Future Crimes Inside The Digital Underground And The Battle For Our Connected World

As a business leader, you might think you have cybersecurity under control because you have a great IT team. But managing cyber risk requires more than firewalls and good passwords. Cash flow, insurance, relationships, and legal affairs for an organization all play major roles in managing cyber risk. Treating cybersecurity as “just an IT problem” leaves an organization exposed and unprepared. Therefore, executives must take charge of the big picture. Cybersecurity: A Business Solution is a concise guide to managing cybersecurity from a business perspective, written specifically for the leaders of small and medium businesses. In this book you will find a step-by-step approach to managing the financial impact of cybersecurity. The strategy provides the knowledge you need to steer technical experts toward solutions that fit your organization’s business mission. The book also covers common pitfalls that lead to a false sense of security. And, to help offset the cost of higher security, it explains how you can leverage investments in cybersecurity to capture market share and realize more profits. The book’s companion material also includes an executive guide to The National Institute of Standards and Technology (NIST) Cybersecurity Framework. It offers a business level overview of the following key terms and concepts, which are central to managing its adoption. TiersProfilesFunctionsInformative References

This book covers the developing field of open source research and discusses how to use social media, satellite imagery, big data analytics, and user-generated content to strengthen human rights research and investigations. The topics are presented in an accessible format through extensive use of images and data visualization (éditeur).

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.

From the New York Times bestselling author of How We Got To Now, Farsighted, and Extra Life Combining the deft social analysis of Where Good Ideas Come From with the optimistic arguments of Everything Bad Is Good For You, New York Times bestselling author Steven Johnson’s Future Perfect makes the case that a new model of political change is on the rise, transforming everything from local governments to classrooms, from protest movements to health care. Johnson paints a compelling portrait of this new political worldview -- influenced by the success and interconnectedness of the Internet, by peer networks, but not dependent on high-tech solutions -- that breaks with the conventional categories of liberal or conservative, public vs. private thinking. With his acclaimed gift for multi-disciplinary storytelling and big idea books, Johnson explores this new vision of progress through a series of fascinating narratives: from the “miracle on the Hudson” to the planning of the French railway system; from the battle against malnutrition in Vietnam to a mysterious outbreak of strange smells in downtown Manhattan; from underground music video artists to the invention of the Internet itself. At a time when the conventional wisdom holds that the political system is hopelessly gridlocked with

old ideas, Future Perfect makes the timely and inspiring case that progress is still possible, and that innovative strategies are on the rise. This is a hopeful, affirmative outlook for the future, from one of the most brilliant and inspiring visionaries of contemporary culture.

"The co-author of Moral Machines explores accountability challenges related to a world shaped by such technological innovations as combat drones, 3-D printers and synthetic organisms to consider how people of the near future can be protected, "--Novelist.

As society continues to rely heavily on technological tools for facilitating business, e-commerce, banking, and communication, among other applications, there has been a significant rise in criminals seeking to exploit these tools for their nefarious gain. Countries all over the world are seeing substantial increases in identity theft and cyberattacks, as well as illicit transactions, including drug trafficking and human trafficking, being made through the dark web internet. Sex offenders and murderers explore unconventional methods of finding and contacting their victims through Facebook, Instagram, popular dating sites, etc., while pedophiles rely on these channels to obtain information and photographs of children, which are shared on hidden community sites. As criminals continue to harness technological advancements that are outpacing legal and ethical standards, law enforcement and government officials are faced with the challenge of devising new and alternative strategies to identify and apprehend criminals to preserve the safety of society. The Encyclopedia of Criminal Activities and the Deep Web is a three-volume set that includes comprehensive articles covering multidisciplinary research and expert insights provided by hundreds of leading researchers from 30 countries including the United States, the United Kingdom, Australia, New Zealand, Germany, Finland, South Korea, Malaysia, and more. This comprehensive encyclopedia provides the most diverse findings and new methodologies for monitoring and regulating the use of online tools as well as hidden areas of the internet, including the deep and dark web. Highlighting a wide range of topics such as cyberbullying, online hate speech, and hacktivism, this book will offer strategies for the prediction and prevention of online criminal activity and examine methods for safeguarding internet users and their data from being tracked or stalked. Due to the techniques and extensive knowledge discussed in this publication it is an invaluable addition for academic and corporate libraries as well as a critical resource for policy makers, law enforcement officials, forensic scientists, criminologists, sociologists, victim advocates, cybersecurity analysts, lawmakers, government officials, industry professionals, academicians, researchers, and students within this field of study.

Crime and Punishment in the Future Internet is an examination of the development and impact of digital frontier technologies (DFTs) such as Artificial Intelligence, the Internet of things, autonomous mobile robots, and blockchain on offending, crime control, the criminal justice system, and the discipline of criminology. It poses criminological, legal, ethical, and policy questions linked to such development and anticipates the impact of DFTs on crime and offending. It forestalls their wide-ranging consequences, including the proliferation of new types of vulnerability, policing and other mechanisms of social control, and the threat of pervasive and intrusive surveillance. Two key concerns lie at the heart of this volume. First, the book investigates the origins and development of emerging DFTs and their interactions with criminal behaviour, crime prevention, victimisation, and crime control. It also investigates the future advances and likely impact of such processes on a range of social actors: citizens, non-citizens, offenders, victims of crime, judiciary and law enforcement, media, NGOs. This book does not adopt technological determinism that suggests technology alone drives social development. Yet, while it is impossible to know where the emerging technologies are taking us, there is no doubt that DFTs will shape the way we engage with and experience criminal behaviour in the twenty-first century. As such, this book starts the conversation about a range of essential topics that this expansion brings to social sciences, and begins to decipher challenges we will be facing in the future. An accessible and compelling read, this book will

appeal to those engaged with criminology, sociology, politics, policymaking, and all those interested in the impact of DFTs on the criminal justice system.

World-renowned economist Klaus Schwab, Founder and Executive Chairman of the World Economic Forum, explains that we have an opportunity to shape the fourth industrial revolution, which will fundamentally alter how we live and work. Schwab argues that this revolution is different in scale, scope and complexity from any that have come before. Characterized by a range of new technologies that are fusing the physical, digital and biological worlds, the developments are affecting all disciplines, economies, industries and governments, and even challenging ideas about what it means to be human. Artificial intelligence is already all around us, from supercomputers, drones and virtual assistants to 3D printing, DNA sequencing, smart thermostats, wearable sensors and microchips smaller than a grain of sand. But this is just the beginning: nanomaterials 200 times stronger than steel and a million times thinner than a strand of hair and the first transplant of a 3D printed liver are already in development. Imagine "smart factories" in which global systems of manufacturing are coordinated virtually, or implantable mobile phones made of biosynthetic materials. The fourth industrial revolution, says Schwab, is more significant, and its ramifications more profound, than in any prior period of human history. He outlines the key technologies driving this revolution and discusses the major impacts expected on government, business, civil society and individuals. Schwab also offers bold ideas on how to harness these changes and shape a better future--one in which technology empowers people rather than replaces them; progress serves society rather than disrupts it; and in which innovators respect moral and ethical boundaries rather than cross them. We all have the opportunity to contribute to developing new frameworks that advance progress.

INTERNATIONAL BESTSELLER “Fascinating ... A powerful, exhortatory call to arms.”-New York Times Book Review “A David-and-Goliath story for the digital age ... Thrilling.”-Foreign Policy The page-turning inside story of the global team wielding the internet to fight for facts and combat autocracy-revealing the extraordinary ability of ordinary people to hold the powerful to account. In 2018, Russian exile Sergei Skripal and his daughter were nearly killed in an audacious poisoning attempt in Salisbury, England. Soon, the identity of one of the suspects was revealed: he was a Russian spy. This huge investigative coup wasn't pulled off by an intelligence agency or a traditional news outlet. Instead, the scoop came from Bellingcat, the open-source investigative team that is redefining the way we think about news, politics, and the digital future. We Are Bellingcat tells the inspiring story of how a college dropout pioneered a new category of reporting and galvanized citizen journalists-working together from their computer screens around the globe-to crack major cases, at a time when fact-based journalism is under assault from authoritarian forces. Founder Eliot Higgins introduces readers to the tools Bellingcat investigators use, tools available to anyone, from software that helps you pinpoint the location of an image, to an app that can nail down the time that photo was taken. This book digs deep into some of Bellingcat's most important investigations-the downing of flight MH17 over Ukraine, Assad's use of chemical weapons in Syria, the identities of alt-right protestors in Charlottesville-with the drama and gripping detail of a spy novel.

The variety, pace, and power of technological innovations that have emerged in the 21st Century have been breathtaking. These technological developments, which include advances in networked information and communications, biotechnology, neurotechnology, nanotechnology, robotics, and environmental engineering technology, have raised a number of vital and complex questions. Although these technologies

have the potential to generate positive transformation and help address 'grand societal challenges', the novelty associated with technological innovation has also been accompanied by anxieties about their risks and destabilizing effects. Is there a potential harm to human health or the environment? What are the ethical implications? Do this innovations erode of antagonize values such as human dignity, privacy, democracy, or other norms underpinning existing bodies of law and regulation? These technological developments have therefore spawned a nascent but growing body of 'law and technology' scholarship, broadly concerned with exploring the legal, social and ethical dimensions of technological innovation. This handbook collates the many and varied strands of this scholarship, focusing broadly across a range of new and emerging technology and a vast array of social and policy sectors, through which leading scholars in the field interrogate the interfaces between law, emerging technology, and regulation. Structured in five parts, the handbook (I) establishes the collection of essays within existing scholarship concerned with law and technology as well as regulatory governance; (II) explores the relationship between technology development by focusing on core concepts and values which technological developments implicate; (III) studies the challenges for law in responding to the emergence of new technologies, examining how legal norms, doctrine and institutions have been shaped, challenged and destabilized by technology, and even how technologies have been shaped by legal regimes; (IV) provides a critical exploration of the implications of technological innovation, examining the ways in which technological innovation has generated challenges for regulators in the governance of technological development, and the implications of employing new technologies as an instrument of regulatory governance; (V) explores various interfaces between law, regulatory governance, and new technologies across a range of key social domains.

Now a New York Times bestseller! There is a Threat Lurking Online with the Power to Destroy Your Finances, Steal Your Personal Data, and Endanger Your Life. In Spam Nation, investigative journalist and cybersecurity expert Brian Krebs unmasks the criminal masterminds driving some of the biggest spam and hacker operations targeting Americans and their bank accounts. Tracing the rise, fall, and alarming resurrection of the digital mafia behind the two largest spam pharmacies-and countless viruses, phishing, and spyware attacks-he delivers the first definitive narrative of the global spam problem and its threat to consumers everywhere. Blending cutting-edge research, investigative reporting, and firsthand interviews, this terrifying true story reveals how we unwittingly invite these digital thieves into our lives every day. From unassuming computer programmers right next door to digital mobsters like "Cosma"-who unleashed a massive malware attack that has stolen thousands of Americans' logins and passwords-Krebs uncovers the shocking lengths to which these people will go to profit from our data and our wallets. Not only are hundreds of thousands of Americans exposing themselves to fraud and dangerously toxic products from rogue online pharmacies, but even those who never open junk messages are at risk. As Krebs notes, spammers can-and do-hack into accounts through these emails, harvest personal information like usernames and passwords, and sell them on the digital black market. The fallout from this global epidemic doesn't just cost consumers and companies billions, it costs lives too. Fast-paced and utterly gripping, Spam Nation ultimately proposes concrete solutions for protecting ourselves online and stemming

this tidal wave of cybercrime-before it's too late. "Krebs's talent for exposing the weaknesses in online security has earned him respect in the IT business and loathing among cybercriminals... His track record of scoops...has helped him become the rare blogger who supports himself on the strength of his reputation for hard-nosed reporting." -Bloomberg Businessweek

Ideal for allied health and pre-nursing students, Alcamos Fundamentals of Microbiology, Body Systems Edition, retains the engaging, student-friendly style and active learning approach for which award-winning author and educator Jeffrey Pommerville is known. It presents diseases, complete with new content on recent discoveries, in a manner that is directly applicable to students and organized by body system. A captivating art program, learning design format, and numerous case studies draw students into the text and make them eager to learn more about the fascinating world of microbiology.

“Brilliantly researched and written.”—Jon Snow, Channel 4 News “A comprehensive and intelligible account of the elusive world of hacking and cybercrime over the last two decades. . . . Lively, insightful, and, often, alarming.”—Ewen MacAskill, Guardian On May 4, 2000, an email that read “kindly check the attached LOVELETTER” was sent from a computer in the Philippines. Attached was a virus, the Love Bug, and within days it had been circulated across the globe, paralyzing banks, broadcasters, and businesses in its wake, and extending as far as the UK Parliament and, reportedly, the Pentagon. The outbreak presaged a new era of online mayhem: the age of Crime Dot Com. In this book, investigative journalist Geoff White charts the astonishing development of hacking, from its conception in the United States’ hippy tech community in the 1970s, through its childhood among the ruins of the Eastern Bloc, to its coming of age as one of the most dangerous and pervasive threats to our connected world. He takes us inside the workings of real-life cybercrimes, drawing on interviews with those behind the most devastating hacks and revealing how the tactics employed by high-tech crooks to make millions are being harnessed by nation states to target voters, cripple power networks, and even prepare for cyber-war. From Anonymous to the Dark Web, Ashley Madison to election rigging, Crime Dot Com is a thrilling, dizzying, and terrifying account of hacking, past and present, what the future has in store, and how we might protect ourselves from it.

Leading innovation expert Alec Ross explains what's next for the world, mapping out the advances and stumbling blocks that will emerge in the next ten years—for businesses, governments, and the global community—and how we can navigate them. While Alec Ross was working as Hillary Clinton's Senior Advisor on Innovation, he traveled to forty-one countries. He visited some of the toughest places in the world—from refugee camps of Congo to Syrian war zones. From phone-charger stands in Rwanda to R&D labs in South Korea, Ross has seen what the future holds. Over the past two decades, the Internet has radically changed markets and businesses worldwide. InThe Industries of the Future, Ross shows us what's next, highlighting the best opportunities for progress and explaining why countries thrive or sputter. He examines the specific fields that will most shape our economic future over the next ten years, including cybercrime and cybersecurity, the commercialization of genomics, the next step for big data, and the coming impact of digital technology on money, payments, and markets. And in each of these realms, Ross addresses the toughest

questions: How will we have to adapt to the changing nature of work? Is the prospect of cyberwar sparking the next arms race? How can the world's rising nations hope to match Silicon Valley in creating their own innovation hotspots? Ross blends storytelling and economic analysis to give a vivid and informed perspective on how sweeping global trends are affecting the ways we live, incorporating the insights of leaders ranging from the founders of Google and Twitter to defense experts like David Petraeus. The Industries of the Future takes the intimidating, complex topics that many of us know to be important and boils them down into clear, plain-spoken language. This is an essential work for understanding how the world works—now and tomorrow—and a must-read for businesspeople, in every sector, from every country.

Presents a controversial history of violence which argues that today's world is the most peaceful time in human existence, drawing on psychological insights into intrinsic values that are causing people to condemn violence as an acceptable measure.

This book has a two-fold mission: to explain and facilitate digital transition in business organizations using information and communications technology and to address the associated growing threat of cyber crime and the challenge of creating and maintaining effective cyber protection. The book begins with a section on Digital Business Transformation, which includes chapters on tools for integrated marketing communications, human resource workplace digitalization, the integration of the Internet of Things in the workplace, Big Data, and more. The technologies discussed aim to help businesses and entrepreneurs transform themselves to align with today’s modern digital climate. The Evolution of Business in the Cyber Age: Digital Transformation, Threats, and Security provides a wealth of information for those involved in the development and management of conducting business online as well as for those responsible for cyber protection and security. Faculty and students, researchers, and industry professionals will find much of value in this volume.

In a revealing study of how digital dossiers are created (usually without our knowledge), the author argues that we must rethink our understanding of what privacy is and what it means in the digital age, and then reform the laws that define and regulate it. Reprint.

Willie Sutton, a notorious American bank robber of fifty years ago, was once asked why he persisted in robbing banks. "Because that's where the money is," he is said to have replied. The theory that crime follows opportunity has become established wisdom in criminology; opportunity reduction has become one of the fundamental principles of crime prevention. "The enormous benefits of telecommunications are not without cost." It could be argued that this quotation from Crime in the Digital Age, is a dramatic understatement. Grabosky and Smith advise us that the criminal opportunities which accompany these newest technological changes include: illegal interception of telecommunications; electronic vandalism and terrorism; theft of telecommunications services; telecommunications piracy; transmission of pornographic and other offensive material; telemarketing fraud; electronic funds transfer crime; electronic money laundering; and finally, telecommunications in furtherance of other criminal conspiracies. However, although digitization has facilitated a great deal of criminal activity, the authors suggest that technology also provides the means to prevent and detect such crimes. Moreover, the varied nature of these crimes defies a single policy solution. Grabosky and Smith take us through this electronic minefield and discuss the issues facing Australia as well as the international community and law enforcement agencies.

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

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

Social Ecology in the Digital Age: Solving Complex Problems in a Globalized World provides a comprehensive overview of social ecological theory, research, and practice. Written by renowned expert Daniel Stokols, the book distills key principles from diverse strands of ecological science, offering a robust framework for transdisciplinary research and societal problem-solving. The existential challenges of the 21st Century - global climate change and climate-change denial, environmental pollution, biodiversity loss, food insecurity, disease pandemics, inter-ethnic violence and the threat of nuclear war, cybercrime, the Digital Divide, and extreme poverty and income inequality confronting billions each day - cannot be understood and managed adequately from narrow disciplinary or political perspectives. Social Ecology in the Digital Age is grounded in scientific research but written in a personal and informal style from the vantage point of a former student, current teacher and scholar who has contributed over four decades to the field of social ecology. The book will be of interest to scholars, students, educators, government leaders and community practitioners working in several fields including social and human ecology, psychology, sociology, anthropology, criminology, law, education, biology, medicine, public health, earth system and sustainability science, geography, environmental design, urban planning, informatics, public policy and global governance. Winner of the 2018 Gerald L. Young Book Award from The Society for Human Ecology "Exemplifying the highest standards of scholarly work in the field of human ecology." https://societyforhumanecology.org/human-ecology-homepage/awards/gerald-l-young-book-award-in-human-ecology/ The book traces historical origins and conceptual foundations of biological, human, and social ecology Offers a new conceptual framework that brings together earlier approaches to social ecology and extends them in novel directions Highlights the interrelations between four distinct but closely intertwined spheres of human environments: our natural, built, sociocultural, and virtual (cyber-based) surroundings Spans local to global scales and individual, organizational, community, regional, and global levels of analysis Applies core principles of social ecology to identify multi-level strategies for promoting personal and public health, resolving complex social problems, managing global environmental change, and creating resilient and sustainable communities Underscores social ecology's vital importance for understanding and managing the environmental and political upheavals of the

21st Century Highlights descriptive, analytic, and transformative (or moral) concerns of social ecology Presents strategies for educating the next generation of social ecologists emphasizing transdisciplinary, team-based, translational, and transcultural approaches

'This is the most important - and fascinating - book yet written about how the digital age will affect our world' Walter Isaacson, author of Steve Jobs From two leading thinkers, the widely anticipated book that describes a new, hugely connected world of the future, full of challenges and benefits which are ours to meet and harness. The New Digital Age is the product of an unparalleled collaboration: full of the brilliant insights of one of Silicon Valley's great innovators - what Bill Gates was to Microsoft and Steve Jobs was to Apple, Schmidt (along with Larry Page and Sergey Brin) was to Google - and the Director of Google Ideas, Jared Cohen, formerly an advisor to both Secretaries of State Condoleezza Rice and Hillary Clinton. Never before has the future been so vividly and transparently imagined. From technologies that will change lives (information systems that greatly increase productivity, safety and our quality of life, thought-controlled motion technology that can revolutionise medical procedures, and near-perfect translation technology that allows us to have more diversified interactions) to our most important future considerations (curating our online identity and fighting those who would do harm with it) to the widespread political change that will transform the globe (through transformations in conflict, increasingly active and global citizenries, a new wave of cyber-terrorism and states operating simultaneously in the physical and virtual realms) to the ever present threats to our privacy and security, Schmidt and Cohen outline in great detail and scope all the promise and peril awaiting us in the coming decades. A breakthrough book - pragmatic, inspirational and totally fascinating. Whether a government, a business or an individual, we must understand technology if we want to understand the future. 'A brilliant guidebook for the next century . . . Schmidt and Cohen offer a dazzling glimpse into how the new digital revolution is changing our lives' Richard Branson

Top cybersecurity journalist Kim Zetter tells the story behind the virus that sabotaged Iran’s nuclear efforts and shows how its existence has ushered in a new age of warfare—one in which a digital attack can have the same destructive capability as a megaton bomb. In January 2010, inspectors with the International Atomic Energy Agency noticed that centrifuges at an Iranian uranium enrichment plant were failing at an unprecedented rate. The cause was a complete mystery—apparently as much to the technicians replacing the centrifuges as to the inspectors observing them. Then, five months later, a seemingly unrelated event occurred: A computer security firm in Belarus was called in to troubleshoot some computers in Iran that were crashing and rebooting repeatedly. At first, the firm’s programmers believed the malicious code on the machines was a simple, routine piece of malware. But as they and other experts around the world investigated, they discovered a mysterious virus of unparalleled complexity. They had, they soon learned, stumbled upon the world’s first digital weapon. For Stuxnet, as it came to be known, was unlike any other virus or worm built before: Rather than simply hijacking targeted computers or stealing information from them, it escaped the digital realm to wreak actual, physical destruction on a nuclear facility. In these pages, Wired journalist Kim Zetter draws on her extensive sources and expertise to tell the story behind Stuxnet’s planning, execution, and discovery, covering its genesis in the corridors of Bush’s White House and its unleashing on systems in Iran—and telling the spectacular, unlikely tale of the security geeks who managed to unravel a sabotage campaign years in the making. But Countdown to Zero Day ranges far beyond Stuxnet itself. Here, Zetter shows us how digital warfare developed in the US. She takes us inside today’s flourishing zero-day “grey markets,” in which intelligence agencies and militaries pay huge sums for the malicious code they need to carry out infiltrations and attacks. She reveals just how vulnerable many of our own critical systems are to Stuxnet-like strikes, from nation-state adversaries and anonymous hackers alike—and shows us just what might happen should our infrastructure be targeted by such an

attack. Propelled by Zetter's unique knowledge and access, and filled with eye-opening explanations of the technologies involved, Countdown to Zero Day is a comprehensive and prescient portrait of a world at the edge of a new kind of war.

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.

Cyberspace is all around us. We depend on it for everything we do. We have reengineered our business, governance, and social relations around a planetary network unlike any before it. But there are dangers looming, and malign forces are threatening to transform this extraordinary domain. In Black Code, Ronald J. Deibert, a leading expert on digital technology, security, and human rights, lifts the lid on cyberspace and shows what's at stake for Internet users and citizens. As cyberspace develops in unprecedented ways, powerful agents are scrambling for control. Predatory cyber criminal gangs such as Koobface have made social media their stalking ground. The discovery of Stuxnet, a computer worm reportedly developed by Israel and the United States and aimed at Iran's nuclear facilities, showed that state cyberwar is now a very real possibility. Governments and corporations are in collusion and are setting the rules of the road behind closed doors. This is not the way it was supposed to be. The Internet's original promise of a global commons of shared knowledge and communications is now under threat. Drawing on the first-hand experiences of one of the most important protagonists in the battle — the Citizen Lab and its global network of frontline researchers, who have spent more than a decade cracking cyber espionage rings and uncovering attacks on citizens and NGOs worldwide — Black Code takes readers on a fascinating journey into the battle for cyberspace. Thought-provoking, compelling, and sometimes frightening, it is a wakeup call to citizens who have come to take the Internet for granted. Cyberspace is ours, it is what we make of it, Deibert argues, and we need to act now before it slips through our grasp.

THE INSTANT NEW YORK TIMES BESTSELLER SHORTLISTED FOR THE FT & McKINSEY BUSINESS BOOK OF THE YEAR AWARD 2021 'An intricately detailed, deeply sourced and reported history of the origins and growth of the cyberweapons market . . . Hot, propulsive . . . Sets out from the start to scare us out of our complacency' New York Times 'A terrifying exposé' The Times 'Part John le Carré and more parts Michael Crichton . . . Spellbinding' New Yorker Zero day: a software bug that allows a hacker to break in and scamper through the world's computer networks invisibly until discovered. One of the most coveted tools in a spy's arsenal, a zero day has the power to tap into any iPhone, dismantle safety controls at a chemical plant and shut down the power in an entire nation – just ask the Ukraine. Zero days are the blood diamonds of the security trade, pursued by nation states, defense contractors, cybercriminals, and security defenders alike. In this market, governments aren't regulators; they are clients – paying huge sums to hackers willing to turn over gaps in the Internet, and stay silent about them. This Is How They Tell Me the World Ends is cybersecurity reporter Nicole Perlroth's discovery, unpacked. A intrepid journalist unravels an opaque, code-driven market from the outside in – encountering spies, hackers, arms dealers, mercenaries and a few unsung heroes along the way. As the stakes get higher and higher in the rush to push the world's critical infrastructure online, This Is How They Tell Me the World Ends is the urgent and alarming discovery of one of the world's most extreme threats.

Storing Digital Binary Data into Cellular DNA demonstrates how current digital information

storage systems have short longevity and limited capacity, also pointing out that their production and consumption of data exceeds supply. Author Rocky Termanini explains the DNA system and how it encodes vast amounts of data, then presents information on the emergence of DNA as a storage technology for the ever-growing stream of data being produced and consumed. The book will be of interest to a range of readers looking to understand this game-changing technology, including researchers in computer science, biomedical engineers, geneticists, physicians, clinicians, law enforcement and cybersecurity experts. Presents a comprehensive reference on the fascinating and emerging technology of DNA storage Helps readers understand key concepts on how DNA works as an information storage system Provides readers with key information on the technologies used to work with DNA data encoding, such as CRISPR Covers emerging areas of application and ethical concern, such as Smart Cities, cybercrime and cyberwarfare Includes coverage of synthesizing DNA-encoded data, sequencing DNA-encoded data, and fusing DNA with Digital Immunity Ecosystems (DIE)

As the 2020 global lockdown became a universal strategy to control the COVID-19 pandemic, social distancing triggered a massive reliance on online and cyberspace alternatives and switched the world to the digital economy. Despite their effectiveness for remote work and online interactions, cyberspace alternatives ignited several Cybersecurity challenges. Malicious hackers capitalized on global anxiety and launched cyberattacks against unsuspecting victims. Internet fraudsters exploited human and system vulnerabilities and impacted data integrity, privacy, and digital behaviour. Cybersecurity in the COVID-19 Pandemic demystifies Cybersecurity concepts using real-world cybercrime incidents from the pandemic to illustrate how threat actors perpetrated computer fraud against valuable information assets particularly healthcare, financial, commercial, travel, academic, and social networking data. The book simplifies the socio-technical aspects of Cybersecurity and draws valuable lessons from the impacts COVID-19 cyberattacks exerted on computer networks, online portals, and databases. The book also predicts the fusion of Cybersecurity into Artificial Intelligence and Big Data Analytics, the two emerging domains that will potentially dominate and redefine post-pandemic Cybersecurity research and innovations between 2021 and 2025. The book's primary audience is individual and corporate cyberspace consumers across all professions intending to update their Cybersecurity knowledge for detecting, preventing, responding to, and recovering from computer crimes. Cybersecurity in the COVID-19 Pandemic is ideal for information officers, data managers, business and risk administrators, technology scholars, Cybersecurity experts and researchers, and information technology practitioners. Readers will draw lessons for protecting their digital assets from email phishing fraud, social engineering scams, malware campaigns, and website hijacks.

This book presents a comprehensive study of different tools and techniques available to perform network forensics. Also, various aspects of network forensics are reviewed as well as related technologies and their limitations. This helps security practitioners and researchers in better understanding of the problem, current solution space, and future research scope to detect and investigate various network intrusions against such attacks efficiently. Forensic computing is rapidly gaining importance since the amount of crime involving digital systems is steadily increasing. Furthermore, the area is still underdeveloped and poses many technical and legal challenges. The rapid development of the Internet over the past decade appeared to have facilitated an increase in the incidents of online attacks. There are many reasons which are motivating the attackers to be fearless in carrying out the attacks. For example, the speed with which an attack can be carried out, the anonymity provided by the medium, nature of medium where digital information is stolen without actually removing it, increased availability of potential victims and the global impact of the attacks are some of the aspects. Forensic analysis is performed at two different levels: Computer Forensics and Network Forensics.

Computer forensics deals with the collection and analysis of data from computer systems, networks, communication streams and storage media in a manner admissible in a court of law. Network forensics deals with the capture, recording or analysis of network events in order to discover evidential information about the source of security attacks in a court of law. Network forensics is not another term for network security. It is an extended phase of network security as the data for forensic analysis are collected from security products like firewalls and intrusion detection systems. The results of this data analysis are utilized for investigating the attacks. Network forensics generally refers to the collection and analysis of network data such as network traffic, firewall logs, IDS logs, etc. Technically, it is a member of the already-existing and expanding the field of digital forensics. Analogously, network forensics is defined as "The use of scientifically proved techniques to collect, fuses, identifies, examine, correlate, analyze, and document digital evidence from multiple, actively processing and transmitting digital sources for the purpose of uncovering facts related to the planned intent, or measured success of unauthorized activities meant to disrupt, corrupt, and or compromise system components as well as providing information to assist in response to or recovery from these activities." Network forensics plays a significant role in the security of today's organizations. On the one hand, it helps to learn the details of external attacks ensuring similar future attacks are thwarted. Additionally, network forensics is essential for investigating insiders' abuses that constitute the second costliest type of attack within organizations. Finally, law enforcement requires network forensics for crimes in which a computer or digital system is either being the target of a crime or being used as a tool in carrying a crime. Network security protects the system against attack while network forensics focuses on recording evidence of the attack. Network security products are generalized and look for possible harmful behaviors. This monitoring is a continuous process and is performed all through the day. However, network forensics involves post mortem investigation of the attack and is initiated after crime notification. There are many tools which assist in capturing data transferred over the networks so that an attack or the malicious intent of the intrusions may be investigated. Similarly, various network forensic frameworks are proposed in the literature.

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.

Winner, 2018 Law & Legal Studies PROSE Award The consequences of big data and algorithm-driven policing and its impact on law enforcement In a high-tech command center in

downtown Los Angeles, a digital map lights up with 911 calls, television monitors track breaking news stories, surveillance cameras sweep the streets, and rows of networked computers link analysts and police officers to a wealth of law enforcement intelligence. This is just a glimpse into a future where software predicts future crimes, algorithms generate virtual “most-wanted” lists, and databanks collect personal and biometric information. The Rise of Big Data Policing introduces the cutting-edge technology that is changing how the police do their jobs and shows why it is more important than ever that citizens understand the far-reaching consequences of big data surveillance as a law enforcement tool. Andrew Guthrie Ferguson reveals how these new technologies —viewed as race-neutral and objective—have been eagerly adopted by police departments hoping to distance themselves from claims of racial bias and unconstitutional practices. After a series of high-profile police shootings and federal investigations into systemic police misconduct, and in an era of law enforcement budget cutbacks, data-driven policing has been billed as a way to “turn the page” on racial bias. But behind the data are real people, and difficult questions remain about racial discrimination and the potential to distort constitutional protections. In this first book on big data policing, Ferguson offers an examination of how new technologies will alter the who, where, when and how we police. These new technologies also offer data-driven methods to improve police accountability and to remedy the underlying socio-economic risk factors that encourage crime. The Rise of Big Data Policing is a must read for anyone concerned with how technology will revolutionize law enforcement and its potential threat to the security, privacy, and constitutional rights of citizens. Read an excerpt and interview with Andrew Guthrie Ferguson in The Economist.

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.

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.

The charismatic forger immortalized in Catch Me If You Can exposes the astonishing tactics of today's identity theft criminals and offers powerful strategies to thwart them based on his second career as an acclaimed fraud-fighting consultant. When Frank Abagnale trains law enforcement officers around the country about identity theft, he asks officers for their names and addresses and nothing more. In a matter of hours he can obtain everything he would need to steal their lives: Social Security numbers, dates of birth, current salaries, checking account numbers, the names of everyone in their families, and more. This illustrates how easy it is for anyone from anywhere in the world to assume our identities and in a matter of hours devastate our lives in ways that can take years to recover from. Considering that a fresh victim is hit every four seconds, Stealing Your Life is the reference everyone needs by an unsurpassed authority on the latest identity theft schemes. Consider these sobering facts: • Six out of ten American companies and government agencies have already been hacked. • An estimated 80 percent of birth certificate requests are fulfilled through the mail for people using only a name and a return address. • Americans write 39 billion checks a year, and half of them never reconcile their bank statements. • A Social Security number costs $49 on the black market. A driver's license goes for $90. A birth certificate will set you back $79. Abagnale offers dozens of concrete steps to transform anyone from an easy mark into a hard case that criminals are likely to bypass: • Don't allow your kids to use the computer on which you do online banking and store financial records (children are apt to download games and attachments that host damaging viruses or attract spyware). • Beware of offers that appeal to greed or fear in exchange for personal data. • Monitor your credit report regularly and know if anyone's been "knocking on your door." • Read privacy statements carefully and choose to opt out of sharing information whenever possible. Brimming with anecdotes of creative criminality that are as entertaining as they are enlightening, Stealing Your Life is the practical way to shield yourself from one of today's most nefarious and common crimes.

The terrifying new role of technology in a world at war

Today's digital economy is uniquely dependent on the Internet, yet few users or decision makers have more than a rudimentary understanding of the myriad of online risks that threaten us. Cyber crime is one of the main threats to the integrity and availability of data and systems. From insiders to complex external attacks and industrial worms, modern business faces unprecedented challenges; and while cyber security and digital intelligence are the necessary responses to this challenge, they are understood by only a tiny minority. In his second book on high-tech risks, Mark Johnson goes far beyond enumerating past cases and summarising legal or regulatory requirements. He describes in plain, non-technical language how cyber crime has evolved and the nature of the very latest threats. He confronts issues that are not addressed by codified rules and practice guidelines, supporting this with over 30

valuable illustrations and tables. Written for the non-technical layman and the high tech risk manager alike, the book also explores countermeasures, penetration testing, best practice principles, cyber conflict and future challenges. A discussion of Web 2.0 risks delves into the very real questions facing policy makers, along with the pros and cons of open source data. In a chapter on Digital Intelligence readers are provided with an exhaustive guide to practical, effective and ethical online investigations. Cyber Crime, Security and Digital Intelligence is an important work of great relevance in today's interconnected world and one that nobody with an interest in either risk or technology should be without.

NEW YORK TIMES and WALL STREET JOURNAL BESTSELLER One of the world's leading authorities on global security, Marc Goodman takes readers deep into the digital underground to expose the alarming ways criminals, corporations, and even countries are using new and emerging technologies against you--and how this makes everyone more vulnerable than ever imagined. Technological advances have benefited our world in immeasurable ways, but there is an ominous flip side: our technology can be turned against us. Hackers can activate baby monitors to spy on families, thieves are analyzing social media posts to plot home invasions, and stalkers are exploiting the GPS on smart phones to track their victims' every move. We all know today's criminals can steal identities, drain online bank accounts, and wipe out computer servers, but that's just the beginning. To date, no computer has been created that could not be hacked--a sobering fact given our radical dependence on these machines for everything from our nation's power grid to air traffic control to financial services. Yet, as ubiquitous as technology seems today, just over the horizon is a tidal wave of scientific progress that will leave our heads spinning. If today's Internet is the size of a golf ball, tomorrow's will be the size of the sun. Welcome to the Internet of Things, a living, breathing, global information grid where every physical object will be online. But with greater connections come greater risks. Implantable medical devices such as pacemakers can be hacked to deliver a lethal jolt of electricity and a car's brakes can be disabled at high speed from miles away. Meanwhile, 3-D printers can produce AK-47s, bioterrorists can download the recipe for Spanish flu, and cartels are using fleets of drones to ferry drugs across borders. With explosive insights based upon a career in law enforcement and counterterrorism, Marc Goodman takes readers on a vivid journey through the darkest recesses of the Internet. Reading like science fiction, but based in science fact, Future Crimes explores how bad actors are primed to hijack the technologies of tomorrow, including robotics, synthetic biology, nanotechnology, virtual reality, and artificial intelligence. These fields hold the power to create a world of unprecedented abundance and prosperity. But the technological bedrock upon which we are building our common future is deeply unstable and, like a house of cards, can come crashing down at any moment. Future Crimes provides a mind-blowing glimpse into the dark side of technological innovation and the unintended consequences of our connected world. Goodman offers a way out with clear steps we must take to survive the progress unfolding before us. Provocative, thrilling, and ultimately empowering, Future Crimes will serve as an urgent call to action that shows how we can take back control over our own devices and harness technology's tremendous power for the betterment of humanity--before it's too late. From the Hardcover edition.

The author examines the controversies surrounding cyber-harassment, arguing that it

should be considered a matter for civil rights law and that social norms of decency and civility must be leveraged to stop it.

NEW YORK TIMES and WALL STREET JOURNAL BESTSELLER ONE OF THE WASHINGTON POST'S 10 BEST BOOKS OF 2015 One of the world's leading authorities on global security, Marc Goodman takes readers deep into the digital underground to expose the alarming ways criminals, corporations, and even countries are using new and emerging technologies against you—and how this makes everyone more vulnerable than ever imagined. Technological advances have benefited our world in immeasurable ways, but there is an ominous flip side: our technology can be turned against us. Hackers can activate baby monitors to spy on families, thieves are analyzing social media posts to plot home invasions, and stalkers are exploiting the GPS on smart phones to track their victims' every move. We all know today's criminals can steal identities, drain online bank accounts, and wipe out computer servers, but that's just the beginning. To date, no computer has been created that could not be hacked—a sobering fact given our radical dependence on these machines for everything from our nation's power grid to air traffic control to financial services. Yet, as ubiquitous as technology seems today, just over the horizon is a tidal wave of scientific progress that will leave our heads spinning. If today's Internet is the size of a golf ball, tomorrow's will be the size of the sun. Welcome to the Internet of Things, a living, breathing, global information grid where every physical object will be online. But with greater connections come greater risks. Implantable medical devices such as pacemakers can be hacked to deliver a lethal jolt of electricity and a car's brakes can be disabled at high speed from miles away. Meanwhile, 3-D printers can produce AK-47s, bioterrorists can download the recipe for Spanish flu, and cartels are using fleets of drones to ferry drugs across borders. With explosive insights based upon a career in law enforcement and counterterrorism, Marc Goodman takes readers on a vivid journey through the darkest recesses of the Internet. Reading like science fiction, but based in science fact, Future Crimes explores how bad actors are primed to hijack the technologies of tomorrow, including robotics, synthetic biology, nanotechnology, virtual reality, and artificial intelligence. These fields hold the power to create a world of unprecedented abundance and prosperity. But the technological bedrock upon which we are building our common future is deeply unstable and, like a house of cards, can come crashing down at any moment. Future Crimes provides a mind-blowing glimpse into the dark side of technological innovation and the unintended consequences of our connected world. Goodman offers a way out with clear steps we must take to survive the progress unfolding before us. Provocative, thrilling, and ultimately empowering, Future Crimes will serve as an urgent call to action that shows how we can take back control over our own devices and harness technology's tremendous power for the betterment of humanity—before it's too late.