Cyber Attacks And The Exploitable Imperfections Of International Law

"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.

This book explores how best to recalibrate our understanding of international lawmaking through the lens of increased reporting and legal debate around covert and quasi-covert uses of force. Recent changes in practice and communication call for closer attention to be paid to the requirement of publicity for state practice, since they challenge the perception of the concepts 'public' and 'covert', and thus raise questions as to the impact that covert and quasi-covert acts do and should have on the development of international law. It is argued that, in order to qualify as such practice, acts must be both publicly known and acknowledged. The book further examines how state silence around covert and quasi-covert operations has opened up significant space for legal scholars and other experts to influence the development of international law.

An accessible introduction to cybersecurity concepts and practices Cybersecurity Essentials provides a comprehensive introduction to the field, with expert coverage of essential topics required for entry-level cybersecurity certifications. An effective defense consists of four distinct challenges: securing the infrastructure, securing devices, securing local networks, and securing the perimeter. Overcoming these challenges requires a detailed understanding of the concepts and practices within each realm. This book covers each challenge individually for greater depth of information, with real-world scenarios that show what vulnerabilities look like in everyday computing scenarios. Each part concludes with a summary of key concepts, review questions, and hands-on exercises, allowing you to test your understanding while exercising your new critical skills. Cybersecurity jobs range from basic configuration to advanced systems analysis and defense assessment. This book provides the foundational information you need to understand the basics of the field, identify your place within it, and start down the security certification path. Learn security and surveillance fundamentals Secure and protect remote access and devices Understand network topologies, protocols, and strategies Identify threats and mount an effective defense Cybersecurity Essentials gives you the building blocks for an entry level security certification and provides a foundation of cybersecurity knowledge

Cyber-crime increasingly impacts both the online and offline world, and targeted attacks play a significant role in disrupting services in both. Targeted attacks are those that are aimed at a particular individual, group, or type of site or service. Unlike worms and viruses that usually attack indiscriminately, targeted attacks involve intelligence-gathering and planning to a degree that drastically changes its profile. Individuals, corporations, and even governments are facing new threats from targeted attacks. Targeted Cyber Attacks examines real-world examples of directed attacks and provides insight into what techniques and resources are used to stage these attacks so that you can counter them more effectively. A well-structured introduction into the world of

targeted cyber-attacks Includes analysis of real-world attacks Written by cyber-security researchers and experts

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

Cyber-Attacks and the Exploitable Imperfections of International LawBRILL

Move beyond the foundations of machine learning and game theory in cyber security to the latest research in this cutting-edge field In Game Theory and Machine Learning for Cyber Security, a team of expert security researchers delivers a collection of central research contributions from both machine learning and game theory applicable to cybersecurity. The distinguished editors have included resources that address open research questions in game theory and machine learning applied to cyber security systems and examine the strengths and limitations of current game theoretic models for cyber security. Readers will explore the vulnerabilities of traditional machine learning algorithms and how they can be mitigated in an adversarial machine learning approach. The book offers a comprehensive suite of solutions to a broad range of technical issues in applying game theory and machine learning to solve cyber security challenges. Beginning with an introduction to foundational concepts in game theory, machine learning, cyber security, and cyber deception, the editors provide readers with resources that discuss the latest in hypergames, behavioral game theory, adversarial machine learning, generative adversarial networks, and multi-agent reinforcement learning. Readers will also enjoy: A thorough introduction to game theory for cyber deception, including scalable algorithms for identifying stealthy attackers in a game theoretic framework, honeypot allocation over attack graphs, and behavioral games for cyber deception An exploration of game theory for cyber security, including actionable game-theoretic adversarial intervention detection against persistent and advanced threats Practical discussions of adversarial machine learning for cyber security, including adversarial machine learning in 5G security and machine learning-driven fault injection in cyber-physical systems In-depth examinations of generative models for cyber security Perfect for researchers, students, and experts in the fields of computer science and engineering, Game Theory and Machine Learning for Cyber Security is also an indispensable resource for industry professionals, military personnel, researchers, faculty, and students with an interest in cyber security.

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

This definitive reference resource on cyber warfare covers all aspects of this headline topic, providing historical context of cyber warfare and an examination its rapid development into a potent technological weapon of the 21st century. • Provides comprehensive coverage of the major individuals, organizations, impacts, and issues related to cyber warfare that enables readers to better understanding of the impact of cyber warfare on modern conflicts • Includes a detailed chronology that documents the evolution and use of cyber warfare over

the past few decades • Supplies further readings and a lengthy bibliography that offer a wealth of options to students conducting extensive research on the subject

The increased use of technology is necessary in order for industrial control systems to maintain and monitor industrial, infrastructural, or environmental processes. The need to secure and identify threats to the system is equally critical. Securing Critical Infrastructures and Critical Control Systems: Approaches for Threat Protection provides a full and detailed understanding of the vulnerabilities and security threats that exist within an industrial control system. This collection of research defines and analyzes the technical, procedural, and managerial responses to securing these systems.

Your one-stop guide to know digital extortion and it's prevention. Key Features A complete guide to how ransomware works Build a security mechanism to prevent digital extortion. A practical approach to knowing about, and responding to, ransomware. Book Description Ransomware has turned out to be the most aggressive malware and has affected numerous organizations in the recent past. The current need is to have a defensive mechanism in place for workstations and servers under one organization. This book starts by explaining the basics of malware, specifically ransomware. The book provides some quick tips on malware analysis and how you can identify different kinds of malware. We will also take a look at different types of ransomware, and how it reaches your system, spreads in your organization, and hijacks your computer. We will then move on to how the ransom is paid and the negative effects of doing so. You will learn how to respond quickly to ransomware attacks and how to protect yourself. The book gives a brief overview of the internals of security software and Windows features that can be helpful in ransomware prevention for administrators. You will also look at practical use cases in each stage of the ransomware phenomenon. The book talks in detail about the latest ransomware attacks involving WannaCry, Petya, and BadRabbit. By the end of this book, you will have end-to-end knowledge of the trending malware in the tech industry at present. What you will learn Understand malware types and malware techniques with examples Obtain a quick malware analysis Understand ransomware techniques, their distribution, and their payment mechanism Case studies of famous ransomware attacks Discover detection technologies for complex malware and ransomware Configure security software to protect against ransomware Handle ransomware infections Who this book is for This book is targeted towards security administrator, security analysts, or any stakeholders in the security sector who want to learn about the most trending malware in the current market: ransomware.

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.

The current IT environment deals with novel, complex approaches such as information privacy, trust, digital forensics, management, and human aspects. This volume includes papers offering research contributions that focus both on access control in complex environments as well as other aspects of computer security and privacy.

Follow step-by-step guidance to craft a successful security program. You will identify with the paradoxes of information security and discover handy tools that hook security controls into business processes. Information security is more than configuring firewalls, removing viruses, hacking machines, or setting passwords. Creating and promoting a successful security program requires skills in organizational consulting, diplomacy, change management, risk analysis, and out-of-the-box thinking. What You Will Learn: Build a security program that will fit neatly into an organization and change dynamically to suit both the needs of the organization and survive constantly changing threats Prepare for and pass such common audits as PCI-DSS, SSAE-16, and ISO 27001 Calibrate the scope, and customize security controls to fit into an organization’s culture Implement the most challenging processes, pointing out common pitfalls and distractions Frame security and risk issues to be clear and actionable so that decision makers, technical personnel, and users will listen and value your advice Who This Book Is For: IT professionals moving into the security field; new security managers, directors, project heads, and would-be CISOs; and security specialists from other disciplines moving into information security (e.g., former military security professionals, law enforcement professionals, and physical security professionals)

The SANS Institute maintains a list of the "Top 10 Software Vulnerabilities." At the current time, over half of these vulnerabilities are exploitable by Buffer Overflow attacks, making this class of attack one of the most common and most dangerous weapon used by malicious attackers. This is the first book specifically aimed at detecting, exploiting, and preventing the most common and dangerous attacks. Buffer overflows make up one of the largest collections of vulnerabilities in existence; And a large percentage of possible remote exploits are of the overflow variety. Almost all of the most devastating computer attacks to hit the Internet in recent years including SQL Slammer, Blaster, and I Love You attacks. If executed properly, an overflow vulnerability will allow an attacker to run arbitrary code on the victim’s machine with the equivalent rights of whichever process was overflowed. This is often used to provide a remote shell onto the victim machine, which can be used for further exploitation. A buffer overflow is an unexpected behavior that exists in certain programming languages. This book provides specific, real code examples on exploiting buffer overflow attacks from a hacker's perspective and defending against these attacks for the software

developer. Over half of the "SANS TOP 10 Software Vulnerabilities" are related to buffer overflows. None of the current-best selling software security books focus exclusively on buffer overflows. This book provides specific, real code examples on exploiting buffer overflow attacks from a hacker's perspective and defending against these attacks for the software developer.

NASA relies on a series of computer networks to carry out its various missions, including controlling spacecraft like the International Space Station and conducting science missions like the Hubble Telescope. Therefore, it is imperative that NASA protect its computer networks from cyber attacks that could disrupt operations or result in the loss of sensitive data. In this audit, we evaluated whether NASA protected information technology (IT) assets on its Agency-wide mission computer network from Internet-based cyber attacks. Specifically, we assessed whether NASA adequately protected these IT assets from Internet-based attacks by regularly assessing risks and identifying and mitigating vulnerabilities. We also reviewed internal controls as appropriate. Details of the audit's scope and methodology are in Appendix A. We found that computer servers on NASA's Agency-wide mission network had high-risk vulnerabilities that were exploitable from the Internet. Specifically, six computer servers associated with IT assets that control spacecraft and contain critical data had vulnerabilities that would allow a remote attacker to take control of or render them unavailable. Moreover, once inside the Agency-wide mission network, the attacker could use the compromised computers to exploit other weaknesses we identified, a situation that could severely degrade or cripple NASA's operations. We also found network servers that revealed encryption keys, encrypted passwords, and user account information to potential attackers. These data are sensitive and provide attackers additional ways to gain unauthorized access to NASA networks. These deficiencies occurred because NASA had not fully assessed and mitigated risks to its Agency-wide mission network and was slow to assign responsibility for IT security oversight to ensure the network was adequately protected. In a May 2010 audit report, we recommended that NASA immediately establish an IT security oversight program for this key network.1 However, even though the Agency concurred with the recommendation it remained unimplemented as of February 2011. Until NASA addresses these critical deficiencies and improves its IT security practices, the Agency is vulnerable to computer incidents that could have a severe to catastrophic effect on Agency assets, operations, and personnel. In order to strengthen the Agency's IT security program, we urge NASA to expedite implementation of our May 2010 recommendation to establish an IT security oversight program for NASA's Agency-wide mission network. We also recommend that NASA Mission Directorates (1) immediately identify Internet-accessible computers on their mission networks and take prompt action to mitigate identified risks and (2) continuously monitor Agency mission networks for Internet-accessible computers and take prompt action to mitigate identified risks. Finally, to help ensure that all

threats and vulnerabilities to NASA's IT assets are identified and promptly addressed, we recommend that NASA's Chief Information Officer, in conjunction with the Mission Directorates, conduct an Agency-wide IT security risk assessment. In response to a draft of this report, the Chief Information Officer and Mission Directorates concurred with our recommendations. The Chief Information Officer stated that she will work with the Mission Directorates and Centers to develop a comprehensive approach to ensure that Internet-accessible computers on NASA's mission networks are routinely identified, vulnerabilities are continually evaluated, and risks are promptly mitigated by September 30, 2011. In addition, the Chief Information Officer said she will develop and implement a strategy for conducting an Agency-wide risk assessment by August 31, 2011. The full text of NASA's comments can be found in Appendix B. We consider the Chief Information Officer's proposed actions to be responsive to our recommendations.

This textbook is for courses in cyber security education that follow National Initiative for Cybersecurity Education (NICE) KSAs work roles and framework, that adopt the Competency-Based Education (CBE) method. The book follows the CBT (KSA) general framework, meaning each chapter contains three sections, knowledge and questions, and skills/labs for Skills and Abilities. The author makes an explicit balance between knowledge and skills material in information security, giving readers immediate applicable skills. The book is divided into seven parts: Securely Provision; Operate and Maintain; Oversee and Govern; Protect and Defend; Analysis; Operate and Collect; Investigate. All classroom materials (in the book an ancillary) adhere to the NICE framework. Mirrors classes set up by the National Initiative for Cybersecurity Education (NICE) Adopts the Competency-Based Education (CBE) method of teaching, used by universities, corporations, and in government training Includes content and ancillaries that provide skill-based instruction on compliance laws, information security standards, risk response and recovery, and more

A cyber-attack not like all others, it seemed to be the first of its kind, it literarily broke the internet for a day, the 21 October 2016 was the day a sophisticated Distributed Denial Of Service (DDoS) Cyber-Attack crippled the services of a Domain Name Service (DNS) Provider offering services to some 25% of the Internet, and yes of the whole world wide web (WWW), this book reveals some of the behind-the-scene considerations, and shows the challenges of information security in giant organizations, an Advanced Persistent Attack (APT) of this kind offers a unique overview of the cybersecurity unseen and unexpected exploitable Threats but they almost always start from the human factor and end by it. Have a good read.

Internet of Things (IoT) is an ecosystem comprised of heterogeneous connected devices that communicate to deliver capabilities making our living, cities, transport, energy, and other areas more intelligent. This book delves into the different cyber-security domains and their challenges due to the massive amount and the heterogeneity of devices. This book introduces readers to the inherent concepts of IoT. It offers case studies showing how IoT counteracts the cyber-security concerns for domains. It provides suggestions on how to mitigate cyber threats by compiling a catalogue of threats that currently comprise the contemporary threat landscape. It then examines different security measures that can be applied to system installations or operational environment and discusses how these measures may alter the threat exploitability level and/or the level of the technical impact. Professionals, graduate students, researchers, academicians, and institutions that are interested in acquiring knowledge in the areas of IoT and cyber-security, will find this book of interest.

This textbook presents a proven, mature Model-Based Systems Engineering (MBSE)

methodology that has delivered success in a wide range of system and enterprise programs. The authors introduce MBSE as the state of the practice in the vital Systems Engineering discipline that manages complexity and integrates technologies and design approaches to achieve effective, affordable, and balanced system solutions to the needs of a customer organization and its personnel. The book begins with a summary of the background and nature of MBSE. It summarizes the theory behind Object-Oriented Design applied to complex system architectures. It then walks through the phases of the MBSE methodology, using system examples to illustrate key points. Subsequent chapters broaden the application of MBSE in Service-Oriented Architectures (SOA), real-time systems, cybersecurity, networked enterprises, system simulations, and prototyping. The vital subject of system and architecture governance completes the discussion. The book features exercises at the end of each chapter intended to help readers/students focus on key points, as well as extensive appendices that furnish additional detail in particular areas. The self-contained text is ideal for students in a range of courses in systems architecture and MBSE as well as for practitioners seeking a highly practical presentation of MBSE principles and techniques.

With our ever-increasing reliance on computer technology in every field of modern life, the need for continuously evolving and improving cyber security remains a constant imperative. This book presents the 3 keynote speeches and 10 papers delivered at the 2nd Singapore Cyber Security R&D Conference (SG-CRC 2017), held in Singapore, on 21-22 February 2017. SG-CRC 2017 focuses on the latest research into the techniques and methodologies of cyber security. The goal is to construct systems which are resistant to cyber-attack, enabling the construction of safe execution environments and improving the security of both hardware and software by means of mathematical tools and engineering approaches for the design, verification and monitoring of cyber-physical systems. Covering subjects which range from messaging in the public cloud and the use of scholarly digital libraries as a platform for malware distribution, to low-dimensional bigram analysis for mobile data fragment classification, this book will be of interest to all those whose business it is to improve cyber security.

A June 2014 PriceWaterHouseCoopers survey found that 69% of U.S. business leaders worried that cyber threats would harm their company's growth. As corporate information networks become increasingly interconnected with third-party vendors, suppliers, business partners, and customers, the threat of exploitable vulnerabilities expands. Recent cyber attacks against Anthem and Sony Pictures, as well as the theft of up to $1 billion dollars from European banks, illustrate the devastating damage cyber attacks can cause. Cybersecurity has moved to the forefront of the national debate among leaders in the business community, national security experts, and privacy advocates. President Obama has signed an executive order addressing information-sharing about online threats. In addition, House and Senate Committees have begun to hold hearings on cybersecurity issues and draft legislation addressing cyber threat information-sharing and data breach notification. Cyberattacks continue to cost the economy roughly $100 billion a year. Corporations collect and utilize a lot of personal information about their customers and employees. It is imperative that those businesses employ more effective means to safeguard it.

Computers at Risk presents a comprehensive agenda for developing nationwide policies and practices for computer security. Specific recommendations are provided for industry and for government agencies engaged in computer security activities. The volume also outlines problems and opportunities in computer security research, recommends ways to improve the research infrastructure, and suggests topics for investigators. The book explores the diversity of the field, the need to engineer countermeasures based on speculation of what experts think computer attackers may do next, why the technology community has failed to respond to the need for enhanced security systems, how innovators could be encouraged to bring more

options to the marketplace, and balancing the importance of security against the right of privacy.

There are hundreds--if not thousands--of techniques used to compromise both Windows and Unix-based systems. Malicious code and new exploit scripts are released on a daily basis, and each evolution becomes more and more sophisticated. Keeping up with the myriad of systems used by hackers in the wild is a formidable task, and scrambling to patch each potential vulnerability or address each new attack one-by-one is a bit like emptying the Atlantic with paper cup.If you're a network administrator, the pressure is on you to defend your systems from attack. But short of devoting your life to becoming a security expert, what can you do to ensure the safety of your mission critical systems? Where do you start?Using the steps laid out by professional security analysts and consultants to identify and assess risks, Network Security Assessment offers an efficient testing model that an administrator can adopt, refine, and reuse to create proactive defensive strategies to protect their systems from the threats that are out there, as well as those still being developed.This thorough and insightful guide covers offensive technologies by grouping and analyzing them at a higher level--from both an offensive and defensive standpoint--helping administrators design and deploy networks that are immune to offensive exploits, tools, and scripts. Network administrators who need to develop and implement a security assessment program will find everything they're looking for--a proven, expert-tested methodology on which to base their own comprehensive program--in this time-saving new book.

This report provides strategic advice on preparing for and responding to potential global shocks.

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.

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.

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

Zero-day vulnerabilities--software vulnerabilities for which no patch or fix has been publicly released-- and their exploits are useful in cyber operations--whether by criminals, militaries, or governments--as well as in defensive and academic settings. This report provides findings from real-world zero-day vulnerability and exploit data that could augment conventional proxy examples and expert opinion, complement current efforts to create a framework for deciding whether to disclose or retain a cache of zero-day vulnerabilities and exploits, inform ongoing policy debates regarding stockpiling and vulnerability disclosure, and add extra context for those examining the implications and resulting liability of attacks and data breaches for U.S. consumers, companies, insurers, and for the civil justice system broadly. The authors provide insights about the zero-day vulnerability research and exploit development industry; give information on what

proportion of zero-day vulnerabilities are alive (undisclosed), dead (known), or somewhere in between; and establish some baseline metrics regarding the average lifespan of zero-day vulnerabilities, the likelihood of another party discovering a vulnerability within a given time period, and the time and costs involved in developing an exploit for a zero-day vulnerability"--Publisher's description.

Ten Strategies of a World-Class Cyber Security Operations Center conveys MITRE's accumulated expertise on enterprise-grade computer network defense. It covers ten key qualities of leading Cyber Security Operations Centers (CSOCs), ranging from their structure and organization, to processes that best enable smooth operations, to approaches that extract maximum value from key CSOC technology investments. This book offers perspective and context for key decision points in structuring a CSOC, such as what capabilities to offer, how to architect large-scale data collection and analysis, and how to prepare the CSOC team for agile, threat-based response. If you manage, work in, or are standing up a CSOC, this book is for you. It is also available on MITRE's website, www.mitre.org.

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.

Cyber Attacks, Student Edition, offers a technical, architectural, and management approach to solving the problems of protecting national infrastructure. This approach includes controversial themes such as the deliberate use of deception to trap intruders. This volume thus serves as an attractive framework for a new national strategy for cyber security. A specific set of criteria requirements allows any organization, such as a government agency, to integrate the principles into their local environment. In this edition, each principle is presented as a separate security strategy and illustrated with compelling examples. The book adds 50-75 pages of new material aimed specifically at enhancing the student experience and making it more attractive for instructors teaching courses such as cyber security, information security, digital security, national security, intelligence studies, technology and infrastructure protection. It now also features case

studies illustrating actual implementation scenarios of the principles and requirements discussed in the text, along with a host of new pedagogical elements, including chapter outlines, chapter summaries, learning checklists, and a 2-color interior. Furthermore, a new and complete ancillary package includes test bank, lesson plans, PowerPoint slides, case study questions, and more. This text is intended for security practitioners and military personnel as well as for students wishing to become security engineers, network operators, software designers, technology managers, application developers, etc. Provides case studies focusing on cyber security challenges and solutions to display how theory, research, and methods, apply to real-life challenges Utilizes, end-of-chapter case problems that take chapter content and relate it to real security situations and issues Includes instructor slides for each chapter as well as an instructor's manual with sample syllabi and test bank

This book offers a comprehensive analysis of the international law applicable to cyber operations, including a systematic examination of attribution, lawfulness and remedies. It demonstrates the importance of countermeasures as a form of remedies and also shows the limits of international law, highlighting its limits in resolving issues related to cyber operations. There are several situations in which international law leaves the victim State of cyber operations helpless. Two main streams of limits are identified. First, in the case of cyber operations conducted by non-state actors on the behalf of a State, new technologies offer various ways to coordinate cyber operations without a high level of organization. Second, the law of State responsibility offers a range of solutions to respond to cyber operations and seek reparation, but it does not provide an answer in every case and it cannot solve the problem related to technical capabilities of the victim.

Cyber-Attacks and the Exploitable Imperfections of International Law reveals elements of existing jus ad bellum and jus in bello regimes that are unable to accommodate the threats posed by cyber-attacks. It maps out legal gaps, deficiencies, and uncertainties, which international actors may seek to exploit to their political benefit.

A comprehensive analysis of the international law applicable to cyber operations, including a systematic study of attribution, lawfulness and remedies.

Enhance your organization's secure posture by improving your attack and defense strategies Key Features Gain a clear understanding of the attack methods, and patterns to recognize abnormal behavior within your organization with Blue Team tactics. Learn to unique techniques to gather exploitation intelligence, identify risk and demonstrate impact with Red Team and Blue Team strategies. A practical guide that will give you hands-on experience to mitigate risks and prevent attackers from infiltrating your system. Book Description The book will start talking about the security posture before moving to Red Team tactics, where you will learn the basic syntax for the Windows and Linux tools that are commonly used to perform the necessary operations. You will also gain hands-on experience of using new Red Team techniques with powerful tools such as python and PowerShell, which will enable you to discover vulnerabilities in your system and how to exploit them. Moving on, you will learn how a system is usually compromised by adversaries, and how they hack user's identity, and the various tools used by the Red Team to find vulnerabilities in a system. In the next section, you will learn about the defense strategies followed by the Blue Team to enhance the overall security of a system. You will also learn about an in-depth strategy to ensure that there are security controls in each network layer, and how you can carry out the recovery process of a compromised system. Finally, you will learn how to create a vulnerability management strategy and the different techniques for manual log analysis. By the end of this book, you will be well-versed with Red Team and Blue Team techniques and will have learned the techniques used nowadays to attack and defend systems. What you will learn Learn the importance of having a solid

foundation for your security posture Understand the attack strategy using cyber security kill chain Learn how to enhance your defense strategy by improving your security policies, hardening your network, implementing active sensors, and leveraging threat intelligence Learn how to perform an incident investigation Get an in-depth understanding of the recovery process Understand continuous security monitoring and how to implement a vulnerability management strategy Learn how to perform log analysis to identify suspicious activities Who this book is for This book aims at IT professional who want to venture the IT security domain. IT pentester, Security consultants, and ethical hackers will also find this course useful. Prior knowledge of penetration testing would be beneficial.

This must-have guide features simple explanations, examples and advice to help you be security-aware online in the digital age.

This reference work examines how sophisticated cyber-attacks and innovative use of social media have changed conflict in the digital realm, while new military technologies such as drones and robotic weaponry continue to have an impact on modern warfare. • Provides fascinating information about cyber weapons that effectively strike through cyberspace to weaken and even cripple its target • Demonstrates how social media is employed in conflicts in innovative ways, including communication, propaganda, and psychological warfare • Explores potential technology avenues related to ensuring the continued military advantages of the United States • Identifies and describes nuclear, precision, and other technological capabilities that have historically been the preserve of superpowers but have been newly acquired by various states

Penetration testers simulate cyber attacks to find security weaknesses in networks, operating systems, and applications. Information security experts worldwide use penetration techniques to evaluate enterprise defenses. In Penetration Testing, security expert, researcher, and trainer Georgia Weidman introduces you to the core skills and techniques that every pentester needs. Using a virtual machine–based lab that includes Kali Linux and vulnerable operating systems, you'll run through a series of practical lessons with tools like Wireshark, Nmap, and Burp Suite. As you follow along with the labs and launch attacks, you'll experience the key stages of an actual assessment—including information gathering, finding exploitable vulnerabilities, gaining access to systems, post exploitation, and more. Learn how to: –Crack passwords and wireless network keys with brute-forcing and wordlists –Test web applications for vulnerabilities –Use the Metasploit Framework to launch exploits and write your own Metasploit modules –Automate social-engineering attacks –Bypass antivirus software –Turn access to one machine into total control of the enterprise in the post exploitation phase You'll even explore writing your own exploits. Then it's on to mobile hacking—Weidman's particular area of research—with her tool, the Smartphone Pentest Framework. With its collection of hands-on lessons that cover key tools and strategies, Penetration Testing is the introduction that every aspiring hacker needs.