DarkMarket: How Hackers Became The New Mafia

The true story of Max Butler, the master hacker who ran a billion dollar cyber crime network. The word spread through the hacking underground like some unstoppable new virus: an audacious crook had staged a hostile takeover of an online criminal network that siphoned billions of dollars from the US economy. The culprit was a brilliant programmer with a hippie ethic and a supervillain's double identity. Max 'Vision' Butler was a white-hat hacker and a celebrity throughout the programming world, even serving as a consultant to the FBI. But there was another side to Max. As the black-hat 'Iceman', he'd seen the fraudsters around him squabble, their ranks riddled with infiltrators, their methods inefficient, and in their dysfunction was the ultimate challenge: he would stage a coup and steal their ill-gotten gains from right under their noses. Through the story of Max Butler's remarkable rise, KINGPIN lays bare the workings of a silent crime wave affecting millions worldwide. It exposes vast online-fraud supermarkets stocked with credit card numbers, counterfeit cheques, hacked bank accounts and fake passports. Thanks to Kevin Poulsen's remarkable access to both cops and criminals, we step inside the quiet,desperate battle that law enforcement fights against these scammers. And learn that the boy next door may not be all he seems.

Unnatural Selection is the first book to examine the rise of the "technocentric being"□or geek□who personifies a distinct new phase in human evolution. People considered geeks often have behavioral or genetic traits that were previously considered detrimental. But the new environment of the Anthropocene period□the Age of Man□has created a kind of digital greenhouse that actually favors their traits, enabling many non-neurotypical people to bloom. They resonate with the technological Zeitgeist in a way that turns their weaknesses into strengths. Think of Mark Zuckerberg versus the towering, Olympics-bound Winklevoss twins in the movie Social Network. Roeder suggests that the rise of the geek is not so much the product of Darwinian "natural selection" as of man-made□or unnatural□selection. He explains why geeks have become so phenomenally successful in such a short time and why the process will further accelerate, driven by breakthroughs in genetic engineering, neuropharmacology, and artificial intelligence. His book offers a fascinating synthesis of the latest trends in these fields and predicts a twenty-first century "cognitive arms race" in which new technology will enable everyone to become more intelligent and "geek-like."

Digital technology experts at the Citizen Lab uncover an espionage network affecting more than 100 countries.

Criminal activities in cyberspace are increasingly facilitated by burgeoning black markets. This report characterizes these markets and how they have grown into their current state to provide insight into how their existence can harm the information security environment. Understanding these markets lays the groundwork for exploring options to minimize their potentially harmful influence.

A Practical Guide for Managers

The Rebirth of History

CyberThieves, CyberCops and You

Unnatural Selection
Malevolent Actors, Criminal Opportunities, and Strategic Competition
International Politics, Concepts and Organization
Politics, Policy, Prospects

What people are saying about Inside Cyber Warfare "The necessary handbook for the 21st century." --Lewis Shepherd, Chief Tech Officer and Senior Fellow, Microsoft Institute for Advanced Technology in Governments "A must-read for policy makers and leaders who need to understand the big-picture landscape of cyber war." --Jim Stogdill, CTO, Mission Services Accenture You may have heard about "cyber warfare" in the news, but do you really know what it is? This book provides fascinating and disturbing details on how nations, groups, and individuals throughout the world are using the Internet as an attack platform to gain military, political, and economic advantages over their adversaries. You'll learn how sophisticated hackers working on behalf of states or organized crime patiently play a high-stakes game that could target anyone, regardless of affiliation or nationality. Inside Cyber Warfare goes beyond the headlines of attention-grabbing DDoS attacks and takes a deep look inside multiple cyber-conflicts that occurred from 2002 through summer 2009. Learn how cyber attacks are waged in open conflicts, including recent hostilities between Russia and Georgia, and Israel and Palestine Discover why Twitter, Facebook, LiveJournal, Vkontakte, and other sites on the social web are mined by the intelligence services of many nations Read about China's commitment to penetrate the networks of its technologically superior adversaries as a matter of national survival Find out why many attacks originate from servers in the United States, and who's responsible Learn how hackers are "weaponizing" malware to attack vulnerabilities at the application level

Account of the 1989 revolution in Eastern Europe plus a new chapter bringing events up to date considering the long-term influences to determine the future of the region.

The Internet is constantly evolving, and has economic, political and social importance as a public good. A coherent strategy for Internet governance is needed to ensure that difficult tradeoffs between competing interests, as well as between distinct public values, are managed in a consistent, transparent and accountable manner that accurately reflects public priorities. In Organized Chaos: Reimagining the Internet, edited by Mark Raymond and Gordon Smith, leading experts address a range of pressing challenges, including cyber security issues and civil society hacktivism by groups such as Anonymous, and consider the international political

implications of some of the most likely Internet governance scenarios in the 2015–2020 time frame. Together, the chapters in this volume provide a clear sense of the critical problems facing efforts to update and redefine Internet governance, the appropriate modalities for doing so, and the costs and benefits associated with the most plausible outcomes. This foundation provides the basis for the development of the research-based, high-level strategic vision required to successfully navigate a complex, shifting and uncertain governance environment. How will governments and courts protect civil liberties in this new era of hacktivism? Ethical Hacking discusses the attendant moral and legal issues. The first part of the 21st century will likely go down in history as the era when ethical hackers opened governments and the line of transparency moved by force. One need only read the motto “we open governments” on the Twitter page for Wikileaks to gain a sense of the sea change that has occurred. Ethical hacking is the non-violent use of a technology in pursuit of a cause—political or otherwise—which is often legally and morally ambiguous. Hacktivists believe in two general but spirited principles: respect for human rights and fundamental freedoms, including freedom of expression and personal privacy; and the responsibility of government to be open, transparent and fully accountable to the public. How courts and governments will deal with hacking attempts which operate in a grey zone of the law and where different ethical views collide remains to be seen. What is undisputed is that Ethical Hacking presents a fundamental discussion of key societal questions. A fundamental discussion of key societal questions. This book is published in English. - La première moitié du XXIe siècle sera sans doute reconnue comme l’époque où le piratage éthique a ouvert de force les gouvernements, déplaçant les limites de la transparence. La page twitter de Wikileaks enchâsse cet ethos à même sa devise, « we open governments », et sa volonté d’être omniprésent. En parallèle, les grandes sociétés de technologie comme Apple se font compétition pour produire des produits de plus en plus sécuritaires et à protéger les données de leurs clients, alors même que les gouvernements tentent de limiter et de décrypter ces nouvelles technologies d’encryption. Entre-temps, le marché des vulnérabilités en matière de sécurité augmente à mesure que les experts en sécurité informatique vendent des vulnérabilités de logiciels des grandes technologies, dont Apple et Google, contre des sommes allant de 10 000 à 1,5 million de dollars. L’activisme en sécurité est à la hausse. Le piratage éthique est l’utilisation non-violence d’une technologie quelconque en soutien d’une cause politique ou autre qui est souvent ambigue d’un point de vue juridique et moral. Le hacking éthique peut

désigner les actes de vérification de pénétration professionnelle ou d'experts en sécurité informatique, de même que d'autres formes d'actions émergentes, comme l'hacktivisme et la désobéissance civile en ligne. L'hacktivisme est une forme de piratage éthique, mais également une forme de militantisme des droits civils à l'ère numérique. En principe, les adeptes du hacktivisme croient en deux grands principes : le respect des droits de la personne et les libertés fondamentales, y compris la liberté d'expression et à la vie privée, et la responsabilité des gouvernements d'être ouverts, transparents et pleinement redevables au public. En pratique, toutefois, les antécédents comme les agendas des hacktivistes sont fort diversifiés. Il n'est pas clair de quelle façon les tribunaux et les gouvernements traiteront des tentatives de piratage eu égard aux zones grises juridiques, aux approches éthiques conflictuelles, et compte tenu du fait qu'il n'existe actuellement, dans le monde, presque aucune exception aux provisions, en matière de cybercrime et de crime informatique, liées à la recherche sur la sécurité ou l'intérêt public. Il sera également difficile de déterminer le lien entre hacktivisme et droits civils. Ce livre est publié en anglais.

International Security

Markets for Cybercrime Tools and Stolen Data

The Black Box Society

A Journey Through the Global Criminal Underworld

Big Data Analytics

Crime Without Frontiers

Organized Chaos

Inside the Dark Web provides a broad overview of emerging digital threats and computer crimes, with an emphasis on cyberstalking, hacktivism, fraud and identity theft, and attacks on critical infrastructure. The book also analyzes the online underground economy and digital currencies and cybercrime on the dark web. The book further explores how dark web crimes are conducted on the surface web in new mediums, such as the Internet of Things (IoT) and peer-to-peer file sharing systems as well as dark web forensics and mitigating techniques. This book starts with the fundamentals of the dark web along with explaining its threat landscape. The book then introduces the Tor browser, which is used to access the dark web ecosystem. The book continues to take a deep dive into cybersecurity criminal activities in the dark net and analyzes the malpractices used to secure your system. Furthermore, the book digs deeper into the forensics of dark web, web content analysis, threat intelligence, IoT, crypto market, and cryptocurrencies. This book is a comprehensive guide

for those who want to understand the dark web quickly. After reading Inside the Dark Web, you'll understand The core concepts of the dark web. The different theoretical and cross-disciplinary approaches of the dark web and its evolution in the context of emerging crime threats. The forms of cybercriminal activity through the dark web and the technological and "social engineering" methods used to undertake such crimes. The behavior and role of offenders and victims in the dark web and analyze and assess the impact of cybercrime and the effectiveness of their mitigating techniques on the various domains. How to mitigate cyberattacks happening through the dark web. The dark web ecosystem with cutting edge areas like IoT, forensics, and threat intelligence and so on. The dark web-related research and applications and up-to-date on the latest technologies and research findings in this area. For all present and aspiring cybersecurity professionals who want to upgrade their skills by understanding the concepts of the dark web, Inside the Dark Web is their one-stop guide to understanding the dark web and building a cybersecurity plan.

'Breaking Bad meets City of God' Roberto Saviano, author of Gomorrah HUSBAND. This is the story of an ordinary man who became the king of the largest slum in Rio, the head of a drug cartel and Brazil's most notorious criminal. FATHER. A man who tried to bring welfare and justice to a playground of gang culture and destitution, while everyone around him drew guns and partied. DRUG LORD. It's a story of gold-hunters and evangelical pastors, bent police and rich-kid addicts, politicians and drug lords and the battle for the beautiful but damned city of Rio. MOST WANTED CRIMINAL.

In 2004, a California computer whiz named Barrett Lyon uncovered the identity of a hacker running major assaults on business websites. Without fully grasping the repercussions, he set on an investigation that led him into the heart of the Russian mob. Cybercrime was evolving. No longer the domain of small-time thieves, it had been discovered by sophisticated gangs. They began by attacking corporate websites but increasingly stole financial data from consumers and defense secrets from governments. While Barrett investigated the cutting edge of technology crime, the U.S. government struggled to catch up. Britain, however, was a different story. In the late 1990s, the Queen herself had declared safe e-commerce a national security priority. Agents from the London-based National Hi-Tech Crime Unit sought out Barrett and enlisted his help. They also sent detective Andrew Crocker, a Welsh former boxer, to Russia to track down and prosecute the hackers—and to find out who they worked for. Fatal System Error penetrates both the Russian cyber-mob and the American mafia as the two fight over the Internet's massive spoils. It takes readers into the murky hacker underground, traveling the globe from San Francisco to Costa Rica, London, and Russia. Using unprecedented access to mob businesses and Russian officials, it shows how top criminals earned protection from the Russian government—and how Barrett Lyon and Andrew Crocker got closer to the titans of the underground economy than any previous outsider. Together, their stories explain why cybercrime is much worse than you thought—and why the

Internet might not survive.

Before the Internet became widely known as a global tool for terrorists, one perceptive U.S. citizen recognized its ominous potential. Armed with clear evidence of computer espionage, he began a highly personal quest to expose a hidden network of spies that threatened national security. But would the authorities back him up? Cliff Stoll's dramatic firsthand account is "a computer-age detective story, instantly fascinating [and] astonishingly gripping" (Smithsonian). Cliff Stoll was an astronomer turned systems manager at Lawrence Berkeley Lab when a 75-cent accounting error alerted him to the presence of an unauthorized user on his system. The hacker's code name was "Hunter"—a mysterious invader who managed to break into U.S. computer systems and steal sensitive military and security information. Stoll began a one-man hunt of his own: spying on the spy. It was a dangerous game of deception, broken codes, satellites, and missile bases—a one-man sting operation that finally gained the attention of the CIA . . . and ultimately trapped an international spy ring fueled by cash, cocaine, and the KGB.

The Secret Algorithms That Control Money and Information

Learn Ethical Hacking from Scratch

Crime Dot Com

Kingpin

Ethical Hacking

Fatal System Error

E-newsletter of the United Nations Office for South-South Cooperation

This unique and lively history of Balkan geopolitics since the early nineteenth century gives readers the essential historical background to recent events in this war-torn area. No other book covers the entire region, or offers such profound insights into the roots of Balkan violence, or explains so vividly the origins of modern Serbia, Croatia, Bosnia, Greece, Bulgaria, Romania, and Albania. Misha Glenny presents a lucid and fair-minded account of each national group in the Balkans and its struggle for statehood. The narrative is studded with sharply observed portraits of kings, guerrillas, bandits, generals, and politicians. Glenny also explores the often-catastrophic relationship between the Balkans and the Great Powers, raising some disturbing questions about Western intervention.

"This extraordinarily powerful book demonstrates how utterly we lack the shared supranational tools needed to fight cybercrime. Essential reading." --Roberto Saviano, author of Gommorah The benefits of living in a digital, globalized 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 might care to relieve us of them? In this fascinating and compelling book, Misha Glenny, author of the international best seller McMafia, explores the three fundamental threats facing us in the twenty-first century: cybercrime, cyberwarfare and

cyberindustrial espionage. Governments and the private sector are losing billions of dollars each year fighting an ever-morphing, often invisible and often supersmart new breed of criminal: the hacker. Glenny has traveled and trawled the world. 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 Scunthorpe, England, or Agent Keith Mularski in Pittsburgh, Pennsylvania, 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.

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.

This volume explores the contemporary challenges to US national cybersecurity. Taking stock of the field, it features contributions by leading experts working at the intersection between academia and government and offers a unique overview of some of the latest debates about national cybersecurity. These contributions showcase the diversity of approaches and issues shaping contemporary understandings of cybersecurity in the West, such as deterrence and governance, cyber intelligence and big data, international cooperation, and public–private collaboration. The volume's main contribution lies in its effort to settle the field around three main themes exploring the international politics, concepts, and organization of contemporary cybersecurity from a US perspective. Related to these themes, this volume pinpoints three pressing challenges US decision makers and their allies currently face as they attempt to govern cyberspace: maintaining international order, solving conceptual puzzles to harness the modern information environment, and coordinating the efforts of diverse partners. The volume will be of much interest to students of cybersecurity, defense studies, strategic studies, security studies, and IR in general.

Seriously Organised Crime

Surveillance, Privacy, and the Dark Side of the Internet

Inside Cyber Warfare

One Man and the Battle for Rio

The Economics of Information Security and Privacy

From Viruses to Vote Rigging, How Hacking Went Global

The Fall of Yugoslavia

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.

Development Challenges, South-South Solutions is the monthly e-newsletter of the United Nations Office for South-South Cooperation in UNDP (www.southerninnovator.org). It has been published every month since 2006. Its sister publication, Southern Innovator magazine, has been published since 2011. ISSN 2227-3905 Stories by David South UN Office for South-South Cooperation Contact the Office to receive a copy of the new global magazine Southern Innovator. Issues 1, 2, 3, 4 and 5 are out now and are about innovators in mobile phones and information technology, youth and entrepreneurship, agribusiness and food security, cities and urbanization and waste and recycling. Why not consider sponsoring or advertising in an issue of Southern Innovator? Or work with us on an insert or supplement of interest to our readers? Follow @SouthSouth1.

With this book, managers and decision makers are given the tools to make more informed decisions about

big data purchasing initiatives. Big Data Analytics: A Practical Guide for Managers not only supplies descriptions of common tools, but also surveys the various products and vendors that supply the big data market.Comparing and contrasting the dif

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

Reimagining the Internet

CUCKOO'S EGG

DarkMarket

Dawn of the Code War

Your stepping stone to penetration testing

The Deviant Security Practices of Cyber Crime

The Third Balkan War

Every day, corporations are connecting the dots about our personal behavior—silently scrutinizing clues left behind by our work habits and Internet use. But who connects the dots about what firms are doing with all this information? Frank Pasquale exposes how powerful interests abuse secrecy for profit and explains ways to rein them in.

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.

NEW YORK TIMES BESTSELLER. The unbelievable true story of the man who built a billion-dollar online drug empire from his bedroom—and almost got away with it In 2011, a twenty-six-year-old libertarian programmer named Ross Ulbricht launched the ultimate free market: the Silk Road, a clandestine Web site hosted on the Dark Web where anyone could trade anything—drugs, hacking software, forged passports, counterfeit cash, poisons—free of the government's watchful eye. It wasn't long before the media got wind of the new Web site where anyone—not just teenagers and weed dealers but terrorists and black hat hackers—could buy and sell contraband detection-free. Spurred by a public outcry, the federal government launched an epic two-year manhunt for the site's elusive proprietor, with no leads, no witnesses, and no clear jurisdiction. All the investigators knew was that whoever was running the site called himself the Dread Pirate Roberts. The Silk Road quickly ballooned into $1.2 billion enterprise, and Ross embraced his new role as kingpin. He enlisted a loyal crew of allies in high and low places, all as addicted to the danger and thrill of running an illegal marketplace as their customers were to the heroin they sold. Through his network he got wind of the target on his back and took drastic steps to protect himself—including ordering a hit on a former employee. As Ross made plans to disappear forever, the Feds raced against the clock to catch a man they weren't sure even existed, searching for a needle in the haystack of the global Internet. Drawing on exclusive access to key players and two billion digital words and images Ross left behind, Vanity Fair correspondent and New York Times bestselling author Nick Bilton offers a tale filled with twists and turns, lucky breaks and unbelievable close calls. It's a story of the boy next door's ambition gone criminal, spurred on by the clash between the new world of libertarian-leaning, anonymous, decentralized Web advocates and the old world of government control, order, and the rule of law. Filled with

unforgettable characters and capped by an astonishing climax, American Kingpin might be dismissed as too outrageous for fiction. But it's all too real.

"Vigorous, passionate, humane, and extremely readable. . . For an account of what has actually happened. . . Glenny's book so far stands unparalleled."--The New Republic The fall of Yugoslavia tells the whole, true story of the Balkan Crisis--and the ensuing war--for those around the world who have watched the battle unfold with a mixture of horror, dread, and confusion. When Croatia and Slovenia declared their independence in June 1991, peaceful neighbors of four decades took up arms against each other once again and a savage war flared in the Balkans. The underlying causes go back to business left unfinished by both the Second and First World Wars. In this acclaimed book, now revised and updated with a new chapter on the Dayton Accords and the subsequent U.S. involvement, Misha Glenny offers a sobering eyewitness chronicle of the events that rekindled the violent conflict, a lucid and impartial analysis of the politics behind them, and incisive portraits of the main personalities involved. Above all, he shows us the human realities behind the headlines, and puts in its true, historical context one of the most ferocious civil wars of our time.

Hackers' Bazaar

Freedom (TM)

Cyberspace

The true story of Max Butler, the master hacker who ran a billion dollar cyber crime network

Nemesis

McMafia

Critique, Social Media and the Information Society

The Improbable War explains why conflict between the USA and China cannot be ruled out. In 1914 war between the Great Powers was considered unlikely, yet it happened. We learn only from history, and popular though the First World War analogy is, the lessons we draw from its outbreak are usually mistaken. Among these errors is the tendency to over-estimate human rationality. All major conflicts of the past 300 years have been about the norms and rules of the international system. In China and the US the world confronts two 'exceptional' powers whose values differ markedly, with China bidding to challenge the

current order. The 'Thucydidean Trap' - when a conservative status quo power confronts a rising new one - may also play its part in precipitating hostilities. To avoid stumbling into an avoidable war both Beijing and Washington need a coherent strategy, which neither of them has. History also reveals that war evolves continually. The next global conflict is likely to be played out in cyberspace and outer space and like all previous wars it will have devastating consequences. Such a war between the United States and China may seem improbable, but it is all too possible, which is why we need to discuss it now.
The inside story of how America's enemies launched a cyber war against us-and how we've learned to fight back With each passing year, the internet-linked attacks on America's interests have grown in both frequency and severity. Overmatched by our military, countries like North Korea, China, Iran, and Russia have found us vulnerable in cyberspace. The "Code War" is upon us. In this dramatic book, former Assistant Attorney General John P. Carlin takes readers to the front lines of a global but little-understood fight as the Justice Department and the FBI chases down hackers, online terrorist recruiters, and spies. Today, as our entire economy goes digital, from banking to manufacturing to transportation, the potential targets for our enemies multiply. This firsthand account is both a remarkable untold story and a warning of dangers yet to come.
“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.
In this powerful and groundbreaking book, Misha Glenny takes us on a journey through the new world of international organised crime. For three years, he has been recording the stories of gun runners in Ukraine, money launderers in Dubai, drug syndicates in Canada, cyber criminals in Brazil, racketeers in Japan and many more.During his investigation of the dark side, he has spoken to countless gangsters, policemen and victims of organised crime while also exploring the ferocious consumer demand for drugs, trafficked women, illegal labour and arms across five continents. The journey begins with an appalling and inexplicable murder in England's stockbroker belt and continues with stories that are often horrifying, sometimes inspiring, usually bizarre and occasionally funny. But together they build a breathtaking picture of the shadow economy that has grown so fast that it may now account for about 20% of the world's GDP. Usually the preserve of sensationalist reporting in the tabloid press, organised crime has seeped into our lives in so many ways and often without our knowledge. This consistently riveting account unveils the nature of crime in today's world but it also offers profound insights into the pitfalls of a globalisation where the rules dividing the legal from the illegal are often far from clear. McMafia unpicks the nexus of crime, politics and money worldwide which have become entangled and interdependent in entirely novel forms since the 1980s. It argues that conventional policing methods are no longer appropriate to deal with a problem whose roots lie in global poverty and the ever widening divisions between rich and poor.

American Kingpin

Nationalism, War, and the Great Powers, 1804-2011

The Improbable War

How One Hacker Took Over the Billion-Dollar Cybercrime Underground
How Hackers Became the New Mafia
McMafia (Movie Tie-In)
Eastern Europe in the Age of Democracy

In times of global capitalist crisis we are witnessing a return of critique in the form of a surging interest in critical theories (such as the critical political economy of Karl Marx) and social rebellions as a reaction to the commodification and instrumentalization of everything. On one hand, there are overdrawn claims that social media (Twitter, Facebook, YouTube, etc) have caused uproars in countries like Tunisia and Egypt. On the other hand, the question arises as to what actual role social media play in contemporary capitalism, crisis, rebellions, the strengthening of the commons, and the potential creation of participatory democracy. The commodification of everything has resulted also in a commodification of the communication commons, including Internet communication that is today largely commercial in character. This book deals with the questions of what kind of society and what kind of Internet are desirable, how capitalism, power structures and social media are connected, how political struggles are connected to social media, what current developments of the Internet and society tell us about potential futures, how an alternative Internet can look like, and how a participatory, commons-based Internet and a co-operative, participatory, sustainable information society can be achieved.

Now a major television series starring James Norton (War & Peace, Happy Valley) and created by Oscar-nominated screenwriter and film director Hossein Amini (Drive) and James Watkins (The Woman in Black), co-produced by BBC, AMC, and Cuba Pictures. In this powerful and groundbreaking work, award-winning author and journalist Misha Glenny takes us on a journey through the new world of international organized crime. Tracing the history of the shadow economy, Glenny exposes the nexus of crime, politics, and money that has come to shape and inform the post – Cold War era. From gun runners in the Ukraine to money launderers in Dubai, cyber criminals in Brazil, and racketeers in Japan, McMafia builds a breathtaking picture of a secret and bloody business. This edition features a new chapter reflecting on the expansion of McMafia culture in the past decade and its infiltration of major institutions of the global elite — including the most powerful centres of government — brought to light by revelations such as WikiLeaks and the Panama Papers.

Former hacker Kevin Poulsen has, over the past decade, built a reputation as one of the top investigative reporters on the cybercrime beat. In Kingpin, he pours his unmatched access and expertise into book form for the first time, delivering a gripping cat-and-mouse narrative—and an unprecedented view into the twenty-first century ' s signature form of organized crime. The word spread through the hacking underground like some unstoppable new virus: Someone—some brilliant, audacious crook—had just staged a hostile takeover of an online criminal network that siphoned billions of dollars from the US economy. The FBI rushed to launch an ambitious undercover operation aimed at tracking down this new kingpin; other agencies around the world deployed dozens of moles and double agents. Together, the cybercops lured numerous unsuspecting hackers into their clutches. . . . Yet at every turn, their main quarry displayed an uncanny ability to sniff out their snitches and see through their plots. The culprit they sought was the most unlikely of criminals: a brilliant programmer with a hippie ethic and a supervillain ' s double identity. As prominent " white-hat " hacker Max " Vision " Butler, he was a celebrity throughout the programming world, even

serving as a consultant to the FBI. But as the black-hat "Iceman," he found in the world of data theft an irresistible opportunity to test his outsized abilities. He infiltrated thousands of computers around the country, sucking down millions of credit card numbers at will. He effortlessly hacked his fellow hackers, stealing their ill-gotten gains from under their noses. Together with a smooth-talking con artist, he ran a massive real-world crime ring. And for years, he did it all with seeming impunity, even as countless rivals ran afoul of police. Yet as he watched the fraudsters around him squabble, their ranks riddled with infiltrators, their methods inefficient, he began to see in their dysfunction the ultimate challenge: He would stage his coup and fix what was broken, run things as they should be run—even if it meant painting a bull's-eye on his forehead. Through the story of this criminal's remarkable rise, and of law enforcement's quest to track him down, Kingpin lays bare the workings of a silent crime wave still affecting millions of Americans. In these pages, we are ushered into vast online-fraud supermarkets stocked with credit card numbers, counterfeit checks, hacked bank accounts, dead drops, and fake passports. We learn the workings of the numerous hacks—browser exploits, phishing attacks, Trojan horses, and much more—these fraudsters use to ply their trade, and trace the complex routes by which they turn stolen data into millions of dollars. And thanks to Poulsen's remarkable access to both cops and criminals, we step inside the quiet, desperate arms race that law enforcement continues to fight with these scammers today. Ultimately, Kingpin is a journey into an underworld of startling scope and power, one in which ordinary American teenagers work hand in hand with murderous Russian mobsters and where a simple Wi-Fi connection can unleash a torrent of gold worth millions.

"This volume has three parts: the first focuses on cyberspace itself; the second on some of the major forms of malevolence or threats that have become one of its defining characteristics; and the third on possible responses to these threats. One of the most significant features of cyberspace, however, is that it is becoming a risky place for the entire spectrum of users: nation-states, nongovernmental and transnational organizations, commercial enterprises, and individuals. Yet it is a space of opportunities -- for benevolent, neutral, and malevolent actors. Moreover, the authors identify and assess the challenges and threats to security that can arise in cyberspace because of its unique nature. In the final section, the authors discuss a variety of responses, with some suggesting that the most favored options being pursued by the United States are poorly conceived and ill-suited to the tasks at hand"--Publisher's web site.

Black Code

Inside the Dark Web

US National Cybersecurity

Mapping the Cyber Underworld

The Epic Hunt for the Criminal Mastermind Behind the Silk Road

America's Battle Against Russia, China, and the Rising Global Cyber Threat

Encyclopedia of Criminal Activities and the Deep Web

In the late 1990s, researchers began to grasp that the roots of many information security failures can be better explained with the language of economics than by pointing to instances of technical flaws. This led to a thriving new interdisciplinary research field combining economic and engineering insights, measurement approaches and methodologies to ask fundamental questions concerning the viability of a free and open

information society. While economics and information security comprise the nucleus of an academic movement that quickly drew the attention of thinktanks, industry, and governments, the field has expanded to surrounding areas such as management of information security, privacy, and, more recently, cybercrime, all studied from an interdisciplinary angle by combining methods from microeconomics, econometrics, qualitative social sciences, behavioral sciences, and experimental economics. This book is structured in four parts, reflecting the main areas: management of information security, economics of information security, economics of privacy, and economics of cybercrime. Each individual contribution documents, discusses, and advances the state of the art concerning its specific research questions. It will be of value to academics and practitioners in the related fields.

Misha Glenny's groundbreaking study of global organized crime is now the inspiration for an 8-part AMC crime drama starring James Norton (War and Peace), Juliet Rylance, and David Strathairn. With the collapse of the Soviet Union, the fall of the Berlin Wall, and the deregulation of international financial markets in 1989, governments and entrepreneurs alike became intoxicated by dreams of newly opened markets. But no one could have foreseen that the greatest success story to arise from these events would be the worldwide rise of organized crime. Today, it is estimated that illegal trade accounts for one-fifth of the global GDP. In this fearless and wholly authoritative investigation of the seemingly insatiable demand for illegal wares, veteran reporter Misha Glenny travels across five continents to speak with participants from every level of the global underworld--police, victims, politicians, and even the criminals themselves. What follows is a groundbreaking, propulsive look at an unprecedented phenomenon from a savvy, street-wise guide.

This innovative new text focuses on the politics of international security: how and why issues are interpreted as threats to international security and how such threats are managed. After a brief introduction to the field and its major theories and approaches, the core chapters systematically analyze the major issues on the contemporary international security agenda. Each is examined according to a common framework that brings out the nature of the threat and the responses open to policy makers. From war, terrorism and weapons of mass destruction, through environmental and economic crises, to epidemics, cyber-war and piracy, the twenty-first century world seems beset by a daunting range of international security problems. At the same time, the academic study of security has become more fragmented and contested than ever before as new actors, issues and theories increasingly challenge traditional concepts and approaches. This new edition has been heavily revised to discuss for the failings of the Obama admiration and its strategic partners on a number of different security issues, and the constant, evolving instances of turmoil the world has experienced since, whilst providing the skills students need to conduct their own research of international security issues occurring outside of this text, and for issues yet to occur. Cyber security, the 'Arab Spring' revolutions, the Ebola outbreak, and the refugee crisis are just some examples of the plethora of subjects that Smith analyses within this text. This textbook is an essential for those studying international security, whether at undergraduate or postgraduate level as part of a degree in international relations, politics, and other social sciences more generally. New to this Edition: - Chapter on cyber security - Up-to-date issues and field coverage - New 'mini-case studies' in each chapter - Updated analytical/pedagogical framework Pioneering framework for students to apply theory and empirical evidence correctly to tackle analytical and comparative tasks concerning both traditional and non-traditional security issues

Documents how a troubled young computer hacker seized control of a massive international computer fraud network in 2006, tracing the efforts of FBI and Secret Service agents as well as an undercover operator to locate and arrest him. Reprint.

Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It

Future Crimes
Inside the Business of Cybercrime
Industry of Anonymity
China, The United States and Logic of Great Power Conflict
The Balkans
Development Challenges, South-South Solutions: March 2013 Issue

Now a major BBC series starring James Norton Have you ever bought a pirate DVD? Taken drugs? Fallen for a phishing scam? Organised crime is part of all our worlds - often without us even knowing. McMafia is a journey through the new world of international organised crime, from gunrunners in Ukraine to money launderers in Dubai, by way of drug syndicates in Canada and cyber criminals in Brazil. During his investigation into the dark side Misha Glenny speaks to countless gangsters, policemen and victims of organized crime, and also explores the ferocious consumer demands for drugs, trafficked women, illegal labour and arms across five continents.

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.

Learn how to hack systems like black hat hackers and secure them like security experts Key Features Understand how computer systems work and their vulnerabilities Exploit weaknesses and hack into machines to test their security Learn how to secure systems from hackers Book Description This book starts with the basics of ethical hacking, how to practice hacking safely and legally, and how to install and interact with Kali Linux and the Linux terminal. You will explore network hacking, where you will see how to test the security of wired and wireless networks. You'll also learn how to crack the password for any Wi-Fi network (whether it uses WEP, WPA, or WPA2) and spy on the connected devices. Moving on, you will discover how to gain access to remote computer systems using client-side and server-side attacks.

You will also get the hang of post-exploitation techniques, including remotely controlling and interacting with the systems that you compromised. Towards the end of the book, you will be able to pick up web application hacking techniques. You'll see how to discover, exploit, and prevent a number of website vulnerabilities, such as XSS and SQL injections. The attacks covered are practical techniques that work against real systems and are purely for educational purposes. At the end of each section, you will learn how to detect, prevent, and secure systems from these attacks. What you will learn Understand ethical hacking and the different fields and types of hackers Set up a penetration testing lab to practice safe and legal hacking Explore Linux basics, commands, and how to interact with the terminal Access password-protected networks and spy on connected clients Use server and client-side attacks to hack and control remote computers Control a hacked system remotely and use it to hack other systems Discover, exploit, and prevent a number of web application vulnerabilities such as XSS and SQL injections Who this book is for Learning Ethical Hacking from Scratch is for anyone interested in learning how to hack and test the security of systems like professional hackers and security experts.

The New York Times bestseller Daemon unleashed a terrifying technological vision of an all-powerful, malicious computer program. Now, our world is the Daemon's world–unless someone stops it once and for all... The Daemon is in absolute control, using an expanded network of shadowy operatives to tear apart civilization and build it anew. Even as civil war breaks out in the American Midwest in a wave of nightmarish violence, former detective Pete Sebeck–the Daemon's most powerful, though reluctant, operative–must lead a small band of enlightened humans in a movement designed to protect the new world order. But the private armies of global business are preparing to crush the Daemon once and for all. In a world of shattered loyalties, collapsing societies, and seemingly endless betrayal, the only thing worth fighting for may be nothing less than the freedom of all humankind.

The Hunt for the New Crime Lords Who Are Bringing Down the Internet

Why the Geeks Will Inherit the Earth