Cyber Attack Cybercrime Cyberwarfare Cybercomplacency Is Hollywoods Blueprint For Chaos Coming True In The Brown Stuff Series Book 1

This publication highlights the fast-moving technological advancement and infiltration of Artificial Intelligence into society. Concepts of evolution of society through interconnectivity are explored, together with how the fusion of human and technological interaction leading to Augmented Humanity is fast becoming more than just an endemic phase, but a cultural phase shift to digital societies. It aims to balance both the positive progressive outlooks such developments bring with potential issues that may stem from innovation of this kind, such as the invasive procedures of bio hacking or ethical connotations concerning the usage of digital twins. This publication will also give the reader a good level of understanding on fundamental cyber defence principles, interactions with Critical National Infrastructure (CNI) and the Command, Control, Communications and Intelligence (C3I) decision-making framework. A detailed view of the cyber-attack landscape will be garnered; touching on the tactics, techniques and procedures used, red and blue teaming initiatives, cyber resilience and the protection of larger scale systems. The integration of AI, smart societies, the human-centric approach and Augmented Humanity is discernible in the exponential growth, collection and use of [big] data; concepts woven throughout the diversity of topics covered in this publication; which also discusses the privacy and transparency of data ownership, and the potential dangers of exploitation through social media. As humans are become ever more interconnected, with the prolificacy of smart wearable devices and wearable body area networks, the availability of and abundance of user data and metadata derived from individuals has grown exponentially. The notion of data ownership, privacy and situational awareness are now at the forefront in this new age.

Cyberspace, where information--and hence serious value--is stored and manipulated, is a tempting target. An attacker could be a person, group, or state and may disrupt or corrupt the systems from which cyberspace is built. When states are involved, it is tempting to compare fights to warfare, but there are important differences. The author addresses these differences and ways the United States protect itself in the face of attack.

"What were we? What are we?’ This is a recapitulation of the story of India from 1956 until 2014. It chronicles one of the most wonderful systems that have ever been developed on earth by an ancient and cultured social group that had been a pioneer in the establishment of welfare measures for both the ‘haves’ and the ‘have-nots’. The system referred to here is The Indian Banking System which, by its magical philosophy of “Save and Prosper”, has been the instrument of change. A large group of people have benefitted in one way or the other by this enchanting industry and all that it has had to offer. They chose to pay tributes out of respect for the system – and hence, this book. — Bang...oh...Bank...! But money was not everything. I realized that working in the bank brought with it a certain kind of dignity and social standing – which was quite a big deal in those days. Family, future, security, status etc. Yes, those days a bank employee was regarded highly by society. He was a sought-after groom in the marriage market. The liberalization era brought about important changes in the functioning of banks. The industry was the nerve-centre for all financial operations in the country. In order to meet the emerging need to match International Standards, automation and computerization of all core banking operations became the norm — A Banker’s Diary. When the computerisation wave swept the nation’s banks, lakhs and lakhs of precious public money was spent. The importance of Exceptional Reports was understood, and these exceptional reports were implemented by all the banks in all earnestness. But, the follow-up of the reports generated by the system and their consequences was not really done with the same amount of earnestness with which the scheme was implemented — Password Compromise. Human Resources or HR is perhaps the most valuable asset in any organisation. It is the human resource that exploits and makes use of other resources in the organization so as to achieve organizational objectives. The aim of the Human Resource Department, or by whatever name it is known – such as Personnel Department, P& IR and such else, is established to get the best out of the workforce of the organisation. For the achievement of organisational purpose, there are many sub-systems in the Human Resources Department, such as Grievance Handling, Counselling, Performance Appraisals, Career Planning, Training & Development Programs and such else. — A new born baby given new life to a Bank Office. All promises became true. All performances were spot-on. This is truer than the truth. Banking in India was promising, and encouraged the growth of India into becoming a vibrant and energetic economic power. That dream has now become reality. Now, India has become a force to reckon with in terms of economic development. No other country can afford to ignore India. I will not, for a change, make a conventional call that banks are at a cross-roads. We have crossed all of them, if you wish please, and there are only roads ahead. Rest assured that Indian Banking will survive at all times. — Banking Highway. . The Heads of Banks nodded, some applauded The higher-ups had no knowledge of what this barefoot banker was doing. They had to rely on him. He had the independence, freedom and autonomy necessary for decentralized decision making. He knew the way his Manager in Chennai was exceeding his authority and used to write to the head office to ratify his decisions in the past. He did the same thing with success. But the Regional Manager kept mum, it was his style. Wait for results: if they were positive, well, he could confirm all actions done at grass-roots. If the results were bad the axe could fall on. A prudent banker should observe ‘how men of prudence, discretion and intelligence manage their own affairs in regard to the permanent disposition of their funds considering probable income, as well as probable safety of the money involved’. (1830 Massachusetts Court definition) — Barefoot banker."

Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Recently, terrorist groups have been conducting more passive forms of information warfare. It is reported that these terrorist groups are using the Internet to conduct their operations by employing email and file encryption and steganography, as well as conducting web defacement attacks. Information Warfare (IW) has been around since the dawn of war. Information warfare has been and remains a critical element in deciding the outcome of military battles. According to Denning, “Information warfare consists of those actions intended to protect, exploit, corrupt, deny, or destroy information or information resources in order to achieve a significant advantage, objective, or victory over an adversary. This book discusses the nature and impact of cyber terrorism with the methods that have proven to be effective in law enforcement.

ICIW2012

Ethics and Cyber Warfare

Cybercrime Futures

Learn The Basics of Cyber Security, Threat Management, Cyber Warfare Concepts and Executive-Level Policies.

Cyberdeterrence and Cyberwar

Cyber Strategy

Cybercrimes are a threat and as dangerous as an armed intruder—yet millions of Americans are complacent or simply uninformed of how to protect themselves. The Secret to Cybersecurity closes that knowledge gap by using real-life examples to educate readers. It’s 2 a.m.—do you know who your child is online with? According to author Scott Augenbaum, between 80 to 90 percent of students say they do whatever they want on their smartphones—and their parents don’t have a clue. Is that you? What about your online banking passwords, are they safe? Has your email account or bank/debit card ever been compromised? In 2018, there were data breaches at several major companies—If those companies have your credit or debit information, that affects you. There are bad people in the world, and they are on the internet. They want to hurt you. They are based all over the world, so they’re hard at “work” when even you’re sleeping. They use automated programs to probe for weaknesses in your internet security programs. And they never stop. Cybercrime is on the increase internationally, and it’s up to you to protect yourself. But how? The Secret to Cybersecurity is the simple and straightforward plan to keep you, your family, and your business safe. Written by Scott Augenbaum, a 29-year veteran of the FBI who specialized in cybercrimes, it uses real-life examples to educate and inform readers, explaining who/why/how so you’ll have a specific takeaway to put into action for your family. Learn about the scams, methods, and ways that cyber criminals operate—and learn how to avoid being the next cyber victim.

Much of a society’s resources are devoted to dealing with, or preparing for the possibility of, crime. The dominance of concerns about crime also hint at the broader implications that offending has for many different facets of society. They suggest that rather than being an outlawed subset of social activity, crime is an integrated aspect of societal processes. This book reviews some of the direct and indirect social impacts of criminality, proposing that this is worthwhile, not just in terms of understanding crime, but also because of how it elucidates more general social considerations. A range of studies that examine the interactions between crime and society are brought together, drawing on a wide range of countries and cultures including India, Israel, Nigeria, Turkey, and the USA, as well as the UK and Ireland. They include contributions from many different social science disciplines, which, taken together, demonstrate that the implicit and direct impact of crime is very widespread indeed. The chapters in this book were originally published as a special issue of Contemporary Social Science.

In May 2021, Jim Gosler, known as the Godfather and commander of US agencies’ cyber offensive capability, said, ''Either the Intelligence Community (IC) would grow and adapt, or the Internet would eat us alive.'' Mr Gosler was speaking at his retirement only several months before the terrorist attacks of 9/11. He possibly did not realise the catalyst or the tsunami that he and his tens of thousands of US IC offensive website operatives had created and commenced. Over the last two decades, what Mr Gosler and his army of Internet keyboard warriors created would become the modus operandi for every faceless, nameless, state-sponsored or individual cybercriminal to replicate against an unwary, ill-protected, and ignorant group of executives and security professionals who knew little to nothing about the clandestine methods of infiltration and weaponisation of the Internet that the US and UK agencies led, all in the name of security. This book covers many cyber and ransomware attacks and events, including how we have gotten to the point of massive digital utilisation, particularly during the global lockdown and COVID-19 pandemic, to online spending that will see twice the monetary amount lost to cybercrime than what is spent online. There is little to no attribution, and with the IC themselves suffering cyberattacks, they are all blamed on being sophisticated ones, of course. We are witnessing the undermining of our entire way of life, our economies, and even our liberties. The IC has lots to answer for and unequivocally created the disastrous situation we are currently in. They currently have little to no answer. We need—no, we must demand—change. That change must start by ensuring the Internet and all connections to it are secure and no longer allow easy access and exfiltration for both the ICs and cybercriminals.

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.

Cyber War

A Multidisciplinary Approach

Educating a Cybersecurity Workforce

Cyber-Crime And Crime Law

Measuring Cybersecurity and Cyber Resiliency

This report presents a framework for the development of metrics--and a method for scoring them--that indicates how well a U.S. Air Force mission or system is expected to perform in a cyber-contested environment. There are two types of cyber metrics: working-level metrics to counter an adversary's cyber operations and institutional-level metrics to capture any cyber-related organizational deficiencies.

Some pundits claim cyber weaponry is the most important military innovation in decades, a transformative new technology that promises a paralyzing first-strike advantage difficult for opponents to deter. Yet, what is cyber strategy? How do actors use cyber capabilities to achieve a position of advantage against rival states? This book examines the emerging art of cyber strategy and its integration as part of a larger approach to coercion by states in the international system between 2000 and 2014. To this end, the book establishes a theoretical framework in the coercion literature for evaluating the efficacy of cyber operations. Cyber coercion represents the use of manipulation, denial, and punishment strategies in the digital frontier to achieve some strategic end. As a contemporary form of covert action and political warfare, cyber operations rarely produce concessions and tend to achieve only limited, signaling objectives. When cyber operations do produce concessions between rival states, they tend to be part of a larger integrated coercive strategy that combines network intrusions with other traditional forms of statecraft such as military threats, economic sanctions, and diplomacy. The books finds that cyber operations rarely produce concessions in isolation. They are additive instruments that complement traditional statecraft and coercive diplomacy. The book combines an analysis of cyber exchanges between rival states and broader event data on political, military, and economic interactions with case studies on the leading cyber powers: Russia, China, and the United States. The authors investigate cyber strategies in their integrated and isolated contexts, demonstrating that they are useful for maximizing informational asymmetries and disruptions, and thus are important, but limited coercive tools. This empirical foundation allows the authors to explore how leading actors employ cyber strategy and the implications for international relations in the 21st century. While most military plans involving cyber attributes remain highly classified, the authors piece together strategies based on observations of attacks over time and through the policy discussion in unclassified space. The result will be the first broad evaluation of the efficacy of various strategic options in a digital world.

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

This report argues that national strategy must be reviewed and adapted if it is to take proper account of cyber warfare. The report's key findings include: Cyber warfare can enable actors to achieve their political and strategic goals without the need for armed conflict; Cyberspace gives disproportionate power to small and otherwise relatively insignificant actors; Operating behind false IP addresses, foreign servers and aliases, attackers can act with almost complete anonymity and relative impunity, at least in the short term; In cyberspace the boundaries are blurred between the military and the civilian, and between the physical and the virtual; and power can be exerted by states or non-state actors, or by proxy; Cyberspace should be viewed as the 'fifth battlespace', alongside the more traditional arenas of land, air, sea and space. Cyber warfare is best understood as a new but not entirely separate component of this multifaceted conflict environment; The transatlantic relationship is important for a variety of reasons where cyber warfare is concerned. Close cooperation between the United States and the United Kingdom in intelligence and military matters has extended into cyberspace, enabling both states to influence the domain in a way that is difficult, if not impossible, for any other bilateral partnership or alliance to match.

Bang...Oh...Bank...!

This Is How They Tell Me the World Ends

Discover the Trade's Secret Attack Strategies And Learn Essential Prevention And Damage Control Mechanism

The Art of Cyber Security - A practical guide to winning the war on cyber crime

Cybersecurity For Beginners

Cyber Crime and Cyber Terrorism Investigator's Handbook

Effective Surveillance for Homeland Security: Balancing Technology and Social Issues provides a comprehensive survey of state-of-the-art methods and tools for the surveillance and protection of citizens and critical infrastructures against natural and deliberate threats. Focusing on current technological challenges involving multi-disciplinary prob

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

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 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.

How Hackers Became the New Mafia

Charting a Course Toward Cybersecurity

Government Policy Toward Open Source Software

Cyber Attack, Cybercrime, Cyberwarfare - Cybercomplacency

Order and Disorder in the International System

Cyber Terrorism and Information Warfare

Originally published in hardcover in 2016 by Simon & Schuster.

Since 2002, there has been an enormous increase in the number of known server vulnerabilities, leaving the traditional defensive solutions far behind. Today, attackers have improved on the sophistication used and the nature of the crime has changed. For example, web attacks between 2008 and 2010 caused 53 Seattle-based enterprises to face damages worth $3 million. Most such attacks are because of complacency and not remaining alert to the threat. The CEO's Manual on Cyber Security teaches you how to educate employees as well as develop a framework for security management against social engineering, keeping your corporation one step ahead of the attackers. It also details how enterprises can implement defenses against social engineering within their security policy. In this book you will learn how to avoid and prevent all of the following and more: Web Attacks Social Engineering Denial of Service caused by botnets Cloud Hacks Attacks via the Universal Serial Bus Clickjacking and cross-site scripting Phishing attacks from trusted third parties Data Exfiltration SSFR Attacks and CRIME (Compression Ratio Info-Leak Made Easy). Don't let your company fall victim to the thousands that will try to compromise its security and take it for all they can. Simply following the steps outlined in this book and being proactive can save you millions.

This report, the second in a series, reveals insights from chief information security officers; examines network defense measures and attacker-created countermeasures; and explores software vulnerabilities and inherent weaknesses.

This book addresses a host of issues raised by the rapid growth of open source software, including government subsidies for research and development, government procurement policy, and patent and copyright policy. Contributors offer diverse perspectives on a phenomenon that has become a lightning rod for controversy in the field of information technology.

Protecting Critical Infrastructure at the State and Local Level

Dark Territory

The CEO's Manual On Cyber Security

Is Hollywood's Blueprint for Chaos Coming True

Protecting Our Future

On Cyber Warfare

An essential, eye-opening book about cyberterrorism, cyber war, and the next great threat to our national security. “Cyber War may be the most important book about national security policy in the last several years.” –Slate Former presidential advisor and counter-terrorism expert Richard A. Clarke sounds a timely and chilling warning about America’s vulnerability in a terrifying new international conflict. Cyber War is a powerful book about technology, government, and military strategy; about criminals, spies, soldiers, and hackers. It explains clearly and convincingly what cyber war is, and how vulnerable we are as a nation and as individuals to the vast and looming web of cyber criminals. Every concerned American should read this startling and explosive book that offers an insider’s view of White House ‘Situation Room’ operations and carries the reader to the frontlines of our cyber defense. Cyber War exposes a virulent threat to our nation’s security.

Cybersecurity has become a topic of concern over the past decade as private industry, public administration, commerce, and communication have gained a greater online presence. As many individual and organizational activities continue to evolve in the digital sphere, new vulnerabilities arise. Cybersecurity Policies and Strategies for Cyberwarfare Prevention serves as an integral publication on the latest legal and defensive measures being implemented to protect individuals, as well as organizations, from cyber threats. Examining online criminal networks and threats in both the public and private spheres, this book is a necessary addition to the reference collections of IT specialists, administrators, business managers, researchers, and students interested in uncovering new ways to thwart cyber breaches and protect sensitive digital information.

International human rights law offers an overarching international legal framework to help determine the legality of the use of any weapon, as well as its lawful supply. It governs acts of States and non-State actors alike. In doing so, human rights law embraces international humanitarian law regulation of the use of weapons in armed conflict and disarmament law, as well as international criminal justice standards. In situations of law enforcement (such as counterpiracy, prisons, ordinary policing, riot control, and many peace operations), human rights law is the primary legal frame of reference above domestic criminal law. This important and timely book draws on all aspects of international weapons law and proposes a new view on international law governing weapons. Also included is a specific discussion on armed drones and cyberattacks, two highly topical issues in international law and international relations.

Cyber security involves protecting organisations from cyber risks, the threats to organisations caused by digital technology. These risks can cause direct damage to revenues and profits as well as indirect damage through reduced efficiency, lower employee morale, and reputational damage. Cyber security is often thought to be the domain of specialist IT professionals however, cyber risks are found across and within organisations. Unfortunately, many managers outside IT feel they are ill equipped to deal with cyber risks and the use of jargon makes the subject especially hard to understand. For this reason cyber threats are worse than they really need to be. The reality is that the threat from cyber risks is constantly growing, thus non-technical managers need to understand and manage it. As well as offering practical advice, the author guides readers through the processes that will enable them to manage and mitigate such threats and protect their organisations.

The Secret History of Cyber War

A Simple Plan to Protect Your Family and Business from Cybercrime

Cyber Crime, Security and Digital Intelligence

CyberThieves, CyberCops and You

The Evolving Character of Power and Coercion

Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity

"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 volume examines the complex international system of the twenty first century from a variety of perspectives. Proceeding from critical theoretical perspectives and incorporating case studies, the chapters focus on broad trends as well as micro-realities of a Post-Westphalian international system. The process of transformation and change of the international system has been an ongoing cumulative process. Many forces including conflict, technological innovation, and communication have contributed to the creation of a transnational world with political, economic, and social implications for all societies. Transnationalism functions both as an integrative factor and one which exposes the existing and the newly emerging divisions between societies and cultures and between nations and states. The chapters in this volume demonstrate that re-thinking fundamental assumptions as well as theoretical and methodological premises is central to understanding the dynamics of interdependence.

In the world of technology, cybersecurity is, without a doubt, one of the most dynamic topics of our times. Protecting Our Future brings together a range of experts from across the cybersecurity spectrum and shines a spotlight on operational challenges and needs across the workforce: in military, health care, international relations, telecommunications, finance, education, utilities, government, small businesses, and nonprofits. Contributors offer an assessment of strengths and weaknesses within each subfield, and, with deep subject-matter expertise, they introduce practitioners, as well as those considering a future in cybersecurity, to the challenges and opportunities when building a cybersecurity workforce.

This book is about cyber security, but it’s also about so much more; it’s about giving you the skills to think creatively about your role in the cyber security industry. In Part 1, the author discusses his thoughts on the cyber security industry and how those that operate within it should approach their role with the mindset of an artist. Part 2 explores the work of Sun Tzu’s The Art of War. The author analyses key sections and reviews them through the lens of cyber security and data protection to derive how his teachings can be used within the cyber security industry. Although Tzu’s book on military strategy, tactics and operations was written more than 2,000 years ago, The Art of Cyber Security - A practical guide to winning the war on cyber crime reflects on how relevant Tzu’s words are for today’s technological era. This book celebrates the individuals who are striving to protect us in an ever-expanding technological era. Data and technology are so important to our lives, that protecting people who use technology is incredibly important. The professionals working to protect children, adults and corporations have a tough job, and this book celebrates their work while advocating ways for improving cyber security services and fighting cyber crime. This book will challenge your thinking and force you to approach cyber security and data protection from theoretical, philosophical, strategic, tactical and operational perspectives.

Cyber-Physical Security

The Defender’s Dilemma

An Introduction for Non-Technical Managers

Weapons under International Human Rights Law

An Independent Report for AVG Technologies

Winner of the FT & McKinsey Business Book of the Year Award 2021

From North Korea's recent attacks on Sony to perpetual news reports of successful hackings and criminal theft, cyber conflict has emerged as a major topic of public concern. Yet even as attacks on military, civilian, and commercial targets have escalated, there is not yet a clear set of ethical guidelines that apply to cyber warfare. Indeed, like terrorism, cyber warfare is commonly believed to be a war without rules. Given the prevalence cyber warfare, developing a practical moral code for this new form of conflict is more important than ever. In Ethics and Cyber Warfare, internationally-respected ethicist George Lucas delves into the confounding realm of cyber conflict. Comparing "state-sponsored hacktivism" to the transformative impact of "irregular warfare" in conventional armed conflict, Lucas offers a critique of legal approaches to governance, and outlines a new approach to ethics and "just war" reasoning. Lucas draws upon the political philosophies of Alasdair MacIntyre, John Rawls, and Jurgen Habermas to provide a framework for understanding these newly-emerging standards for cyber conflict, and ultimately presents a professional code of ethics for a new generation of "cyber warriors." Lucas concludes with a discussion of whether preemptive self-defense efforts - such as the massive government surveillance programs revealed by Edward Snowden - can ever be justified, addressing controversial topics such as privacy, anonymity, and public trust. Well-reasoned and timely, Ethics and Cyber Warfare is a must-read for anyone with an interest in philosophy, ethics, or cybercrime. "

"A new report commissioned by the internet security company AVG reveals how the explosion in size and complexity of global cyber crime, combined with the surprising complacency of younger users, is putting lives at risk. The report, authored by the research agency The Future Laboratory, reveals that while cybercriminals and malicious programs are becoming increasingly sophisticated and difficult to detect, users are, alarmingly, becoming less vigilant about protecting their online devices. The combination of these two factors presents a potentially disastrous cybercrime scenario. The key findings of the report were as follows: 1) Cybercrime is on the increase as the tools and tactics which were previously used by hackers to cause disruption to machines and networks have been monetized by criminal gangs through bank fraud and ID theft; 2) Smart phones are no longer just phones, they are mini PCs, and consumers fail to realize that this makes them as vulnerable to cybercrime as a computer; 3) Consumers are aware of the need for antivirus protection but nearly one in ten of those surveyed fail to keep their protection updated. Alarmingly, the 18-35 age group (often cited as the group which is most digitally aware) is particularly complacent about this. Increasing integration of the internet into physical systems makes us increasingly vulnerable to cyber-attack. The 'Internet of Things' will soon become part of our connected world, opening new opportunities for hackers to cause harm and havoc.

"The never-before-told story of the computer scientists and the NSA, Pentagon, and White House policymakers who invented and employ the wars of the present and future--the cyber wars where every country can be a major power player and every hacker a mass destroyer, as reported by a Pulitzer Prize--winning security and defense journalist"--

Introduction to Cyber-Warfare: A Multidisciplinary Approach, written by experts on the front lines, gives you an insider's look into the world of cyber-warfare through the use of recent case studies. The book examines the issues related to cyber warfare not only from a computer science perspective but from military, sociological, and scientific perspectives as well. You'll learn how cyber-warfare has been performed in the past as well as why various actors rely on this new means of warfare and what steps can be taken to prevent it. Provides a multi-disciplinary approach to cyber-warfare, analyzing the information technology, military, policy, social, and scientific issues that are in play Presents detailed case studies of cyber-attack including inter-state cyber-conflict (Russia-Estonia), cyber-attack as an element of an information operations strategy (Israel-Hezbollah,) and cyber-attack as a tool against dissidents within a state (Russia, Iran) Explores cyber-attack conducted by large, powerful, non-state hacking organizations such as Anonymous and LulzSec Covers cyber-attacks directed against infrastructure, such as water treatment plants and power-grids, with a detailed account of Stuxent

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

The Secret to Cybersecurity

The Quest for Responsible Security in the Age of Digital Warfare
DarkMarket
International Cyber Incidents
Future Crimes

"Cyber Attack, CyberCrime, CyberWarfare CyberComplacency" is one of the few books that covers destructive Computer Network Attacks in the Internet and in CyberSpace. It is an in-depth reference that covers DDOS from motivation, identification, analysis and mitigation. By the author of the consistently top-selling in class "How to Cheat at Managing Information Security" and like that book, proceeds go to charity. Osborne starts with Network/Internet provider business practices and existing monitoring & detection systems. It shows the current focus on other forms of attacks including traditional electronic espionage, counter-terrorism and malware. It then describes various mechanisms for estimation of Cyberattack impact covering direct cost, indirect cost, and customer churn. It gradually drills down covering the various attacks types right down to the packet trace level, and how to detect them. These chapters are culminated with a full description of mitigation techniques, traditional and cutting edge again these are described in clear English but reinforced with common device configuration for the technical reader. The penultimate section highlights details of vulnerabilities in the Physical, Human, Mobile Apps, SCADA, Software security, BGP, and DNS elements of Cybersecurity. These include those that are currently utilised, that were predicted and have since been exploited during the publication process, and those that have yet to be leveraged. The last chapter explores the concept of a Firesale and how Hollywood's blueprint for Armageddon could be implemented in reality.

If you want to protect yourself and your family from the increasing risk of cyber-attacks, then keep reading. Cybersecurity for Beginners: Discover the Trade's Secret Attack Strategies And Learn Essential Prevention And Damage Control Mechanism will be the book you'll want to read to understand why cybersecurity is so important, and how it's impacting everyone who uses the Internet in 2019 and beyond. Each day, cybercriminals look for ways to hack into the systems and networks of major corporations and organizations-financial institutions, our educational systems, healthcare facilities and more. Already, it has cost billions of dollars in losses worldwide. This is only the tip of the iceberg in cybercrime. Needless to mention that individuals are terrorized by someone hacking into their computer, stealing personal and sensitive information, opening bank accounts and purchasing with their credit card numbers. Identity theft and financial losses are what a victim suffers from a cyber-attack. Cybercrimes are a threat to our well-being and as dangerous as someone literally breaking into your home. Yet, there are millions of Americans who continue to remain uninformed or complacent about how they should protect themselves. Cybersecurity for Beginners closes the knowledge gap by using real-life examples to educate readers. This book is a straightforward guide to keep you, your family and your business safe. Learn how cybercriminals operate, which secret methods they use, what they look for in vulnerabilities, and learn how to avoid being their next victim. To give you an idea of what the costs of cybercrime are: 2016-In one of the largest breaches of all time, 3 billion Yahoo accounts were hacked 2017-The U.S. is the most attacked country with 303 known large-scale attacks over the last three years2018-The hacking of "My Fitness Pal," affecting 150 million users2019-Businesses fall victim every 14 seconds to a ransomware attack causing its damage costs to increase to $11.5 billion by end of the year 2019. Cybersecurity for Beginners tells you: How to avoid getting locked out of your own systems Learn how you can identify weak points in your security defense setup Socking insights how you get infected on a legitimate website even when you don't click on anything How to prevent snooping from third parties in your private communications The one key technology to look out for that will disrupt the world of cybersecurity The most important facts and figures to be up on cybersecurity in 2019 9 powerful resources to track global cybercrime activities in real-time What the future of cybersecurity holds and how legislation worldwide will address consumer privacy And much more. This book will help you to become more vigilant and protective of your devices and networks even if you're an absolute beginner in the world of digital security. So, if you want to protect yourself and your family in the event of a cyberattack, then click the "add to cart" now!

"The Internet Is A Warzone - Cyber Security and Online Threat Management has Become a Requirement Today" Technology is changing fast, we know this. But A.I. and Automation are game changers for security and threatsCompanies that can use technology wisely and well are booming, companies that make bad or no technology choices collapse and disappear. The cloud, smart devices and the ability to connect almost any object to the internet are an essential landscape to use but are also fraught with new risks and dangers of a magnitude never seen before. The bad actors are in on this too and it creates a real problem right now for every individual and business.This book is for anyone that has an interest to protect themselves digitally, for the aspiring cyber security job entrant or seeker that needs some base knowledge to get in the field, for the smart business owner or executive that wants to prevent that one event that can wipe out their business overnight, or present a smart plant to prevent that to your boss.This book was written to provide easy insights in the essentials of cyber security, even if you have a non-technical background.Cybercrimes and attacks are a real threat and are as dangerous as an armed intruder - yet millions of Americans and businesses are complacent or simply uninformed of how to protect themselves. "Learn the Basics of Cyber Security, Threat Management, Cyber Warfare Concepts and Executive-Level Policies"closes that knowledge gap in a simple easy read by using real-life threat scenarios and methodologies.Did You Know? Your home router is being scanned and pinged from automated software that can do this with millions of IP addresses globally. It's not even a person, hacking has become automated, and you are the target. You have network intrusions, web app attacks, router firmware attacks and exploits (how often do you log into your home router to check logs?), hardly anyone does this..Why are you a target? Because any information that can be gathered about you can be sold to the cyber black market for huge profits, when gathered in a pool with others. Why do you think those massive cyber attacks on companies like Target and Walmart acquire databases of millions of customers, because the goals is to resell all that information to a criminal buyer for massive profits.Often hackers will not even use the info they are stealing (notice this is a verb and not past tense) from you, but will simply collect and pool with other victims on a global and persistent basis, all for the simple goal of profit. Real hackers don't care about you; they just want your data and information.It is similar to the "legal hackers", which I refer to as marketing analytic companies, such as; independent analytics vendors, trackers, Google and Facebook, for example, that track your every moment across online websites and physical stores, then sell your intimate data to marketers or companies that pay for online ads, and also to government agencies. But this is legal and there is nothing to stop it because it has already been in place now for over 15+ years and there are laws the marketing companies have to comply with, and they are quite strict and come with severe penalties for violations.Do you even have an Ethernet connected computer anymore at home? What about your business, do you have a well-configured firewall, wireless security policy, segmented networks, acceptable use policies and a cyber attack disaster plan?Do you even know what a cyber attack looks like? Here is realistic example;NOTHING. A moderate cyber attack on a business OR HOME can happen without you even knowing. Don't delay, scroll to the top and click the "Buy Now" button to get instant access to this book, if you purchase the Paperback version, you get the Kindle copy for FREE.

WINNER OF THE FT & McKINSEY BUSINESS BOOK OF THE YEAR AWARD 2021 The instant New York Times bestseller A Financial Times and The Times Book of the Year 'A terrifying exposé' The Times 'Part John le Carré . . . Spellbinding' New Yorker We plug in anything we can to the internet. We can control our entire lives, economy and grid via a remote web control. But over the past decade, as this transformation took place, we never paused to think that we were also creating the world's largest attack surface. And that the same nation that maintains the greatest cyber advantage on earth could also be among its most vulnerable. Filled with spies, hackers, arms dealers and a few unsung heroes, This Is How They Tell Me the World Ends is an astonishing and gripping feat of journalism. Drawing on years of reporting and hundreds of interviews, Nicole Perlroth lifts the curtain on a market in shadow, revealing the urgent threat faced by us all if we cannot bring the global cyber arms race to heel.

The Next Threat to National Security and What to Do About It
Effective Surveillance for Homeland Security
Cyber Security
Crime and Society
Cybersecurity Policies and Strategies for Cyberwarfare Prevention
ICIW2012-Proceedings of the 7th International Conference on Information Warfare and Security