Cybercrime Criminal Threats From Cyberspace Crime Media And Popular Culture

This book examines the European arrest warrant as a successful and effective instrument for judicial co-operation in criminal matters in the European Union. Providing comprehensive content and combining theoretical and practical aspects, it covers all of the major issues surrounding the European arrest warrant. The book analyses its genesis, main features, surrender procedure, case law, implementation and the latest developments. Instead of focusing solely on a criminal law approach, it also considers the subject from the perspective of European Union law and constitutional law.

"This 10-volume compilation of authoritative, research-based articles contributed by thousands of researchers and experts from all over the world emphasized modern issues and the presentation of potential opportunities, prospective solutions, and future directions in the field of information science and technology"--Provided by publisher.

A current, behind-the-scenes introduction to the rapidly evolving phenomenon of domestic and international cybercrime, including new coverage of cyberterrorism, cyberwarfare, and emerging cyberthreats. * Provides an accessible,

comprehensive, and interesting overview of cybercrime and what it means for the average citizen * Explains why domestic law enforcement (state and federal) is essentially ineffective against the cybercrime that primarily comes from abroad * Underscores the serious threat and risk to all U.S. citizens and corporate entities of having their private data, money, and online systems stolen by cybercriminals—thieves that can confidently operate with impunity from being caught or prosecuted * Provides insights from an highly respected expert author and speaker on the subjects of cybercrime, cyberterrorism, and cyberwarfare Never HIGHLIGHT a Book Again Includes all testable terms, concepts, persons, places, and events. Cram101 Just the FACTS101 studyguides gives all of the outlines, highlights, and quizzes for your textbook with optional online comprehensive practice tests. Only Cram101 is Textbook Specific. Accompanies: 9780872893795. This item is printed on demand.

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. Never HIGHLIGHT a Book Again! Virtually all of the testable terms, concepts, persons, places, and events from the textbook are included. Cram101 Just the FACTS101 studyguides give all of the outlines, highlights, notes, and quizzes for your textbook with optional online comprehensive practice tests. Only Cram101 is Textbook Specific. Accompanys: 9780313365461 .

"Digital Evidence and Computer Crime" provides the knowledge necessary to uncover and use digital evidence effectively in any kind of investigation. This completely updated edition provides the introductory materials that new students require, and also expands on the material presented in previous editions to help students develop these skills.

Cybercriminals are criminals in the truest sense of the word. However, their techniques are highly specialized and technical. Their crimes are high-impact and often global, but, simultaneously, they are difficult to trace, often leading investigators on thrilling chases in an underworld society of coders and hackers.

To combat the devastating work of cybercriminals, the need for cybercrime investigators has increased exponentially. This book will introduce readers to the dark world of cybercrime, the various disguises cybercrime can take, and the increased need to combat cybercrime, as well as highlight the fascinating world of cybercrime investigation, including training, education, real-world cases, and typical salary ranges.

"Read about this history of cybercrime, and learn about the different types of scams--from phising to spam to hacking--that take place on the internet"--Provided by publisher.

Digital technology has revitalized the landscape of the global economy. As digital currency, such as bitcoin and IOTA, continues to become more prominent in society, conducting further research in this area is vital to promoting economic advancements. Digital Currency: Breakthroughs in Research and Practice is a critical source of academic knowledge on the use of computers, smartphones, and the internet to purchase goods and services using virtual currency. The security and privacy aspects of using digital currency are also explored. Highlighting a range of pertinent topics such as electronic commerce, online transaction payment, and web-based electronic money, this book is an ideal reference source for business executives, financial analysts, business

professionals, economists, IT professionals, and researchers interested in emerging trends in digital currency and finance.

Since the birth of criminal copyright in the nineteenth century, the copyright system has blurred the distinction between civil and criminal infringements. Today, in many jurisdictions, infringement of copyrighted materials can result in punitive fines and even incarceration. In this illuminating book, Eldar Haber analyses the circumstances, justifications, and ramifications of the criminalization process and tells the story of how a legal right in the private enforcement realm has become over-criminalized. He traces the origins of criminal copyright legislation and follows the movement of copyright criminalization and enforcement on local and global scales. This important work should be read by anyone concerned with the future of copyright and intellectual property in the digital era.

The manner in which criminal investigators are trained is neither uniform nor consistent, ranging from sophisticated training protocols in some departments to on-the-job experience alongside senior investigators in others. Ideal for students taking a first course in the subject as well as professionals in need of a refresher, Introduction to Crimin

Research on cybercrime has been largely bifurcated, with social science and

computer science researchers working with different research agendas. These fields have produced parallel scholarship to understand cybercrime offending and victimization, as well as techniques to harden systems from compromise and understand the tools used by cybercriminals. The literature developed from these two fields is diverse and informative, but until now there has been minimal interdisciplinary scholarship combining their insights in order to create a more informed and robust body of knowledge. This book offers an interdisciplinary approach to research on cybercrime and lays out frameworks for collaboration between the fields. Bringing together international experts, this book explores a range of issues from malicious software and hacking to victimization and fraud. This work also provides direction for policy changes to both cybersecurity and criminal justice practice based on the enhanced understanding of cybercrime that can be derived from integrated research from both the technical and social sciences. The authors demonstrate the breadth of contemporary scholarship as well as identifying key questions that could be addressed in the future or unique methods that could benefit the wider research community. This edited collection will be key reading for academics, researchers, and practitioners in both computer security and law enforcement. This book is also a comprehensive resource for postgraduate and advanced undergraduate students undertaking

courses in social and technical studies.

Providing scholars with a comprehensive international resource, a common point of entry into cutting edge contemporary research and a snapshot of the state and scope of the field, this Handbook takes a broad approach to its subject matter, disciplinarily, geographically, and systemically.

Cybercrime has become increasingly prevalent in the new millennium as computer-savvy criminals have developed more sophisticated ways to victimize people online and through other digital means. The Law of Cybercrimes and Their Investigations is a comprehensive text exploring the gamut of issues surrounding this growing phenomenon. After an introduction to the history of computer crime, the book reviews a host of topics including: Information warfare and cyberterrorism Obscenity, child pornography, sexual predator conduct, and online gambling Cyberstalking, cyberharassment, cyberbullying, and other types of unlawful expression Auction fraud, Ponzi and pyramid schemes, access device fraud, identity theft and fraud, securities and bank fraud, money laundering, and electronic transfer fraud Data privacy crimes, economic espionage, and intellectual property crimes Principles applicable to searches and seizures of computers, other digital devices, and peripherals Laws governing eavesdropping, wiretaps, and other investigatory devices The admission of digital evidence in

court Procedures for investigating cybercrime beyond the borders of the prosecuting jurisdiction Each chapter includes key words or phrases readers should be familiar with before moving on to the next chapter. Review problems are supplied to test assimilation of the material, and the book contains weblinks to encourage further study.

This book focuses on the phenomenon of hacktivism and how it has been dealt with up to now in the United States and the United Kingdom. After discussing the birth of the phenomenon and the various relevant groups, from Electronic Disturbance Theater to Anonymous, their philosophies and tactics, this timely and original work attempts to identify the positive and negative aspects hacktivism through an analysis of free speech and civil disobedience theory. Engaging in this process clarifies the dual nature of hacktivism, highlighting its potential for positive contributions to contemporary politics, whilst also demonstrating the risks and harms flowing from its controversial and legally ambiguous nature. Based on this hybrid nature of hacktivism, Karagiannopoulos proceeds to offer a critique of the current responses towards such practices and their potential for preserving the positive elements, whilst mitigating the risks and harms involved in such political practices. Finally, the study focuses on identifying an alternative, symbiotic rationale for responding to hacktivism, based on a

cluster of micro-interventions moving away from the conflict-based criminal justice model and the potentially unjust and inefficacious results it entails. Strategic Intelligence Management introduces both academic researchers and law enforcement professionals to contemporary issues of national security and information management and analysis. This contributed volume draws on state-of-the-art expertise from academics and law enforcement practitioners across the globe. The chapter authors provide background, analysis, and insight on specific topics and case studies. Strategic Intelligent Management explores the technological and social aspects of managing information for contemporary national security imperatives. Academic researchers and graduate students in computer science, information studies, social science, law, terrorism studies, and politics, as well as professionals in the police, law enforcement, security agencies, and government policy organizations will welcome this authoritative and wide-ranging discussion of emerging threats. Hot topics like cyber terrorism, Big Data, and Somali pirates, addressed in terms the layperson can understand, with solid research grounding Fills a gap in existing literature on intelligence, technology, and national security Intelligent data analytics for terror threat prediction is an emerging field of research at the intersection of information science and computer science, bringing with it a new era of tremendous opportunities and challenges due to plenty of easily available criminal data for further analysis. This book provides innovative insights that will help obtain interventions to undertake emerging dynamic scenarios of criminal activities. Furthermore, it presents emerging issues, challenges and management strategies in public safety and crime control

development across various domains. The book will play a vital role in improvising human life to a great extent. Researchers and practitioners working in the fields of data mining, machine learning and artificial intelligence will greatly benefit from this book, which will be a good addition to the state-of-the-art approaches collected for intelligent data analytics. It will also be very beneficial for those who are new to the field and need to quickly become acquainted with the best performing methods. With this book they will be able to compare different approaches and carry forward their research in the most important areas of this field, which has a direct impact on the betterment of human life by maintaining the security of our society. No other book is currently on the market which provides such a good collection of state-of-the-art methods for intelligent data analytics-based models for terror threat prediction, as intelligent data analytics is a newly emerging field and research in data mining and machine learning is still in the early stage of development.

This author team had students in mind when they wrote the book on Criminal Law. Criminal Law: Core Concepts uses examples and case excerpts that are interesting and informative, along with logically organized, plain-English discussion of the Model Penal Code. This is the basis for developing a solid understanding of criminal law concepts. One look inside this book and you ll notice that every page promises unobstructed learning. You ll see an uncluttered page design, uncluttered coverage, writing uncluttered by legalese, and case excerpts uncluttered by extraneous detail Everything in this book serves a purpose. Criminal Law: Core Concepts features: A commitment to clarity, reflected in the writing style, organization, pedagogy, and design Shrewd case editing that hones in on salient themes and principles Engaging and informative examples throughout the text Plain English discussion of the Model

Penal Code Timely coverage of contemporary topics, such as street crime

A powerful, uncompromising explanation of how subtle sources of hatred contained throughout our media and culture have resulted in a tolerance for hate crimes in America. • Provides readers with an understanding of how deeply embedded in daily cultural practices the roots of hatred are in American culture • Spotlights the role of cultural institutions such as the media, political rhetoric, and the entertainment industry in fostering an atmosphere of hate • Portrays hate crime as unexceptional in American culture rather than isolated acts of deviant individuals • Examines media depictions of those considered "Other" throughout American history, including enemies during war, immigrants, different racial and religious groups, and those whose sexual identities have been deemed "Other"

CybercrimeCriminal Threats from CyberspaceCybercrimeCriminal Threats from CyberspaceABC-CLIO

This book examines the mutual recognition of judicial decisions in European criminal law as a cornerstone of judicial co-operation in criminal matters in the European Union. Providing comprehensive content and combining theoretical and practical aspects, it covers all of the major issues surrounding mutual recognition. The book analyses its definition, genesis, principles, case law, implementation and evaluation. Special attention is given to mutual recognition measures, namely European arrest warrant (i.e. surrender procedure), mutual recognition of custodial sentences, and measures involving deprivation of liberty, mutual recognition of probation measures and alternative sanctions, mutual recognition of financial penalties, mutual recognition of confiscation orders, the European supervision order in pre-trial procedures (i.e. mutual recognition of supervision measures as an alternative to provisional

detention), the European investigation order (i.e. free movement of evidence), and the European protection order (i.e. mutual recognition of protection orders). Instead of focusing solely on a criminal law approach, the book also considers the subject from the perspectives of European Union law and International criminal law.

With its focus on recent detective series featuring female investigators, this collection analyzes the authors' treatment of current social, political and economic problems in Spain and beyond, in addition to exploring interrelations between gender, globalization, the environment and technology. The contributions here reveal the varied ways in which the use of a series allows for a deeper consideration of such issues, in addition to permitting the more extensive development of the protagonist investigator and her reactions to, and methods of, dealing with personal and professional challenges of the twenty-first century. In these stories, the authors employ strategies that break with long-standing conventions, developing crime fiction in unexpected ways, incorporating elements of science fiction, the supernatural, and the historical novel, as well as varied geographical settings (small towns, provincial cities, and rural communities) beyond the urban environment, all of which contributes to the reinvigoration of the genre.

The SAGE Encyclopedia of the Internet addresses the many related topics pertaining to cyberspace, email, the World Wide Web, and social media. Entries will range from popular topics such as Alibaba and YouTube to important current controversies such as Net Neutrality and cyberterrorism.

The Encyclopedia of Crime and Punishment provides the most comprehensive reference for a vast number of topics relevant to crime and punishment with a unique

focus on the multi/interdisciplinary and international aspects of these topics and historical perspectives on crime and punishment around the world. Named as one of Choice's Outstanding Academic Titles of 2016 Comprising nearly 300 entries, this invaluable reference resource serves as the most up-to-date and wide-ranging resource on crime and punishment Offers a global perspective from an international team of leading scholars, including coverage of the strong and rapidly growing body of work on criminology in Europe, Asia, and other areas Acknowledges the overlap of criminology and criminal justice with a number of disciplines such as sociology, psychology, epidemiology, history, economics, and public health, and law Entry topics are organized around 12 core substantive areas: international aspects, multi/interdisciplinary aspects, crime types, corrections, policing, law and justice, research methods, criminological theory, correlates of crime, organizations and institutions (U.S.), victimology, and special populations Organized, authored and Edited by leading scholars, all of whom come to the project with exemplary track records and international standing 3 Volumes www.crimeandpunishmentencyclopedia.com

Jonathan Lusthaus lifts the veil on cybercriminals in the most extensive account yet of the lives they lead and the vast international industry they have created. Having traveled to hotspots around the world to meet with hundreds of law enforcement agents, security gurus, hackers, and criminals, he charts how this industry based on anonymity works.

Most books on cybercrime are written by national security or political experts, and rarely propose an integrated and comprehensive approach to cybercrime, cyber-terrorism, cyber-war and cyber-security. This work develops approaches to crucial cyber-security issues that are non-political, non-partisan, and non-governmental. It informs readers throug

By its very nature digital crime may present a number of specific detection and investigative challenges. The use of steganography to hide child abuse images for example, can pose the kind of technical and legislative problems inconceivable just two decades ago. The volatile nature of much digital evidence can also pose problems, particularly in terms of the actions of the 'first officer on the scene'. There are also concerns over the depth of understanding that 'generic' police investigators may have concerning the possible value (or even existence) of digitally based evidence. Furthermore, although it is perhaps a cliché to claim that digital crime (and cybercrime in particular) respects no national boundaries, it is certainly the case that a significant proportion of investigations are likely to involve multinational cooperation, with all the complexities that follow from this. This groundbreaking volume offers a theoretical perspective on the policing of digital crime in the western world. Using numerous case-study examples to illustrate the theoretical material introduced this volume examine the organisational context for policing digital crime as well as crime prevention and detection. This work is a must-read for all academics, police practitioners and

investigators working in the field of digital crime.

Technology has become increasingly important to both the function and our understanding of the justice process. Many forms of criminal behaviour are highly dependent upon technology, and crime control has become a predominantly technologically driven process – one where 'traditional' technological aids such as fingerprinting or blood sample analysis are supplemented by a dizzying array of tools and techniques including surveillance devices and DNA profiling. This book offers the first comprehensive and holistic overview of global research on technology, crime and justice. It is divided into five parts, each corresponding with the key stages of the offending and justice process: Part I addresses the current conceptual understanding of technology within academia and the criminal justice system; Part II gives a comprehensive overview of the current relations between technology and criminal behaviour; Part III explores the current technologies within crime control and the ways in which technology underpins contemporary formal and informal social control; Part IV sets out some of the fundamental impacts technology is now having upon the judicial process; Part V reveals the emerging technologies for crime, control and justice and considers the extent to which new technology can be effectively regulated. This landmark collection will be essential reading for academics, students and theorists within criminology, sociology, law, engineering and technology, and computer science, as well as practitioners and professionals working within and around the criminal justice

system.

Cybercrime is a very real threat in our Internet-connected society. This anthology provides your readers with a solid base of knowledge on cybercrime and provides resources that help to develop critical thinking skills. The essays in this volume offer a broad array of viewpoints. Students are encouraged to see the validity of divergent opinions, so that they may understand issues inclusively. A question-and-response format prompts readers to examine complex issues from multiple viewpoints. Readers will debate whether cybercrime poses a serious problem for U.S. security, whether cybercrime against individuals is a serious problem, and what should be done to protect internet users from cybercrime.

This timely guide reminds readers of their legal rights and responsibilities online. Reviewed by legal experts, it outlines the laws of cyberspace and some of the common activities and practices that can trip up young Web users. It also offers readers an overview of what to expect if they or someone they know gets into legal trouble, including what happens in court and what their rights are. Real-life events help explain what can happen when the law is disregarded. It also highlights some perhaps surprising legal parameters, in hopes of keeping readers mindful of safe, responsible, and legal Internet use.

This fascinating and timely book traces the emergence and evolution of cybercrime as an increasingly intransigent threat to society. * A chronology traces the emergence and

evolution of cybercrime from the 1950s to the present * Detailed descriptions and analysis of real cybercrime cases illustrate what cybercrime is and how cybercriminals operate

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

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

This concise volume takes care of two major issues at once; providing readers with a more worldwide view than American-centric information, and educating readers about cybercrime. This volume of essays from international sources explores the vulnerability of countries and people to cybercrime. Readers will explore cybercrime law worldwide, and take a look at the role of organized crime in cybercrime. They will also take a deep

dive into cyber espionage and cyber terrorism. Countries and cultures that readers will learn about include South Africa, Singapore, Pakistan, China, Canada, Thailand, Australia, Russia, and the United Kingdom.

Technology has become deeply integrated into modern society and various activities throughout everyday life. However, this increases the risk of vulnerabilities, such as hacking or system errors, among other online threats. Cybersecurity Breaches and Issues Surrounding Online Threat Protection is an essential reference source for the latest scholarly research on the various types of unauthorized access or damage to electronic data. Featuring extensive coverage across a range of relevant perspectives and topics, such as robotics, cloud computing, and electronic data diffusion, this publication is ideally designed for academicians, researchers, computer engineers, graduate students, and practitioners seeking current research on the threats that exist in the world of technology.

Social media hasn't just changed society—it's changing the way in which criminal law is prosecuted, defended, and adjudicated. This fascinating book explains how. • Examines the criminal justice system from multiple perspectives in order to give fair attention to the successful uses of social media as well as the abuses • Comprehensively covers current issues that have broad, long-term repercussions for the criminal justice system • Provides a convenient overview of all the information related to social media and criminal law in one place • Cites relevant cases and

statutes

This single-source reference will help students and general readers alike understand the most critical issues facing American society today. • Four volumes divided by subject area • 225 entries written by experienced researchers and professionals who are experts in their fields • Charts and graphs • Comprehensive bibliographies at the end of each topic volume • Sidebars containing interesting and useful tangents to the main discussion • Further reading section at end of each entry, including Internet links Offering a comprehensive analysis, bestselling COMPARATIVE CRIMINAL JUSTICE SYSTEMS, 5e compares the various criminal justice systems throughout the world using six model countries: China, England, France, Germany, Japan, and Saudi Arabia. The book illustrates the different types of law and justice systems while exploring the historical, political, economic, social, and cultural influences on each system. It examines important aspects of each type of justice system--common law, civil law, socialist law, and sacred (Islamic) law--to highlight the similarities and differences of each. Completely up to date, it provides expanded coverage of such high-profile topics as human trafficking, Internet pornography, identity theft, transnational policing, terrorism and more. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

This volume provides an overview of cyber economic crime in India, analyzing fifteen years of data and specific case studies from Mumbai to add to the limited research in

cyber economic crime detection. Centering around an integrated victim-centered approach to investigating a global crime on the local level, the book examines the criminal justice system response to cyber economic crime and proposes new methods of detection and prevention. It considers the threat from a national security perspective, a cybercrime perspective, and as a technical threat to business and technology installations. Among the topics discussed: Changing landscape of crime in cyberspace Cybercrime typology Legal framework for cyber economic crime in India Cyber security mechanisms in India A valuable resource for law enforcement and police working on the local, national, and global level in the detection and prevention of cybercrime, Cyber Economic Crime in India will also be of interest to researchers and practitioners working in financial crimes and white collar crime.

Copyright: 755c8293d9d2c6d5cbaad295b20b70c9