Ethics And Policies For Cyber Operations

In its 4th edition, this book remains focused on increasing public awareness of the nature and motives of cyber vandalism and cybercriminals, the weaknesses inherent in cyberspace infrastructure, and the means available to protect ourselves and our society. This new edition aims to integrate security education and awareness with discussions of morality and ethics. The reader will gain an understanding of how the security of information in general and of computer networks in particular, on which our national critical infrastructure and, indeed, our lives depend, is based squarely on the individuals who build the hardware and design and develop the software that run the networks that store our vital information. Addressing security issues with ever-growing social networks are two new chapters: “Security of Mobile Systems” and “Security in the Cloud Infrastructure.” Instructors considering this book for use in a course may request an examination copy here.

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. "

Cyber environments have become a fundamental part of educational institutions, causing a need for understanding the impact and general principles of ethical computer use in academia. With the rapid increase in the use of digital technologies in classrooms and workplaces worldwide, it is important that part of the training that takes place for students is how to be good cyber citizens, who are ethical in the decisions that they make and in their interactions with others across digital platforms. Emerging Trends in Cyber Ethics and Education is a pivotal reference source that provides vital research on the application of ethics and education within online environments. While highlighting topics such as computer simulation, corporate e-learning, and plagiarism detection, this publication explores effective ways of utilizing digital landscapes for online education, as well as the methods of improving cyber security frameworks. This book is ideally designed for educators, IT developers, education professionals, education administrators, researchers, and upper-level graduate students seeking current research on secure and educational interactions in digital landscapes.

Presents theories and models associated with information privacy and safeguard practices to help anchor and guide the development of technologies, standards, and best practices. Provides recent, comprehensive coverage of all issues related to information security and ethics, as well as the opportunities, future challenges, and emerging trends related to this subject.

Examining the thematic intersection of law, technology and violence, this book explores cyber attacks against states and current international law on the use of force. The theory of information ethics is used to critique the law's conception of violence and to develop an informational approach as an alternative way to think about cyber attacks. Cyber attacks against states constitute a new form of violence in the information age, and international law on the use of force is limited in its capacity to regulate them. This book draws on Luciano Floridi's theory of information ethics to critique the narrow conception of violence embodied in the law and to develop an alternative way to think about cyber attacks, violence, and the state. The author uses three case studies - the 2007 cyber attacks against Estonia, the Stuxnet incident involving Iran that was discovered in 2010, and the cyber attacks used as part of the Russian interference in the 2016 US presidential election - to demonstrate that an informational approach offers a means to reimagine the state as an entity and cyber attacks as a form of violence against it. This interdisciplinary approach will appeal to an international audience of scholars in international law, international relations, security studies, cyber security, and anyone interested in the issues surrounding emerging technologies.

As society continues to heavily rely on software and databases, the risks for cyberattacks have increased rapidly. As the dependence on computers has become gradually widespread throughout communities and governments, there is a need for cybersecurity programs that can assist in protecting sizeable networks and significant amounts of data at once. Implementing overarching security policies for software systems is integral to protecting community-wide data from harmful attacks. Establishing Cyber Security Programs Through the Community Cyber Security Maturity Model (CCSMM) is an essential reference source that discusses methods in applying sustainable cybersecurity programs and policies within organizations, governments, and other communities. Featuring research on topics such as community engagement, incident planning methods, and information sharing, this book is ideally designed for cybersecurity professionals, security analysts, managers, researchers, policymakers, students, practitioners, and academicians seeking coverage on novel policies and programs in cybersecurity implementation.

Traditional marketing techniques have become outdated by the emergence of the internet, and for companies to survive in the new technological marketplace, they must adopt digital marketing and business analytics practices. Unfortunately, with the benefits of improved storage and flow of information comes the risk of cyber-attack. Business Analytics and Cyber Security Management in Organizations compiles innovative research from international professionals discussing the opportunities and challenges of the new era of online business. Outlining updated discourse for business analytics techniques, strategies for data storage, and encryption in emerging markets, this book is ideal for business professionals, practicing managers, and students of business.

Leaders from academia and industry offer guidance for professionals and general readers on ethical questions posed by modern technology.

An Introduction

Countering Cyber Attacks and Preserving the Integrity and Availability of Critical Systems

Cyberethics: Morality and Law in Cyberspace

Does the word "hacking" scare you? Do you know if your personal information was stolen from your account? Have you always wanted to learn how to protect your system from such attacks? Do you want to learn the secrets of ethical hackers? If you answered yes to all these questions, you've come to the right place. Generally, hacking has earned a negative reputation and has become associated with cyberattacks and breaches in cybersecurity. But this is not always true. If this is your first book on hacking, you will become more acquainted with the world of hacking as this book gives a simple overview of ethical hacking. The term "ethical hacker" emerged in the late 1970s when the US government hired expert groups called "red teams" to hack their own computer system. Hackers are cyber-experts who lawfully or illegally hack. You enter the security system of a computer network to retrieve or recollect information. This book will talk about: What is ethical hacking Who should i protect my business from? Skills every hacker needs Different types of hacking over the years Hacking risks for businesses Protecting businesses from cybercrime Protecting your family from cyber attacks Secret social media hacks you want to try now ..and much, much more! This book bundle is perfect for beginners, a comprehensive guide that will show you the easy way to overcoming cybersecurity, computer hacking, wireless network and penetration testing. So if you want to learn more about Cybersecurity and Ethical Hacking, scroll up and click "add to cart"!

Cyber warfare has become more pervasive and more complex in recent years. It is difficult to regulate, as it holds an ambiguous position within the laws of war. This book investigates the legal and ethical ramifications of cyber war, considering which sets of laws apply to it, and how it fits into traditional ideas of armed conflict.

Following an opening section that defines cyberethics, this anthology of 26 essays explores anonymity, personal identity, and the moral dimensions of creating new personalities; privacy; ownership of intellectual property and copyright law; and the impact of computers on democracy and community. Annotation copyrighted by Book News, Inc., Portland, OR

"This book examines the concept of ethics in the digital environment through the framework of digitalization"--

Revised and updated to reflect new technologies in the field, the fourth edition of this popular text takes an in-depth look at the social costs and moral problems that have emerged by the ever expanding use of the Internet, and offers up-to-date legal and philosophical examinations of these issues. It focuses heavily on content control, free speech, intellectual property, and security while delving into new areas of blogging and social networking. Case studies throughout discuss real-world events and include coverage of numerous hot topics. In the process of exploring current issues, it identifies legal disputes that will likely set the standard for future cases.Instructor Resouces:-PowerPoint Lecture Outlines

The shortcomings of modern cryptography and its weaknesses against computers that are becoming more powerful necessitate serious consideration of more robust security options. Quantum cryptography is sound, and its practical implementations are becoming more mature. Many applications can use quantum cryptography as a backbone, including key distribution, secure direct communications, large prime factorization, e-commerce, e-governance, quantum internet, and more. For this reason, quantum cryptography is gaining interest and importance among computer and security professionals. Quantum Cryptography and the Future of Cyber Security is an essential scholarly resource that provides the latest research and advancements in cryptography and cyber security through quantum applications. Highlighting a wide range of topics such as e-commerce, machine learning, and privacy, this book is ideal for security analysts, systems engineers, software security engineers, data scientists, vulnerability analysts, professionals, academicians, researchers, security professionals, policymakers, and students.

In today?s globalized world, businesses and governments rely heavily on technology for storing and protecting essential information and data. Despite the benefits that computing systems offer, there remains an assortment of issues and challenges in maintaining the integrity and confidentiality of these databases. As professionals become more dependent cyberspace, there is a need for research on modern strategies and concepts for improving the security and safety of these technologies. Modern Theories and Practices for Cyber Ethics and Security Compliance is a collection of innovative research on the concepts, models, issues,

challenges, innovations, and mitigation strategies needed to improve cyber protection. While highlighting topics including database governance, cryptography, and intrusion detection, this book provides guidelines for the protection, safety, and security of business data and national infrastructure from cyber-attacks. It is ideally designed for security analysts, law enforcement, researchers, legal practitioners, policymakers, business professionals, governments, strategists, educators, and students seeking current research on combative solutions for cyber threats and attacks.

The arrival of the information age and the expansion of digital revolution from the 1990s brought an entirely unique set of crimes and criminality in the modern world--described as cybercrimes. One of the major policy concerns in almost all countries of the world today is the control and containment of cybercrimes. Cybercrimes challenge the very core of societal growth, security, and governance, and the growth and organization of almost all aspects of modern societies are centered on the use of computers and the internet. The criminal use of the computer and the internet can bring an unprecedented degree of harm and destruction, not just in the progress but also in the very continuity and survival of modern digital civilization. The new brave world of hyper connectivity is bringing a new age of social and cultural disorder, misinformation, confusion, and convulsions. Recent years have seen, in almost all countries of the world, the growth of new laws, regulations, and institutions to secure the internet and save the world from the destructions of cybercrime. In the emerging field of cybersecurity, there is now a compelling need to understand the global landscape of cybersecurity laws and regulations. Advancements in Global Cyber Security Laws and Regulations focuses on global cybersecurity laws and regulations in some of the major countries and regions including the United States, Europe, India, the Middle East, and the African and Pacific regions. Issues such as global regulations, global regimes, and global governance of the internet are covered alongside legal issues related to digital evidence, computer forensics, and cyber prosecution and convictions. This book is ideally intended for professionals, digital crime experts, security analysts, IT consultants, cybersecurity and cybercrime researchers, leaders, policymakers, government officials, practitioners, stakeholders, researchers, academicians, and students interested in how cybersecurity is legally defined and conceptualized and how cybercrimes are prosecuted and adjudicated in different countries and cultures.

Advancements in Global Cyber Security Laws and Regulations
Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities
Computer Network Security and Cyber Ethics, 4th ed.
Cyber Law and Ethics
NATO CCD COE Workshop on 'ethics and Policies for Cyber Warfare' (Magdalen College, Oxford)
Cybersecurity Policies and Strategies for Cyberwarfare Prevention
Law and Ethics for Virtual Conflicts
Regulation of the Connected World
The Quest for Responsible Security in the Age of Digital Warfare
Ethics, Legal, Risks, and Policies
Cybersecurity Breaches and Issues Surrounding Online Threat Protection

"This book is the first of its kind to introduce the integration of ethics, laws, risks, and policies in cyberspace. The book will advance understanding of the ethical and legal aspects of cyberspace followed by the risks involved along with current and proposed cyber policies. This book serves as a summary of the state of the art of cyber laws in the United States and considers more than 50 cyber laws. It also, importantly, incorporates various risk management and security strategies from a number of organizations. Using easy-to-understand language and incorporating case studies, the authors begin with the consideration of ethics and law in cybersecurity and then go on to take into account risks and security policies. The section on risk covers risk identification, risk analysis, risk assessment, risk management, and risk remediation. The very important and exquisite topic of cyber insurance is covered as well-its benefits, types, coverage, etc. The section on cybersecurity policy acquaints readers with the role of policies in cybersecurity and how they are being implemented by means of frameworks. The authors provide a policy overview followed by discussions of several popular cybersecurity frameworks, such as NIST, COBIT, PCI/DSS, ISO series, etc. Each chapter is followed by an overall summary and review that highlights the key points as well as questions for readers to evaluate their understanding based on the chapter content. Cybersecurity: Ethics, Legal, Risks, and Policies is a valuable resource for a large audience that includes instructors, students, professionals in specific fields as well anyone and everyone who is an essential constituent of cyberspace. With increasing cybercriminal activities, it is more important than ever to know the laws and how to secure data and devices"--

Ethical values in computing are essential for understanding and maintaining the relationship between computing professionals and researchers and the users of their applications and programs. While concerns about cyber ethics and cyber law are constantly changing as technology changes, the intersections of cyber ethics and cyber law are still underexplored. Investigating Cyber Law and Cyber Ethics: Issues, Impacts and Practices discusses the impact of cyber ethics and cyber law on information technologies and society. Featuring current research, theoretical frameworks, and case studies, the book will highlight the ethical and legal practices used in computing technologies, increase the effectiveness of computing students and professionals in applying ethical values and legal statues, and provide insight on ethical and legal discussions of real-world applications.

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.

Offers a practical guide on cyber ethics that can help students become safe, smart cyber citizens.

This new textbook offers an accessible introduction to the topic of cybersecurity ethics. The book is split into three parts. Part I provides an introduction to the field of ethics, philosophy and philosophy of science, three ethical frameworks – virtue ethics, utilitarian ethics and communitarian ethics – and the notion of ethical hacking. Part II applies these frameworks to particular issues within the field of cybersecurity, including privacy rights, intellectual property and piracy, surveillance, and cyberethics in relation to military affairs. The third part concludes by exploring current codes of ethics used in cybersecurity. The overall aims of the book are to: provide ethical frameworks to aid decision making; present the key ethical issues in relation to computer security; highlight the connection between values and beliefs and the professional code of ethics. The textbook also includes three different features to aid students: 'Going Deeper' provides background information on key individuals and concepts; 'Critical Issues' features contemporary case studies; and 'Applications' examine specific technologies or practices which raise ethical issues. The book will be of much interest to students of cybersecurity, cyberethics, hacking, surveillance studies, ethics and information science.

Technology has become deeply integrated into modern society and various activities throughout everyday life. However, this increases the risk of vulnerabilities, such as hacking or system errors, among other online threats. Cybersecurity Breaches and Issues Surrounding Online Threat Protection is an essential reference source for the latest scholarly research on the various types of unauthorized access or damage to electronic data. Featuring extensive coverage across a range of relevant perspectives and topics, such as robotics, cloud computing, and electronic data diffusion, this publication is ideally designed for academicians, researchers, computer engineers, graduate students, and practitioners seeking current research on the threats that exist in the world of technology.

This book is the first of its kind to introduce the integration of ethics, laws, risks, and policies in cyberspace. The book will advance understanding of the ethical and legal aspects of cyberspace followed by the risks involved along with current and proposed cyber policies. This book serves as a summary of the state of the art of cyber laws in the United States and considers more than 50 cyber laws. It also, importantly, incorporates various risk management and security strategies from a number of organizations. Using easy-to-understand language and incorporating case studies, the authors begin with the consideration of ethics and law in cybersecurity and then go on to take into account risks and security policies. The section on risk covers risk identification, risk analysis, risk assessment, risk management, and risk remediation. The very important and exquisite topic of cyber insurance is covered as well--its benefits, types, coverage, etc. The section on cybersecurity policy acquaints readers with the role of policies in cybersecurity and how they are being implemented by means of frameworks. The authors provide a policy overview followed by discussions of several popular cybersecurity frameworks, such as NIST, COBIT, PCI/DSS, ISO series, etc. Each chapter is followed by an overall summary and review that highlights the key points as well as questions for readers to evaluate their understanding based on the chapter content. Cybersecurity: Ethics, Legal, Risks, and Policies is a valuable resource for a large audience that includes instructors, students, professionals in specific fields as well anyone and everyone who is an essential constituent of cyberspace. With increasing cybercriminal activities, it is more important than ever to know the laws and how to secure data and devices.

Cyberspace is composed of a multitude of different spaces where users can represent themselves in many divergent ways. Why in a video game, is it more acceptable to murder or maim than rape? After all, in each case, it is only pixels that are being assaulted. This book avoids wrestling with the common question of whether the virtual violation of real-world taboos is right or wrong, and instead provides a theoretical framework that helps us understand why such distinctions are typically made, and explores the psychological impact of violating offline taboos within cyberspace. The authors discuss such online areas as: 'Reality' sites depicting taboo images Social networking websites and online chatrooms Online dating websites Video game content. This book considers whether there are some interactions that should not be permissible even virtually. It also examines how we might be able to cope with the potential moral freedoms afforded by cyberspace, and who might be vulnerable to such freedoms of action and representation within this virtual space. This book is ideal for researchers and students of internet psychology, philosophy and social policy, as well as therapists, those interested in computer science, law, media and communication studies

Cybersecurity
Business Analytics and Cyber Security Management in Organizations
A Moral and Psychological Examination of Cyberspace
Investigating Cyber Law and Cyber Ethics: Issues, Impacts and Practices
Cyber Attacks and International Law on the Use of Force
Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications
Cyber Ethics
Establishing Cyber Security Programs Through the Community Cyber Security Maturity Model (CCSMM)
Cybersecurity Ethics
Cyber Security Practitioner's Guide
Psychological and Behavioral Examinations in Cyber Security

As the advancement of technology continues, cyber security continues to play a significant role in today□s world. With society becoming more dependent on the internet, new opportunities for virtual attacks can lead to the exposure of critical information. Machine and deep learning techniques to prevent this exposure of information are being applied to address mounting concerns in computer security. The Handbook of Research on Machine and Deep Learning Applications for Cyber Security is a pivotal reference source that provides vital research on the application of machine learning techniques for network security research. While highlighting topics such as web security, malware detection, and secure information sharing, this publication explores recent research findings in the area of electronic security as well as challenges and countermeasures in cyber security research. It is ideally designed for software engineers, IT specialists, cybersecurity analysts, industrial experts, academicians, researchers, and post-graduate students.

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.

This book presents 12 essays that focus on the analysis of the problems prompted by cyber operations (COs). It clarifies and discusses the ethical and regulatory problems raised by the deployment of cyber capabilities by a state's army to inflict disruption or damage to an adversary's targets in or through cyberspace. Written by world-leading philosophers, ethicists, policy-makers, and law and military experts, the essays cover such topics as the conceptual novelty of COs and the ethical problems that this engenders; the applicability of existing conceptual and regulatory frameworks to COs deployed in case of conflicts; the definition of deterrence strategies involving COs; and the analysis of models to foster cooperation in managing cyber crises. Each essay is an invited contribution or a revised version of a paper originally presented at the workshop on Ethics and Policies for Cyber Warfare, organized by the NATO Cooperative Cyber Defence Centre of Excellence in collaboration with the University of Oxford. The volume endorses a multi-disciplinary approach, as such it offers a comprehensive overview of the ethical, legal, and policy problems posed by COs and of the different approaches and methods that can be used to solve them. It will appeal to a wide readership, including ethicists, philosophers, military experts, strategy planners, and law- and policy-makers.

"This edited book serves as a guide for certification training, the study of countermeasures to prevent and stop cybercrimes, cyberterrorism, cybertheft, identity theft and computer related crimes"--

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.

Explores the ethical issues of cyberpsychology research and praxes, which arise in algorithmically paired people and technologies. 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.

Through the rise of big data and the internet of things, terrorist organizations have been freed from geographic and logistical confines and now have more power than ever before to strike the average citizen directly at home. This, coupled with the inherently asymmetrical nature of cyberwarfare, which grants great advantage to the attacker, has created an unprecedented national security risk that both governments and their citizens are woefully ill-prepared to face. Examining cyber warfare and terrorism through a critical and academic perspective can lead to a better understanding of its foundations and implications. Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications is an essential reference for the latest research on the utilization of online tools by terrorist organizations to communicate with and recruit potential extremists and examines effective countermeasures employed by law enforcement agencies to defend against such threats. Highlighting a range of topics such as cyber threats, digital intelligence, and counterterrorism, this multi-volume book is ideally designed for law enforcement, government officials, lawmakers, security analysts, IT specialists, software developers, intelligence and security practitioners, students, educators, and researchers.

Engineering a Better Society
Issues, Impacts and Practices
A NATO Cooperative Cyber Defence Centre of Excellence Initiative
Information Security and Ethics: Concepts, Methodologies, Tools, and Applications
Ethical Hacking Techniques and Countermeasures for Cybercrime Prevention
Cyberethics
Multidisciplinary Approaches to Ethics in the Digital Era
Ethical Hacking and Cybersecurity
Emerging Trends in Cyber Ethics and Education
Transcending Taboos
Ethics and Policies for Cyber Operations

The United States is increasingly dependent on information and information technology for both civilian and military purposes, as are many other nations. Although there is a substantial literature on the potential impact of a cyberattack on the societal infrastructure of the United States, little has been written about the use of cyberattack as an instrument of U.S. policy. Cyberattacks--actions intended to damage adversary computer systems or networks--can be used for a variety of military purposes. But they also have application to certain missions of the intelligence community, such as covert action. They may be useful for certain domestic law enforcement purposes, and some analysts believe that they might be useful for certain private sector entities who are themselves under cyberattack. This report considers all of these applications from an integrated perspective that ties together technology, policy, legal, and ethical issues. Focusing on the use of cyberattack as an instrument of U.S. national policy, Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities explores important characteristics of cyberattack. It describes the current international and domestic legal structure as it might apply to cyberattack, and considers analogies to other domains of conflict to develop relevant insights. Of special interest to the military, intelligence, law enforcement, and homeland security communities, this report is also an essential point of departure for nongovernmental researchers interested in this rarely discussed topic.

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.

A primer on legal issues relating to cyberspace, this textbook introduces business, policy and ethical considerations raised by our use of information technology. With a focus on the most significant issues impacting internet users and businesses in the United States of America, the book provides coverage of key topics such as social media, online privacy, artificial intelligence and cybercrime as well as emerging themes such as doxing, ransomware, revenge porn, data-mining, e-sports and fake news. The

authors, experienced in journalism, technology and legal practice, provide readers with expert insights into the nuts and bolts of cyber law. Cyber Law and Ethics: Regulation of the Connected World provides a practical presentation of legal principles, and is essential reading for non-specialist students dealing with the intersection of the internet and the law.

In an era of unprecedented volatile political and economic environments across the world, computer-based cyber security systems face ever growing challenges. While the internet has created a global platform for the exchange of ideas, goods and services, it has also created boundless opportunities for cyber crime. The debate over how to plan for the cyber security of the future has focused the minds of developers and scientists alike. This book aims to provide a reference on current and emerging issues on systems security from the lens of autonomy, artificial intelligence and ethics as the race to fight and prevent cyber crime becomes increasingly pressing.

Communications Principles and Policies of the Internet
Cyber Security and the Politics of Time
Handbook of Research on Machine and Deep Learning Applications for Cyber Security
Report
Social & Moral Issues in the Computer Age
The Ethics of Cybersecurity
Quantum Cryptography and the Future of Cyber Security
The Turn to Information Ethics