Budapest Convention On Cybercrime Wordpress


Cybercrime Modern societies are to a great extent dependent on computers and information systems, but there is a negative side to the use of information and communication technology – the rise of a new kind of criminality not traditionally addressed by the law. Technological developments and the changing nature of cybercrime itself force legislators to deal with new objects and redefine concepts. Taking into account legislative and case law developments, this book provides a thorough analysis of the legal regulation of attacks against information systems in European, international, and comparative law contexts. It covers legal issues not only pertaining to attacks arising in criminal law but also such...
crucial problems as the conflict of cybercrime investigation and prosecution with fundamental rights to privacy and freedom of expression. The authors’ in-depth response to doctrinal and practical issues related to the application of cybercrime regulation include such elements, issues, and aspects as the following: • legal harmonization of cybercrime law; • jurisdictional issues in the investigation and prosecution of cybercrime; • prevention of cyber attacks; • personal data and privacy implications; • hacking of cell phones; • enforcement and forensics in cybercrime law; • states and legal persons as perpetrators of cybercrime; • European Programme for Critical Infrastructure Protection; • Cybercrime Convention of 2001; • Directive 2013/40/EU; • identity theft; • the Snowden revelations and their lessons; • principles, problems, and shortcomings of digital evidence; • legal status of the IP address; • the security and data breach notification as a compliance and transparency tool; • profile and motivation of perpetrators of cyber attacks; • cybercrime as a parallel economy; and • use of cryptocurrency as a means for blackmail operations. Technical definitions, case law, and analysis of both substantive law and procedural law contribute to a comprehensive understanding of cybercrime regulation and its current evolution in practice.

Addressing a topic of growing importance in unprecedented detail, this book will be welcomed by professionals and authorities dealing with cybercrime, including lawyers, judges, academics, security professionals, information technology experts, and law enforcement agencies.

Cybersecurity The rapid development of information technology has exacerbated the need for robust personal data protection, the right to which is safeguarded by both European Union (EU) and Council of Europe (CoE) instruments. Safeguarding this important right entails new and significant challenges as technological advances expand the frontiers of areas such as surveillance, communication interception and data storage. This handbook is designed to familiarise legal practitioners not specialised in data protection with this emerging area of the law. It provides an overview of the EU’s and the CoE’s applicable legal frameworks. It also explains key case law, summarising major rulings of both the Court of Justice of the European Union and the European Court of Human Rights. In addition, it presents hypothetical scenarios that serve as practical illustrations of the diverse issues encountered in this ever-evolving field.

Disha 365 Current Affairs Analysis Vol. 2 for UPSC IAS/ IPS Prelim & Main Exams 2020 This updated edition of a well-known comprehensive analysis of the criminalization of cyberattacks adds important new guidance to the legal framework on cybercrime, reflecting new legislation, technological developments, and the changing nature of cybercrime itself. The focus is not only on criminal law aspects but also on issues of data protection, jurisdiction, electronic evidence, enforcement, and digital forensics. It provides a thorough analysis of the legal regulation of attacks against information systems in the European, international, and comparative law contexts. Among the new and continuing aspects of cybersecurity covered are the following: the conflict of cybercrime investigation and prosecution with fundamental rights to privacy and freedom of expression; the 2016 Directive on security of network and information systems (NIS Directive); the General Data Protection Regulation (GDPR); the role of national computer security incident response teams (CSIRTs); the European Union (EU) response to new technologies involving payment instruments, including virtual currencies and digital wallets; the EU Commission’s legislative proposals to enhance cross-border gathering of electronic evidence; internet service providers’ role in fighting cybercrime; measures combatting identity theft, spyware, and malware; states and legal persons as perpetrators of cybercrime; and the security and data breach notification as a compliance and transparency tool. Technical definitions, case law, and analysis of both substantive law and procedural law contribute to a comprehensive understanding of cybercrime regulation and its current evolution in practice.

Addressing a topic of growing importance in unprecedented detail, this new edition of a much-relied-upon resource will be welcomed by professionals and authorities dealing with cybercrime, including lawyers, judges, academics, security professionals, information technology experts, and law enforcement agencies.

Cybercrime Cybersecurity Key Legal Considerations for the Aviation and Space Sectors Federico Bergamasco, Roberto Cassar, Rada Popova & Benjamyn I. Scott As the aviation and space sectors become ever more connected to cyberspace and reliant on relevant 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 of 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.

EU Internet Law in the Digital Single Market Advancements in technology have seen gambling behaviour transverse a new path. The law has not kept pace with such advances, leaving grey areas of concern undisputed and unregulated. The authors provide a critical discussion on laws relating to gambling.

Council of Europe – Highlights 2019 This timely book examines crucial developments in the field of privacy law, efforts by legal systems to impose their data protection standards beyond their borders and claims by states to assert sovereignty over data. By bringing together renowned international privacy experts from the EU and the US, the book provides an accurate analysis of key trends and prospects in the transatlantic context, including spaces of tensions and cooperation between the EU and the US in the field of data protection law. The chapters explore recent legal and policy developments both in the private and law enforcement sectors, including recent rulings by the Court of Justice of the EU dealing with Google and Facebook, recent legislative initiatives in the EU and the US such as the CLOUD Act and the e-evidence proposal, as well as ongoing efforts to strike a transatlantic deal in the field of data sharing. All of the topics are thoroughly examined and presented in an accessible way that will appeal to scholars in the fields of law, political science and international relations, as well as to a wider and non-specialist audience. The book is an essential guide to understanding contemporary challenges to data protection across the Atlantic.

The Convention entered into force for the United Kingdom on 1 September 2011. The Convention was previously published as Miscellaneous No. 2 (2010) Cm 7862 (ISBN 9780101786225)

The Legal Regulation of Cyber Attacks

The Routledge Handbook of EU–Russia Relations As technology develops and internet-enabled devices become more prevalent new opportunities exist for that technology to be exploited by criminals. One result of this is that cybercrime is increasingly recognised as a distinct branch of criminal law. This book is designed for students studying cybercrime for the first time, enabling them to get to grips with an area of rapid change. The book offers a thematic and critical overview of cybercrime, introducing the key principles and clearly showing the connections between topics as well as highlighting areas subject to debate. Written with an emphasis on the law in the UK but considering in detail the Council of Europe’s important Convention on Cybercrime, this text also covers the jurisdictional aspects of cybercrime in international law. Themes discussed include crimes against computers, property, offensive content, and offences against the person, and recent controversial areas such as cyberterrorism and cyber-harassment are explored. Clear, concise and critical, this text offers a valuable overview of this fast-paced and growing area of law.

Comparative Criminology in Asia

The Legal Regulation of Cyber Attacks

The Routledge Handbook of EU–Russia Relations As technology develops and internet-enabled devices become ever more prevalent new opportunities exist for that technology to be exploited by criminals. One result of this is that cybercrime is increasingly recognised as a distinct branch of criminal law. This book is designed for students studying cybercrime for the first time, enabling them to get to grips with an area of rapid change. The book offers a thematic and critical overview of cybercrime, introducing the key principles and clearly showing the connections between topics as well as highlighting areas subject to debate. Written with an emphasis on the law in the UK but considering in detail the Council of Europe’s important Convention on Cybercrime, this text also covers the jurisdictional aspects of cybercrime in international law. Themes discussed include crimes against computers, property, offensive content, and offences against the person, and recent controversial areas such as cyberterrorism and cyber-harassment are explored. Clear, concise and critical, this text offers a valuable overview of this fast-paced and growing area of law.

Comparative Criminology in Asia
forms (robotics, anonymous payment), the opportunities and burdens of privacy self management, the differentiating role privacy can play in innovation. The book also discusses EU policies with respect to Big and Open Data and provides advice to policy makers regarding these topics. Also attention is being paid to regulation and its effects, for instance in case of the so-called 'EU-cookie law' and groundbreaking cases, such as Europe v. Facebook. This interdisciplinary book was written during what may turn out to be the final stages of the process of the fundamental revision of the current EU data protection law by the Data Protection Package proposed by the European Commission. It discusses open issues and daring and prospective approaches. It will serve as an insightful resource for readers with an interest in privacy and data protection.

Monthly Current Affairs August 2020 This volume introduces readers to regulatory theory. Aimed at practitioners, postgraduate students and those interested in regulation as a cross-cutting theme in the social sciences, Regulatory Theory includes chapters on the social-psychological foundations of regulation as well as theories of regulation such as responsive regulation, smart regulation and nodal governance. It explores the key themes of compliance, legal pluralism, meta-regulation, the rule of law, risk, accountability, globalisation and regulatory capitalism. The environment, crime, health, human rights, investment, migration and tax are among the fields of regulation considered in this groundbreaking book. Each chapter introduces the reader to key concepts and ideas and contains suggestions for further reading. The contributors, who either are or have been connected to the Regulatory Institutions Network (RegNet) at The Australian National University, include John Braithwaite, Valerie Braithwaite, Peter Grabosky, Neil Cunningham, Fiona Haines, Terry Halliday, David Levi-Faur, Christine Parker, Colin Scott and Clifford Shearing.

Convention on Cybercrime As this edition of the Council of Europe Highlights was being finalised, our societies were facing unprecedented medical, social and economic challenges due to the coronavirus crisis. The Council of Europe’s task is to assist our member states in making sure that the measures they take to fight the pandemic do not unduly risk the protection of our common European values of democracy, rule of law and human rights. We are reminded of the foundation of these values this year which marks the 70th anniversary of the European Convention on Human Rights. 2019 – the year covered by these Highlights - marked the 70th anniversary of the Treaty of London in 1949 when the Council of Europe was founded. Since then, Europe has undergone tectonic shifts of its political and economic landscape, not least with the emergence and enlargement of the European Union. The Council of Europe has maintained its own distinct role and place in the international institutional architecture. However, as many of the activities highlighted in this document demonstrate, the Council of Europe and the European Union now work together closely and in a complementary way in the interest of Europe’s citizens. Foreword by Daniel Höltgen (Director of Communications, Spokesperson for the Secretary General) This publication presents the work carried out in 2019 by the different bodies and sectors of the Council of Europe, highlighting its particular strengths and achievements.

Introduction to Cyber Politics and Policy

Cybersecurity in France As society continues to rely heavily on technological tools for facilitating business, e-commerce, banking, and communication, among other applications, there has been a significant rise in criminals seeking to exploit these tools for their nefarious gain. Countries all over the world are seeing substantial increases in identity theft and cyberattacks, as well as illicit transactions, including drug trafficking and human trafficking, being made through the dark web internet. Sex offenders and murderers explore unconventional methods of finding and contacting their victims through Facebook, Instagram, popular dating sites, etc., while pedophiles rely on these channels to obtain information and photographs of children, which are shared on hidden community sites. As criminals continue to harness technological advancements that are outpacing legal and ethical standards, law enforcement and government officials are faced with the challenge of devising new and alternative strategies to identify and apprehend criminals to preserve the safety of society. The Encyclopedia of Criminal Activities and the Deep Web is a three-volume set that includes comprehensive articles covering multidisciplinary research and expert insights provided by hundreds of leading researchers from 30 countries including the United States, the United Kingdom, Australia, New Zealand, Germany, Finland, South Korea, Malaysia, and more. This comprehensive encyclopedia provides the most diverse findings and new methodologies for monitoring and regulating the use of online tools as well as hidden areas of the internet, including the deep and dark web. Highlighting a wide range of topics such as cyberbullying, online hate speech, and hacktivism, this book will offer strategies for the prediction and prevention of online criminal activity and examine methods for safeguarding internet users and their data from being tracked or stalked. Due to the techniques and extensive knowledge discussed in this publication it is an invaluable addition for academic and corporate libraries as well as a critical resource for policy makers, law enforcement officials, forensic scientists, criminologists, sociologists, victim advocates, cybersecurity analysts, lawmakers, government officials, industry professionals, academicians, researchers, and students within this field of study.

The Legal Regulation of Cyber Attacks This compact, highly engaging book examines the international legal regulation of both the conduct of States among themselves and conduct towards individuals, in relation to the use of cyberspace. Chapters introduce the perspectives of various stakeholders and the challenges for international law. The author discusses State responsibility and key cyberspace rights issues, and takes a detailed look at cyber warfare, espionage, crime and terrorism. The work also covers the situation of non-State actors and quasi-State actors (such as IS, or ISIS, or ISIL) and concludes with a consideration of future prospects for the international law of cyberspace. Readers may explore international rules in the areas of jurisdiction of States in cyberspace, responsibility of States for cyber activities, human rights in the cyber world, permissible responses to cyber attacks, and more. Other topics addressed

Page 4/7
include the rules of engagement in cyber warfare, suppression of cyber crimes, permissible limits of cyber espionage, and suppression of cyber-related terrorism. Chapters feature explanations of case law from various jurisdictions, against the background of real-life cyber-related incidents across the globe. Written by an internationally recognized practitioner in the field, the book objectively guides readers through on-going debates on cyber-related issues against the background of international law. This book is very accessibly written and is an enlightening read. It will appeal to a wide audience, from international lawyers to students of international law, military strategists, law enforcement officers, policy makers and the lay person.

The Oxford Handbook of the International Law of Global Security The second edition of the definitive guide to cybersecurity law, updated to reflect recent legal developments The revised and updated second edition of Cybersecurity Law offers an authoritative guide to the key statutes, regulations, and court rulings that pertain to cybersecurity. Written by an experienced cybersecurity lawyer and law professor, the second edition includes new and expanded information that reflects the latest changes in laws and regulations. The book includes material on recent FTC data security consent decrees and data breach litigation. Topics covered reflect new laws, regulations, and court decisions that address financial sector cybersecurity, the law of war as applied to cyberspace, and recently updated guidance for public companies’ disclosure of cybersecurity risks. This important guide: Provides a new appendix, with 15 edited opinions covering a wide range of cybersecurity-related topics, for students learning via the caselaw method Includes new sections that cover topics such as: compelled access to encrypted devices, New York’s financial services cybersecurity regulations, South Carolina’s insurance sector cybersecurity law, the Internet of Things, bug bounty programs, the vulnerability equities process, international enforcement of computer hacking laws, the California Consumer Privacy Act, and the European Union’s Network and Information Security Directive Contains a new chapter on the critical topic of law of cyberwar Presents a comprehensive guide written by a noted expert on the topic Offers a companion Instructor-only website that features discussion questions for each chapter and suggested exam questions for each chapter Written for students and professionals of cybersecurity, cyber operations, management-oriented information technology (IT), and computer science, Cybersecurity Law, Second Edition is the up-to-date guide that covers the basic principles and the most recent information on cybersecurity laws and regulations. JEFF KOSSEFF is Assistant Professor of Cybersecurity Law at the United States Naval Academy in Annapolis, Maryland. He was a finalist for the Pulitzer Prize, and a recipient of the George Polk Award for national reporting.

Confronting Cyberespionage Under International Law


Data Protection Beyond Borders This Brief presents the overarching framework in which each nation is developing its own cyber-security policy, and the unique position adopted by France. Modern informational crises have penetrated most societal arenas, from healthcare, politics, economics to the conduct of business and welfare. Witnessing a convergence between information warfare and the use of “fake news”, info-destabilization, cognitive warfare and cyberwar, this book offers a unique perspective on modern cyberwarfare campaigns, escalation and de-escalation of cyber- conflicts. As organizations are more and more dependent on information for the continuity and stability of their operations, they also become more vulnerable to cyber-destabilization, either genuine, or deliberate for the purpose of gaining geopolitical advantage, waging wars, conducting intellectual theft and a wide range of crimes. Subsequently, the regulation of cyberspace has grown into an international effort where public, private and sovereign interests often collide. By analyzing the particular case of France national strategy and capabilities, the authors investigate the difficulty of obtaining a global agreement on the regulation of cyber-warfare. A review of the motives for disagreement between parties suggests that the current regulation framework is not adapted to the current technological change in the cybersecurity domain. This book suggests a paradigm shift in handling and anchoring cyber-regulation into a new realm of behavioral and cognitive sciences, and their application to machine learning and cyber-defense.

ECCWS 2017 16th European Conference on Cyber Warfare and Security

Research Anthology on Artificial Intelligence Applications in Security The Routledge Handbook of EU-Russia Relations offers a comprehensive overview of the changing dynamics in relations between the EU and Russia provided by leading experts in the field. Coherently organised into seven parts, the book provides a structure through which EU-Russia relations can be studied in a comprehensive yet manageable fashion. It provides readers with the tools to deliver critical analysis of this sometimes volatile and polarising relationship, so new events and facts can be conceptualised in an objective and critical manner. Informed by high-quality academic research and key bilateral data/statistics, it further brings scope, balance and depth, with chapters contributed by a range of experts from the EU, Russia and beyond. Chapters deal with a wide range of policy areas and issues that are highly topical and fundamental to understanding the continuing development of EU-Russia relations, such as political and security relations, economic relations, social relations and regional and global governance. The Routledge Handbook of EU-Russia Relations aims to promote dialogue between the different research agendas in EU-Russia relations, as well as between Russian and Western scholars and, hopefully, also between civil societies. As such, it will be an essential reference for scholars, students, researchers, policymakers and journalists interested and working in the fields of Russian politics/studies, EU studies/politics/EU-Russia politics/studies, post-Communist/post-Soviet politics and international relations. The Routledge Handbook of EU-Russia Relations is part of a mini-series Europe in the World Handbooks examining EU-regional relations established by Professor Wei Shen.
Financial Crime and Gambling in a Virtual World Cybercrimes are often viewed as technical offenses that require technical solutions, such as antivirus programs or automated intrusion detection tools. However, these crimes are committed by individuals or networks of people which prey upon human victims and are detected and prosecuted by criminal justice personnel. As a result, human decision-making plays a substantial role in the course of an offence, the justice response, and policymakers' attempts to legislate against these crimes. This book focuses on the human factor in cybercrime: its offenders, victims, and parties involved in tackling cybercrime. The distinct nature of cybercrime has consequences for the entire spectrum of crime and raises myriad questions about the nature of offending and victimization. For example, are cybercriminals the same as traditional offenders, or are there new offender types with distinct characteristics and motives? What foreground and situational characteristics influence the decision-making process of offenders? Which personal and situational characteristics provide an increased or decreased risk of cybercrime victimization? This book brings together leading criminologists from around the world to consider these questions and examine all facets of victimization, offending, offender networks, and policy responses.

Cybersecurity Law Seminar paper from the year 2018 in the subject Computer Science - Internet, New Technologies, language: English, abstract: Public Interest Litigation (PIL) is a relatively new topic in the legal arena. PIL in cybercrimes and internet-related issues brings about a spic and span area of debate and thoughts in the ever increasing spectrum of law. Both in Bangladesh and rest of the World it has become a hot stock. In this report I tried to find out the past and present scenarios of PIL in cybercrimes and internet-related issues. I have tried to interview the most prominent experts on cyber law and PIL from Bangladesh and abroad. I have taken help mainly from various authentic websites and books. The existing legal framework of PIL on cybercrimes is explored in this report before the analysis progress to the needs for regulatory reforms towards an effective legal regime. I hope this report will provide a valuable guideline to the policy makers for ensuring the prevention of cybercrimes.

Public International Law of Cyberspace

Policing in the Era of AI and Smart Societies The substantially revised second edition of the Handbook of Security provides the most comprehensive analysis of scholarly security debates and issues to date. Including contributions from some of the world's leading scholars it critiques the way security is provided and managed.

EU Cyber Security Strategy and Programs Handbook Volume 1 Strategic Information and Regulations Contrasts democratic and authoritarian approaches to international law, explaining how their interaction will affect the world in the future.

Data Protection on the Move Derived from the renowned multi-volume International Encyclopaedia of Laws, this practical analysis of the structure, competence, and management of The African Union (AU) provides substantial and readily accessible information for lawyers, academics, and policymakers likely to have dealings with its activities and data. No other book gives such a clear, uncomlicated description of the organization’s role, its rules and how they are applied, its place in the framework of international law, or its relations with other organizations. The monograph proceeds logically from the organization's genesis and historical development to the structure of its membership, its various organs and their mandates, its role in intergovernmental cooperation, and its interaction with decisions taken at the national level. Its competence, its financial management, and the nature and applicability of its data and publications are fully described. Systematic in presentation, this valuable time-saving resource offers the quickest, easiest way to acquire a sound understanding of the workings of The African Union (AU) for all interested parties. Students and teachers of international law will find it especially valuable as an essential component of the rapidly growing and changing global legal milieu.

Convention on Cybercrime We have witnessed a digital revolution that affects the dynamics of existing traditional social, economic, political and legal systems. This revolution has transformed espionage and its features, such as its purpose and targets, methods and means, and actors and incidents, which paves the way for the emergence of the term cyberespionage. This book seeks to address domestic and international legal tools appropriate to adopt in cases of cyberespionage incidents. Cyberespionage operations of state or non-state actors are a kind of cyber attack, which violates certain principles of international law but also constitute wrongful acquisition and misappropriation of the data. Therefore, from the use of force to state responsibility, international law offers a wide array of solutions; likewise, domestic regulations through either specialized laws or general principles stipulate civil and criminal remedies against cyberespionage. Confronting Cyberespionage Under International Law examines how espionage and its applications have transformed since World War II and how domestic and international legal mechanisms can provide effective legal solutions to this change, hindering the economic development and well-being of individuals, companies and states to the detriment of others. It shows the latest state of knowledge on the topic and will be of interest to researchers, academics, legal practitioners, legal advisors and students in the fields of international law, information technology law and intellectual property law.

Convention on Cybercrime Mauritius Internet and E-Commerce Investment and Business Guide - Strategic and Practical Information: Regulations and Opportunities

Regulatory Theory This edited volume presents the diversity of comparative criminology research in Asia, and the complex theoretical and methodological issues involved in conducting comparative research. With contributors both from the West and the East exploring these questions, the Editors have created a balanced resource, as well as set an agenda for future research. The increasing pace of globalization...
means that researchers should be armed with an understanding of how criminal justice systems work across the world. In the past, comparative research largely compared Western countries to each other, or involved researchers from a Western perspective examining an Asian country, with models and theories developed in the West considered to have universal applications. This work aims to correct that gap, by providing a critical examination of comparative research, presenting quantitative and qualitative research data, and asking new questions that challenge prevailing research norms and provide an agenda for future research. This work will be of interest for researchers across the field of Criminology, particularly those with an interest in International and Comparative Research, research on or about Asia, and related disciplines such as Sociology, Demography, and Social Policy. “This fine collection that goes to the rich distinctiveness of Asian criminology. The editors have brought together a wonderful collection of authors mainly from the region. The distinctiveness of values and relational practices in Asia are recurrent themes that are well developed in this book and help us to make sense of patterns of crime and criminal justice in Asia.” John Braithwaite, Australian National University “What theoretical, methodological, and practical issues must we confront in conducting cross-cultural studies encompassing Western and Asian countries? Comparative Criminology in Asia discusses these issues and presents exemplary comparative research. The introductory chapter and the introduction to each part by the co-editors are lucid and highly educational. This collection must be required reading for every serious scholar and aspiring graduate student in Asian countries so that criminological and criminal justice studies will be brought to a much higher level of sophistication.” Setsuo Miyazawa, UC Hastings “Can there be - and should there be -- a distinctive Asian criminology? What would this involve? The answer depends on what one thinks of the universalistic explanatory claims of Western criminology. Will these claims become self- fulfilling as these societies add to colonial influences a more deliberate borrowing of criminal justice models and established ways of pursuing discipline of criminology? Or will a more critical spirit prevail? This welcome edited collection by Liu, Travers and Chang provides an excellent starting point for reflecting on these and other questions. Rather than attempting to provide descriptions of the variety of similarities and differences in this region (though there are some fascinating case studies of these) the focus is even more on exploring the theoretical approaches and methodologies used in comparing institutional and cultural differences by Asian criminologists and others.” David Nelken, King’s College, London “Criminologists can no longer ignore the impact of globalization on the pattern and amount of crime as we experienced recently, nor can we ignore the global change of criminal justice policies to deal with crime. There is, therefore, a desperate need to collect data on how crime and criminal justice are influenced by globalization across Asian countries. On the other hand, there are debates on the issue of culture-specific vs. pan-culture theories of crime. This collection addresses both issues in an interesting way. Its publication is timely and welcome.” Chuen-Jim Sheu, National Taipei University Encyclopedia of Criminal Activities and the Deep Web

Handbook on European data protection law The book analyses a broad range of relevant aspects as the outer space and cyber space domain do not only present analogies but are also strongly interrelated. This may occur on various levels by technologies but also in regard to juridical approaches, each nevertheless keeping its particularities. Since modern societies rely increasingly on space applications that depend on cyber space, it is important to investigate how cyberspace and outer space are connected by their common challenges. Furthermore, this book discusses not only questions around their jurisdictions, but also whether the private space industry can escape jurisdiction by dematerializing the space resource commercial processes and assets thanks to cyber technology. In addition, space and cyberspace policies are analysed especially in view of cyber threats to space communications. Even the question of an extraterrestrial citizenship in outer space and cyberspace may raise new views. Finally, the interdependence between space and cyberspace also has an important role to play in the context of increasing militarization and emerging weaponization of outer space. Therefore, this book invites questioning the similarities and interrelations between Outer Space and Cyber Space in the same way as it intends to strengthen them.

Copyright code : a16e61038a06747d5773288c4ffeb2d00