Cyber Espionage E Cyber Counterintelligence Spionaggio E Controspionaggio Cibernetico

The probability of a world-wide cyber conflict is small. Yet the probability of forms of cyber conflict, regional or even global, could be argued as being very high. Small countries are usually signatories to military and economic alliances with major world powers but rely heavily on the technical ability of these powers in protecting their own national interests. They may be considered to be IT ’technology colonies’. Their cyber infrastructure is usually fully imported and their ability to assess it is limited. This book poses the question: to what extent should, or can, a small country prepare itself for handling the broad range of cyber threats? Looking at cyber-warfare, cyber-terrorism, cyber-crime and associated concerns, national experts from New Zealand, Australia, The Netherlands, and Poland present analyses of cyber-defence realities, priorities and options for smaller countries. They show that what is needed is the ability of small nations to be able to define and prepare appropriate responses such as the role of military/law enforcement/business entities, continuity and resilience strategies, incident response and business continuity plans and more for handing nationally-aimed cyber-attacks particularly where these address national critical infrastructures.

Cybersecurity and Human Rights in the Age of Cyberveillance is a collection of articles by distinguished authors from the US and Europe and presents contemporary perspectives on the limits of human rights in the international internet community.

Cyber espionage e cyber counterintelligence. Spionaggio e controspionaggio ciberneticoNational Security and Counterintelligence in the Era of Cyber EspionageIGI Global

Adopting a multidisciplinary perspective, this book explores the key challenges associated with the proliferation of cyber capabilities. Over the past two decades, a new man-made domain of conflict has materialized. Alongside armed conflict in the domains of land, sea, air, and space, hostilities between different types of political actors are now taking place in cyberspace. This volume addresses the challenges posed by cyberspace hostility from theoretical, political, strategic and legal perspectives. In doing so, and in contrast to current literature, cyber-security is analysed through a multidimensional lens, as opposed to being treated solely as a military or criminal issues, for example. The individual chapters map out the different scholarly and political positions associated with various key aspects of cyber conflict and seek to answer the following questions: do existing theories provide sufficient answers to the current challenges posed by conflict in cyberspace, and, if not, could alternative approaches be developed?; how do states and non-state actors make use of cyber-weapons when pursuing strategic and political aims?; and, how does the advent of conflict in cyberspace challenge our established legal framework? By asking important strategic questions on the theoretical, strategic, ethical and legal implications and challenges of the proliferation of cyber warfare capabilities, the book seeks to stimulate research into an area that has hitherto been neglected. This book will be of much interest to students of cyber-conflict and cyber-warfare, war and conflict studies, international relations, and security studies.

Effective administration of government and governmental organizations is a crucial part of achieving success in those organizations. With the widespread knowledge and use of e-government, the intent and evaluation of its services continue to focus on meeting the needs and satisfaction of its citizens. Strategic Management and Innovative Applications of E-Government is a pivotal reference source that provides organizational and managerial directions, applications, and theoretical and philosophical discussions on current issues relating to the practice of electronic government. While highlighting topics such as citizen trust in government and smart government, this publication explores electronic government technology adoption, as well as the methods of government social media practices. This book is a vital reference source for policy makers, IT specialists, government professionals, academicians, researchers, and graduate-level students seeking current research on e-government applications.

This encyclopedia will be an essential resource for our times, reflecting the fact that we currently are living in an expanding data-driven world. Technological advancements and other related trends are contributing to the production of an astoundingly large and exponentially increasing collection of data and information, referred to in popular vernacular as “Big Data.” Social media and crowdsourcing platforms and various applications ? “apps” ? are producing reams of information from the instantaneous transactions and input of millions and millions of people around the globe. The Internet-of-Things (IoT), which is expected to comprise tens of billions of objects by the end of this decade, is actively sensing real-time intelligence on nearly every aspect of our lives and environment. The Global Positioning System (GPS) and other location-aware technologies are producing data that is specific down to particular latitude and longitude coordinates and seconds of the day. Large-scale instruments, such as the Large Hadron Collider (LHC), are collecting massive amounts of data on our planet and even distant corners of the visible universe. Digitization is being used to convert large collections of documents from print to digital format, giving rise to large archives of unstructured data. Innovations in technology, in the areas of Cloud and molecular computing, Artificial Intelligence/Machine Learning, and Natural Language Processing (NLP), to name only a few, also are greatly expanding our capacity to store, manage, and process Big Data. In this context, the Encyclopedia of Big Data is being offered in recognition of a world that is rapidly moving from gigabytes to terabytes to petabytes and beyond. While indeed large data sets have long been around and in use in a variety of fields, the era of Big Data in which we now live departs from the past in a number of key respects and with this departure comes a fresh set of challenges and opportunities that cut across and affect multiple sectors and disciplines, and the public at large. With expanded analytical capacities at hand, Big Data is now being used for scientific inquiry and experimentation in nearly every (if not all) disciplines, from the social sciences to the humanities to the natural sciences, and more. Moreover, the use of Big Data has been well established beyond the Ivory Tower. In today's economy, businesses simply cannot be competitive without engaging Big Data in one way or another in support of operations, management, planning, or simply basic hiring decisions. In all levels of government, Big Data is being used to engage citizens and to guide policy making in pursuit of the interests of the public and society in general. Moreover, the changing nature of Big Data also raises new issues and concerns related to, for example, privacy, liability, security, access, and even the veracity of the data itself. Given the complex issues attending Big Data, there is a real need for a reference book that covers the subject from a multi-disciplinary, cross-sectoral, comprehensive, and international perspective. The Encyclopedia of Big Data will address this need and will be the first of such reference books to do so. Featuring some 500 entries, from "Access" to "Zillow," the Encyclopedia will serve as a fundamental resource for researchers and students, for decision makers and leaders, and for business analysts and purveyors. Developed for those in academia, industry, and government, and others with a general interest in Big Data, the encyclopedia will be aimed especially at those involved in its collection, analysis, and use. Ultimately, the Encyclopedia of Big Data will provide a common platform and language covering the breadth and depth of the topic for different segments, sectors, and disciplines.

The COVID-19 pandemic has affected individuals and caused destabilization of households and business activities. In emerging economies, many sectors and companies, especially small and medium enterprises (SMEs), are severely influenced by the reduction or cessation of economic activity. Overcoming the COVID-19 virus and allowing the world to heal will allow the economy to grow more resilient. First, however, we must understand that old managerial practices can no longer generate competitive advantage in the post-pandemic world. Public Health and Economic Resiliency in the Post-COVID-19 Era presents epidemiological studies of the COVID-19 pandemic, identifies the impacts it has on human health, and analyzes the impacts on public health and economy. This management tool also discusses the socio-economic human vulnerability related to the COVID-19 pandemic. Covering topics such as risk analysis, quality management systems, and therapeutic systems, this book is a dynamic resource for academic researchers and investigators, university professors, students, epidemiologists, health professionals, economists, managers, sociologists, physicians, policymakers, government officials, and academicians.

Dependence on computers has had a transformative effect on human society. Cybernetics is now woven into the core functions of virtually every basic institution, including our oldest ones. War is one such institution, and the digital revolution's impact on it has been profound. The American military, which has no peer, is almost completely reliant on high-tech computer systems. Given the Internet's potential for full-spectrum surveillance and information disruption, the marshaling of computer networks represents the next stage of cyberwar. Indeed, it is upon us already. The recent Stuxnet episode, in which Israel fed a malignant computer virus into Iran's nuclear facilities, is one such example. Penetration into US government computer systems by Chinese hackers-presumably sponsored by the Chinese government-is another. Together, they point to a new era in the evolution of human conflict. In Cybersecurity and Cyerbwar: What Everyone Needs to Know, noted experts Peter W. Singer and Allan Friedman lay out how the revolution in military cybernetics occurred and explain where it is headed. They begin with an explanation of what cyberspace is before moving on to discussions of how it can be exploited and why it is so hard to defend. Throughout, they discuss the latest developments in military and security technology. Singer and Friedman close with a discussion of how people and governments can protect themselves. In sum, Cybersecurity and Cyerbwar is the definitive account on the subject for the educated general reader who wants to know more about the nature of war, conflict, and security in the twenty-first century.

Cyber weapons and the possibility of cyber conflict—including interference in foreign political campaigns, industrial sabotage, attacks on infrastructure, and combined military campaigns—require policymakers, scholars, and citizens to rethink twenty-first-century warfare. Yet because cyber capabilities are so new and continually developing, there is little agreement about how they will be deployed, how effective they can be, and how they can be managed. Written by leading scholars, the fourteen case studies in this volume will help policymakers, scholars, and students make sense of contemporary cyber conflict through historical analogies to past military-technological problems. The chapters are divided into three groups. The first—What Are Cyber Weapons Like?—examines the characteristics of cyber capabilities and how their use for intelligence gathering, signaling, and precision striking compares with earlier technologies for such missions. The second section—What Might Cyber Wars Be Like?—explores how lessons from several wars since the early nineteenth century, including the World Wars, could apply—or not—to cyber conflict in the twenty-first century. The final section—What Is Preventing and/or Managing Cyber Conflict Like?—offers lessons from past cases of managing threatening actors and technologies.

Complete proceedings of the 14th European Conference on Cyber Warfare and Security Hatfield UK Published by Academic Conferences and Publishing International Limited

As both a physical living space and emotional environment, cities impact human beings in a number of ways. These ways include but are not limited to the kinds of relationship that may exist among the varying categories of inhabitants of the city, the organization of and accessibility to leaning resources and facilities, the types and rates of migration impacting the city, the security level of the city, and the livelihood networks existing within the city. Learning Cities, Town Planning, and the Creation of Livelihoods is an essential research publication that explores livelihood types and lifelong learning typologies required by cities as well as the relationship between higher education and improved livelihood outcomes. Featuring a broad range of topics such as learning needs, economy, and technologically advanced societies, this book is ideally designed for policymakers, academicians, researchers, students, social workers, educators, politicians, and environmentalists.

Cyber risk has become increasingly reported as a major problem for financial sector businesses. It takes many forms including fraud for purely monetary gain, hacking by people hostile to a company causing business interruption or damage to reputation, theft by criminals or malicious individuals of the very large amounts of customer information (“big data”) held by many companies, misuse including accidental misuse or lack of use of such data, loss of key intellectual property, and the theft of health and medical data which can have a profound effect on the insurance sector. This book assesses the major cyber risks to businesses and discusses how they can be managed and the risks reduced. It includes case studies of the situation in different financial sectors and countries in relation to East Asia, Europe and the United States. It takes an interdisciplinary approach assessing cyber risks and management solutions from an economic, management risk, legal, security intelligence, insurance, banking and cultural perspective.

The advent of cyberspace has led to a dramatic increase in state-sponsored political and economic espionage. This monograph argues that these practices represent a threat to the maintenance of international peace and security and assesses the extent to which international law regulates this conduct. The traditional view among international legal scholars is that, in the absence of direct and specific international law on the topic of espionage, cyber espionage constitutes an extra-legal activity that is unconstrained by international law. This monograph challenges that assumption and reveals that there are general principles of international law as well as specialised international legal regimes that indirectly regulate cyber espionage. In terms of general principles of international law, this monograph explores how the rules of territorial sovereignty, non-intervention and the non-use of force apply to cyber espionage. In relation to specialised regimes, this monograph investigates the role of diplomatic and consular law, international human rights law and the law of the World Trade Organization in addressing cyber espionage. This monograph also examines whether developments in customary international law have carved out espionage exceptions to those international legal rules that otherwise prohibit cyber espionage as well as considering whether the doctrines of self-defence and necessity can be invoked to justify cyber espionage. Notwithstanding the applicability of international law, this monograph concludes that policymakers should nevertheless devise an international law of espionage which, as lex specialis, contains rules that are specifically designed to confront the growing threat posed by cyber espionage.

The rate of cybercrimes is increasing because of the fast-paced advancements in computer and internet technology. Crimes employing mobile devices, data embedding/mining systems, computers, network communications, or any malware impose a huge threat to data security. Countering Cyber Attacks and Preserving the Integrity and Availability of Critical Systems addresses current problems and issues emerging in cyber forensics and investigations and proposes new solutions that can be adopted and implemented to counter security breaches within various organizations. The publication examines a variety of topics such as advanced techniques for forensic developments in computer and communication-link environments and legal perspectives including procedures for cyber investigations, standards, and policies. It is designed for policymakers, forensic analysts, technology developers, security administrators, academicians, researchers, and students.

In-depth counterintelligence tactics to fight cyber-espionage "A comprehensive and unparalleled overview of the topic by experts in the field."--Slashdot Expose, pursue, and prosecute the perpetrators of advanced persistent threats (APTs) using the tested security techniques and real-world case studies featured in this one-of-a-kind guide. Reverse Deception: Organized Cyber Threat Counter-Exploitation shows how to assess your network’s vulnerabilities, zero in on targets, and effectively block intruders. Discover how to set up digital traps, misdirect and divert attackers, configure honeypots, mitigate encrypted crimeware, and identify malicious software groups. The expert authors provide full coverage of legal and ethical issues, operational vetting, and security team management. Establish the goals and scope of your reverse deception campaign Identify, analyze, and block APTs Engage and catch nefarious individuals and their organizations Assemble cyber-profiles, incident analyses, and intelligence reports Uncover, eliminate, and autopsy crimeware, trojans, and botnets Work with intrusion detection, anti-virus, and digital forensics tools Employ stealth honeynet, honeypot, and sandbox technologies Communicate and collaborate with legal teams and law enforcement

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

A chilling and revelatory appraisal of the new faces of espionage and warfare on the digital battleground Shortly after 9/11, Joel Brenner entered the inner sanctum of American espionage, first as the inspector general of the National Security Agency, then as the head of counterintelligence for the director of National Intelligence. He saw at close range the battleground on which adversaries are attacking us: cyberspace. Like the rest of us, governments and corporations inhabit “glass houses,” all but transparent to a new generation of spies who operate remotely from such places as China, the Middle East, Russia, and even France. In this urgent wake-up call, Brenner draws on his extraordinary background to show what we can—and cannot—do to prevent cyber spies and hackers from compromising our security and stealing our latest technology.

"A comprehensive overview of cyber intelligence, explaining what it is, why it is needed, who is doing it, and how it is done"--

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.

This book presents an interdisciplinary examination of cross-Taiwan Strait relations and the complex dynamics at play in the region. Since the election of Ma Ying-jeou as Taiwan’s president in 2008, the relationship across the Taiwan Strait—long viewed as one of Asia’s most volatile potential flashpoints—has experienced a remarkable détente. Whether the relationship has been truly transformed, however, remains an open question and the Taiwan Strait remains a central regional and global security issue.

A return to turbulence in the Taiwan Strait could also add a new dimension of instability in the already tense maritime disputes in the East and South China Seas. While the relationship across the Taiwan Strait remains critically important, it is also changing rapidly, and the chapters in this volume present new thinking to help make sense of complex cross-Strait dynamics. Specifically, these essays explore different security and/or globalization dimensions of China-Taiwan ties as well as the globalization-security linkages that have emerged. As the balance of power in Asia shifts dramatically, several chapters in this volume explore how traditional security forces are evolving. At the same time, there are new dynamics emerging as a consequence of globalization forces, such as the tremendous economic and social integration across the Taiwan Strait, and several chapters in this volume consider some of these new problems. Finally, several chapters consider the often under-researched dynamics associated with the globalization/security interface such as cyber threats, transnational criminal networks and the security spill-over impact of production globalization. This book will of much interest to students of Chinese Politics, Asian Security, globalisation, diplomacy and International Relations.

The internet has become a vital part of modern society, with its impact reaching from private lives into the public sphere. However, along with its positive effects, the dissemination of this technology has created opportunities for increased cyber terrorism activities. Combating Internet-Enabled Terrorism: Emerging Research and Opportunities is an informative resource that highlights developments that will aid in combating internet-based hostility and violence. Featuring extensive coverage on relevant topics that include social media, military tactics, and counterterrorism, this publication will provide insight into the world of internet terrorism to researchers, academicians, and graduate students in this field.

As technology continues to advance, the threats imposed on these innovations also continue to grow and evolve. As such, law enforcement specialists diligently work to counteract these threats, promote national safety, and defend the individual rights of citizens. National Security and Counterintelligence in the Era of Cyber Espionage highlights technological advancements in intelligence systems and law enforcement in relation to cybercrime and reconnaissance issues. Focusing on current and emergent threats to national security, as well as the technological advancements being adopted within the intelligence field, this book is an exhaustive reference source for government officials, researchers, graduate-level students, and intelligence and enforcement specialists interested in novel measures in being implemented in the prevention of cybercrime and terrorism.

Providing an invaluable introductory resource for students studying cyber warfare, this book highlights the evolution of cyber conflict in modern times through dozens of key primary source documents related to its development and implementation. This meticulously curated primary source collection is designed to offer a broad examination of key documents related to cyber warfare, covering the subject from multiple perspectives. The earliest documents date from the late 20th century, when the concept and possibility of cyber attacks became a reality, while the most recent documents are from 2019. Each document is accompanied by an introduction and analysis written by an expert in the field that provides the necessary context for readers to learn about the complexities of cyber warfare. The title's nearly 100 documents are drawn primarily but not exclusively from government sources and allow readers to understand how policy, strategy, doctrine, and tactics of cyber warfare are created and devised, particularly in the United States. Although the United States is the global leader in cyber capabilities and is largely driving the determination of norms within the cyber domain, the title additionally contains a small number of international documents. This invaluable work will serve as an excellent starting point for anyone seeking to understand the nature and character of international cyber warfare.

Covers in detail one of the defining forms of conflict of the 21st century—cyber warfare will significantly impact virtually every American citizen over the next two decades Provides more than 90 primary source documents and matching analysis, allowing readers to investigate the underpinnings of cyber warfare Enables readers to see the development of different concepts of cyber warfare through its chronological organization Reflects the deep knowledge of an editor who is a noted expert in cyber warfare and has taught for the United States Air Force for more than a decade

This book focuses on software architecture and the value of architecture in the development of long-lived, mission-critical, trustworthy software-systems. The author introduces and demonstrates the powerful strategy of “Managed Evolution,” along with the engineering best practice known as “Principle-based Architecting.” The book examines in detail architecture principles for e.g., Business Value, Changeability, Resilience, and Dependability. The author argues that the software development community has a strong responsibility to produce and operate useful, dependable, and trustworthy software. Software should at the same time provide business value and guarantee many quality-of-service properties, including security, safety, performance, and integrity. As Dr. Furrer states, “Producing dependable software is a balancing act between investing in the implementation of business functionality and investing in the quality-of-service properties of the software-systems." The book presents extensive coverage of such concepts as: Principle-Based Architecting Managed Evolution Strategy The Future Principles for Business Value Legacy Software Modernization/Migration Architecture Principles for Changeability Architecture Principles for Resilience Architecture Principles for Dependability The text is supplemented with numerous figures, tables, examples and illustrative quotations. Future-Proof Software-Systems provides a set of good engineering practices, devised for integration into most software development processes dedicated to the creation of software-systems that incorporate Managed Evolution. Presented from a criminal justice perspective, Cyberspace, Cybersecurity, and Cybercrime introduces students to the interdisciplinary field of cybercrime by exploring the theoretical, practical, and legal framework it operates under, along with strategies to combat it. Authors Janine Kremling and Amanda M. Sharp Parker provide a straightforward overview of cybercrime, cyberthreats, and the vulnerabilities individuals, businesses, and governments face everyday in a digital environment. Highlighting the latest empirical research findings and challenges that cybercrime and cybersecurity pose for those working in the field of criminal justice, this book exposes critical issues related to privacy, terrorism, hacktivism, the dark web, and much more. Focusing on the past, present, and future impact of cybercrime and cybersecurity, it details how criminal justice professionals can be prepared to confront the changing nature of cybercrime. Instructors! Sign in at study.sagepub.com/kremling for PowerPoint slides, test banks, and more!

Cyber security has become a topic of concern over the past decade. As many individual and organizational activities continue to evolve digitally, it is important to examine the psychological and behavioral aspects of cyber security. Psychological and Behavioral Examinations in Cyber Security is a critical scholarly resource that examines the relationship between human behavior and interaction and cyber security. Featuring coverage on a broad range of topics, such as behavioral analysis, cyberpsychology, and online privacy, this book is geared towards IT specialists, administrators, business managers, researchers, and students interested in online decision making in cybersecurity.

There is little doubt that cyber-space has become the battle space for confrontations. However, to conduct cyber operations, a new armory of weapons needs to be employed. No matter how many, or how sophisticated an aggressor's kinetic weapons are, they are useless in cyber-space. This book looks at the milieu of the cyber weapons industry, as well as the belligerents who use cyber weapons. It discusses what distinguishes these hardware devices and software programs from computer science in general. It does this by focusing on specific aspects of the topic—contextual issues of why cyber-space is the new battleground, defensive cyber weapons, offensive cyber weapons, dual-use weapons, and the implications these weapons systems have for practice. Contrary to popular opinion, the use of cyber weapons is not limited to nation states; though this is where the bulk of news reporting focuses. The reality is that there isn’t a sector of the political-economy that is immune to cyber skirmishes. So, this book looks at cyber weapons not only by national security agencies and the military, but also by law enforcement, and the business sector—the latter includes administrations termed non-government organisations (NGOs). This book offers study material suitable for a wide-ranging audience—students, professionals, researchers, policy officers, and ICT specialists.

Now available in a new edition entitled GLASS HOUSES: Privacy, Secrecy, and Cyber Insecurity in a Transparent World. A former top-level National Security Agency insider goes behind the headlines to explore America's next great battleground: digital security. An urgent wake-up call that identifies our foes; unveils their methods; and charts the dire consequences for government, business, and individuals. Shortly after 9/11, Joel Brenner entered the inner sanctum of American espionage, first as the inspector general of the National Security Agency, then as the head of counterintelligence for the director of national intelligence. He saw at close range the battleground on which our adversaries are now attacking us-cyberspace. We are at the mercy of a new generation of spies who operate remotely from China, the Middle East, Russia, even France, among many other places. These operatives have already shown their ability to penetrate our power plants, steal our latest submarine technology, rob our banks, and invade the Pentagon's secret communications systems. Incidents like the WikiLeaks posting of secret U.S. State Department cables hint at the urgency of this problem, but they hardly reveal its extent or its danger. Our government and corporations are a "glass house," all but transparent to our adversaries. Counterfeit computer chips have found their way into our fighter aircraft; the Chinese stole a new radar system that the navy spent billions to develop; our own soldiers used intentionally corrupted thumb drives to download classified intel from laptops in Iraq. And much more. Dispatches from the corporate world are just as dire. In 2008, hackers lifted customer files from the Royal Bank of Scotland and used them to withdraw $9 million in half an hour from ATMs in the United States, Britain, and Canada. If that was a traditional heist, it would be counted as one of the largest in history. Worldwide, corporations lose on average $5 million worth of intellectual property apiece annually, and big companies lose many times that. The structure and culture of the Internet favor spies over governments and corporations, and hackers over privacy, and we've done little to alter that balance. Brenner draws on his extraordinary background to show how to right this imbalance and bring to cyberspace the freedom, accountability, and security we expect elsewhere in our lives. In America the Vulnerable, Brenner offers a chilling and revelatory appraisal of the new faces of war and espionage-virtual battles with dangerous implications for government, business, and all of us.

Global change and advancing technology have transformed the government sector with the use of information and communication technology to improve service delivery. The use of such technologies in electronic and mobile government services raises issues relating to security, privacy, and data protection. Security Frameworks in Contemporary Electronic Government is a pivotal reference source that provides vital research on the application of special security requirements in electronic government transactions. While highlighting topics such as digital environments, public service delivery, and cybercrime, this publication explores the difficulties and challenges faced in implementing e-government technologies, as well as the different aspects of security in e-government. This book is ideally designed for policymakers, software developers, IT specialists, government officials, academicians, researchers, and students seeking current research on secure environments in electronic and mobile government.

Designed for university students in the burgeoning field of intelligence studies and professional training classes, Counterintelligence Theory and Practice provides all the elements required for a successful counterintelligence operation. Exploring issues relating to national security, military, law enforcement, as well as corporate private affairs, Hank Prunckun uses his experience as a professional to explain both the theoretical basis and practical application for real counterintelligence craft. Each chapter contains key words and phrases and a number of study questions and learning activities that make the book a comprehensive tool for learning how to be a counterintelligence professional.

Recently, the public sector has given an increasing amount of national and international attention to electronic government systems. Therefore, it is inevitable that the theoretical implications and intersections between information technology and governmental matters are more widely discussed. Public Information Management and E-Government:

Policy and Issues offers a fresh, comprehensive dialogue on issues that occur between the public management and information technology domains. With its focus on political issues and their effects on the larger public sector, this book is valuable for administrators, researchers, students, and educators who wish to gain foundational and theoretical knowledge on e-government policies.

In our hyper-connected digital world, cybercrime prevails as a major threat to online security and safety. New developments in digital forensics tools and an understanding of current criminal activities can greatly assist in minimizing attacks on individuals, organizations, and society as a whole. The Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance combines the most recent developments in data protection and information communication technology (ICT) law with research surrounding current criminal behaviors in the digital sphere. Bridging research and practical application, this comprehensive reference source is ideally designed for use by investigators, computer forensics practitioners, and experts in ICT law, as well as academicians in the fields of information security and criminal science.