Cybercrime In Progress Theory And Prevention Of Technology Enabled Offenses Crime Science Series

Proceedings of a Workshop on Deterring CyberattacksThe Palgrave Handbook of International Cybercrime and CyberdevianceThe Routledge Handbook of Technology, Crime and JusticeEmerging Cyber Threats and Cognitive VulnerabilitiesNew Perspectives on CybercrimeEvolutionary Concepts in End User Productivity and Performance: Applications for Organizational ProgressCorporate Hacking and Technology-driven CrimeCyberspace, Cybersecurity, and CybercrimeWhite-Collar CrimeCybercrime and Digital ForensicsThe Human Factor of CybercrimeAutomating Open Source IntelligenceDigital CriminologyCyber CriminologyCybercrime, Digital Forensics and JurisdictionTen Strategies of a World-Class Cybersecurity Operations CenterPolicing Cyber CrimeVictimology and Victim AssistanceAt the Nexus of Cybersecurity and Public PolicyCybercrime and Digital ForensicsStrengthening Forensic Science in the United StatesPolicing Cybercrime and CyberterrorCyber Crime: Concepts, Methodologies, Tools and ApplicationsMeasurement Problems in Criminal Justice ResearchPersonal CybersecurityCybercrime, Organized Crime, and Societal ResponsesCrimes of the InternetCybercrime Through an Interdisciplinary LensCrime and the InternetSurveillance, Privacy and Public SpaceCrime ScienceInternational and

Transnational Crime and JusticeCyber-Physical SecurityWomen in the Criminal Justice SystemCybercrime in ProgressRegulatory TheoryCriminology and Public PolicyCyber crime strategyThe Psychology of Cyber Crime: Concepts and PrinciplesExam Prep for: Cybercrime in Progress; Theory and

Proceedings of a Workshop on Deterring Cyberattacks

Victimization through the Internet is becoming more prevalent as cyber criminals have developed more effective ways to remain anonymous. And as more personal information than ever is stored on networked computers, even the occasional or non-user is at risk. A collection of contributions from worldwide experts and emerging researchers, Cyber Criminology: Exploring Internet Crimes and Criminal Behavior explores today's interface of computer science, Internet science, and criminology. Topics discussed include: The growing menace of cyber crime in Nigeria Internet gambling and digital piracy Sexual addiction on the Internet, child pornography, and online exploitation of children Terrorist use of the Internet Cyber stalking and cyber bullying The victimization of women on social networking websites Malware victimization and hacking The Islamic world in cyberspace and the propagation of Islamic ideology via the Internet Human rights concerns that the digital age has created Approaching the topic from a social science perspective, the book explores methods for determining the causes of computer crime

victimization by examining an individual's lifestyle patterns. It also publishes the findings of a study conducted on college students about online victimization. Advances in information and communications technologies have created a range of new crime problems that did not exist two decades ago. Opportunities for various criminal activities to pervade the Internet have led to the growth and development of cyber criminology as a distinct discipline within the criminology framework. This volume explores all aspects of this nascent field and provides a window on the future of Internet crimes and theories behind their origins. K. Jaishankar was the General Chair of the First International Conference of the South Asian Society of Criminology and Victimology (SASCV), held January 15-17, 2011 at the Hotel Jaipur Greens in Jaipur, Rajasthan, India.

The Palgrave Handbook of International Cybercrime and Cyberdeviance

Women in the Criminal Justice System: Tracking the Journey of Females and Crime provides a rare up-to-date examination of women both as offenders and employees in the criminal justice system. While the crime rate in the United States is currently decreasing, the rate of female incarceration is rising. Female participation in the criminal justice wo

The Routledge Handbook of Technology, Crime and Justice

Presented from a criminal justice perspective, Cyberspace, Cybersecurity, and Cybercrime introduces students to the interdisciplinary field of cybercrime by exploring the theoretical, practical, and legal framework it operates under, along with strategies to combat it. Authors Janine Kremling and Amanda M. Sharp Parker provide a straightforward overview of cybercrime, cyberthreats, and the vulnerabilities individuals, businesses, and governments face everyday in a digital environment. Highlighting the latest empirical research findings and challenges that cybercrime and cybersecurity pose for those working in the field of criminal justice, this book exposes critical issues related to privacy, terrorism, hacktivism, the dark web, and much more. Focusing on the past, present, and future impact of cybercrime and cybersecurity, it details how criminal justice professionals can be prepared to confront the changing nature of cybercrime.

Emerging Cyber Threats and Cognitive Vulnerabilities

The purpose of Policing Cybercrime and Cyberterror is to provide an in-depth discussion of the perceptions and responses of U.S. law enforcement agencies at all levels in dealing with cybercrime and cyberterror. The themes for this book include the challenges that cybercrime and digital evidence handling pose for local

and state agencies, the jurisdictional and investigative hurdles that hinder the response capabilities of police agencies, and the complexities of the actual investigation of these offenses and their impact on officers. This text analyzes data collected from local law enforcement agencies in the U.S., in order to understand officer perceptions of and responses to cybercrime and cyberterrorism, along with samples from digital forensic examiners, to understand their stress, satisfaction, secondary trauma, and coping mechanisms in response to work experiences. The findings demonstrate the realities of policing cybercrimes and those involving digital evidence processing relative to traditional offenses. Policing Cybercrime and Cyberterror addresses a gap in the policing literature by examining the various technological and policy changes needed to increase the investigative response of police agencies, along with various internal policies to improve support for forensic investigators.

New Perspectives on Cybercrime

As more individuals own and operate Internet-enabled devices and more critical government and industrial systems rely on advanced technologies, the issue of cybercrime has become a crucial concern for both the general public and professionals alike. The Psychology of Cyber Crime: Concepts and Principles aims to be the leading reference examining the psychology of cybercrime. This book considers many aspects of cybercrime, including research on offenders, legal

issues, the impact of cybercrime on victims, punishment, and preventative measures. It is designed as a source for researchers and practitioners in the disciplines of criminology, cyberpsychology, and forensic psychology, though it is also likely to be of significant interest to many students of information technology and other related disciplines.

Evolutionary Concepts in End User Productivity and Performance: Applications for Organizational Progress

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.

Corporate Hacking and Technology-driven Crime

Today, public space has become a fruitful venue for surveillance of many kinds. Emerging surveillance technologies used by governments, corporations, and even individual members of the public are reshaping the very nature of physical public space. Especially in urban environments, the ability of individuals to remain private or anonymous is being challenged. Surveillance, Privacy, and Public Space problematizes our traditional understanding of 'public space'. The chapter authors explore intertwined concepts to develop current privacy theory and frame future scholarly debate on the regulation of surveillance in public spaces. This book also explores alternative understandings of the impacts that modern living and technological progress have on the experience of being in public, as well as the very nature of what public space really is. Representing a range of disciplines and methods, this book provides a broad overview of the changing nature of public space and the complex interactions between emerging forms of surveillance and personal privacy in these public spaces. It will appeal to scholars and students in a variety of academic disciplines, including sociology, surveillance studies, urban studies, philosophy, law, communication and media studies, political science, and criminology.

Cyberspace, Cybersecurity, and Cybercrime

We depend on information and information technology (IT) to make many of our day-to-day tasks easier and more convenient. Computers play key roles in transportation, health care, banking, and energy. Businesses use IT for payroll and accounting, inventory and sales, and research and development. Modern military forces use weapons that are increasingly coordinated through computer-based networks. Cybersecurity is vital to protecting all of these functions. Cyberspace is vulnerable to a broad spectrum of hackers, criminals, terrorists, and state actors. Working in cyberspace, these malevolent actors can steal money, intellectual property, or classified information; impersonate law-abiding parties for their own purposes; damage important data; or deny the availability of normally accessible services. Cybersecurity issues arise because of three factors taken together - the presence of malevolent actors in cyberspace, societal reliance on IT for many important functions, and the presence of vulnerabilities in IT systems. What steps can policy makers take to protect our government, businesses, and the public from those would take advantage of system vulnerabilities? At the Nexus of Cybersecurity and Public Policy offers a wealth of information on practical measures, technical and nontechnical challenges, and potential policy responses. According to this report, cybersecurity is a never-ending battle; threats will evolve as adversaries adopt new tools and techniques to compromise security. Cybersecurity is therefore an ongoing process that needs to evolve as new threats are identified. At the Nexus of Cybersecurity and Public Policy is a call for action to make cybersecurity a public safety priority. For a number of years, the

cybersecurity issue has received increasing public attention; however, most policy focus has been on the short-term costs of improving systems. In its explanation of the fundamentals of cybersecurity and the discussion of potential policy responses, this book will be a resource for policy makers, cybersecurity and IT professionals, and anyone who wants to understand threats to cyberspace.

White-Collar Crime

Most major crime in this country emanates from two major data sources. The FBIâ€™s Uniform Crime Reports has collected information on crimes known to the police and arrests from local and state jurisdictions throughout the country. The National Crime Victimization Survey, a general population survey designed to cover the extent, nature, and consequences of criminal victimization, has been conducted annually since the early1970s. This workshop was designed to consider similarities and differences in the methodological problems encountered by the survey and criminal justice research communities and what might be the best focus for the research community. In addition to comparing and contrasting the methodological issues associated with self-report surveys and official records, the workshop explored methods for obtaining accurate self-reports on sensitive questions about crime events, estimating crime and victimization in rural counties and townships and developing unbiased prevalence and incidence rates for rate events among population subgroups.

Cybercrime and Digital Forensics

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.

The Human Factor of Cybercrime

Ten Strategies of a World-Class Cyber Security Operations Center conveys MITRE's accumulated expertise on enterprise-grade computer network defense. It covers ten key qualities of leading Cyber Security Operations Centers (CSOCs), ranging from their structure and organization, to processes that best enable smooth operations, to approaches that extract maximum value from key CSOC technology investments. This book offers perspective and context for key decision points in structuring a CSOC, such as what capabilities to offer, how to architect large-scale data collection and analysis, and how to prepare the CSOC team for agile, threat-based response. If you manage, work in, or are standing up a CSOC, this book is for you. It is also available on MITRE's website, www.mitre.org.

Automating Open Source Intelligence

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.

Digital Criminology

This exciting and timely collection showcases recent work on Cybercrime by members of Uclan Cybercrime Research Unit [UCRU], directed by Dr Tim Owen at the University of Central Lancashire, UK. This book offers up-to-date perspectives on Cybercrime based upon a Realist social ontology, alongside suggestions for how research into Cybercrime might move beyond what can be seen as the main theoretical obstacles facing criminological theory: the stagnation of critical criminology and the nihilistic relativism of the postmodern and post-structuralist cultural turn. Organised into three sections; 'Law and Order in Cyberspace', 'Gender and Deviance in Cyberspace', and 'Identity and Cyberspace', this cutting-edge volume explores some of the most crucial issues we face today on the internet: grooming, gendered violence, freedom of speech and intellectual property crime. Providing unique new theory on Cybercrime, this book will appeal to scholars and advanced students of Criminology, Law, Sociology, Philosophy, Policing and Forensic Science, Information Technology and Journalism, in addition to professionals working within law and order agencies and the security services.

Cyber Criminology

Victimology and Victim Assistance offers insights into the criminal justice system from the perspective of often overlooked participants—victims. Delving into victim involvement in the criminal justice system, the impact of crime on victims, and new directions in victimology and victim assistance, authors Yoshiko Takahashi and

Chadley James provide crucial insights and practical applications into the field of victim assistance. With an emphasis on advocacy, intervention, and restoration, this book examines real issues and barriers in the criminal justice system for victims and offers a way forward for future criminal justice or other human service professionals.

Cybercrime, Digital Forensics and Jurisdiction

This book offers a comprehensive and integrative introduction to cybercrime. It provides an authoritative synthesis of the disparate literature on the various types of cybercrime, the global investigation and detection of cybercrime and the role of digital information, and the wider role of technology as a facilitator for social relationships between deviants and criminals. It includes coverage of: key theoretical and methodological perspectives; computer hacking and malicious software; digital piracy and intellectual theft; economic crime and online fraud; pornography and online sex crime; cyber-bullying and cyber-stalking; cyber-terrorism and extremism; digital forensic investigation and its legal context around the world; the law enforcement response to cybercrime transnationally; cybercrime policy and legislation across the globe. The new edition features two new chapters, the first looking at the law enforcement response to cybercrime and the second offering an extended discussion of online child pornography and sexual exploitation. This book includes lively and engaging features, such as discussion

questions, boxed examples of unique events and key figures in offending, quotes from interviews with active offenders, and a full glossary of terms. This new edition includes QR codes throughout to connect directly with relevant websites. It is supplemented by a companion website that includes further exercises for students and instructor resources. This text is essential reading for courses on cybercrime, cyber-deviancy, digital forensics, cybercrime investigation, and the sociology of technology.

Ten Strategies of a World-Class Cybersecurity Operations Center

The emergence of the World Wide Web, smartphones, and computers has transformed the world and enabled individuals to engage in crimes in a multitude of new ways. Criminological scholarship on these issues has increased dramatically over the last decade, as have studies on ways to prevent and police these offenses. This book is one of the first texts to provide a comprehensive review of research regarding cybercrime, policing and enforcing these offenses, and the prevention of various offenses as global change and technology adoption increases the risk of victimization around the world. Drawing on a wide range of literature, Holt and Bossler offer an extensive synthesis of numerous contemporary topics such as theories used to account for cybercrime, policing in domestic and

transnational contexts, cybercrime victimization and issues in cybercrime prevention. The findings provide a roadmap for future research in cybercrime, policing, and technology, and discuss key controversies in the existing research literature in a way that is otherwise absent from textbooks and general cybercrime readers. This book is an invaluable resource for academics, practitioners, and students interested in understanding the state of the art in social science research. It will be of particular interest to scholars and students interested in cybercrime, cyber-deviance, victimization, policing, criminological theory, and technology in general.

Policing Cyber Crime

This book provides an introduction to crime science, setting out its essentials. It provides a major statement of the nature and aspirations of crime science, and presents a series of case studies providing examples, in different settings, of the approach in action, ranging from preventing crime within correctional institutions to the use of techniques such as DNA fast tracking for burglary.

Victimology and Victim Assistance

Emerging Cyber Threats and Cognitive Vulnerabilities identifies the critical role

human behavior plays in cybersecurity and provides insights into how human decision-making can help address rising volumes of cyberthreats. The book examines the role of psychology in cybersecurity by addressing each actor involved in the process: hackers, targets, cybersecurity practitioners and the wider social context in which these groups operate. It applies psychological factors such as motivations, group processes and decision-making heuristics that may lead individuals to underestimate risk. The goal of this understanding is to more quickly identify threat and create early education and prevention strategies. This book covers a variety of topics and addresses different challenges in response to changes in the ways in to study various areas of decision-making, behavior, artificial intelligence, and human interaction in relation to cybersecurity. Explains psychological factors inherent in machine learning and artificial intelligence Discusses the social psychology of online radicalism and terrorist recruitment Examines the motivation and decision-making of hackers and "hacktivists" Investigates the use of personality psychology to extract secure information from individuals

At the Nexus of Cybersecurity and Public Policy

"This book aims to represent some of the most current investigations into a wide range of end-user computing issues, enhancing understanding of recent developments"--Provided by publisher.

Cybercrime and Digital Forensics

Algorithms for Automating Open Source Intelligence (OSINT) presents information on the gathering of information and extraction of actionable intelligence from openly available sources, including news broadcasts, public repositories, and more recently, social media. As OSINT has applications in crime fighting, state-based intelligence, and social research, this book provides recent advances in text mining, web crawling, and other algorithms that have led to advances in methods that can largely automate this process. The book is beneficial to both practitioners and academic researchers, with discussions of the latest advances in applications, a coherent set of methods and processes for automating OSINT, and interdisciplinary perspectives on the key problems identified within each discipline. Drawing upon years of practical experience and using numerous examples, editors Robert Layton, Paul Watters, and a distinguished list of contributors discuss Evidence Accumulation Strategies for OSINT, Named Entity Resolution in Social Media, Analyzing Social Media Campaigns for Group Size Estimation, Surveys and qualitative techniques in OSINT, and Geospatial reasoning of open data. Presents a coherent set of methods and processes for automating OSINT Focuses on algorithms and applications allowing the practitioner to get up and running quickly Includes fully developed case studies on the digital underground and predicting crime through OSINT Discusses the ethical considerations when using publicly available online data

Strengthening Forensic Science in the United States

The emergence of the World Wide Web, smartphones, and Computer-Mediated Communications (CMCs) profoundly affect the way in which people interact online and offline. Individuals who engage in socially unacceptable or outright criminal acts increasingly utilize technology to connect with one another in ways that are not otherwise possible in the real world due to shame, social stigma, or risk of detection. As a consequence, there are now myriad opportunities for wrongdoing and abuse through technology. This book offers a comprehensive and integrative introduction to cybercrime. It is the first to connect the disparate literature on the various types of cybercrime, the investigation and detection of cybercrime and the role of digital information, and the wider role of technology as a facilitator for social relationships between deviants and criminals. It includes coverage of: key theoretical and methodological perspectives, computer hacking and digital piracy, economic crime and online fraud, pornography and online sex crime, cyber-bulling and cyber-stalking, cyber-terrorism and extremism, digital forensic investigation and its legal context, cybercrime policy. This book includes lively and engaging features, such as discussion questions, boxed examples of unique events and key figures in offending, quotes from interviews with active offenders and a full glossary of terms. It is supplemented by a companion website that includes further students exercises and instructor resources. This text is essential reading for courses on cybercrime, cyber-deviancy, digital forensics, cybercrime investigation

and the sociology of technology.

Policing Cybercrime and Cyberterror

The infusion of digital technology into contemporary society has had significant effects for everyday life and for everyday crimes. Digital Criminology: Crime and Justice in Digital Society is the first interdisciplinary scholarly investigation extending beyond traditional topics of cybercrime, policing and the law to consider the implications of digital society for public engagement with crime and justice movements. This book seeks to connect the disparate fields of criminology, sociology, legal studies, politics, media and cultural studies in the study of crime and justice. Drawing together intersecting conceptual frameworks, Digital Criminology examines conceptual, legal, political and cultural framings of crime, formal justice responses and informal citizen-led justice movements in our increasingly connected global and digital society. Building on case study examples from across Australia, Canada, Europe, China, the UK and the United States, Digital Criminology explores key questions including: What are the implications of an increasingly digital society for crime and justice? What effects will emergent technologies have for how we respond to crime and participate in crime debates? What will be the foundational shifts in criminological research and frameworks for understanding crime and justice in this technologically mediated context? What does it mean to be a 'just' digital citizen? How will digital communications and

social networks enable new forms of justice and justice movements? Ultimately, the book advances the case for an emerging digital criminology: extending the practical and conceptual analyses of 'cyber' or 'e' crime beyond a focus foremost on the novelty, pathology and illegality of technology-enabled crimes, to understandings of online crime as inherently social.

Cyber Crime: Concepts, Methodologies, Tools and Applications

Discover the most prevalent cyber threats against individual users of all kinds of computing devices. This book teaches you the defensive best practices and state-of-the-art tools available to you to repel each kind of threat. Personal Cybersecurity addresses the needs of individual users at work and at home. This book covers personal cybersecurity for all modes of personal computing whether on consumer-acquired or company-issued devices: desktop PCs, laptops, mobile devices, smart TVs, WiFi and Bluetooth peripherals, and IoT objects embedded with network-connected sensors. In all these modes, the frequency, intensity, and sophistication of cyberattacks that put individual users at risk are increasing in step with accelerating mutation rates of malware and cybercriminal delivery systems. Traditional anti-virus software and personal firewalls no longer suffice to guarantee personal security. Users who neglect to learn and adopt the new ways of protecting themselves in their work and private environments put themselves, their associates, and their companies at risk of inconvenience, violation, reputational

damage, data corruption, data theft, system degradation, system destruction, financial harm, and criminal disaster. This book shows what actions to take to limit the harm and recover from the damage. Instead of laying down a code of "thou shalt not" rules that admit of too many exceptions and contingencies to be of much practical use, cloud expert Marvin Waschke equips you with the battlefield intelligence, strategic understanding, survival training, and proven tools you need to intelligently assess the security threats in your environment and most effectively secure yourself from attacks. Through instructive examples and scenarios, the author shows you how to adapt and apply best practices to your own particular circumstances, how to automate and routinize your personal cybersecurity, how to recognize security breaches and act swiftly to seal them, and how to recover losses and restore functionality when attacks succeed. What You'll Learn Discover how computer security works and what it can protect us from See how a typical hacker attack works Evaluate computer security threats to the individual user and corporate systems Identify the critical vulnerabilities of a computer connected to the Internet Manage your computer to reduce vulnerabilities to yourself and your employer Discover how the adoption of newer forms of biometric authentication affects you Stop your router and other online devices from being co-opted into disruptive denial of service attacks Who This Book Is For Proficient and technically knowledgeable computer users who are anxious about cybercrime and want to understand the technology behind both attack and defense but do not want to go so far as to become security experts.

Some of this audience will be purely home users, but many will be executives, technical managers, developers, and members of IT departments who need to adopt personal practices for their own safety and the protection of corporate systems. Many will want to impart good cybersecurity practices to their colleagues. IT departments tasked with indoctrinating their users with good safety practices may use the book as training material.

Measurement Problems in Criminal Justice Research

Personal Cybersecurity

"This book addresses various aspects of hacking and technology-driven crime, including the ability to understand computer-based threats, identify and examine attack dynamics, and find solutions"--Provided by publisher.

Cybercrime, Organized Crime, and Societal Responses

Is the internet really powerful enough to allow a sixteen year old to become the biggest threat to world peace since Adolf Hitler? Are we all now susceptible to cyber-criminals who can steal from us without even having to leave the comfort of

their own armchairs? These are fears which have been articulated since the popular development of the internet, yet criminologists have been slow to respond to them. Consequently, questions about what cybercrimes are, what their impacts will be and how we respond to them remain largely unanswered. Organised into three sections, this book engages with the various criminological debates that are emerging over cybercrime. The first section looks at the general problem of crime and the internet. It then describes what is understood by the term 'cybercrime' by identifying some of the challenges for criminology. The second section explores the different types of cybercrime and their attendant problems. The final section contemplates some of the challenges that cybercrimes give rise to for the criminal justice system.

Crimes of the Internet

The thoroughly updated Second Edition of White Collar Crime: The Essentials continues to be a comprehensive, yet concise, resource addressing the most important topics students need to know about white-collar crime. Author Brian K. Payne provides a theoretical framework and context for students that explores such timely topics as crimes by workers, sales-oriented systems, crimes in the health care system, crimes by criminal justice professionals and politicians, crimes in the educational system, crimes in economic and technological systems, corporate crime, environmental crime, and more. This easy to read teaching tool is

a valuable resource for any course that covers white-collar crime.

Cybercrime Through an Interdisciplinary Lens

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.

Crime and the Internet

Provides a key textbook on the nature of international and transnational crimes and the delivery of justice for crime control and prevention.

Surveillance, Privacy and Public Space

Threatening the safety of individuals, computers, and entire networks, cyber crime attacks vary in severity and type. Studying this continually evolving discipline involves not only understanding different types of attacks, which range from identity theft to cyberwarfare, but also identifying methods for their prevention. Cyber Crime: Concepts, Methodologies, Tools and Applications is a three-volume reference that explores all aspects of computer-based crime and threats, offering solutions and best practices from experts in software development, information security, and law. As cyber crime continues to change and new types of threats emerge, research focuses on developing a critical understanding of different types of attacks and how they can best be managed and eliminated.

Crime Science

This timely book provides contributions on international, comparative crime

phenomena: gangs, trafficking, fear of crime, and crime prevention. It highlights contributions originally prepared for the XVII World Congress of Criminology and for the 2015 Cybercrime Conference in Oñati, Spain which have been selected, reviewed, and adapted for inclusion in this volume. The work features international contributors sharing the latest research and approaches from a variety of global regions. The first part examines the impact of gangs on criminal activities and violence. The second part explores illegal trafficking of people, drugs, and other illicit goods as a global phenomenon, aided by the ease of international travel, funds transfer, and communication. Finally, international approaches to crime detection prevention are presented. The work provides case studies and fieldwork that will be relevant across a variety of disciplines and a rich resource for future research. This work is relevant for researchers in criminology and criminal justice, as well as related fields such as international and comparative law, public policy, and public health.

International and Transnational Crime and Justice

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.

Cyber-Physical Security

Examines the links between criminological theory and criminal justice policy and practice.

Women in the Criminal Justice System

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 ground-breaking 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 Gunningham, Fiona Haines, Terry Halliday, David Levi-Faur, Christine Parker, Colin Scott and Clifford Shearing.

Cybercrime in Progress

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.

Regulatory Theory

This book contains 31 original scholarly articles on all aspects of cybercrime--from emerging global crimes of the Internet, to criminological perspectives on cybercrime to investigating and prosecuting cybercrimes. Offering a collection of previously unpublished works, this book examines emerging global crimes, challenges faced by law enforcement, and the underlying reasons for the rise in such activities. Through a variety of essays, it explores the role of the cybercriminal, the victim, and the cybercriminal's impact on the criminal justice system.

Criminology and Public Policy

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.

Cyber crime strategy

The Psychology of Cyber Crime: Concepts and Principles

This book focuses on the vulnerabilities of state and local services to cyber-threats and suggests possible protective action that might be taken against such threats.

Cyber-threats to U.S. critical infrastructure are of growing concern to policymakers, managers and consumers. Information and communications technology (ICT) is ubiquitous and many ICT devices and other components are interdependent; therefore, disruption of one component may have a negative, cascading effect on others. Cyber-attacks might include denial of service, theft or manipulation of data. Damage to critical infrastructure through a cyber-based attack could have a significant impact on the national security, the economy, and the livelihood and safety of many individual citizens. Traditionally cyber security has generally been viewed as being focused on higher level threats such as those against the internet or the Federal government. Little attention has been paid to cyber-security at the state and local level. However, these governmental units play a critical role in providing services to local residents and consequently are highly vulnerable to cyber-threats. The failure of these services, such as waste water collection and water supply, transportation, public safety, utility services, and communication services, would pose a great threat to the public. Featuring contributions from leading experts in the field, this volume is intended for state and local government officials and managers, state and Federal officials, academics, and public policy specialists.

Exam Prep for: Cybercrime in Progress; Theory and

Scores of talented and dedicated people serve the forensic science community,

performing vitally important work. However, they are often constrained by lack of adequate resources, sound policies, and national support. It is clear that change and advancements, both systematic and scientific, are needed in a number of forensic science disciplines to ensure the reliability of work, establish enforceable standards, and promote best practices with consistent application. Strengthening Forensic Science in the United States: A Path Forward provides a detailed plan for addressing these needs and suggests the creation of a new government entity, the National Institute of Forensic Science, to establish and enforce standards within the forensic science community. The benefits of improving and regulating the forensic science disciplines are clear: assisting law enforcement officials, enhancing homeland security, and reducing the risk of wrongful conviction and exoneration. Strengthening Forensic Science in the United States gives a full account of what is needed to advance the forensic science disciplines, including upgrading of systems and organizational structures, better training, widespread adoption of uniform and enforceable best practices, and mandatory certification and accreditation programs. While this book provides an essential call-to-action for congress and policy makers, it also serves as a vital tool for law enforcement agencies, criminal prosecutors and attorneys, and forensic science educators.