Computer Crime Information Warfare Economic Espionage Carolina Academic Press Law Casebook Serie

When people think of hackers, they usually think of a lone wolf acting with the intent to garner personal data for identity theft and fraud. But what about the corporations and government entities that use hacking as a strategy for managing risk? Why Hackers Win asks the pivotal question of how and why the instrumental uses of invasive software by corporations and government agencies contribute to social change. Through a critical communication and media studies lens, the book focuses on the struggles of breaking and defending the “trusted systems” underlying our everyday use of technology. It compares the United States and the European Union, exploring how cybersecurity and hacking accelerate each other in digital capitalism, and how the competitive advantage that hackers can provide corporations and governments may actually afford new venues for commodity development and exchange. Presenting prominent case studies of communication law and policy, corporate hacks, and key players in the global cybersecurity market, the book proposes a political economic model of new markets for software vulnerabilities and exploits, and clearly illustrates the social functions of hacking.

This book explores current and emerging trends in policy, strategy, and practice related to cyber operations conducted by states and non-state actors. The book examines in depth the nature and dynamics of conflicts in the cyberspace, the geopolitics of cyber conflicts, defence strategy and practice, cyber intelligence and information security.

"This book reviews problems, issues, and presentations of the newest research in the field of cyberwarfare and cyberterrorism. While enormous efficiencies have been gained as a result of computers and telecommunications technologies, use of these systems and networks translates into a major concentration of information resources, createing a vulnerability to a host of attacks and exploitations"--Provided by publisher.

The major aim of Cyberspace and the State is to provide conceptual orientation on the new strategic environment of the Information Age. It seeks to restore the equilibrium of policy-makers which has been disturbed by recent cyber scares, as well as to bring clarity to academic debate on the subject particularly in the fields of politics and international relations, war and strategic studies. Its main chapters explore the impact of cyberspace upon the most central aspects of statehood and the state system?power, sovereignty, war, and dominion. It is concerned equally with practice as with theory and may be read in that sense as having two halves.

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.

Describes strategies used to attack the information infastructure and provides information on short and long-term solutions.

China's emergence as a great power in the twenty-first century is strongly enabled by cyberspace. Leveraged information technology integrates Chinese firms into the global economy, modernizes infrastructure, and increases internet penetration which helps boost export-led growth. China's pursuit of "informatization" reconstructs industrial sectors and solidifies the transformation of the Chinese People's Liberation Army into a formidable regional power. Even as the government censors content online, China has one of the fastest growing internet populations and most of the technology is created and used by civilians. Western political discourse on cybersecurity is dominated by news of Chinese military development of cyberwarfare capabilities and cyber exploitation against foreign governments, corporations, and non-governmental organizations. Western accounts, however, tell only one side of the story. Chinese leaders are also concerned with cyber insecurity, and Chinese authors frequently note that China is also a victim of foreign cyber -- attacks -- predominantly from the United States. China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain is a comprehensive analysis of China's cyberspace threats and policies. The contributors -- Chinese specialists in cyber dynamics, experts on China, and experts on the use of information technology between China and the West -- address cyberspace threats and policies, emphasizing the vantage points of China and the U.S. on cyber exploitation and the possibilities for more positive coordination with the West. The volume's multi-disciplinary, cross-cultural approach does not pretend to offer wholesale resolutions. Contributors take different stances on how problems may be analyzed and reduced, and aim to inform the international audience of how China's political, economic, and security systems shape cyber activities. The compilation provides empirical and evaluative depth on the deepening dependence on shared global information infrastructure and the growing willingness to exploit it for political or economic gain.

This book explores Australia's prospective cyber-warfare requirements and challenges. It describes the current state of planning and thinking within the Australian Defence Force with respect to Network Centric Warfare, and discusses the vulnerabilities that accompany the use by Defence of the National Information Infrastructure (NII), as well as Defence's responsibility for the protection of the NII. It notes the multitude of agencies concerned in various ways with information security, and argues that mechanisms are required to enhance coordination between them. It also argues that Australia has been laggard with respect to the development of offensive cyber-warfare plans and capabilities. Finally, it proposes the establishment of an Australian Cyber-warfare Centre responsible for the planning and conduct of both the defensive and offensive dimensions of cyber-warfare, for developing doctrine and operational concepts, and for identifying new capability requirements. It argues that the matter is urgent in order to ensure that Australia will have the necessary capabilities for conducting technically and strategically sophisticated cyber-warfare activities by the 2020s. The Foreword has been contributed by Professor Kim C. Beazley, former Minister for Defence (1984--90), who describes it as 'a timely book which transcends old debates on priorities for the defence of Australia or forward commitments, (and) debates about globalism and regionalism', and as 'an invaluable compendium' to the current process of refining the strategic guidance for Australia's future defence policies and capabilities.

Today, cyber security, cyber defense, information warfare andcyber warfare issues are among the most relevant topics both at thenational and international level. All the major states of the worldare facing cyber threats and trying to understand how cyberspacecould be used to increase power. Through an empirical, conceptual and theoretical approach, CyberConflict has been written by researchers and experts in the fieldsof cyber security, cyber defense and information warfare. It aimsto analyze the processes of information warfare and cyber

warfarethrough historical, operational and strategic perspectives of cyberattack. It is original in its delivery because of itsmultidisciplinary approach within an international framework, withstudies dedicated to different states – Canada, Cuba, France,Greece, Italy, Japan, Singapore, Slovenia and South Africa –describing the state's application of information warfareprinciples both in terms of global development and"local" usage and examples. Contents 1. Canada's Cyber Security Policy: a Tortuous Path Towarda Cyber Security Strategy, Hugo Loiseau and Lina Lemay. 2. Cuba: Towards an Active Cyber-defense, Daniel Ventre. 3. French Perspectives on Cyber-conflict, Daniel Ventre. 4. Digital Sparta: Information Operations and Cyber-warfare inGreece, Joseph Fitsanakis. 5. Moving Toward an Italian Cyber Defense and Security Strategy,Stefania Ducci. 6. Cyberspace in Japan's New Defense Strategy, DanielVentre. 7. Singapore's Encounter with Information Warfare: FilteringElectronic Globalization and Military Enhancements, AlanChong. 8. A Slovenian Perspective on Cyber Warfare, Gorazd Praprotnik,Iztok Podbregar, Igor Bernik and Bojan Ticar. 9. A South African Perspective on Information Warfare and CyberWarfare, Brett van Niekerk and Manoj Maharaj. 10. Conclusion, Daniel Ventre

Cyberspace attacks continue in the United States with many of these incidents crossing international borders. The global nature of cyberspace makes it difficult to determine if a breach into a computer system is an act of cyberterrorism, cyber crime, or cyber warfare. An attack to steal credit card information may be all three simultaneous. The Department of Defense is ready to protect the nation against all enemies in the air, on the land, or on the sea. These domains are well protected with military forces postured to respond. Our nation's economy is under constant attack through the cyberspace domain. Attacks through electronic means happen at the speed of light and require a quick response to contain. Proactive approaches defend our borders, but not our economy. Instead, the United States has a passive defense relying on the goodwill of commercial enterprises and the investigative approaches of law enforcement agencies. Through the Untied States Cyber Command, the Department of Defense has capability that can be used to defend America. This work looks at the roles and responsibilities of the Department of Defense as it relates to Homeland Defense and the protection of credit card information transitioning across the Internet.

Gives the reader a detailed account of how cyber-security in Switzerland has evolved over the years, using official documents and a considerable amount of inside knowledge. It focuses on key ideas, institutional arrangements, on the publication of strategy papers, and importantly, on processes leading up to these strategy documents. The peculiarities of the Swiss political system, which influence the way cyber-security can be designed and practiced in Switzerland are considered, as well as the bigger, global influences and driving factors that shaped the Swiss approach to cyber-security. It shows that throughout the years, the most important influence on the Swiss policy-approach was the international level, or rather the developments of a cyber-security policy in other states. Even though many of the basic ideas about information-sharing and public-private partnerships were influenced by (amongst others) the US approach to critical infrastructure protection, the peculiarities of the Swiss political system has led to a particular "Swiss solution", which is based on the federalist structures and subsidiary principles, characterized by stability and resilience to external shocks in the form of cyber-incidents. Cybersecurity in Switzerland will be a stimulating read for anybody interested in cyber-security policy, including students, researchers, analysts and policy makers. It contains not only specific material on an interesting case, but also a wealth of background information on different variations of cyber-security, as well as on information-sharing and public-private partnerships.

Blackhatonomics explains the basic economic truths of the underworld of hacking, and why people around the world devote tremendous resources to developing and implementing malware. The book provides an economic view of the evolving business of cybercrime, showing

the methods and motivations behind organized cybercrime attacks, and the changing tendencies towards cyber-warfare. Written by an exceptional author team of Will Gragido, Daniel J Molina, John Pirc and Nick Selby, Blackhatonomics takes practical academic principles and backs them up with use cases and extensive interviews, placing you right into the mindset of the cyber criminal. Historical perspectives of the development of malware as it evolved into a viable economic endeavour Country specific cyber-crime analysis of the United States, China, and Russia, as well as an analysis of the impact of Globalization on cyber-crime Presents the behind the scenes methods used to successfully execute financially motivated attacks in a globalized cybercrime economy Provides unique insights, analysis, and useful tools for justifying corporate information security budgets Provides multiple points of view, from pure research, to corporate, to academic, to law enforcement Includes real world cybercrime case studies and profiles of high-profile cybercriminals

Essay from the year 2011 in the subject Law - European and International Law, Intellectual Properties, grade: 1,7, University of Reading, language: English, abstract: Computers represent a stark example of dual use technology as they can be used for peaceful and military purposes, such as espionage and cyber-attacks. Cyber-attacks are a new tool of coercion, which brings many advantages for potential perpetrators in comparison with conventional attacks. For example, the knowledge and equipment necessary to initiate a computer network attack are widely available. The response of international law to this problem has been slow, attempting to twist existing legal frameworks to fit the new challenge. The present essay considers whether the international community should view computerized network attacks as a prohibited use of force under Article 2(4) of the UN Charter. The first section defines the parameters of cyber-attack and distinguishes it from other forms of computer crime. Several reasons for choosing cyber-attack over conventional weapons are identified. The second section discusses whether cyber-attack constitutes ‘armed force’. Cyber-attack is contrasted with other forms of coercion such as political and economic coercion as well as chemical and biological weapons. The final section poses the question whether cyber-attacks are prohibited by Article 2(4) of the UN Charter, particularly focusing on the issue of consequentiality.

Over the years, a plethora of reports has emerged that assess the causes, dynamics, and effects of cyber threats. This proliferation of reports is an important sign of the increasing prominence of cyber attacks for organizations, both public and private, and citizens all over the world. In addition, cyber attacks are drawing more and more attention in the media. Such efforts can help to better awareness and understanding of cyber threats and pave the way to improved prevention, mitigation, and resilience. This report aims to help in this task by assessing what we know about cyber security threats based on a review of 70 studies published by public authorities, companies, and research organizations from about 15 countries over the last few years. It answers the following questions: what do we know about the number, origin, and impact of cyber attacks? What are the current and emerging cyber security trends? And how well are we prepared to face these threats?

This book introduces policy, government, and security professionalsto the concept of “information warfare,” covering itsevolution over the last decade and its developments among sucheconomic and political giants as China, Russia, Japan, India, andSingapore. The text describes various conceptions of informationwarfare, along with how they function in military, diplomatic,political, and economic contexts. Recent notable cyber attacks areanalyzed, the challenges faced by countries who fail to securetheir cyberspace (Japan, the US, etc.) are enumerated, and ways todistinguish between cybercrime, cyberwarfare, and cyberterrrorismare discussed.

The World Economic Forum regards the threat of cyber attack as one of the top five global risks confronting nations of the world today. Cyber attacks are increasingly targeting the core functions of the economies in nations throughout the world. The threat to attack critical infrastructures, disrupt critical services, and induce a wide range of dam

This ebook is a selective guide designed to help scholars and students of criminology find reliable sources of information by directing them to the best available scholarly materials in whatever form or format they appear from books, chapters, and journal articles to online archives, electronic data sets, and blogs. Written by a leading international authority on the subject, the ebook provides bibliographic information supported by direct recommendations about which sources to consult and editorial commentary to make it clear how the cited sources are interrelated related. A reader will discover, for instance, the most reliable introductions and overviews to the topic, and the most important publications on various areas of scholarly interest within this topic. In criminology, as in other disciplines, researchers at all levels are drowning in potentially useful scholarly information, and this guide has been created as a tool for cutting through that material to find the exact source you need. This ebook is a static version of an article from Oxford Bibliographies Online: Criminology, a dynamic, continuously updated, online resource designed to provide authoritative guidance through scholarship and other materials relevant to the study and practice of criminology. Oxford Bibliographies Online covers most subject disciplines within the social science and humanities, for more information visit www.aboutobo.com.

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.

This book is designed for those who want a better grasp of the nature and existential threat of today’s information wars. It uses a conceptual approach to explain the relevant concepts as well as the structural challenges and responsibilities with which policy makers struggle and practitioners must work.

The First International Conference on Digital Forensics and Cyber Crime (ICDF2C) was held in Albany from September 30 to October 2, 2009. The field of digital for- sics is growing rapidly with implications for several fields including law enforcement, network security, disaster recovery and accounting. This is a multidisciplinary area that requires expertise in several areas including, law, computer science, finance, networking, data mining, and criminal justice. This conference brought together pr- titioners and researchers from diverse fields providing opportunities for business and intellectual engagement among attendees. All the conference sessions were very well attended with vigorous discussions and strong audience interest. The conference featured an excellent program comprising high-quality paper pr- entations and invited speakers from all around the world. The first day featured a plenary session including George Philip, President of University at Albany, Harry Corbit, Suprintendent of New York State Police, and William Pelgrin, Director of New York State Office of Cyber Security and Critical

Infrastructure Coordination. An outstanding keynote was provided by Miklos Vasarhelyi on continuous auditing. This was followed by two parallel sessions on accounting fraud /financial crime, and m- timedia and handheld forensics. The second day of the conference featured a mesm- izing keynote talk by Nitesh Dhanjani from Ernst and Young that focused on psyc- logical profiling based on open source intelligence from social network analysis. The third day of the conference featured both basic and advanced tutorials on open source forensics.

"This book provides relevant frameworks and best practices as well as current empirical research findings for professionals who want to improve their understanding of the impact of cyber-attacks on critical infrastructures and other information systems essential to the smooth running of society, how such attacks are carried out, what measures should be taken to mitigate their impact"--Provided by publisher.

Computer Crime, Information Warfare, and Economic EspionageCyber-threats, Information Warfare, and Critical Infrastructure ProtectionDefending the U.S. HomelandGreenwood Publishing Group

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

The central features of the 'cybered' world of the early 21st century are the interconnectedness of global communications, information and economic infrastructures and the dependence upon those infrastructures in order to govern, to do business or simply to live. This discussion paper is concerned with states and societies (rather than businesses or individuals) and their vulnerability, through interconnectedness and dependence, to aggressive economic action either from, or facilitated by cyber space. This paper is not, therefore, an analysis of the extent and gravity of financial cyber-crime; that subject has been discussed fully elsewhere. Neither does the paper examine child exploitation and other forms of computer-based crime, important though these are. Instead, I ask whether economic cyber warfare should indeed be considered a strategic problem. In the words of the 2010 UK National Security Strategy, national strategy must be 'a combination of ends (what we are seeking to achieve), ways (the ways by which we seek to achieve those ends) and means (the resources we can devote to achieving the ends).' Reversing the trajectory, I ask whether the economy might be the way, and cyberspace the means with which to attack the organization and coherence of a modern developed state; not for financial or criminal gain, and not in order to achieve a terrorist 'spectacular', but for maximal political or strategic ends? I take a stepwise approach to answering this question, beginning with a discussion of economic warfare and then of cyber warfare, before discussing the possibility of the composite idea of economic cyber warfare. What might be the incentives and disincentives to partake in economic cyber warfare, how seriously should it be taken and is the modern state the best

organization to deal with this security challenge?

Information warfare is upon us. In the last two decades, the U.S. economy's infrastructure has undergone a fundamental set of changes, relying increasingly on its service sector and high technology economy. The U.S. depends on computers, electronic data storage and transfers, and highly integrated communications networks. Its rapidly developing new form of critical infrastructure is exceedingly vulnerable to an emerging host of threats. This detailed volume examines the dangers of, and the evolving U.S. policy response to, cyberterrorism.

When the Stuxnet computer worm damaged the Iranian nuclear program in 2010, the public got a small glimpse into modern cyber warfare—without truly realizing the scope of this global conflict. Inside Cyber Warfare provides fascinating and disturbing details on how nations, groups, and individuals throughout the world increasingly rely on Internet attacks to gain military, political, and economic advantages over their adversaries. This updated second edition takes a detailed look at the complex domain of cyberspace, and the players and strategies involved. You'll discover how sophisticated hackers working on behalf of states or organized crime patiently play a high-stakes game that could target anyone, regardless of affiliation or nationality. Discover how Russian investment in social networks benefits the Kremlin Learn the role of social networks in fomenting revolution in the Middle East and Northern Africa Explore the rise of anarchist groups such as Anonymous and LulzSec Look inside cyber warfare capabilities of nations including China and Israel Understand how the U.S. can legally engage in covert cyber operations Learn how the Intellectual Property war has become the primary focus of state-sponsored cyber operations Jeffrey Carr, the founder and CEO of Taia Global, Inc., is a cyber intelligence expert and consultant who specializes in the investigation of cyber attacks against governments and infrastructures by state and non-state hackers.

In order to enable general understanding and to foster the implementation of necessary support measures in organizations, this book describes the fundamental and conceptual aspects of cyberspace abuse. These aspects are logically and reasonably discussed in the fields related to cybercrime and cyberwarfare. The book illustrates differences between the two fields, perpetrators' activities, as well as the methods of investigating and fighting against attacks committed by perpetrators operating in cyberspace. The first chapter focuses on the understanding of cybercrime, i.e. the perpetrators, their motives and their organizations. Tools for implementing attacks are also briefly mentioned, however this book is not technical and does not intend to instruct readers about the technical aspects of cybercrime, but rather focuses on managerial views of cybercrime. Other sections of this chapter deal with the protection against attacks, fear, investigation and the cost of cybercrime. Relevant legislation and legal bodies, which are used in cybercrime, are briefly described at the end of the chapter. The second chapter deals with cyberwarfare and explains the difference between classic cybercrime and operations taking place in the modern inter-connected world. It tackles the following questions: who is committing cyberwarfare; who are the victims and who are the perpetrators? Countries which have an important role in cyberwarfare around the world, and the significant efforts being made to combat cyberwarfare on national and international levels, are mentioned. The common points of cybercrime and cyberwarfare, the methods used to protect against them and the vision of the future of cybercrime and cyberwarfare are briefly described at the end of the book. Contents 1. Cybercrime. 2. Cyberwarfare. About the Authors Igor Bernik is Vice Dean for Academic Affairs and Head of the Information Security Lab at the University of Maribor, Slovenia. He has written and contributed towards over 150 scientific articles and conference papers, and co-authored 4 books. His current research interests concern information/cybersecurity, cybercrime, cyberwarfare and cyberterrorism.

Increased reliance on the Internet and other networked systems raise the risks of cyber attacks that could harm our nation's cyber infrastructure. The cyber infrastructure encompasses a number of sectors including: the nation's mass transit and other transportation

systems; banking and financial systems; factories; energy systems and the electric power grid; and telecommunications, which increasingly rely on a complex array of computer networks, including the public Internet. However, many of these systems and networks were not built and designed with security in mind. Therefore, our cyber infrastructure contains many holes, risks, and vulnerabilities that may enable an attacker to cause damage or disrupt cyber infrastructure operations. Threats to cyber infrastructure safety and security come from hackers, terrorists, criminal groups, and sophisticated organized crime groups; even nation-states and foreign intelligence services conduct cyber warfare. Cyber attackers can introduce new viruses, worms, and bots capable of defeating many of our efforts. Costs to the economy from these threats are huge and increasing. Government, business, and academia must therefore work together to understand the threat and develop various modes of fighting cyber attacks, and to establish and enhance a framework to assess the vulnerability of our cyber infrastructure and provide strategic policy directions for the protection of such an infrastructure. This book addresses such questions as: How serious is the cyber threat? What technical and policy-based approaches are best suited to securing telecommunications networks and information systems infrastructure security? What role will government and the private sector play in homeland defense against cyber attacks on critical civilian infrastructure, financial, and logistical systems? What legal impediments exist concerning efforts to defend the nation against cyber attacks, especially in preventive, preemptive, and retaliatory actions?

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 book presents IT managers with what cyberterrorism and information warfare is and how to handle the problems associated with them"--Provided by publisher.

Conflict and Cooperation in Cyberspace: The Challenge to National Security brings together some of the world’s most distinguished military leaders, scholars, cyber operators, and policymakers in a discussion of current and future challenges that cyberspace poses to the United States and the world. Maintaining a focus on policy-relevant solutions, it offers a well-reasoned study of how to prepare for war, while attempting to keep the peace in the cyberspace domain. The discussion begins with thoughtful contributions concerning the attributes and importance of cyberspace to the American way of life and global prosperity. Examining the truths and myths behind recent headline-grabbing malicious cyber activity, the book spells out the challenges involved with establishing a robust system of monitoring, controls, and sanctions

to ensure cooperation amongst all stakeholders. The desire is to create a domain that functions as a trusted and resilient environment that fosters cooperation, collaboration, and commerce. Additionally, the book: Delves into the intricacies and considerations cyber strategists must contemplate before engaging in cyber war Offers a framework for determining the best ways to engage other nations in promoting global norms of behavior Illustrates technologies that can enable cyber arms control agreements Dispels myths surrounding Stuxnet and industrial control systems General Michael V. Hayden, former director of the National Security Agency and the Central Intelligence Agency, begins by explaining why the policymakers, particularly those working on cyber issues, must come to understand the policy implications of a dynamic domain. Expert contributors from the Air Force Research Institute, MIT, the Rand Corporation, Naval Postgraduate School, NSA, USAF, USMC, and others examine the challenges involved with ensuring improved cyber security. Outlining the larger ethical, legal, and policy challenges facing government, the private sector, civil society, and individual users, the book offers plausible solutions on how to create an environment where there is confidence in the ability to assure national security, conduct military operations, and ensure a vibrant and stable global economy.

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

Each era brings with it new techniques and methods of waging a war. While military scholars and experts have mastered land, sea, air and space warfare, time has come that they studied the art of cyberwar too. Our neighbours have acquired the capabilities to undertake this new form of asymmetric form of warfare. India too therefore needs to acquire the capabilities to counter their threat. Cyber space seems to have invaded every aspect of our life. More and more systems whether public or private are getting automated and networked. This high dependence of our critical infrastructure on Information and Communication Technology exposes it to the vulnerabilities of cyberspace. Enemy now can target such infrastructure through the cyberspace and degrade/ destroy them. This implies that the critical information infrastructure of the country and military networks today are both equally vulnerable to enemy’s cyberattacks. India therefore must protect its critical information infrastructure as she would protect the military infrastructure in the battlefield. Public – Private Partnership model is the only model which would succeed in doing so. While the Government needs to lay down the policies and frame the right laws, private sector needs to invest into cyber security. Organisations at national level and at the level of armed forces need to be raised which can protect our assets and are also capable of undertaking offensive cyber operations. This book is an attempt to understand various nuances of cyber warfare and how it affects our national security. Based on the cyber threat environment, the books recommends a framework of cyber doctrine and cyber strategies as well as organisational structure of various organisations which a nation needs to invest in.

This book creates a framework for understanding and using cyberpower in support of national security. Cyberspace and

cyberpower are now critical elements of international security. United States needs a national policy which employs cyberpower to support its national security interests.

A variety of modern research methods in a number of innovating cyber-security techniques and information management technologies are provided in this book along with new related mathematical developments and support applications from engineering. This allows for the exploration of new approaches, useful practices and related problems for further investigation.Distinguished researchers and scientists coming from different scientific origins present their research and views concerning cyber-security, information warfare and communications systems.Graduate students, scientists and engineers interested in a broad spectrum of current theories, methods, and applications in interdisciplinary fields will find this book invaluable.Topics covered include: Electronic crime and ethics in cyberspace, new technologies in security systems/systems interfaces, economic information warfare, digital security in the economy, human factor evaluation of military security systems, cyber warfare, military communications, operational analysis and information warfare, and engineering applications to security systems/detection theory.

This text introduces the concepts of information warfare from a non-military, organizational perspective. It is designed to stimulate managers to develop policies, strategies, and tactics for the aggressive use and defence of their data and knowledge base. The book covers the full gambit of information warfare subjects from the direct attack on computer systems to the more subtle psychological technique of perception management. It provides the framework needed to build management strategies in this area. The topics covered include the basics of information warfare, corporate intelligence systems, the use of deception, security of systems, modes of attack, a methodology to develop defensive measures, plus specific issues associated with information warfare. This book will be of interest to executives and managers in any public or private organization. Specifically, managers or staff in the areas of information technology, security, knowledge management, public relations, or marketing should find it directly useful. Its main purpose is to make readers aware of the new world of information saturation; thus decreasing the chance that they will become victims of those abusing the information age, whilst at the same time increasing their chances of benefiting from the new opportunities produced. Addresses the issues and implications of cyber warfare and how it directly impacts on companies