Cyber Attacks And The Exploitable Imperfections Of International Law

When somebody should go to the ebook stores, search introduction by shop, shelf by shelf, it is really problematic. This is why we offer the book compilations in this website. It will very ease you to look guide **Cyber Attacks And The Exploitable Imperfections Of International Law** as you such as.

By searching the title, publisher, or authors of guide you really want, you can discover them rapidly. In the house, workplace, or perhaps in your method can be every best area within net connections. If you intention to download and install the Cyber Attacks And The Exploitable Imperfections Of International Law, it is definitely easy then, before currently we extend the partner to purchase and make bargains to download and install Cyber Attacks And The Exploitable Imperfections Of International Law for that reason simple!

Cyber Attacks And The Exploitable Imperfections Of International Law *Downloaded from ftp.wagmtv.com by guest*

KYLEIGH BRAYDON

Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications CRC Press
Cyber Warfare, Second Edition, takes a comprehensive look at how and why digital warfare is waged. The book explores the participants, battlefields, and the tools and techniques used in today's digital conflicts. The concepts discussed gives students of information security a better idea of how cyber conflicts are carried out now, how they will change in the future, and how to detect and defend against espionage, hacktivism, insider threats and non-state actors such as organized criminals and terrorists. This book provides concrete examples and real-world guidance on how to identify and defend a network against malicious attacks. It probes relevant technical and factual information from an insider's point of view, as well as the ethics, laws and consequences of cyber war and how computer criminal law may change as a result. Logical, physical, and psychological weapons used in cyber warfare are discussed. This text will appeal to information security practitioners, network security administrators, computer system administrators, and security analysts. Provides concrete examples and real-world guidance on how to identify and defend your network against malicious attacks Dives deeply into relevant technical and factual information from an insider's point of view Details the ethics, laws and consequences of cyber war and how computer criminal law may change as a result
The Rise of Politically Motivated Cyber Attacks Syngress
This book outlines the complexity in understanding different forms of cyber attacks, the actors involved, and their motivations. It explores the key challenges in investigating and prosecuting politically motivated cyber attacks, the lack of consistency within regulatory frameworks, and the grey zone that this creates, for cybercriminals to operate within. Connecting diverse literatures on cyberwarfare, cyberterrorism, and cyberprotests, and categorising the different actors involved – state-sponsored/supported groups, hacktivists, online protestors – this book compares the means and methods used in attacks, the various attackers, and the current strategies employed by cybersecurity agencies. It examines the current legislative framework and proposes ways in which it could be reconstructed, moving beyond the traditional and fragmented definitions used to manage offline violence. This book is an important contribution to the study of cyber attacks within the areas of criminology, criminal justice, law, and policy. It is a compelling reading for all those engaged in cybercrime, cybersecurity, and digital forensics.
Cyber-Security and Threat Politics John Wiley & Sons
The complete guide to today’s hard-to-defend chained attacks: performing them and preventing them Nowadays, it’s rare for malicious hackers to rely on just one exploit or tool; instead, they use “chained” exploits that integrate multiple forms of attack to achieve their goals. Chained exploits are far more complex and far more difficult to defend. Few security or hacking books cover them well and most don’t cover them at all. Now there’s a book that brings together start-to-finish information about today’s most widespread chained exploits—both how to perform them and how to prevent them. Chained Exploits demonstrates this advanced hacking attack technique through detailed examples that reflect real-world attack strategies, use today’s most common attack tools, and focus on actual high-value targets, including credit card and healthcare data. Relentlessly thorough and realistic, this book covers the full spectrum of attack avenues, from wireless networks to physical access and social engineering. Writing for security, network, and other IT professionals, the authors take you through each attack, one step at a time, and then introduce today’s most effective countermeasures– both technical and human. Coverage includes: Constructing convincing new phishing attacks Discovering which sites other Web users are visiting Wreaking havoc on IT security via wireless networks Disrupting competitors’ Web sites Performing—and preventing—corporate espionage Destroying secure files Gaining access to private healthcare records Attacking the viewers of social networking pages Creating entirely new exploits and more Andrew Whitaker, Director of Enterprise InfoSec and Networking for Training Camp, has been featured in The Wall Street Journal and BusinessWeek. He coauthored Penetration Testing and Network Defense. Andrew was a winner of EC Council’s Instructor of Excellence Award. Keatron Evans is President and Chief Security Consultant of Blink Digital Security, LLC, a trainer for Training Camp, and winner of EC Council’s Instructor of Excellence Award. Jack B. Voth specializes in penetration testing, vulnerability assessment, and perimeter security. He co-owns The Client Server, Inc., and teaches for Training Camp throughout the United States and abroad. informit.com/aw Cover photograph © Corbis / Jupiter Images
Cybersecurity "O'Reilly Media, Inc."
The spectacular cyber attack on Sony Pictures and costly hacks of Target, Home Depot, Neiman Marcus, and databases containing sensitive data on millions of U.S. federal workers have shocked the nation. Despite a new urgency for the president, Congress, law enforcement, and corporate America to address the growing threat, the hacks keep coming—each one more pernicious than the last—from China, Russia, Iran, North Korea, the Middle East, and points unknown. The continuing attacks raise a deeply disturbing question: Is the issue simply beyond the reach of our government, political leaders, business leaders, and technology visionaries to resolve? In Hacked, veteran cybersecurity journalist Charlie Mitchell reveals the innovative, occasionally brilliant, and too-often hapless government and industry responses to growing cybersecurity threats. He examines the internal power struggles in the federal government, the paralysis on Capitol Hill, and the industry's desperate effort to stay ahead of both the bad guys and the government.
Cybersecurity Oxford University Press
Given the growing importance of cyberspace to nearly all aspects of national life, a secure cyberspace is vitally important to the nation, but cyberspace is far from secure today. The United States faces the real risk that adversaries will exploit vulnerabilities in the nation's critical information systems, thereby causing considerable suffering and damage. Online e-commerce business, government agency files, and identity records are all potential security targets. Toward a Safer and More Secure Cyberspace examines these Internet security vulnerabilities and offers a strategy for future research aimed at countering cyber attacks. It also explores the nature of online threats and some of the reasons why past research for improving cybersecurity has had less impact than anticipated, and considers the human resource base needed to advance the cybersecurity research agenda. This book will be an invaluable resource for Internet security professionals, information technologists, policy makers, data stewards, e-commerce providers, consumer protection advocates, and others interested in digital security and safety.
Cyberterrorism Createspace Independent Publishing Platform
"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.
Targeted Cyber Attacks epubli
Why do nations break into one another's most important computer networks? There is an obvious answer: to steal valuable information or to attack. But this isn't the full story. This book draws on often-overlooked documents leaked by Edward Snowden, real-world case studies of cyber operations, and policymaker perspectives to show that intruding into other countries' networks has enormous defensive value as well. Two nations, neither of which seeks to harm the other but neither of which trusts the other, will often find it prudent to launch intrusions. This general problem, in which a nation's means of securing itself threatens the security of others and risks escalating tension, is a bedrock concept in international relations and is called the 'security dilemma'. This book shows not only that the security dilemma applies to cyber operations, but also that the particular characteristics of the digital domain mean that the effects are deeply pronounced. The cybersecurity dilemma is both a vital concern of modern statecraft and a means of accessibly understanding the essential components of cyber operations.
The 2016 Dyn Ddos Cyber Attack Analysis IGI Global
Society is continually transforming into a digitally powered reality due to the increased dependence of computing technologies. The landscape of cyber threats is constantly evolving because of this, as hackers are finding improved methods of accessing essential data. Analyzing the historical evolution of cyberattacks can assist practitioners in predicting what future threats could be on the horizon. Real-Time and Retrospective Analyses of Cyber Security is a pivotal reference source that provides vital research on studying the development of cybersecurity practices through historical and sociological analyses. While highlighting topics such as zero trust networks, geopolitical analysis, and cyber warfare, this publication explores the evolution of cyber threats, as well as improving security methods and their socio-technological impact. This book is ideally designed for researchers, policymakers, strategists, officials, developers, educators, sociologists, and students seeking current research on the evolution of cybersecurity methods through historical analysis and future trends.
Network Attacks and Exploitation Elsevier
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
The Hacker and the State John Wiley & Sons
This book presents a holistic view of the geopolitics of cyberspace that have arisen over the past decade, utilizing recent events to explain the international security dimension of cyber threat and vulnerability, and to document the challenges of controlling information resources and protecting computer systems. How are the evolving cases of cyber attack and breach as well as the actions of government and corporations shaping how cyberspace is governed? What object lessons are there in security cases such as those involving Wikileaks and the Snowden affair? An essential read for practitioners, scholars, and students of international affairs and security, this book examines the widely pervasive and enormously effective nature of cyber threats today, explaining why cyber attacks happen, how they matter, and how they may be managed. The book addresses a chronology of events starting in 2005 to comprehensively explain the international security dimension of cyber threat and vulnerability. It begins with an explanation of contemporary information technology, including the economics of contemporary cloud, mobile, and control systems software as well as how computing and networking—principally the Internet—are interwoven in the concept of cyberspace. Author Chris Bronk, PhD, then documents the national struggles with controlling information resources and protecting computer systems. The book considers major security cases such as Wikileaks, Stuxnet, the cyber attack on Estonia, Shamoon, and the recent exploits of the Syrian Electronic Army. Readers will understand how cyber security in the 21st century is far more than a military or defense issue, but is a critical matter of international law, diplomacy, commerce, and civil society as well.
Strategic Cyber Deterrence Bloomsbury Publishing USA

Corporations, governments, private people, healthcare, and educational institutions are all vulnerable to cyberattacks. Hacking may compromise networks and computer systems, resulting in reputational harm and service outages. The situation is much worse for health-care institutions, since such assaults have the potential to disrupt service delivery, making it harder to write medical prescriptions and begin treatment. These interruptions are harmful to patients' health and well-being, and they may result in death or worse of their diseases. The health of a patient might be jeopardized if information is leaked, particularly if the patient has a prominent position in society. As a consequence of the COVID-19 epidemic, there has been an increase in cyberattacks. These assaults are linked to people's limited time, causing them to spend more time online. Disruption in educational programs has resulted in a dramatic adoption of remote learning without proper precautions to protect against hackers, as is typical. Malware, phishing, and ransomware are examples of typical cyberattacks. Theft of personal information might drive people and businesses to pay a ransom to prevent information being disclosed to the internet. Injection of malware into the system might lead to data theft and compromised information. Network users opening attachments and links without verifying their origins might be the cause of phishing attempts. During phishing operations, cybercriminals often exploit emails from reputable companies. Because of the lack of security mechanisms, the majority of cyberattacks are elegant. Companies continue to use out-of-date software and have no network security safeguards in place. Employees and network users lack internet and network user skills and competences, resulting in the compromise of personal information and financial losses. Critical infrastructure systems, such as power grids and water systems, are vulnerable to cyberattacks. The creation of a cybersecurity framework, as well as cybersecurity awareness training and education, should be among the preventive measures. Machine learning and artificial intelligence are two cybersecurity technologies that might help prevent assaults on computer systems and networks. Financial losses, service disruptions, reputational harm, and damaged key infrastructures might all be reduced as a result of cyberattacks if the strategy is implemented.

Real-Time and Retrospective Analyses of Cyber Security Pearson Education

This work develops perspectives and approaches to crucial cyber-security issues that are non-political, non-partisan, and non-governmental. It informs readers through high-level summaries and the presentation of a consistent approach to several cyber-risk related domains, both from a civilian and a military perspective. It explains fundamental principles in an interdisciplinary manner, thus shedding light on the societal, economic, political, military, and technical issues related to the use and misuse of information and communication technologies.

Cyber Attacks Harvard University Press

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.

Cyberwarfare: An Introduction to Information-Age Conflict IGI Global

About The Book - Cybersecurity is a fast-moving game. If you do not learn to play it well, you may have to pay the price. “The stories of the biggest, most sophisticated and the extremely bizarre cyber-attacks the world has seen are all a part of this fascinating book. It dwells on those attacks that are out of the ordinary, unusual and where hackers have used tactics that could even be thought of as inconceivable.”—Arjun Malhotra, Co-founder of HCL “Cyber Shock captures intricate details of high impact cyberattacks that brought organizations across sectors to the brink, threatening their very existence and survival. Drawing on his extensive experience in various business roles, including as a former CEO and Board member, the author provides a comprehensive, 360-degree perspective on the multifaceted complex challenges and responses arising from cyberattacks.”—Abhay Havaldar, Founder and Managing Partner of Avatar Growth Capital and ex-MD of General Atlantic “A well-researched book for anyone trying to understand the dangers lurking in the cyberworld. Cyber Shock breaks down the elements of a cyberattack and highlights ways in which threat actors develop their strategy and tactics based on their motives and how they look to exploit security weaknesses to launch a variety of cyberattacks using a wide array of techniques and deception.” —D. Sivanandhan, IPS (Retd), former Mumbai, Police Commissioner and Director General of Police About The Author - Ajay Singh has spent over 35 years in the IT industry in different roles and was the CEO of an award winning fintech company for over a decade. He is a Fellow of the Institute of Directors and has authored multiple books on cybersecurity. He is a visiting professor at leading B-schools and serves on the Academic Advisory Board at Pace University's Seidenberg School of Computer Science and Information Systems, New York.

Hack Attack Protecting Yourself in the Age of Cybercrime Rowman & Littlefield

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.

Cybersecurity Threats with New Perspectives Academic Conferences and publishing limited

"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.

Cyber Shock: Cyberattacks that Shook the World Artech House

At its current rate, technological development has outpaced corresponding changes in international law. Proposals to remedy this deficiency have been made, in part, by members of the Shanghai Cooperation Organization (led by the Russian Federation), but the United States and select allies have rejected these proposals, arguing that existing international law already provides a suitable comprehensive framework necessary to tackle cyber-warfare. Cyber-Attacks and the Exploitable Imperfections of International Law does not contest (and, in fact, supports) the idea that contemporary jus ad bellum and jus in bello, in general, can accommodate cyber-warfare. However, this analysis argues that existing international law contains significant imperfections that can be exploited; gaps, not yet filled, that fail to address future risks posed by cyber-attacks.

Cyber Warfare and Cyber Terrorism CRC Press

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

Collaborative Cyber Threat Intelligence Rowman & Littlefield

Inside Cyber Warfare provides fascinating and disturbing details on how nations, groups, and individuals throughout the world use the Internet as an attack platform to gain military, political, and economic advantages over their adversaries. 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. The second edition goes beyond the headlines of attention-grabbing DDoS attacks and takes a deep look inside recent cyber-conflicts, including the use of Stuxnet. It also includes a Forward by Michael Chertoff (former Secretary of Homeland Security) and several guest essays, including one by Melissa Hathaway, former senior advisor to the Director of National Intelligence and Cyber Coordination Executive. Get an in-depth look at hot topics including: The role of social networks in fomenting revolution in the Middle East and Northern Africa The Kremlin's strategy to invest heavily in social networks (including Facebook) and how it benefits the Russian government How the U.S. Cyber Command and equivalent commands are being stood up in other countries The rise of Anonymous with analysis of its anti-structure and operational style or tempo Stuxnet and its predecessors, and what they reveal about the inherent weaknesses in critical infrastructure The Intellectual Property (IP) war, and how it has become the primary focus of state-sponsored cyber operations

Cybersecurity CRC Press

This book examines in depth the major recent cyber attacks that have taken place around the world, discusses the implications of such attacks, and offers solutions to the vulnerabilities that made these attacks possible. Through investigations of the most significant and damaging cyber attacks, the author introduces the reader to cyberwar, outlines an effective defense against cyber threats, and explains how to prepare for future attacks.