discussed in this book – from sovereignty to cybercrime, and from drones to the identification of passengers & privacy – are profoundly affected by algorithms; so are air traffic services and aeronautical communications. All of these aviation-related aspects are addressed in a 75-year-old treaty called the Chicago Convention and its Annexes, which, as this book argues, needs to be reviewed with a focus on its relevance and applicability in connection with Moore's Law, which posits that transistors in computer microchips double in speed, power and performance every two years, while the cost of computers is halved during the same period. Firstly, in terms of traditional territorial sovereignty, we have arrived at a point where there is a concept of data sovereignty and ownership that raises issues of privacy. Data transmission becomes ambivalent in terms of territorial sovereignty, and the Westphalian model may not be the perfect answer. Whether it be the manufacture of airplanes, the transfer of data on individuals, or the transmission of aeronautical and telecommunications information – all have to be carried out in accordance with the same fundamental principle: duty of care. Against the backdrop of the relevant provisions of the Chicago Convention and its Annexes, the detailed analysis presented here covers key areas such as: megatrends; AI and international law in the digital age; blockchain and aviation; drones; aviation and telecommunications; aviation and the Internet; cybersecurity; and digital identification of passengers & privacy. In turn, the book suggests how we can best manage this transition.

ICCWS 2019 14th International Conference on Cyber Warfare and Security - Noëlle van der Waag-Cowling 2019-02-28

Air Transport and Pandemic Law - Ruwantissa Abeyratne 2021-07-27

The book discusses legal, ethical, economic and trade aspects of the Pandemic as it affects air transport. It commences with the chronology of the virus spread and examines the various facets of human existential perspectives affected by the pandemic. Following this background is an evaluation of the effect on trade and economics, as well as the legal and regulatory structure concerning communicable diseases applicable to air transport. There is also a detailed discussion on legal liabilities and responsibilities of the State, airlines, airports and public both collectively and individually in coping with the pandemic against the backdrop of public health and the law. The Conclusion contains various recommendations on proactive measures that could be taken to ensure the establishment of a credible and effective legal and regulatory system to combat future pandemics.

Research Anthology on Artificial Intelligence Applications in Security - Management Association, Information Resources 2020-11-27

As industries are rapidly being digitalized and information is being more heavily stored and transmitted online, the security of information has become a top priority in securing the use of online networks as a safe and effective platform. With the vast and diverse potential of artificial intelligence (AI) applications, it has become easier than ever to identify cyber vulnerabilities, potential threats, and the identification of solutions to these unique problems. The latest tools and technologies for AI applications have untapped potential that conventional systems and human security systems cannot meet, leading AI to be a frontrunner in the fight against malware, cyber-attacks, and various security issues. However, even with the tremendous progress AI has made within the sphere of security, it's important to understand the impacts, implications, and critical issues and challenges of AI applications along with the many benefits and emerging trends in this essential field of security-based research. Research Anthology on Artificial Intelligence Applications in Security seeks to address the fundamental advancements and technologies being used in AI applications for the security of digital data and information. The included chapters cover a wide range of topics related to AI in security stemming from the development and design of these applications, the latest tools and technologies, as well as the utilization of AI and what challenges and impacts have been discovered along the way. This resource work is a critical exploration of the latest research on security and an overview of how AI has impacted the field and will continue to advance as an essential tool for security, safety, and privacy online. This book is ideally intended for cyber security analysts, computer engineers, IT specialists, practitioners, stakeholders, researchers, academicians, and students interested in AI applications in the realm of security research.

The Cyber Threat and Globalization - Jack A. Jarmon 2018-06-26

This book is designed for those who want a better grasp of the nature and existential threat of today's information wars. It uses a conceptual approach to explain the relevant concepts as well as the structural challenges and responsibilities with which policy makers struggle and practitioners must work.

Downloaded from wyoelks.org on by guest

The Baltic Security Puzzle - Mary N. Hampton 2015-10-22
International experts assess the components of the Baltic security puzzle by placing the security and political interests of the states of Latvia, Estonia, and Lithuania within the historical, economic, and political narratives of the greater Baltic region. They first reevaluate Baltic history as a progression of conflict, partial integration, Cold War division, up to today's efforts to build a security community. Next, they focus on economic and social relations by contrasting patterns of democratization, domestic politics, EU membership, and the economics of crime. Lastly, they analyze military security and evolving regional perceptions of threats as well as the dynamics of alliance behavior and the recent geostrategic clashes unearthed by Russia's behavior in Ukraine.
Terrorism Online - Lee Jarvis 2015-03-24
This book investigates the intersection of terrorism, digital technologies and cyberspace. The evolving field of cyber-terrorism research is dominated by single-perspective, technological, political, or sociological texts. In contrast, Terrorism Online uses a multi-disciplinary framework to provide a broader introduction to debates and developments that have largely been conducted in isolation. Drawing together key academics from a range of disciplinary fields, including Computer Science, Engineering, Social Psychology, International Relations, Law and Politics, the volume focuses on three broad themes: 1) how – and why – do terrorists engage with the Internet, digital technologies and cyberspace?; 2) what threat do these various activities pose, and to whom?; 3) how might these activities be prevented, deterred or addressed? Exploring these themes, the book engages with a range of contemporary case studies and different forms of terrorism: from lone-actor terrorists and protest activities associated with 'hacktivist' groups to state-based terrorism. Through the book's engagement with questions of law, politics, technology and beyond, the volume offers a holistic approach to cyberterrorism which provides a unique and invaluable contribution to this subject matter. This book will be of great interest to students of cybersecurity, security studies, terrorism and International Relations.
Optimum Decision Making in Asset Management - Carnero, María Carmen 2016-08-24
Asset management is becoming increasingly important to an organization's strategy, given its effects on cost, production, and quality. No matter the sector, important decisions are made based on techniques and theories that are thought to optimize results; asset management models and techniques could help maximize effectiveness while reducing risk. Optimum Decision Making in Asset Management posits that effective decision making can be augmented by asset management based on mathematical techniques and models. Resolving the problems associated with minimizing uncertainty, this publication outlines a myriad of methodologies, procedures, case studies, and management tools that can help any organization achieve world-class maintenance. This book is ideal for managers, manufacturing engineers, programmers, academics, and advanced management students.
EU Administrative Law - Paul Craig 2018-10-25
The third edition of EU Administrative Law provides comprehensive coverage of the administrative system in the EU and the principles of judicial review that apply in this area. This revised edition provides important updates on each area covered, including new case law; institutional developments; and EU legislation. These changes are located within the framework of broader developments in the EU. The chapters in the first half of the book deal with all the principal variants of the EU administrative regime. Thus there are chapters dealing with the history and taxonomy of the EU administrative regime; direct administration; shared administration; comitology; agencies; social partners; and the open method of coordination. The coverage throughout focuses on the legal regime that governs the particular form of administration and broader issues of accountability, drawing on literature from political science as well as law. The focus in the second part of the book shifts to judicial review. There are detailed chapters covering all principles of judicial review and the discussion of the law throughout is analytical and contextual. It begins with the principles that have informed the development of EU judicial review. This is followed by a chapter dealing with the judicial system and the way in which reform could impact on the subject matter of the book. There are then chapters dealing with competence; access; transparency; process; law, fact and discretion; rights; equality; legitimate expectations; two chapters on proportionality; the precautionary principle; two chapters on remedies; and the Ombudsman.
Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Joshua B. Hill 2016-02-22
Explaining cybercrime in a highly networked world, this book provides a comprehensive yet accessible summary of the history, modern developments, and efforts to combat cybercrime in various forms at all levels of government—international, national, state, and local. • Provides accessible, comprehensive coverage of a complex topic that encompasses identity theft to copyright infringement written for non-technical readers • Pays due attention to important elements of cybercrime that have been largely ignored in the field, especially politics • Supplies examinations of both the domestic and international efforts to combat cybercrime • Serves an ideal text for first-year undergraduate students in criminal justice programs
Big Data Security - Shibakali Gupta 2019-10-08
THE SERIES: FRONTIERS IN COMPUTATIONAL INTELLIGENCE The series Frontiers In Computational Intelligence is envisioned to provide comprehensive coverage and understanding of cutting edge research in computational intelligence. It intends to augment the scholarly discourse on all topics relating to the advances in artifi cial life and machine learning in the form of metaheuristics, approximate reasoning, and robotics. Latest research findings are coupled with applications to varied domains of engineering and computer sciences. This field is steadily growing especially with the advent of novel machine learning algorithms being applied to different domains of engineering and technology. The series brings together leading researchers that intend to continue to advance the field and create a broad knowledge about the most recent research. Series Editor Dr. Siddhartha Bhattacharyya, CHRIST (Deemed to be University), Bangalore, India Editorial Advisory Board Dr. Elizabeth Behrman, Wichita State University, Kansas, USA Dr. Goran Klepac Dr. Leo Mrsic, Algebra University College, Croatia Dr. Aboul Ella Hassanien, Cairo University, Egypt Dr. Jan Platos, VSB-Technical University of Ostrava, Czech Republic Dr. Xiao-Zhi Gao, University of Eastern Finland, Finland Dr. Wellington Pinheiro dos Santos, Federal University of Pernambuco, Brazil
Challenges in Cybersecurity and Privacy - the European Research Landscape - Jorge Bernal Bernabe 2022-09-01
Cybersecurity and Privacy issues are becoming an important barrier for a trusted and dependable global digital society development. Cyber-criminals are continuously shifting their cyber-attacks specially against cyber-physical systems and IoT, since they present additional vulnerabilities due to their constrained capabilities, their unattended nature and the usage of potential untrustworthiness components. Likewise, identity-theft, fraud, personal data leakages, and other related cyber-crimes are continuously evolving, causing important damages and privacy problems for European citizens in both virtual and physical scenarios. In this context, new holistic approaches, methodologies, techniques and tools are needed to cope with those issues, and mitigate cyberattacks, by employing novel cyber-situational awareness frameworks, risk analysis and modeling, threat intelligent systems, cyber-threat information sharing methods, advanced big-data analysis techniques as well as exploiting the benefits from latest technologies such as SDN/NFV and Cloud systems. In addition, novel privacy-preserving techniques, and crypto-privacy mechanisms, identity and eID management systems, trust services, and recommendations are needed to protect citizens' privacy while keeping usability levels. The European Commission is addressing the challenge through different means, including the Horizon 2020 Research and Innovation program, thereby financing innovative projects that can cope with the increasing cyberthreat landscape. This book introduces several cybersecurity and privacy research challenges and how they are being addressed in the scope of 15 European research projects. Each chapter is dedicated to a different funded European Research project, which aims to cope with digital security and privacy aspects, risks, threats and cybersecurity issues from a different perspective. Each chapter includes the project's overviews and objectives, the particular challenges they are covering, research achievements on security and privacy, as well as the techniques, outcomes, and evaluations accomplished in the scope of the EU project. The book is the result of a collaborative effort among relative ongoing European Research projects in the field of privacy and security as well as related cybersecurity fields, and it is intended to explain how these projects meet the main cybersecurity and privacy challenges faced in Europe. Namely, the EU projects analyzed in the book are: ANASTACIA, SAINT, YAKSHA, FORTIKA, CYBECO, SISSDEN, CIPSEC, CS-AWARE. RED-Alert, Truessec.eu. ARIES, LIGHTest, CREDENTIAL, FutureTrust, LEPS. Challenges in Cybersecurity and Privacy - the European Research Landscape is ideal for personnel in

Downloaded from wyoelks.org on by guest

computer/communication industries as well as academic staff and master/research students in computer science and communications networks interested in learning about cyber-security and privacy aspects.

Multi-Objective and Multi-Attribute Optimisation for Sustainable Development Decision Aiding - Samarjit Kar 2019-09-20

Optimization is considered as a decision-making process for getting the most out of available resources for the best attainable results. Many real-world problems are multi-objective or multi-attribute problems that naturally involve several competing objectives that need to be optimized simultaneously, while respecting some constraints or involving selection among feasible discrete alternatives. In this Reprint of the Special Issue, 19 research papers co-authored by 88 researchers from 14 different countries explore aspects of multi-objective or multi-attribute modeling and optimization in crisp or uncertain environments by suggesting multiple-attribute decision-making (MADM) and multi-objective decision-making (MODM) approaches. The papers elaborate upon the approaches of state-of-the-art case studies in selected areas of applications related to sustainable development decision aiding in engineering and management, including construction, transportation, infrastructure development, production, and organization management.

Concise European Data Protection, E-Commerce and IT Law - Serge Gijrath 2018-11-23

Since the second edition (2010) of this invaluable book – primary texts with expert article-by-article commentary on European data protection, e-commerce and information technology (IT) regulation, including analysis of case law – there has been a marked shift in regulatory focus. It can be said that, without knowing it, EU citizens have migrated from an information society to a digital single market to a data-driven economy. This thoroughly revised and updated third edition pinpoints, in a crystal-clear format, the meaning and application of currently relevant provisions enacted at the European and Member State levels, allowing practitioners and other interested parties to grasp the exact status of such laws, whether in force, under construction, controversial or proposed. Material has been rearranged and brought into line with the vibrant and constantly shifting elements in this field, with detailed attention to developments (most new to this edition) in such issues as the following: · cybersecurity; · privacy rights; · supply of digital content; · consumer rights in electronic commerce; · Geo-blocking; · open Internet; · contractual rules for online sale of (tangible) goods; · competition law in the IT sectors; · consumer online dispute resolution; · electronic signatures; and · reuse of public sector information. There is a completely new section on electronic identification, trust and security regulation, defining the trend towards an effective e-commerce framework protecting consumers and businesses accessing content or buying goods and services online. The contributors offer a very useful and practical review and analysis of the instruments, taking into account the fluidity and the transiency of the regulation of these very dynamic phenomena. This book will be quickly taken up by the myriad professionals – lawyers, officials and academics – engaged with data protection, e-commerce and IT on a daily basis.

Downloaded from wyoelks.org on by guest