Budapest Convention On Cybercrime Wordpress

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.

This handbook takes stock of the African Union's Vision 2020 to rid the African continent of wars, civil conflicts, human rights violations, and humanitarian disasters – including violent conflicts and genocide – and provides recommendations on how to address contemporary threats to peace and security in Africa. It explores the continent's current peace and security landscape, including new actors, emerging threats, and the prospects for achieving sustainable peace. With contributions from highly respected experts in the field, both academics and practitioners, the volume unpacks the sources of conflict, instability and the challenges of peace and development, and provides research-based policy advice to guide and inform African governments, policy makers, practitioners, and scholarly audiences on the continent and beyond.

Many international terrorist groups now actively use computers and the Internet to communicate, and several may develop or acquire the necessary technical skills to direct a co-ordinated attack against computers in the United States. A cyberattack intended to harm the U.S. economy would likely

target computers that operate the civilian critical infrastructure and government agencies. However, there is disagreement among some observers about whether a co-ordinated cyberattack against the U.S. critical infrastructure could be extremely harmful, or even whether computers operating the civilian critical infrastructure actually offer an effective target for furthering terrorists' goals. While there is no published evidence that terrorist organisations are currently planning a co-ordinated attack against computers, computer system vulnerabilities persist world-wide, and initiators of the random cyberattacks that plague computers on the Internet remain largely unknown. Reports from security organisations show that random attacks are now increasingly implemented through use of automated tools, called "bots", that direct large numbers of compromised computers to launch attacks through the Internet as swarms. The growing trend toward the use of more automated attack tools has also overwhelmed some of the current methodologies used for tracking Internet cyberattacks. This book provides background

information for three types of attacks against computers (cyberattack, physical attack, and electromagnetic attack), and discusses related vulnerabilities for each type of attack. The book also describes the possible effects of a co-ordinated cyberattack, or computer network attack (CNA), against U.S. infrastructure computers, along with possible technical capabilities of international terrorists. Issues for Congress may include how could trends in cyberattacks be measured more effectively; what is appropriate guidance for DOD use of cyberweapons; should cybersecurity be combined with, or remain separate from, the physical security organization within DHS; how can commercial vendors be encouraged to improve the security of their products; and what are options to encourage U.S. citizens to follow better cybersecurity practices? Appendices to this book describe computer viruses, spyware, and "bot networks", and how malicious programs are used to enable cybercrime and cyberespionage. Also, similarities are drawn between planning tactics currently used by computer hackers and those used by terrorists groups for

conventional attacks.

The federal computer fraud and abuse statute, 18 U.S.C. 1030, outlaws conduct that victimizes computer systems. It is a cyber security law which protects federal computers, bank computers, and computers connected to the Internet. It shields them from trespassing, threats, damage, espionage, and from being corruptly used as instruments of fraud. It is not a comprehensive provision, but instead it fills cracks and gaps in the protection afforded by other federal criminal laws. This report provides a brief sketch of Section 1030 and some of its federal statutory companions, including the amendments found in the Identity Theft Enforcement and Restitution Act, P.L. 110-326. Extensive appendices. This is a print on demand publication.

Cybersecurity Law

Computer Attack and Cyberterrorism

The Cambridge Handbook of Forensic Psychology

Cybercrime

Report (to Accompany Treaty Doc. 108-11).

Public International Law of Cyberspace

Now in its second edition, Cybercrime: Key Issues and Debatesprovides a valuable overview of this fast-paced and growing area of law. 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. The book offers readers 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, new to this edition, cybercrime investigation. Clear, concise and critical, this book is designed for students studying cybercrime for the first time, enabling them to get to grips with an area of rapid change. ybercrime investigation. Clear, concise and critical, this book is designed for students studying cybercrime for the first time, enabling them to get to grips with an area of rapid change.

"English translation originally published in 2016 by Faber and Faber Limited, Great Britain"--Title page verso.

This Major Reference Work synthesizes the global knowledge on cybercrime from the leading international criminologists and scholars across the social sciences. The constant evolution of technology and our relationship to devices and their misuse creates a complex

challenge requiring interdisciplinary knowledge and exploration. This work addresses this need by bringing disparate areas of social science research on cybercrime together. It covers the foundations, history and theoretical aspects of cybercrime, followed by four key sections on the main types of cybercrime: cyber-tresspass, cyber-deception/theft, cyber-porn and obscenity, and cyber-violence, including policy responses to cybercrime. This work will not only demonstrate the current knowledge of cybercrime but also its limitations and directions for future study.

The main Convention (2001) is also available (European Treaty series no. 185) (ISBN 9287148228)

A Global Survey

Handbook on European data protection law

Model-Driven Risk Analysis

EU Internet Law in the Digital Single Market

Control of File Exchange of Illicit Materials in Peer-to-Peer Environments

2018 Edition

In a world of increasing dependence on information technology, the prevention of cyberattacks on a nation's important computer and communications systems and networks is a problem that looms large. Given the demonstrated limitations of passive cybersecurity defense measures, it is natural to consider the possibility that deterrence might play a useful role in preventing cyberattacks against the United States and its vital interests. At the request of the Office of the

Director of National Intelligence, the National Research Council undertook a two-phase project aimed to foster a broad, multidisciplinary examination of strategies for deterring cyberattacks on the United States and of the possible utility of these strategies for the U.S. government. The first phase produced a letter report providing basic information needed to understand the nature of the problem and to articulate important questions that can drive research regarding ways of more effectively preventing, discouraging, and inhibiting hostile activity against important U.S. information systems and networks. The second phase of the project entailed selecting appropriate experts to write papers on questions raised in the letter report. A number of experts, identified by the committee, were commissioned to write these papers under contract with the National Academy of Sciences. Commissioned papers were discussed at a public workshop held June 10-11, 2010, in Washington, D.C., and authors revised their papers after the workshop. Although the authors were selected and the papers reviewed and discussed by the committee, the individually authored papers do not reflect consensus views of the committee, and the reader should view these papers as offering points of departure that can stimulate further work on the topics discussed. The papers presented in this volume are published essentially as received from the authors, with some proofreading corrections made as limited time allowed.

A comprehensive doctrinal analysis of cybercrime laws in four major common law jurisdictions: Australia, Canada, the UK and the US.

The result of a three-year project, this manual addresses the entire spectrum of international legal issues raised by cyber warfare.

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 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.

Routledge Handbook of International Cybersecurity

The CORAS Approach

Whether or not Nepalese legal standard address current and prospective modus operandi of cybercrime in Nepal?

Informing Strategies and Developing Options for U.S. Policy

Understanding Cybercrime

Jurisdiction and the Internet

This book examines how digital communications technologies have transformed modern societies, with profound effects both for everyday life, and for everyday crimes. Sexual violence, which is recognized globally as a significant human rights problem, has likewise changed in the digital age. Through an investigation into our increasingly and ever-normalised digital lives, this study analyses the rise of technology-facilitated sexual assault, ‘revenge pornography’, online sexual harassment and gender-based hate speech. Drawing on ground-breaking research into the nature and extent of technology-

facilitated forms of sexual violence and harassment, the authors explore the reach of these harms, the experiences of victims, the views of service providers and law enforcement bodies, as well as the implications for law, justice and resistance. Sexual Violence in a Digital Age is compelling reading for scholars, activists, and policymakers who seek to understand how technology is implicated in sexual violence, and what needs to be done to address sexual violence in a digital age.

This open access book provides the first comprehensive collection of papers that provide an integrative view on cybersecurity. It discusses theories, problems and solutions on the relevant ethical issues involved. This work is sorely needed in a world where cybersecurity has become indispensable to protect trust and confidence in the digital infrastructure whilst respecting fundamental values like equality, fairness, freedom, or privacy. The book has a strong practical focus as it includes case studies outlining ethical issues in cybersecurity and presenting guidelines and other measures to tackle those issues. It is thus not only relevant for academics but also for practitioners in cybersecurity such as providers of security software, governmental CERTs or Chief Security Officers in companies.

Cyber norms and other ways to regulate responsible state behavior in cyberspace is a fast-moving political and diplomatic field. The academic study of these processes is varied and interdisciplinary, but much of the literature has been organized according to

discipline. Seeking to cross disciplinary boundaries, this timely book brings together researchers in fields ranging from international law, international relations, and political science to business studies and philosophy to explore the theme of responsible state behavior in cyberspace. . Divided into three parts, Governing Cyberspace first looks at current debates in and about international law and diplomacy in cyberspace. How does international law regulate state behaviour and what are its limits? How do cyber superpowers like China and Russia shape their foreign policy in relation to cyberspace? The second focuses on power and governance. What is the role for international organisations like NATO or for substate actors like intelligence agencies? How do they adapt to the realities of cyberspace and digital conflict? How does the classic balance of power play out in cyberspace and how do different states position themselves? The third part takes a critical look at multistakeholder and corporate diplomacy. How do global tech companies shape their role as norm entrepreneurs in cyberspace, and how do their cyber diplomatic efforts relate to their corporate identity?

The development of computer technology and communication provided new means for th diffusion of illegal material, such as child pornographic images and videos. The legal framework to contrast that diffusion lies, at the European level, in EU Directive 2006/24/EC, after the Budapest Convention on Cybercrime, 2001, and in the various transposition laws by the member states (e. g. Law 48 in 2008 in Italy); it deals with:

common and shared definition of crimes, definition of enforcement powers, implementation of international cooperation, encouragement to the adoption of best practices sound from the juridical point of view and based on the state-of-art technological and scientific methods.In particular we examine the situation of child pornography related crimes: Internet users more and more have been using peer-to-peer networks and tools to exchange illicit material due to the ease to avoid interception by police and law enforcement investigations.When it becomes necessary to investigate a crime of this type, there are two main issues: difficulty to identify the crime, such as the exchange of illegal material on peer-to-peer network; and difficulty to analyze data: when a person, starting from an Internet address, is supposed guilty of a crime, quite often investigators have to manage a huge quantity of seized materials.Therefore investigators needs new strategies and software tools to support their tasks.We present Emulforensic, developed in Bologna, a tool to analyze the activities performed through eMule files, and make comparisons with other products that work in the same area such as EspiaMule, developed by Brazilian Federal Police, a software tool capable of monitoring the child pornographic file exchanges in peer-to-peer networks, and FIVES, developed by a European consortium led by Karlstadt University, a flexible software tool-set which allows law enforcement organizations to handle efficiently large amounts of image and video material related to child sexual abuse.We give, finally, an evaluation

and some comments about the trends of diffusion, at European level, of the exchange of materials about child pornography.

Governing Cyberspace

ASEAN Miracle

The Palgrave Handbook of Sustainable Peace and Security in Africa

An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws

Cyber crime strategy

Key Issues and Debates

Cybercrime is remarkably varied and widespread, and financial losses range from a few hundred dollars being extorted to multi-million dollar cyberfraud cases. Increasingly, cybercrime also involves the risk of terrorist attacks bringing down a major part of the Internet. Countries are discovering that it may be impossible for them to prosecute cybercriminals. Cybercrimes, unlike 'ordinary' crimes, are transnational in nature and it is often difficult to say just where they take place. This causes legal problems, since jurisdiction is usually still confined to the place where the crime was committed. A related issue is to what extent the police can investigate cybercrimes across borders, through the Internet: do they infringe the sovereignty of other countries? This

book surveys how these issues in cybercrime jurisdiction are dealt with by countries around the world, including the US, Japan, Korea, India, Brazil, Chile, Australia, New Zealand, Italy, Germany, Belgium, Denmark, and the UK. A score of experts assess how well the laws of their countries and the Cybercrime Convention deal with transnational cybercrime, and how jurisdiction conflicts should be resolved. With this in-depth survey of views and practices of cybercrime jurisdiction, the authors hope to contribute to a more concerted international effort towards effectively fighting cybercrime. The book is therefore highly recommended to policy-makers, members of the judiciary, academics and practitioners. Bert-Jaap Koops is Professor of Regulation & Technology at the Tilburg Institute for Law, Technology, and Society (TILT) of Tilburg University, The Netherlands. Susan W. Brenner is NCR Distinguished Professor of Law & Technology, University of Dayton School of Law, Ohio, US.

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. 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 crypto-currency 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.

Cyber attacks are on the rise. The media constantly report about data breaches and increasingly sophisticated cybercrime. Even governments are affected. At the same time, it is obvious that technology alone cannot solve the problem. What can countries do? Which issues can be addressed by policies and legislation? How to draft a good law? The report assists countries in understanding what cybercrime is about, what the challenges are in fighting such crime and supports them in drafting policies and laws.

Regulatory Competence over Online Activity

Behavior, Power and Diplomacy

A New Verse Translation

Convention on Cybercrime

The Relevance of the Istanbul Convention and the Budapest Convention on Cybercrime in Addressing Online and Technology-facilitated Violence Against Women

Aeneid Book VI

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.

The Legal Regulation of Cyber AttacksKluwer Law International B.V.

Diploma Thesis from the year 2014 in the subject Law - Comparative Legal Systems, Comparative Law, University of Oslo, course: LLM ICTL, language: English, abstract: Broadly, the thesis aims to resolve two research questions. Firstly, whether or not the legal regime of cybercrime in Nepal has been able to address current or prospective modus operandi of cyber related crime? And secondly, whether Nepalese legal regime related to cybercrime is in line with the standards set forth in Convention on Cybercrime, 2001 for addressing the

cybercrime?. The dissertation is substantially based on secondary resources such as scholar's article, books, and data from police, annual report of court and informal unstructured discussion with personnel from relevant authorities. Furthermore, the thesis has undertaken empirical study of cases and reports along with unstructured interview with relevant officials using random purposive sampling. After observation of secondary sources, unstructured interview, the paper has used primary sources such as treaties and laws to make a analytical study where the findings has been analyzed and conclusion has been drawn. 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.

International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked world

Proceedings of a Workshop on Deterring Cyberattacks

Principles of Cybercrime
Tallinn Manual on the International Law Applicable to Cyber Warfare
International cooperation in criminal matters
Budapest 23. XI. 2001

Forensic psychology has developed and extended from an original, narrow focus on presenting evidence to the courts to a wider application across the whole span of civil and criminal justice, which includes dealing with suspects, offenders, victims, witnesses, defendants, litigants and justice professionals. This Handbook provides an encyclopedic-style source regarding the major concerns in forensic psychology. It is an invaluable reference text for practitioners within community, special hospital, secure unit, prison, probation and law enforcement forensic settings, as well as being appropriate for trainees and students in these areas. It will also serve as a companion text for lawyers and psychiatric and law enforcement professionals who wish to be apprised of forensic psychology coverage. Each entry provides a succinct outline of the topic, describes current thinking, identifies relevant consensual or contested aspects and alternative positions. Readers are presented with key issues and directed towards specialized sources for further reference.

Which state has and should have the right and power to regulate sites and online events? Who can apply their defamation or contract law, obscenity standards, gambling or banking regulation, pharmaceutical licensing requirements or hate speech prohibitions to any particular Internet activity? Traditionally, transnational activity has been 'shared out' between national sovereigns with the aid of location-centric rules which can be adjusted to the transnational Internet. But can these allocation rules be stretched indefinitely, and what are the costs for online actors and for states themselves of squeezing global online activity into nation-state law? Does the future of online regulation lie in global legal harmonisation or is it a cyberspace that increasingly mirrors the national borders of the offline world? This 2007 book offers some uncomfortable insights into one of the most important debates on Internet governance.

This protocol covers the full range of research activities in the health field that involve interventions on human beings. It aims to protect the dignity and identity of everyone involved, without discrimination.

The Routledge Handbook of International Cybersecurity examines the development and use of information and communication technologies (ICTs) from the perspective of international peace and security. Acknowledging that the very notion of peace and security has become

more complex, the volume seeks to determine which questions of cybersecurity are indeed of relevance for international peace and security and which, while requiring international attention, are simply issues of contemporary governance or development. The Handbook offers a variety of thematic, regional and disciplinary perspectives on the question of international cybersecurity, and the chapters contextualize cybersecurity in the broader contestation over the world order, international law, conflict, human rights, governance and development. The volume is split into four thematic sections: Concepts and frameworks; Challenges to secure and peaceful cyberspace; National and regional perspectives on cybersecurity; Global approaches to cybersecurity. This book will be of much interest to students of cybersecurity, computer science, sociology, international law, defence studies and International Relations in general.

Additional Protocol to the Convention on Human Rights and Biomedicine, Concerning Biomedical Research

Cybercrime, Digital Forensics and Jurisdiction

Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems

Public Interest Litigation in Cyber Crimes and Internet-Related

Issues. Bangladesh and the Global Perspective
Cybercrime in Nepal

This book presents the latest and most relevant studies, surveys, and succinct reviews in the field of financial crimes and cybercrime, conducted and gathered by a group of top professionals, scholars, and researchers from China, India, Spain, Italy, Poland, Germany, and Russia. Focusing on the threats posed by and corresponding approaches to controlling financial crime and cybercrime, the book informs readers about emerging trends in the evolution of international crime involving cyber-technologies and the latest financial tools, as well as future challenges that could feasibly be overcome with a more sound criminal legislation framework and adequate criminal management. In turn, the book highlights innovative methods for combating financial crime and cybercrime, e.g., establishing an effective supervision system over P2P; encouraging financial innovation and coordination with international anti-terrorism organizations and multiple countries; improving mechanisms for extraditing and punishing criminals who defect to another

country; designing a protection system in accordance with internationally accepted standards; and reforming economic criminal offenses and other methods that will produce positive results in practice. Given its scope, the book will prove useful to legal professionals and researchers alike. It gathers selected proceedings of the 10th International Forum on Crime and Criminal Law in the Global Era (IFCCLGE), held on Nov 20–Dec 1, 2019, in Beijing, China.

The term "risk" is known from many fields, and we are used to references to contractual risk, economic risk, operational risk, legal risk, security risk, and so forth. We conduct risk analysis, using either offensive or defensive approaches to identify and assess risk. Offensive approaches are concerned with balancing potential gain against risk of investment loss, while defensive approaches are concerned with protecting assets that already exist. In this book, Lund, Solhaug and Stølen focus on defensive risk analysis, and more explicitly on a particular approach called CORAS. CORAS is a model-driven method for defensive risk analysis featuring a tool-supported modelling language specially designed to model risks. Their book serves as

an introduction to risk analysis in general, including the central concepts and notions in risk analysis and their relations. The authors' aim is to support risk analysts in conducting structured and stepwise risk analysis. To this end, the book is divided into three main parts. Part I of the book introduces and demonstrates the central concepts and notation used in CORAS, and is largely example-driven. Part II gives a thorough description of the CORAS method and modelling language. After having completed this part of the book, the reader should know enough to use the method in practice. Finally, Part III addresses issues that require special attention and treatment, but still are often encountered in real-life risk analysis and for which CORAS offers helpful advice and assistance. This part also includes a short presentation of the CORAS tool support. The main target groups of the book are IT practitioners and students at graduate or undergraduate level. They will appreciate a concise introduction into the emerging field of risk analysis, supported by a sound methodology, and completed with numerous examples and detailed guidelines.
The Association of Southeast Asian Nations is a miracle. Why?In

an era of growing cultural pessimism, many thoughtful individuals believe that different civilisations-especially Islam and the West-cannot live together in peace. The ten countries of ASEAN provide a thriving counter-example of civilizational co-existence. Here 625m people live together in peace. This miracle was delivered by ASEAN.In an era of growing economic pessimism, where many young people believe that their lives will get worse in coming decades, Southeast Asia bubbles with optimism. In an era where many thinkers predict rising geopolitical competition and tension, ASEAN regularly brings together all the world's great powers.Stories of peace are told less frequently than stories of conflict and war. ASEAN's imperfections make better headlines than its achievements. But in the hands of thinker and writer Kishore Mahbubani, the good news story is also a provocation and a challenge to the rest of the world.This excellent book explains, in clear and simple terms, how and why ASEAN has become one of the most successful regional organizations in the world. - George YeoA powerful and passionate account of how, against all odds, ASEAN transformed the region and why Asia and the world need it even more today. -

Amitav Acharya

The purpose of law is to prevent the society from harm by declaring what conduct is criminal, and prescribing the punishment to be imposed for such conduct. The pervasiveness of the internet and its anonymous nature make cyberspace a lawless frontier where anarchy prevails. Historically, economic value has been assigned to visible and tangible assets. With the increasing appreciation that intangible data disseminated through an intangible medium can possess economic value, cybercrime is also being recognized as an economic asset. The Cybercrime, Digital Forensics and Jurisdiction disseminate knowledge for everyone involved with understanding and preventing cybercrime - business entities, private citizens, and government agencies. The book is firmly rooted in the law demonstrating that a viable strategy to confront cybercrime must be international in scope.

Sexual Violence in a Digital Age

Phenomena, Challenges and Legal Response

The Ethics of Cybersecurity

Protecting Women and Girls from Violence in the Digital Age

(2021)
Cybercrime and Jurisdiction
The Legal Regulation of Cyber Attacks

With the ongoing evolution of the digital society challenging the boundaries of the law, new questions are arising – and new answers being given – even now, almost three decades on from the digital revolution. Written by a panel of legal specialists and edited by experts on EU Internet law, this book provides an overview of the most recent developments affecting the European Internet legal framework, specifically focusing on four current debates. Firstly, it discusses the changes in online copyright law, especially after the enactment of the new directive on the single digital market. Secondly, it analyzes the increasing significance of artificial intelligence in our daily life. The book then addresses emerging issues in EU digital law, exploring out of the box approaches in Internet law. It also presents the last cyber-criminality law trends (offenses, international instrument, behaviors), and discusses the evolution of personal data protection. Lastly, it evaluates the degree of consumer and corporate protection in the digital environment, demonstrating that now, more than ever, EU Internet law is based on a combination of copyright, civil, administrative, criminal, commercial and banking laws.

The Istanbul Convention is the most far-reaching international treaty to tackle violence against women and domestic violence. Its comprehensive set of provisions spans far-

ranging preventive and protective measures as well as a number of obligations to ensure an adequate criminal justice response to such serious violations of human rights. The Budapest Convention on Cybercrime is the most relevant international agreement on cybercrime and electronic evidence. It provides for the criminalisation of offences against and by means of computers, procedural law tools to secure electronic evidence, and for international co-operation among Parties.

The Government published the UK Cyber Security Strategy in June 2009 (Cm. 7642, ISBN 97801017674223), and established the Office of Cyber Security to provide strategic leadership across Government. This document sets out the Home Office's approach to tackling cyber crime, showing how to tackle such crimes directly through the provision of a law enforcement response, and indirectly through cross-Government working and through the development of relationships with industry, charities and other groups, as well as internationally. The publication is divided into five chapters and looks at the following areas, including: the broader cyber security context; cyber crime: the current position; the Government response and how the Home Office will tackle cyber crime.

Convention Européenne Sur la Violence Et Les Débordements de Spectateurs Lors de Manifestations Sportives Et Notamment de Matches de Football

The Palgrave Handbook of International Cybercrime and Cyberdeviance

Cybercrimes and Financial Crimes in the Global Era
Additional Protocol to the European Outline Convention on Transfrontier Co-operation Between Territorial Communities Or Authorities
Council of Europe Convention on Cybercrime (Treaty Doc. 108-11)