Digital Crime Terrorism 3rd Edition

This two-volume work offers a comprehensive examination of the distressing topics of transnational crime and the implications for global security. • Represents global collaboration among contributors including scholars from respected universities in Europe, North America, and Australia; professionals at public policy research institutes; and researchers at several United Nations entities • Provides perspectives from contributors of geographic diversity and varied backgrounds that combine to form a global panorama of crime and security topics • Provides readers a single work to learn about both specific transnational crimes (Volume 1) and efforts to prevent and combat those crimes (Volume 2) • Prefaces each chapter with an introduction that contextualizes content for closer reading

Placing terrorists and terrorist activities within their sociopolitical settings, this volume contains essays by 16 experts on the major theories, typologies, concepts, strategies, tactics, ideologies, practices, implications of, and responses to contemporary political terrorism. New to this edition are essays on typologies and state terrorism in international affairs, and terrorism within Latin America, the Middle East, the United States, Western Europe, and sub-Saharan Africa. The authors demystify the myths of contemporary political terrorism, and conclude with discussions of the interrelationship among political terrorism, the media and civil liberties; counterterrorism policies; the threat that terrorists will go nuclear; and the international terrorist network. ISBN 0-8247-7814-6: $45.00.

Technological advances, although beneficial and progressive, can lead to vulnerabilities in system networks and security. While researchers attempt to find solutions, negative uses of technology continue to create new security threats to users. New Threats and Countermeasures in Digital Crime and Cyber Terrorism brings together research-based chapters and case studies on security techniques and current methods being used to identify and overcome technological vulnerabilities with an emphasis on security issues in mobile computing and online activities. This book is an essential reference source for researchers, university academics, computing professionals, and upper-level students interested in the techniques, laws, and training initiatives currently being implemented and adapted for secure computing.

Mass-Mediated Terrorism, Second Edition, an in-depth look at terrorism, political violence, and mass media, shows how terrorists exploit global media networks and information highways to carry news of their violence along with "propaganda of the deed." To what extent is the media advancing or obstructing the propaganda and policy goals of terrorists and their targets? Has the Internet strengthened the hands of terrorists to organize, recruit, and spread propaganda? How have targets of terrorism used the media to manipulate public opinion and advance their own agendas? From U.S. cases to incidents abroad, this award-winning book explores the use of political violence for the sake of publicity, media coverage of counterterrorism policies and its affect on political decision making, and the impact of new media. This revised second edition, which includes a new chapter on public opinion, is updated with analysis of the Iraq war, increasing terrorist attacks abroad, and subsequent counterterrorism measures. It also contains new information on the Arab satellite network Al-Jazeera and the use of the Internet in terrorist efforts. Mass-Mediated Terrorism offers a blueprint both for effective public information and media relations during terrorism crises as well as for ethical news coverage of major terrorism incidents. Introduction to Homeland Security, Third Edition provides the latest developments in the policy and operations of domestic security efforts of the agencies under the U.S. Department of Homeland Security. This includes the FBI, Secret Service, FEMA, the Coast Guard, TSA and numerous other federal agencies responsible for critical intelligence, emergency response, and the safety and security of U.S. citizens at home and abroad. Changes in DHS and domestic security are presented from pre-

September 11, 2001 days, to include the formation of DHS under President George W. Bush, all the way through to the current administration. Through this, the many transformative events are looked at through the lens of DHS's original establishment, and the frequent changes to the various agencies, organization, reporting structure, funding, and policies that have occurred since. This new edition is completely updated and includes coverage of topics relevant to homeland security operations not covered in any other text currently available. This includes highlighting the geopolitical context and the nature of global terrorism—and their implications—specifically as they relate to threats to the United States. Partnerships and collaboration with global allies are highlighted in the context of their relevance to international trade, domestic policies, training, and security. The book ends with a look at emerging threats and potential new, creative solutions—and initiatives in-process within the government—to respond to and address such threats. Key Features: Explores the history and formation of the Department of Homeland Security, recent developments, as well as the role and core missions of core agencies within DHS Outlines man-made threats, intelligence challenges, and intra-agency communication, planning, and operations Looks critically at the role of geopolitical dynamics, key international allies, and their influence on domestic policy and decision-making Covers the latest developments in programs, legislation, and policy relative to all transportation and border security issues Examines current issues and emerging global threats associated with extremism and terrorism Addresses natural and man-made disasters and the emergency management cycle in preparing for, mitigating against, responding to, and recovering from such events Introduction to Homeland Security, Third Edition remains the premier textbook for criminal justice, homeland security, national security, and intelligence programs in universities and an ideal reference for professionals as well as policy and research institutes.

In response to the current terrorist threat, law enforcement agencies at every level have expanded technological and intelligence-gathering initiatives in order to support new tactical, investigative and deployment strategies. The demand for homeland security requires that agencies hire professional and specially-trained criminal and intelligence a

As personal data continues to be shared and used in all aspects of society, the protection of this information has become paramount. While cybersecurity should protect individuals from cyber-threats, it also should be eliminating any and all vulnerabilities. The use of hacking to prevent cybercrime and contribute new countermeasures towards protecting computers, servers, networks, web applications, mobile devices, and stored data from black hat attackers who have malicious intent, as well as to stop against unauthorized access instead of using hacking in the traditional sense to launch attacks on these devices, can contribute emerging and advanced solutions against cybercrime. Ethical Hacking Techniques and Countermeasures for Cybercrime Prevention is a comprehensive text that discusses and defines ethical hacking, including the skills and concept of ethical hacking, and studies the countermeasures to prevent and stop cybercrimes, cyberterrorism, cybertheft, identity theft, and computer-related crimes. It broadens the understanding of cybersecurity by providing the necessary tools and skills to combat cybercrime. Some specific topics include top cyber investigation trends, data security of consumer devices, phases of hacking attacks, and stenography for secure image transmission. This book is relevant for ethical hackers, cybersecurity analysts, computer forensic experts, government officials, practitioners, researchers, academicians, and students interested in the latest techniques for preventing and combatting cybercrime.

This is the eBook of the printed book and may not include any media, website access codes, or print supplements that may come packaged with the bound book. This text uses a conversational tone to the writing designed to convey complex technical issues as understandable concepts. Digital Crime and Digital Terrorism, 3e, is written in a user-friendly fashion, designed to be understandable by even the most technologically challenged reader. Issues addressed in the book include descriptions of the types of crimes and terrorist acts committed using computer technology, theories addressing hackers and other types of digital criminals, an overview of the legal strategies and tactics targeting this type of crime, and in-depth coverage of investigating and researching digital crime, digital terrorism, and information warfare. Additionally, upon completion of the text, readers should find themselves better prepared for further study into the growing problems of crime, terrorism and information warfare being committed using computer technology. Teaching and Learning This easy-to-read text offers an overview of both the technological and behavioral aspects of digital crime and terrorism. It provides: Up-to-date coverage of the digital crime, digital terrorism and the information warfare problem: Introducesstudents to the types of crimes, acts of terrorism, and information warfare that are committed using computers, networks, and the Internet Outstanding pedagogical features: Encourages students to develop critical thinking skills with numerous examples and exercises Exceptional instructor resources: Makes class preparation quick and easy with innovative features

Crime Prevention: Principles, Perspectives and Practices is a concise, comprehensive introduction to the theory and practice of crime prevention. The authors contend that crime prevention strategies should include both social prevention and environmental prevention. It embraces these strategies as an alternative to policing, criminal justice and 'law and order'. Part 1 presents an overview of the history and theory of crime prevention, featuring chapters on social prevention, environmental prevention and evaluation. Part 2 explores the practice of crime prevention and the real life challenges of implementation, including policy making, prevention in public places, dealing with social disorder and planning for the future. Crime Prevention provides readers with an understanding of the political dimension of crime prevention and the ability to critically analyse prevention techniques. It is essential reading for undergraduate students of criminology, crime prevention and public policy.

The third edition of this book presents the history of computer crime and cybercrime from the very beginning with punch cards, to the latest developments - including the attacks in the context of the 2016 US Election. Today the technological development of social media, such as Google, Facebook, YouTube, Twitter, and more, have been so rapid and the impact on society so fast and enormous, that codes of ethics, and public sentiments of justice implemented in criminal legislations, have not kept pace. Conducts in social media need a better protection by criminal laws. The United Nations Declarations and principles for the protection of individual and human rights are fundamental rights also in Cyberspace. The same rights that people have offline must also be protected online. Cyber attacks against critical information infrastructures of sovereign States, public institutions, private industry and individuals, must necessitate a response for global solutions. In conducting investigation and prosecution of cybercrime countries should understand that international coordination and cooperation are necessary in prosecuting cross-border cybercrime. It is critical that the police work closely with government and other elements of the criminal justice system, Interpol, Europol and other international organizations.

Society, Ethics, and the Law: A Reader is an engaging, thoughtful, and academic text designed to help students make connections to ethical issues using real-world examples and thought-provoking discussion questions.

A book that students find interesting and instructors consider educationally valuable, this Fifth Edition of Contemporary Criminal Law combines traditional concepts with thought-provoking cases and engaging learning tools. Taking a casebook approach, the text covers both foundational and emerging legal topics such as terrorism, gangs, cybercrime, and hate crimes, illustrated by real-life examples that students connect with. Clear explanations of criminal law and defenses are complemented by provocative, well-edited cases followed by discussion questions to stimulate critical thinking and in-class discussion. The book provides a contemporary perspective on criminal law that encourages students to actively read and analyze the text. The Fifth Edition is enhanced throughout by new cases that offer the most up-to-date coverage of evolving legal opinions and developments in criminal law. New to This Edition New cases illuminate important concepts, including decisions on criminal acts, criminal intent, parties, corporate crime, kidnapping, identity theft, computer crime, prostitution, terrorism, and more. One or more new You Decide sections in most chapters clarify concepts to illustrate the complexity of legal analysis and enhance the interactive character of the text. Additional hypothetical problems are available on the companion site. New Crime in the News features look at recent events such as the criminal trial of Dylann Roof, the dark web, and the leaking of confidential government documents to help students apply important concepts to real-world scenarios. New and expanded discussions of critical topics cover the Second Amendment and gun control, the Trump administration's stance on marijuana, sentencing guidelines, and criminal defenses.

Gus Martin’s Understanding Homeland Security provides students with a comprehensive introduction to U.S. homeland security in the modern world, with a focus on the post-September 11, 2001 era. This insightful resource examines the theories, agency missions, laws, and regulations governing the homeland security enterprise through the lens of threat scenarios and countermeasures related to terrorism, natural disasters, emergency management, cyber security, and much more. The Third Edition keeps readers on the forefront of homeland security with coverage of cutting-edge topics, such as the role of FEMA and preparedness planning; the role of civil liberty and countering extremism through reform; and hackings during the 2016 and 2018 U.S. elections. Readers will gain much-needed insight into the complex nature of issues surrounding today’s homeland security and learn to think critically to analyze and respond to various threat environments.

Cyber Crime and Cyber Terrorism Investigator’s Handbook is a vital tool in the arsenal of today’s computer programmers, students, and investigators. As computer networks become ubiquitous throughout the world, cyber crime, cyber terrorism, and cyber war have become some of the most concerning topics in today’s security landscape. News stories about Stuxnet and PRISM have brought these activities into the public eye, and serve to show just how effective, controversial, and worrying these tactics can become. Cyber Crime and Cyber Terrorism Investigator’s Handbook describes and analyzes many of the motivations, tools, and tactics behind cyber attacks and the defenses against them. With this book, you will learn about the technological and logistic framework of cyber crime, as well as the social and legal backgrounds of its prosecution and investigation. Whether you are a law enforcement professional, an IT specialist, a researcher, or a student, you will find valuable insight into the world of cyber crime and cyber warfare. Edited by experts in computer security, cyber investigations, and counter-terrorism, and with contributions from computer researchers, legal experts, and law enforcement professionals, Cyber Crime and Cyber Terrorism Investigator’s Handbook will serve as your best reference to the modern world of cyber crime. Written by experts in cyber crime, digital investigations, and counter-terrorism Learn the motivations, tools, and tactics used by cyber-attackers, computer security professionals, and investigators Keep up to date on current national and international law regarding cyber crime and cyber terrorism See just how significant cyber crime has become, and how important cyber law enforcement is in the modern world

The authoritative compendium for students of terrorism and counterterrorism.

Completely revised and updated, this new edition of Terror in the Mind of God incorporates the events of September 11, 2001 into Mark Juergensmeyer's landmark study of religious terrorism. Juergensmeyer explores the 1993 World Trade Center explosion, Hamas suicide bombings, the Tokyo subway nerve gas attack, and the killing of abortion clinic doctors in the United States. His personal interviews with 1993 World Trade Center bomber Mahmud Abouhalima, Christian Right activist Mike Bray, Hamas leaders Sheik Yassin and Abdul Azis Rantisi, and Sikh political leader Simranjit Singh Mann, among others, take us into the mindset of those who perpetrate and support violence in the name of religion.

Cybercrime is a complex and ever-changing phenomenon. This book offers a clear and engaging introduction to this fascinating subject by situating it in the wider context of social, political, cultural and economic change. Taking into account recent developments in social networking and mobile communications, this new edition tackles a range of themes spanning criminology, sociology, law, politics and cultural studies, including: - computer hacking - cyber-terrorism - piracy and intellectual property theft - financial fraud and identity theft - hate speech - internet pornography - online stalking - policing the internet -

surveillance and censorship Complete with useful recommendations for further reading, incisive discussion questions and an updated glossary of key terms, Cybercrime and Society is an essential resource for all students and academics interested in cybercrime and the future of the Internet.

Are you currently helping organisations to navigate digital transformation and disruption? Are you leading your organisation towards a digital future, in an intensely competitive, uncertain market? Strive is a book written by an experienced business psychologist with over twenty years of experience, primarily for consultants, coaches, trainers and human resource management professionals. The book will also resonate with leaders in business who appreciate rigour, academic grounding and authenticity over hype. Dr Kiran Chitta reviews much of the existing literature on organisational and leadership agility. In addition he shares a profoundly personal perspective, anchored in his life and work. His case material is reflective and authentic. It will resonate with those who are looking for inspiration, honesty and actionable principles derived from real work. The book provides a compelling and usable model for agility which is explored in depth. Covering the most recent academic literature, the book points the way to the agile future of work in a digital era.

In the digital era, the Internet has evolved into a ubiquitous aspect of modern society. With the prominence of the Dark Web, understanding the components of the Internet and its available content has become increasingly imperative. The Dark Web:

Breakthroughs in Research and Practice is an innovative reference source for the latest scholarly material on the capabilities, trends, and developments surrounding the secrecy of the Dark Web. Highlighting a broad range of perspectives on topics such as cyber crime, online behavior, and hacking, this book is an ideal resource for researchers, academics, graduate students, and professionals interested in the Dark Web.

Criminalistics is designed for criminal justice students with little to no background in biology or chemistry. The essentials to forensic science are all there, including fingerprint identification, DNA, ballistics, detection of forgeries, forensic toxicology, computer forensics, and the identification and analysis of illicit drugs.

The ability of law enforcement agencies to manage intelligence is key to fighting the war on terror, and a critical foundation of intelligence-led policing is proper analysis of the information gained. Terrorism and Organized Hate Crime: Intelligence Gathering, Analysis, and Investigations, Third Edition provides a methodical approach to analyzing homeland security needs, enabling the law enforcement community to understand the vital role it plays in the war on terrorism. Using techniques applicable to the private and the public sector, the book combines academic, research, and practitioner perspectives to establish a protocol for effectively gathering, analyzing, investigating, and disseminating criminal intelligence. The book demonstrates how to recognize the indicators of an impending act of terrorism or mass violence, how to deter an attack, and how to transform information into intelligence to meet community demands for safety and security. New chapters in this third edition focus on source development and their use in investigations, the role of fusion centers, terrorism financing, the handling of classified materials, and the National Suspicious Activity Reporting (SAR) Initiative. The book also discusses pre-incident indicators, the radicalization process, and behavioral traits associated with terrorism. A one-stop resource for the homeland security, intelligence analyst, and investigative professional, this volume arms those tasked with protecting the public with a solid blueprint for combating and investigating crimes associated with terrorism and hate.

Violence at work, ranging from bullying and mobbing, to threats by psychologically unstable co-workers, sexual harassment and homicide, is increasing worldwide and has reached epidemic levels in some countries. This updated and revised edition looks at the full range of aggressive acts, offers new information on their occurrence and identifies occupations and situations at particular risk. It is organised in three sections: understanding violence at work; responding to violence at work; future action.

Designed for students that are not biology, chemistry, or physics majors, this fully revised and updated Third Edition of the best-selling Criminalistics: Forensic Science, Crime, and Terrorism provides a comprehensive introduction to forensic science, the scientific principles that are the underpinnings of crime analysis, and the practical application of these principles. Essential topics such as fingerprint identification, DNA, ballistics, detection of forgeries, forensic toxicology, computer forensics, and the identification and analysis of illicit drugs are thoroughly explained in a reader-friendly manner. Unlike comparable texts, the Third Edition includes coverage of important terrorism and homeland security issues, including explosives, cybercrime, cyberterrorism, and weapons of mass destruction. The text is also the only book on the market with a detailed description of DNA and CODIS techniques used by professionals.

The Third Edition of Terrorism in Perspective, like its two successful predecessors, takes a broad-based approach that emphasizes the historical, cultural, political, religious, social, and economic factors that underlie an understanding of both global and domestic terrorism. This unique text-reader combines original essays with the best of the existing literature on terrorism. Each chapter of this text begins with an overview essay written by the authors, followed by two relevant and engaging articles culled from a wide variety of popular, academic, and governmental sources. This is the only major terrorism text to incorporate readings from top terrorism experts into a traditional textbook format, allowing readers to deepen their understanding of each aspect of terrorism.

Population Health Informatics addresses the growing opportunity to utilize technology to put into practice evidence-based solutions to improve population health outcomes across diverse settings. The book focuses on how to operationalize population informatics solutions to address important public health challenges impacting individuals, families, communities, and the environment in which they live. The book uniquely uses a practical, step-by-step approach to implement evidence-based, data- driven population informatics solutions.

This book critically examines the complex interactions between media and crime. Written with an engaging and authoritative voice, it guides you through all the key issues, ranging from news reporting of crime, media constructions of children and women, moral panics, and media and the police to 'reality' crime shows, surveillance and social control. This third edition: Explores innovations in technology and forms of reporting, including citizen journalism. Examines the impact of new media including mobile, Internet and digital technologies, and social networking sites. Features chapters dedicated to the issues around cybercrime and crime film, along with new content on terrorism and the media. Shows you how to research media and crime. Includes discussion questions, further reading and a glossary. Now features a companion website, complete with links to journal articles, relevant websites and blogs. This is essential reading for your studies in criminology, media studies, cultural studies and sociology.

The Key Approaches to Criminology series celebrates the removal of traditional barriers between disciplines and, specifically, reflects criminology’s interdisciplinary nature and focus. It brings together some of the leading scholars working at the intersections of criminology and related subjects. Each book in the series helps readers to make intellectual connections between criminology and other discourses, and to understand the importance of studying crime and criminal justice within the context of broader debates. The series is intended to have appeal across the entire range of undergraduate and postgraduate studies and beyond, comprising books which offer introductions to the fields as well as advancing ideas and knowledge in their subject areas.

Revised edition of: Digital crime and digital terrorism / Robert W. Taylor ... [et al.], 2nd ed.

This volume deals with the very novel issue of cyber laundering. The book investigates the problem of cyber laundering legally and sets out why it is of a grave legal concern locally and internationally. The book looks at the current state of laws and how they do not fully come to grips with the problem. As a growing practice in these modern times, and manifesting through technological innovations, cyber laundering is the birth child of money laundering and cybercrime. It concerns how the internet is used for 'washing' illicit proceeds of crime. In addition to exploring the meaning and ambits of the problem with concrete real-life examples, more importantly, a substantial part of the work innovates ways in which the dilemma can be curbed legally. This volume delves into a very grey area of law, daring a yet unthreaded territory and scouring undiscovered paths where money laundering, cybercrime, information technology and international law converge. In addition to unearthing such complexity, the hallmark of this book is in the innovative solutions and dynamic remedies it postulates.

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.

"This book reviews problems, issues, and presentations of the newest research in the field of cyberwarfare and cyberterrorism. While enormous efficiencies have been gained as a result of computers and telecommunications technologies, use of these systems and networks translates into a major concentration of information resources, createing a vulnerability to a host of attacks and exploitations"--Provided by publisher.

Updated to include the most current events and information on cyberterrorism, the second edition of Computer Forensics: Cybercriminals, Laws, and Evidence continues to balance technicality and legal analysis as it enters into the world of cybercrime by exploring what it is, how it is investigated, and the regulatory laws around the collection and use of electronic evidence. Students are introduced to the technology involved in computer forensic investigations and the technical and legal difficulties involved in searching, extracting, maintaining, and storing electronic evidence, while simultaneously looking at the legal implications of such

investigations and the rules of legal procedure relevant to electronic evidence. Significant and current computer forensic developments are examined, as well as the implications for a variety of fields including computer science, security, criminology, law, public policy, and administration.
Cyberterrorism and the misuse of Internet for terrorist purposes represents a serious threat, since many essential aspects of today's society are completely dependent upon the functioning of computer systems and the Internet. Further to the adoption by the Council of Europe of the Cybercrime Convention (2001) and the Convention on the Prevention of Terrorism (2005), its Committee of Experts on Terrorism (CODEXTER) has been studying this matter and surveying the situation in member states to evaluate whether existing legal instruments are sufficient to combat this emerging form of crime. This publication contains an expert report prepared by the Max Planck Institute, which evaluates the main problems that arise in the context of cyberterrorism and provides recommendations, together with reports on the situation in the member and observer states of the Council of Europe and the relevant Council of Europe conventions

This book examines the UK’s response to terrorist communication. Its principle question asks, has individual privacy and collective security been successfully managed and balanced? The author begins by assessing several technologically-based problems facing British law enforcement agencies, including use of the Internet; the existence of ‘darknet’; untraceable Internet telephone calls and messages; smart encrypted device direct messaging applications; and commercially available encryption software. These problems are then related to the traceability and typecasting of potential terrorists, showing that law enforcement agencies are searching for needles in the ever-expanding haystacks. To this end, the book examines the bulk powers of digital surveillance introduced by the Investigatory Powers Act 2016. The book then moves on to assess whether these new powers and the new legislative safeguards introduced are compatible with international human rights standards. The author creates a ‘digital rights criterion’ from which to challenge the bulk surveillance powers against human rights norms. Lord Carlile of Berriew CBE QC in recommending this book notes this particular legal advancement, commenting that rightly so the author concludes the UK has fairly balanced individual privacy with collective security. The book further analyses the potential impact on intelligence exchange between the EU and the UK, following Brexit. Using the US as a case study, the book shows that UK laws must remain within the ambit of EU law and the Court of Justice of the European Union's (CJEU's) jurisprudence, to maintain the effectiveness of the exchange. It addresses the topics with regard to terrorism and counterterrorism methods and will be of interest to researchers, academics, professionals, and students researching counterterrorism and digital electronic communications, international human rights, data protection, and international intelligence exchange. How do we understand illicit violence? Can we prevent it? Building on behavioral science and economics, this book begins with the idea that humans are more predictable than we like to believe, and this ability to model human behavior applies equally well to leaders of violent and coercive organizations as it does to everyday people. Humans ultimately seek survival for themselves and their communities in a world of competition. While the dynamics of 'us vs. them' are divisive, they also help us to survive. Access to increasingly larger markets, facilitated through digital communications and social media, creates more transnational opportunities for deception, coercion, and violence. If the economist's perspective helps to explain violence, then it must also facilitate insights into promoting peace and security. If we can approach violence as behavioral scientists, then we can also better structure our institutions to create policies that make the world a more secure place, for us and for future generations.

This new Handbook provides a comprehensive, state-of-the-art overview of current knowledge and debates on terrorism and counterterrorism, as well as providing a benchmark for future research. The attacks of 9/11 and the ‘global war on terror’ and its various legacies have dominated international politics in the opening decades of the 21st century. In response to the dramatic rise of terrorism, within the public eye and the academic world, the need for an accessible and comprehensive overview of these controversial issues remains profound. The Routledge Handbook of Terrorism and Counterterrorism seeks to fulfil this need. The volume is divided into two key parts: Part I: Terrorism: This section provides an overview of terrorism, covering the history of terrorism, its causes and characteristics, major tactics and strategies, major trends and critical contemporary issues such as radicalisation and cyber-terrorism. It concludes with a series of detailed case studies, including the IRA, Hamas and Islamic State. Part II: Counterterrorism: This part draws on the main themes and critical issues surrounding counterterrorism. It covers the major strategies and policies, key events and trends and the impact and effectiveness of different approaches. This section also concludes with a series of case studies focused on major counterterrorism campaigns. This book will be of great interest to all students of terrorism and counterterrorism, political violence, counter-insurgency, criminology, war and conflict studies, security studies and IR more generally.

This definitive reference resource on cyber warfare covers all aspects of this headline topic, providing historical context of cyber warfare and an examination its rapid development into a potent technological weapon of the 21st century. • Provides comprehensive coverage of the major individuals, organizations, impacts, and issues related to cyber warfare that enables readers to better understanding of the impact of cyber warfare on modern conflicts • Includes a detailed chronology that documents the evolution and use of cyber warfare over the past few decades • Supplies further readings and a lengthy bibliography that offer a wealth of options to students conducting extensive research on the subject

Revised edition of the authors' Digital crime and digital terrorism, [2015]

Digital Crime and Digital TerrorismPrentice Hall

This textbook is a comprehensive introduction to global terrorism, intended to help students understand the history, politics, ideologies & strategies of both contemporary & older terrorist groups.

Is one person's terrorist another's freedom fighter? Is terrorism crime or war? Can there be a "War on Terror"? For many, the terrorist attacks of September 2001 changed the face of the world, pushing terrorism to the top of political agendas, and leading to a series of world events including the war in Iraq and the invasion of Afghanistan. The recent terror attacks in various European cities have shown that terrorism remains a crucial issue today. Charting a clear path through the efforts to understand and explain modern terrorism, Charles Townshend examines the historical, ideological, and local roots of terrorist violence. Starting from the question of why terrorists find it so easy to seize public attention, this new edition analyzes the emergence of terrorism as a political strategy, and discusses the objectives which have been pursued by users of this strategy from French revolutionaries to Islamic jihadists. Considering the kinds of groups and individuals who adopt terrorism, Townshend discusses the emergence of ISIS and the upsurge in individual suicide action, and explores the issues involved in finding a proportionate response to the threat they present, particularly by liberal democratic societies. Analyzing the growing use of knives and other edged weapons in attacks, and the issue of "cyberterror," Townshend details the use of counterterrorist measures, from control orders to drone strikes, including the Belgian and French responses to the Brussels, Paris, Nice, and Rouen attacks. ABOUT THE SERIES: The Very Short Introductions series from Oxford University Press contains hundreds of titles in almost every subject area. These pocket-sized books are the perfect way to get ahead in a new subject quickly. Our expert authors combine facts, analysis, perspective, new ideas, and enthusiasm to make interesting and challenging topics highly readable.