Budapest Convention On Cybercrime Wordpress

Cybercrime: An Encyclopedia of Digital CrimeABC-CLIO

This important reference work is an extensive, up-to-date resource for students wanting to immerse themselves in the world of cybercrime, or for those seeking further knowledge of specific attacks both domestically and internationally. Cybercrime is characterized by criminal acts that take place in the borderless digital realm. It takes on many forms, and its perpetrators and victims are varied. From financial theft, destruction of systems, fraud, corporate espionage, and ransoming of information to the more personal, such as stalking and web-cam spying as well as cyberterrorism, this work covers the full spectrum of crimes committed via cyberspace. This comprehensive encyclopedia covers the most noteworthy attacks while also focusing on the myriad issues that surround cybercrime. It includes entries on such topics as the different types of cyberattacks, cybercrime techniques, specific cybercriminals and cybercrime groups, and cybercrime investigations. While objective in its approach, this book does not shy away from covering such relevant, controversial topics as Julian Assange and Russian interference in the 2016 U.S. presidential election. It also provides detailed information on all of the latest developments in this constantly evolving field. Includes an introductory overview essay that discusses all aspects of cybercrime—how it's defined, how it developed, and its massive expansion in recent years Offers a wide array of entries regarding cybercrime and the many ways it can be committed Explores the largest, most costly cyber attacks on a variety of victims, including corporations, governments, consumers, and individuals Provides up-to-date information on the ever-evolving field of cybercrime

This book presents a novel framework to reconceptualize Internet governance and better manage cyber attacks. Specifically, it makes an original contribution by examining the potential of polycentric regulation to increase accountability through bottom-up action. It also provides a synthesis of the current state of cybersecurity research, bringing features of the cloak and dagger world of cyber attacks to light and comparing and contrasting the cyber threat to all relevant stakeholders. Throughout the book, cybersecurity is treated holistically, covering outstanding issues in law, science, economics, and politics. This interdisciplinary approach is an exemplar of how strategies from different disciplines as well as the private and public sectors may cross-pollinate to enhance cybersecurity. Case studies and examples illustrate what is at stake and identify best practices. The book discusses technical issues of Internet governance and cybersecurity while presenting the material in an informal, straightforward manner. The book is designed to inform readers about the interplay of Internet governance and cybersecurity and the potential of polycentric regulation to help foster cyber peace.

?The use of computers and other technology introduces a range of risks to electoral integrity. Cybersecurity for Elections explains how cybersecurity issues can compromise traditional aspects of elections, explores how cybersecurity interacts with the broader electoral environment, and offers principles for managing cybersecurity risks.

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

International cooperation and international relations with regards to cyberspace Technical challenges and requirements Conflict in cyberspace Regulations and standards Virtualisation

This volume focuses on the responsibilities of online service providers (OSPs) in contemporary societies. It examines the complexity and global dimensions of the rapidly evolving and serious challenges posed by the exponential development of Internet services and resources. It looks at the major actors – such as Facebook, Google, Twitter, and Yahoo! – and their significant influence on the informational environment and users' interactions within it, as well as the responsibilities and liabilities such influence entails. It discusses the position of OSPs as information gatekeepers and how they have gone from offering connecting and information-sharing services to paying members to providing open, free infrastructure and applications that facilitate digital expression and the communication of information. The book seeks consensus on the principles that should shape OSPs' responsibilities and practices, taking into account business ethics and policies. Finally, it discusses the rights of users and international regulations that are in place or currently lacking.

This report provides strategic advice on preparing for and responding to potential global shocks.

This is the first book to present a full, socio-technical-legal picture on the security practices of cyber criminals, based on confidential police sources related to some of the world's most serious and organized criminals.

Cyberspace is everywhere in today's world and has significant implications not only for global economic activity, but also for international politics and transnational social relations. This compilation addresses for the first time the "cyberization" of international relations - the growing dependence of actors in IR on the infrastructure and instruments of the internet, and the penetration of cyberspace into all fields of their activities. The volume approaches this topical issue in a comprehensive and interdisciplinary fashion, bringing together scholars from disciplines such as IR, security studies, ICT studies and philosophy as well as experts from everyday cyber-practice. In the first part, concepts and theories are presented to shed light on the relationship between cyberspace and international relations, discussing implications for the discipline and presenting fresh and innovative theoretical approaches. Contributions in the second part focus on specific empirical fields of activity (security, economy, diplomacy, cultural activity, transnational communication, critical infrastructure, cyber espionage, social media,

and more) and address emerging challenges and prospects for international politics and relations.

Welcome to the all-new second edition of Navigating the Digital Age. This edition brings together more than 50 leaders and visionaries from business, science, technology, government, aca¬demia, cybersecurity, and law enforce¬ment. Each has contributed an exclusive chapter designed to make us think in depth about the ramifications of this digi-tal world we are creating. Our purpose is to shed light on the vast possibilities that digital technologies present for us, with an emphasis on solving the existential challenge of cybersecurity. An important focus of the book is centered on doing business in the Digital Age-par¬ticularly around the need to foster a mu¬tual understanding between technical and non-technical executives when it comes to the existential issues surrounding cybersecurity. This book has come together in three parts. In Part 1, we focus on the future of threat and risks. Part 2 emphasizes lessons from today's world, and Part 3 is designed to help you ensure you are covered today. Each part has its own flavor and personal¬ity, reflective of its goals and purpose. Part 1 is a bit more futuristic, Part 2 a bit more experiential, and Part 3 a bit more practical. How we work together, learn from our mistakes, deliver a secure and safe digital future-those are the elements that make up the core thinking behind this book. We cannot afford to be complacent. Whether you are a leader in business, government, or education, you should be knowledgeable, diligent, and action-oriented. It is our sincerest hope that this book provides answers, ideas, and inspiration.If we fail on the cybersecurity front, we put all of our hopes and aspirations at risk. So we start this book with a simple proposition: When it comes to cybersecurity, we must succeed.

Cyber Crimes against Women in India reveals loopholes in the present laws and policies of the Indian judicial system, and what can be done to ensure safety in cyberspace. The book is a significant contribution to socio-legal research on online crimes targeting teenage girls and women. It shows how they become soft targets of trolling, online grooming, privacy infringement, bullying, pornography, sexual defamation, morphing, spoofing and so on. The authors address various raging debates in the country such as how women can be protected from cybercrimes; what steps can be taken as prevention and as recourse to legal aid and how useful and accessible cyber laws are. The book provides detailed answers to a wide array of questions that bother scholars and charts a way forward.

Electronic commerce (e-commerce) is rapidly transforming the way in which enterprises are interacting among each other as well as with consumers and governments. Despite important potential benefits, businesses and consumers in developing countries were for a long time slow to exploit e-commerce. As a result of changes in the evolving landscape for information and communications technologies (ICTs), this pattern is now changing, and e-commerce is growing rapidly in emerging markets and developing economies. Against this background, this publication revisits the potential opportunities and risks of e-commerce and examines how countries can benefit the most from the phenomenon in today's Information Society. Using official statistics and private sector data, it provides an up-to-date review of global and regional trends related to e-commerce in view of changes in the ICT landscape, focusing on developing countries while drawing lessons from developed countries.

Shortlisted for the Orwell Prize and the CWA Gold Dagger for Non-Fiction Award The benefits of living in a digital, globalised society are enormous; so too are the dangers. The world has become a law enforcer's nightmare and every criminal's dream. We bank online, shop online, date, learn, work and live online. But have the institutions that keep us safe on the streets learned to protect us in the burgeoning digital world? Have we become complacent about our personal security -- sharing our thoughts, beliefs and the details of our daily lives with anyone who cares to relieve us of them? In this fascinating and compelling book, Misha Glenny, author of the international bestseller McMafia, explores the three fundamental threats facing us in the twenty-first century: cyber crime, cyber warfare and cyber industrial

espionage. Governments and the private sector are losing billions of dollars each year, fighting an ever-morphing, often invisible, and highly intelligent new breed of criminal: the hacker. Glenny has travelled and trawled the world. And by exploring the rise and fall of the criminal website, DarkMarket, he has uncovered the most vivid, alarming and illuminating stories. Whether JiLsi or Matrix, Iceman, Master Splynter or Lord Cyric; whether Detective Sergeant Chris Dawson in Bolton or Agent Keith Mularski in Pittsburgh, Glenny has tracked down and interviewed all the players -- the criminals, the geeks, the police, the security experts and the victims -- and he places everyone and everything in a rich brew of politics, economics and history. The result is simply unputdownable. DarkMarket is authoritative and completely engrossing. It's a must-read for everyone who uses a computer: the essential crime book for our times.

The world order built upon the Peace of Westphalia is faltering. State fragility or failure are endemic, with no fewer than one-third of the states in the United Nations earning a "high warning"-or worse-in the Fragile States Index, and an equal number suffering a decline in sustainability over the past decade.1 State weakness invites a range of illicit actors, including international terrorists, globally networked insurgents, and transnational criminal organizations (TCOs). The presence and operations of these entities keep states weak and incapable of effective governance, and limit the possibility of fruitful partnerships with the United States and its allies. Illicit organizations and their networks fuel corruption, eroding state legitimacy among the governed, and sowing doubt that the state is a genuine guardian of the public interest. These networks can penetrate the state, leading to state capture, and even criminal sovereignty.2 A growing number of weak and corrupt states is creating gaping holes in the global rule-based system of states that we depend on for our security and prosperity. Indeed, the chapters of this book suggest the emergence of a highly adaptive and parasitic alternative ecosystem, based on criminal commerce and extreme violence, with little regard for what we commonly conceive of as the public interest or the public good. The last 10 years have seen unprecedented growth in interactivity between and among a wide range of illicit networks, as well as the emergence of hybrid organizations that use methods characteristic of both terrorist and criminal groups. In a convergence of interests, terrorist organizations collaborate with cartels, and trafficking organizations collude with insurgents. International terrorist organizations, such as al-Qaeda and Hezbollah, engage energetically in transnational crime to raise funds for their operations. Prominent criminal organizations like Los Zetas in Mexico and D-Company in Pakistan have adopted the symbolic violence of terrorists-the propaganda of the deed-to secure their "turf." And networked insurgents, such as the Islamic State of Iraq and the Levant (ISIL), the Revolutionary Armed Forces of Colombia (FARC), and the Liberation Tigers of Tamil Eelam (LTTE), have adopted the techniques of both crime and terror.

This revised edition of Bookmarks reflects the end of the coordination of the youth campaign by the Council Europe. The campaign may be officially over, but the education and awareness-raising to counter hate speech and promote human rights values remain an urgent task for young people of all ages. The work of the Council of Europe for democracy is strongly based on education: education in schools, and education as a lifelong learning process of practising democracy, such as in non-formal learning activities. Human rights education and education for democratic citizenship form an integral part of what we have to secure to make democracy sustainable. Hate speech is one of the most worrying forms of racism and discrimination prevailing across Europe and amplified by the Internet and social media. Hate speech online is the visible tip of the iceberg of intolerance and ethnocentrism. Young people are directly concerned as agents and victims of online abuse of human rights; Europe needs young people to care and look after human rights, the life insurance for democracy. Bookmarks was originally published to support the No Hate Speech Movement youth campaign of the Council of Europe for human rights online. Bookmarks is useful for educators wanting to address hate speech online from a human rights perspective, both inside and outside the formal education

system. The manual is designed for working with learners aged 13 to 18 but the activities can be adapted to other age ranges.

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.

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.

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

The growth and health of our digital economies and societies depend on the core protocols and infrastructure of the Internet. This

technical and logical substructure of our digital existence is now in need of protection against unwarranted interference in order to sustain the growth and the integrity of the global Internet. The Internet's key protocols and infrastructure can be considered a global public good that provides benefits to everyone in the world. Countering the growing state interference with this 'public core of the Internet' requires a new international agenda for Internet governance that departs from the notion of a global public good. Core ingredients of this strategy are: - To establish and disseminate an international norm stipulating that the Internet's public core - its main protocols and infrastructure- should be considered a neutral zone, safeguarded against unwarranted intervention by governments. - To advocate efforts to clearly differentiate at the national and international level between Internet security (security of the Internet infrastructure) and national security (security through the Internet). - To broaden the arena for cyber diplomacy to include new coalitions of states (including the so called 'swing states') and private companies, including the large Internet companies as well as Internet intermediaries such as Internet Service Providers.

Effective communication requires a common language, a truth that applies to science and mathematics as much as it does to culture and conversation. Standards and Standardization: Concepts, Methodologies, Tools, and Applications addresses the necessity of a common system of measurement in all technical communications and endeavors, in addition to the need for common rules and guidelines for regulating such enterprises. This multivolume reference will be of practical and theoretical significance to researchers, scientists, engineers, teachers, and students in a wide array of disciplines.

This book offers an introduction to Information Technology with regard to peace, conflict, and security research, a topic that it approaches from natural science, technical and computer science perspectives. Following an initial review of the fundamental roles of IT in connection with peace, conflict and security, the contributing authors address the rise of cyber conflicts via information warfare, cyber espionage, cyber defence and Darknets. The book subsequently explores recent examples of cyber warfare, including: • The Stuxnet attack on Iran’s uranium refining capability • The hacking of the German Federal Parliament’s internal communication system • The Wannacry malware campaign, which used software stolen from a US security agency to launch ransomware attacks worldwide The book then introduces readers to the concept of cyber peace, including a discussion of confidence and security-building measures. A section on Cyber Arms Control draws comparisons to global efforts to control chemical warfare, to reduce the risk of nuclear war, and to prevent the militarization of space. Additional topics include the security of critical information infrastructures, and cultural violence and peace in social media. The book concludes with an outlook on the future role of IT in peace and security. Information Technology for Peace and Security breaks new ground in a largely unexplored field of study, and offers a valuable asset for a broad readership including students, educators and working professionals in computer science, IT security, peace and conflict studies, and political science.

The frontiers are the future of humanity. Peacefully and sustainably managing them is critical to both security and prosperity in the twenty-first century.

This book explores the changing nature of international law and its ability to respond to the contemporary issues related to

international environment, trade and information technology. The evolution of international law has reached a stage where we are witnessing diminishing power of the state and its capacity to deal with the economic matters challenging the existing notions of territory and sovereignty. Recent trends in international law and international relations show that states no longer have exclusive control over the decision-making process at the global level. Keeping this in mind, the book brings together the perspectives of various international and national scholars. The book considers diverse issues such as, sustainable development, climate change, global warming, Rio+20, technology transfer, agro-biodiversity and genetic resource, authority for protection of environment, human right to water, globalization, human rights, sui generis options in IP laws, impact of liberalization on higher education, regulation of international trade, intellectual property rights, collective administration of copyright, broadcast reproduction rights, implementation of copyright law, communication rights under copyright law, arbitration for IP disputes, doctrine of exhaustion of rights, trans-border reputation of trademark, information as an asset, cyber obscenity and pornography, e-governance, taxation of e-commerce, computer crime, information technology, domain names, research excellence in legal education, ideological perspective on legal education, challenges for law teachers, and clinical legal education. The topics, though diverse, are closely interrelated, with the common concern throughout being that the global environment, international trade, information technology and legal education need appropriate national normative and institutional responses as well as the global cooperation of members of the international community. Presenting reflections of a number of Asian, African and European scholars on these varied facets, the book is of great value to scholars, practitioners, teachers and students associated with contemporary international law.

This report examines governance frameworks to counter illicit trade. It looks at the adequacy and effectiveness of sanctions and penalties applicable, the steps parties engaged in illicit trade take to lower the risk of detection - for example through small shipments - and the use of free trade zones as hubs for managing trade in illicit products. It also identifies gaps in enforcement that may need to be addressed. The report provides an overview of selected enforcement issues in BRICS economies (Brazil, China, India, the Russian Federation and South Africa).

Moving toward universal access to financial services is within reach, thanks to new technologies, transformative business models, and ambitious reforms. Instruments such as e-money accounts and mobile accounts, along with debit cards and low-cost traditional bank accounts, can significantly increase financial access for those who are excluded. Bringing e-Money to the Poor: Successes and Failures examines the lessons of success from four country case studies of “gazelles†?†•Kenya, South Africa, Sri Lanka, and Thailand†•that leapt from limitation to innovation by successfully enabling the deployment of e-money technology. These countries have thereby transformed the landscape of financial access to their poor. In addition, two country case studies (Maldives and the Philippines) yield lessons learned from constraints that stalled e-money deployments. Because technology is not a silver bullet, the case studies also explore other strategic elements that need to be in place for a country to expand access to financial services through digital

technology.

This book provides an overview of recent and future legal developments concerning the digital era, to examine the extent to which law has or will further evolve in order to adapt to its new digitalized context. More specifically it focuses on some of the most important legal issues found in areas directly connected with the Internet, such as intellectual property, data protection, consumer law, criminal law and cybercrime, media law and, lastly, the enforcement and application of law. By adopting this horizontal approach, it highlights – on the basis of analysis and commentary of recent and future EU legislation as well as of the latest CJEU and ECtHR case law – the numerous challenges faced by law in this new digital era. This book is of great interest to academics, students, researchers, practitioners and policymakers specializing in Internet law, data protection, intellectual property, consumer law, media law and cybercrime as well as to judges dealing with the application and enforcement of Internet law in practice.

Providing comprehensive coverage of cyberspace and cybersecurity, this textbook not only focuses on technologies but also explores human factors and organizational perspectives and emphasizes why asset identification should be the cornerstone of any information security strategy. Topics include addressing vulnerabilities, building a secure enterprise, blocking intrusions, ethical and legal issues, and business continuity. Updates include topics such as cyber risks in mobile telephony, steganography, cybersecurity as an added value, ransomware defense, review of recent cyber laws, new types of cybercrime, plus new chapters on digital currencies and encryption key management.

The emergence of the cloud as infrastructure: experts from a range of disciplines consider policy issues including reliability, privacy, consumer protection, national security, and copyright. The emergence of cloud computing marks the moment when computing has become, materially and symbolically, infrastructure—a sociotechnical system that is ubiquitous, essential, and foundational. Increasingly integral to the operation of other critical infrastructures, such as transportation, energy, and finance, it functions, in effect, as a meta-infrastructure. As such, the cloud raises a variety of policy and governance issues, among them market regulation, fairness, access, reliability, privacy, national security, and copyright. In this book, experts from a range of disciplines offer their perspectives on these and other concerns. The contributors consider such topics as the economic implications of the cloud's shifting of computing resources from ownership to rental; the capacity of regulation to promote reliability while preserving innovation; the applicability of contract theory to enforce service guarantees; the differing approaches to privacy taken by United States and the European Union in the post-Snowden era; the delocalization or geographic dispersal of the archive; and the cloud-based virtual representations of our body in electronic health data. Contributors Nicholas Bauch, Jean-François Blanchette, Marjory Blumenthal, Sandra Braman, Jonathan Cave, Lothar Determann, Luciana Duranti, Svitlana Kobzar, William Lehr,

David Nimmer, Andrea Renda, Neil Robinson, Helen Rebecca Schindler, Joe Weinman, Christopher S. Yoo
In December 1999, more than forty members of government, industry, and academia assembled at the Hoover Institution to discuss this problem and explore possible countermeasures. The Transnational Dimension of Cyber Crime and Terrorism summarizes the conference papers and exchanges, addressing pertinent issues in chapters that include a review of the legal initiatives undertaken around the world to combat cyber crime, an exploration of the threat to civil aviation, analysis of the constitutional, legal, economic, and ethical constraints on use of technology to control cyber crime, a discussion of the ways we can achieve security objectives through international cooperation, and more. Much has been said about the threat posed by worldwide cyber crime, but little has been done to protect against it. A transnational response sufficient to meet this challenge is an immediate and compelling necessity—and this book is a critical first step in that direction.

This book provides readers with up-to-date research of emerging cyber threats and defensive mechanisms, which are timely and essential. It covers cyber threat intelligence concepts against a range of threat actors and threat tools (i.e. ransomware) in cutting-edge technologies, i.e., Internet of Things (IoT), Cloud computing and mobile devices. This book also provides the technical information on cyber-threat detection methods required for the researcher and digital forensics experts, in order to build intelligent automated systems to fight against advanced cybercrimes. The ever increasing number of cyber-attacks requires the cyber security and forensic specialists to detect, analyze and defend against the cyber threats in almost real-time, and with such a large number of attacks is not possible without deeply perusing the attack features and taking corresponding intelligent defensive actions – this in essence defines cyber threat intelligence notion. However, such intelligence would not be possible without the aid of artificial intelligence, machine learning and advanced data mining techniques to collect, analyze, and interpret cyber-attack campaigns which is covered in this book. This book will focus on cutting-edge research from both academia and industry, with a particular emphasis on providing wider knowledge of the field, novelty of approaches, combination of tools and so forth to perceive reason, learn and act on a wide range of data collected from different cyber security and forensics solutions. This book introduces the notion of cyber threat intelligence and analytics and presents different attempts in utilizing machine learning and data mining techniques to create threat feeds for a range of consumers. Moreover, this book sheds light on existing and emerging trends in the field which could pave the way for future works. The inter-disciplinary nature of this book, makes it suitable for a wide range of audiences with backgrounds in artificial intelligence, cyber security, forensics, big data and data mining, distributed systems and computer networks. This would include industry professionals, advanced-level students and researchers that work within these related fields.

Media scholars, artists, activists, and journalists discuss how the uses of the emerging “Social Web” redefine the public sphere and influence mainstream journalism. In an age of proliferating media and news sources, who has the power to define reality? When the dominant media declared the existence of WMDs in Iraq, did that make it a fact? Today, the “Social Web” (sometimes known as Web 2.0, groupware, or the participatory web)—epitomized by blogs, viral videos, and YouTube—creates new pathways for truths to emerge and makes possible new tactics for media activism. In Digital Media and Democracy, leading scholars in media and communication studies, media activists, journalists, and artists explore the contradiction at the heart of the relationship between truth and power today: the fact that the radical democratization of knowledge and multiplication of sources and voices made possible by digital media coexists with the blatant falsification of information by political and corporate powers. The book maps a new digital media landscape that features citizen journalism, The Daily Show, blogging, and alternative media. The contributors discuss broad questions of media and politics, offer nuanced analyses of change in journalism, and undertake detailed examinations of the use of web-based media in shaping political and social movements. The chapters include not only essays by noted media scholars but also interviews with such journalists and media activists as Amy Goodman of Democracy Now!, Media Matters host Robert McChesney, and Hassan Ibrahim of Al Jazeera. Contributors and Interviewees Shaina Anand, Chris Atton, Megan Boler, Axel Bruns, Jodi Dean, Ron Deibert, Deepa Fernandes, Amy Goodman, Brian Holmes, Hassan Ibrahim, Geert Lovink, Nathalie Magnan, Robert McChesney, Graham Meikle, Susan Moeller, Alessandra Renzi, Ricardo Rosas, Trebor Scholz, D. Travers Scott, Rebecca Statzel

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.

An invaluable resource for students of law, politics, international relations and technology as well as for diplomats and civil society actors, this publication demonstrates how the Council of Europe contributes to ensuring that everyone’s voice online can be heard. This is key to

sustainable, human rights oriented and people-centred digitalisation. Human rights matter on the internet. Without freedom of expression, people cannot participate in everything that the information society has to offer. Yet online free speech is in danger. Between state laws, private rules and algorithms, full participation in the online communicative space faces many challenges. This publication explores the profound impact of the internet on free expression and how it can be effectively secured online. The second, updated edition of this introduction into the protection of freedom of expression online answers essential questions regarding the extent and limits of freedom of expression online and the role of social networks, courts, states and organisations in online communication spaces. In clear language, with vivid examples spanning two decades of internet law, the authors answer questions on freedom of expression in cyberspace. Addressing issues from the protection of bloggers to the right to access online information, the publication also shows the importance of the standard-setting, monitoring and promotion activities of international and non-governmental organisations and includes a chapter on relevant national practice. It pays special attention to the role of European human rights law and the Council of Europe as this region’s most important human rights organisation.

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

The goal of the book is to present the latest research on the new challenges of data technologies. It will offer an overview of the social, ethical and legal problems posed by group profiling, big data and predictive analysis and of the different approaches and methods that can be used to address them. In doing so, it will help the reader to gain a better grasp of the ethical and legal conundrums posed by group profiling. The volume first maps the current and emerging uses of new data technologies and clarifies the promises and dangers of group profiling in real life situations. It then balances this with an analysis of how far the current legal paradigm grants group rights to privacy and data protection, and discusses possible routes to addressing these problems. Finally, an afterword gathers the conclusions reached by the different authors and discuss future perspectives on regulating new data technologies.

Alat bukti berperan penting dalam pembuktian perkara di depan persidangan, karena dengan alat bukti yang cukup dapat dibuktikan salah atau tidaknya pelaku tindak pidana. Alat bukti yang selama ini dikenal dalam persidangan perkara pidana diatur dalam Pasal 184 KUHAP, sedangkan dalam persidangan perkara perdata berpedoman pada Pasal 164 HIR. Seiring dengan kemajuan zaman maka tipologi kejahatan juga semakin berkembang bentuknya, terlebih dengan kecanggihan teknologi saat ini yang sudah memasuki masa revolusi industri 4.0, kejahatan yang dahulunya dilakukan secara konvensional saat ini dilakukan dengan menggunakan teknologi informatika yang canggih, sehingga ada kalanya tidak mudah untuk membuktikan kejahatan tersebut, dan untuk itulah maka diperlukan pembuktian dengan menggunakan bukti elektronik, di mana bukti elektronik ini mulai diakui dalam sistem hukum Indonesia sebagai salah satu alat bukti di persidangan. Para pihak yang terlibat di persidangan tentu saja memerlukan seorang ahli digital forensik yang dapat membuat bukti elektronik itu berbicara di persidangan, sehingga akan membuat terang jalannya persidangan. Buku ini akan mengajak pembacanya untuk memahami seluk beluk mengenai pembuktian, serta bagaimana bukti elektronik tersebut dapat digunakan untuk pembuktian perkara di

persidangan.
Copyright: 61bb524a19039f760453063f804709b9