Law Of Cyber Warfare Ssrn

We depend on information and information technology (IT) to make many of our day-to-day tasks easier and more convenient. Computers play key roles in transportation, health care, banking, and energy. Businesses use IT for payroll and accounting, inventory and sales, and research and development. Modern military forces use weapons that are increasingly coordinated through computer-based networks. Cybersecurity is vital to protecting all of these functions. Cyberspace is vulnerable to a broad spectrum of hackers, criminals, terrorists, and state actors. Working in cyberspace, these malevolent actors can steal money, intellectual property, or classified information; impersonate law-abiding parties for their own purposes; damage important data; or deny the availability of normally accessible services. Cybersecurity issues arise because of three factors taken together - the presence of malevolent actors in cyberspace, societal reliance on IT for many important functions, and the presence of vulnerabilities in IT systems. What steps can policy makers take to protect our government, businesses, and the public from those would take advantage of system vulnerabilities? At the Nexus of Cybersecurity and Public Policy offers a wealth of information on practical measures, technical and nontechnical challenges, and potential policy responses. According to this report, cybersecurity is a never-ending battle; threats will evolve as adversaries adopt new tools and techniques to compromise security. Cybersecurity is therefore an ongoing process that needs to evolve as new threats are identified. At the Nexus of Cybersecurity and Public Policy is a call for action to make cybersecurity a public safety priority. For a number of years, the cybersecurity issue has received increasing public attention; however, most policy focus has been on the short-term costs of improving systems. In its explanation of the fundamentals of cybersecurity and the discussion of potential policy responses, this book will be a resource for policy makers, cybersecurity and IT professionals, and anyone who wants to understand threats to cyberspace.

This book examines the challenges that military forces will face in multinational operations in the 21st century. Expanding on Rupert Smith’s The Utility of Force, the volume assesses the changing parameters within which force as a political instrument is ultimately carried out. By analysing nine carefully selected mission types, the volume presents a comprehensive analysis of key trends and trajectories. Building upon this analysis, the contributors break the trends and parameters down into real and potential tasks and mission types in order to identify concrete implications for military forces in future multinational operations. The context of military intervention in conflicts and crises around the world is rapidly evolving. Western powers’ shrinking ability and desire to intervene makes it pertinent to analyse how the cost of operations can be reduced and, how they can be executed more intelligently in the future. New challenges to international military operations are arising and this book addresses these challenges by focusing on three key areas of change: 1) An increasingly urbanised world; 2) The changing nature of missions; 3) The commercial availability of new technologies. In answering these questions and embracing some of the insights of a growing field of future studies, the volume presents an innovative perspective on future international military operations. This book will be of much interest to students of international intervention, military and strategic studies, war and conflict studies, security studies and IR in general.

The conduct of hostilities via cyberspace poses many issues regarding the application of international humanitarian law. Cyberspace should be considered as a sui generis battlefield when it comes to the study of the applicable law. The present contribution aims to identify some of the key issues arising from the application of the law of targeting to cyber operations in the context of an armed conflict, focusing exclusively on the application of the principle of distinction. The principle of distinction - the cornerstone on which humanitarian law stands - today is shrouded in uncertainty in the context of cyber operations. The key threshold of attack, the definition of military objective and the targeting of dual-use cyber infrastructures and digital data are some key issues that need to be further developed in the context of cyber operations. Finally, with regard to targetable individuals, the status of cyber combatants, cyber levée en masse and the notion of direct participation in cyber hostilities, are underdeveloped legal concepts and need particular interpretation in the context of cyber operations. The complete lack of international jurisprudence and the embryonic state practice on the emerging field of cyber warfare call for the principle of distinction and the relevant provisions of lex lata to be assessed on a humanitarian basis and re-conceptualized in light of the warfare reality. concepts and need particular interpretation in the context of cyber operations. The complete lack of international jurisprudence and the embryonic state practice on the emerging field of cyber warfare call for the principle of distinction and the relevant provisions of lex lata to be assessed on a humanitarian basis and re-conceptualized in light of the warfare reality.

Reconsidering American Civil-Military RelationsThe Military, Society, Politics, and Modern WarOxford University Press, USA

Tallinn Manual 2.0 expands on the highly influential first edition by extending its coverage of the international law governing cyber operations to peacetime legal regimes. The product of a three-year follow-on project by a new group of twenty renowned international law experts, it addresses such topics as sovereignty, state responsibility, human rights, and the law of air, space, and the sea. Tallinn Manual 2.0 identifies 154 'black letter' rules governing cyber operations and provides extensive commentary on each rule. Although Tallinn Manual 2.0 represents the views of the experts in their personal capacity, the project benefitted from the unofficial input of many states and over fifty peer reviewers.

Provides a fresh perspective on ASEAN's role for regional security in Southeast Asia.

Explains how existing and proposed law seek to tackle challenges posed by new and emerging technologies in war and peace.

Emerging technologies have always played an important role in armed conflict. From the crossbow to cyber capabilities, technology that could be weaponized to create an advantage over an adversary has inevitably found its way into military arsenals for use in armed conflict. The weaponization of emerging technologies, however, raises challenging legal issues with respect to the law of armed conflict. As States continue to develop and exploit new technologies, how will the law of armed conflict address the use of these technologies on the battlefield? Is existing law sufficient to regulate new technologies, such as cyber capabilities, autonomous weapons systems, and artificial intelligence? Have emerging technologies fundamentally altered the way we should understand concepts such as law-of-war precautions and the principle of distinction? How can we ensure compliance and accountability in light of technological advancement? This volume of the Lieber Studies explores these critical questions while highlighting the legal challenges--and opportunities--presented by the use of emerging technologies on the battlefield.

Today’s investors need to understand geopolitical trends as a main driving force of markets. This book provides just that: an understanding of the interplay between geopolitics and economics, and of the impact of that dynamic on financial markets. To me, geo-economics is the study of how geopolitics and economics interact in international relations. Plenty of books on geopolitics have been written by eminent experts in politics and international affairs. This book is not one of them. First, I am neither a political scientist nor an expert in international affairs. I am an economist and an investment strategist who has been fascinated by geopolitics for many years. And this fascination has led me to the realization that almost all books and articles written on geopolitics are useless for investors. Political scientists are not trained to think like investors, and they are not typically trained in quantitative methods. Instead, they engage in developing narratives for geopolitical events and processes that pose risks and opportunities for investors. My main problem with these narratives is that they usually do not pass the “so what?” test. Geopolitical risks are important, but how am I to assess which risks are important for my portfolio and which ones are simply noise? Because geopolitics experts focus on politics, they do not provide an answer to this crucial question for investors. What could be important for a geopolitics expert and for global

politics could be totally irrelevant for investors. For example, the US wars in Iraq and Afghanistan have been going on for almost two decades now and have been an important influence on the political discussion in the United States. But for investors, the war in Afghanistan was a total nonevent, and the war in Iraq had only a fleeting influence, when it started in 2003. Geopolitics experts cannot answer the question of which geopolitical events matter for investors and which do not. Unfortunately, some experts thus claim that all geopolitical risks matter and that these risks cannot be quantified but only assessed qualitatively. Nothing could be further from the truth. In the chapters that follow, I discuss geopolitical and geo-economic events from the viewpoint of an investor and show that they can be quantified and introduced as part of a traditional risk management process. I do this in two parts. The first part of this book focuses on geopolitics that matters to investors. It reviews the literature on a range of geopolitical events and shows which events have a material economic effect and which do not. The second part of this book puts the insights from those first chapters into practice by applying them to current geopolitical trends. In this second part, I stick my head out and examine the impact the geopolitical trends have on the economy and financial markets today and their likely development in the coming years. —Joachim Klement, CFA

The result of a three-year project, this manual addresses the entire spectrum of international legal issues raised by cyber warfare.

This book provides an up-to-date, accessible guide to the growing threats in cyberspace that affects everyone from private individuals to businesses to national governments.

An analysis of the status of computer network attacks in international law.

The second edition of the definitive guide to cybersecurity law, updated to reflect recent legal developments The revised and updated second edition of Cybersecurity Law offers an authoritative guide to the key statutes, regulations, and court rulings that pertain to cybersecurity. Written by an experienced cybersecurity lawyer and law professor, the second edition includes new and expanded information that reflects the latest changes in laws and regulations. The book includes material on recent FTC data security consent decrees and data breach litigation. Topics covered reflect new laws, regulations, and court decisions that address financial sector cybersecurity, the law of war as applied to cyberspace, and recently updated guidance for public companies' disclosure of cybersecurity risks. This important guide: Provides a new appendix, with 15 edited opinions covering a wide range of cybersecurity-related topics, for students learning via the caselaw method Includes new sections that cover topics such as: compelled access to encrypted devices, New York's financial services cybersecurity regulations, South Carolina's insurance sector cybersecurity law, the Internet of Things, bug bounty programs, the vulnerability equities process, international enforcement of computer hacking laws, the California Consumer Privacy Act, and the European Union's Network and Information Security Directive Contains a new chapter on the critical topic of law of cyberwar Presents a comprehensive guide written by a noted expert on the topic Offers a companion Instructor-only website that features discussion questions for each chapter and suggested exam questions for each chapter Written for students and professionals of cybersecurity, cyber operations, management-oriented information technology (IT), and computer science, Cybersecurity Law, Second Edition is the up-to-date guide that covers the basic principles and the most recent information on cybersecurity laws and regulations. JEFF KOSSEFF is Assistant Professor of Cybersecurity Law at the United States Naval Academy in Annapolis, Maryland. He was a finalist for the Pulitzer Prize, and a recipient of the George Polk Award for national reporting.

The internet has changed the rules of many industries, and war is no exception. But can a computer virus be classed as an act of war? Does a Denial of Service attack count as an armed attack? And does a state have a right to self-defence when cyber attacked? With the range and sophistication of cyber attacks against states showing a dramatic increase in recent times, this book investigates the traditional concepts of 'use of force', 'armed attack', and 'armed conflict' and asks whether existing laws created for analogue technologies can be applied to new digital developments. The book provides a comprehensive analysis of primary documents and surrounding literature, to investigate whether and how existing rules on the use of force in international law apply to a relatively new phenomenon such as cyberspace operations. It assesses the rules of jus ad bellum and jus in bello, whether based on treaty or custom, and analyses why each rule applies or does not apply to cyber operations. Those rules which can be seen to apply are then discussed in the context of each specific type of cyber operation. The book addresses the key questions of whether a cyber operation amounts to the use of force and, if so, whether the victim state can exercise its right of self-defence; whether cyber operations trigger the application of international humanitarian law when they are not accompanied by traditional hostilities; what rules must be followed in the conduct of cyber hostilities; how neutrality is affected by cyber operations; whether those conducting cyber operations are combatants, civilians, or civilians taking direct part in hostilities. The book is essential reading for everyone wanting a better understanding of how international law regulates cyber combat.

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.

This book presents a novel framework to reconceptualize Internet governance and better manage cyber attacks. Specifically, it makes an original contribution by examining the potential of polycentric regulation to increase accountability through bottom-up action. It also provides a synthesis of the current state of cybersecurity research, bringing features of the cloak and dagger world of cyber attacks to light and comparing and contrasting the cyber threat to all relevant stakeholders. Throughout the book, cybersecurity is treated holistically, covering outstanding issues in law, science, economics, and politics. This interdisciplinary approach is an exemplar of how strategies from different disciplines as well as the private and public sectors may cross-pollinate to enhance cybersecurity. Case studies and examples illustrate what is at stake and identify best practices. The book discusses technical issues of Internet governance and cybersecurity while presenting the material in an informal, straightforward manner. The book is designed to inform readers about the interplay of Internet governance and cybersecurity and the potential of polycentric regulation to help foster cyber peace.

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

Cyber weapons and the possibility of cyber conflict—including interference in foreign political campaigns, industrial sabotage, attacks on infrastructure, and combined military campaigns—require policymakers, scholars, and citizens to rethink twenty-first-century warfare. Yet because cyber capabilities are so new and continually developing, there is

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

The ever increasing use of computers, networks and the Internet has led to the need for regulation in the fields of cybercrime, cybersecurity and national security. This SpringerBrief provides insights into the development of self- and co-regulatory approaches to cybercrime and cybersecurity in the multi-stakeholder environment. It highlights the differences concerning the ecosystem of stakeholders involved in each area and covers government supported initiatives to motivate industry to adopt self-regulation. Including a review of the drawbacks of existing forms of public-private collaboration, which can be attributed to a specific area (cybercrime, cybersecurity and national security), it provides some suggestions with regard to the way forward in self- and co-regulation in securing cyberspace.

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.

This book explores contemporary civil-military relations in the United States. Much of the canonical literature on civil-military relations was either written during or references the Cold War, while other major research focuses on the post-Cold War era, or the first decade of the twenty-first century. A great deal has changed since then. This book considers the implications for civil-military relations of many of these changes. Specifically, it focuses on factors such as breakdowns in democratic and civil-military norms and conventions; intensifying partisanship and deepening political divisions in American society; as well as new technology and the evolving character of armed conflict. Chapters are organized around the principal actors in civil-military relations, and the book includes sections on the military, civilian leadership, and the public. It explores the roles and obligations of each. The book also examines how changes in contemporary armed conflict influence civil-military relations. Chapters in this section examine the cyber domain, grey zone operations, asymmetric warfare and emerging technology. The book thus brings the study of civil-military relations into the contemporary era, in which new geopolitical realities and the changing character of armed conflict combine with domestic political tensions to test, if not potentially redefine, those relations.

In a world of increasing dependence on information technology, the prevention of cyberattacks on a nation's important computer and communications systems and networks is a problem that looms large. Given the demonstrated limitations of passive cybersecurity defense measures, it is natural to consider the possibility that deterrence might play a useful role in preventing cyberattacks against the United States and its vital interests. At the request of the Office of the Director of National Intelligence, the National Research Council undertook a two-phase project aimed to foster a broad, multidisciplinary examination of strategies for deterring cyberattacks on the United States and of the possible utility of these strategies for the U.S. government. The first phase produced a letter report providing basic information needed to understand the nature of the problem and to articulate important questions that can drive research regarding ways of more effectively preventing, discouraging, and inhibiting hostile activity against important U.S. information systems and networks. The second phase of the project entailed selecting appropriate experts to write papers on questions raised in the letter report. A number of experts, identified by the committee, were commissioned to write these papers under contract with the National Academy of Sciences. Commissioned papers were discussed at a public workshop held June 10-11, 2010, in Washington, D.C., and authors revised their papers after the workshop. Although the authors were selected and the papers reviewed and discussed by the committee, the individually authored papers do not reflect consensus views of the committee, and the reader should view these papers as offering points of departure that can stimulate further work on the topics discussed. The papers presented in this volume are published essentially as received from the authors, with some proofreading corrections made as limited time allowed.

This book provides a comparison and practical guide for academics, students, and the business community of the current data protection laws in selected Asia Pacific countries (Australia, India, Indonesia, Japan Malaysia, Singapore, Thailand) and the European Union. The book shows how over the past three decades the range of economic, political, and social activities that have moved to the internet has increased significantly. This technological transformation has resulted in the collection of personal data, its use and storage across international boundaries at a rate that governments have been unable to keep pace. The book highlights challenges and potential solutions related to data protection issues arising from cross-border problems in which personal data is being considered as intellectual property, within transnational contracts and in anti-trust law. The book also discusses the emerging challenges in protecting personal data and promoting cyber security. The book provides a deeper understanding of the legal risks and frameworks associated with data protection law for local, regional and global academics, students, businesses, industries, legal profession and individuals.

"Cyber war is coming," announced a land-mark RAND report in 1993. In 2005, the U.S. Air Force boasted it would now fly, fight, and win in cyberspace, the "fifth domain" of warfare. This book takes stock, twenty years on: is cyber war really coming? Has war indeed entered the fifth domain? Cyber War Will Not Take Place cuts through the hype and takes a fresh look at cyber security. Thomas Rid argues that the focus on war and winning distracts from the real challenge of cyberspace: non-violent confrontation that may rival or even replace violence in surprising ways. The threat consists of three different vectors: espionage, sabotage, and subversion. The author traces the most significant hacks and attacks, exploring the full spectrum of case studies from the shadowy world of computer espionage and weaponised code. With a mix of technical detail and rigorous political analysis, the book explores some key questions: What are cyber weapons? How have they changed the meaning of violence? How likely and how dangerous is crowd-sourced subversive activity? Why has there never been a lethal cyber attack against a country's critical infrastructure? How serious is the threat of "pure" cyber espionage, of exfiltrating

data without infiltrating humans first? And who is most vulnerable: which countries, industries, individuals?

International law's role in governing disasters is undergoing a formative period in its development and reach, in parallel with concerted efforts by the international community to respond more effectively to the increasing number and intensity of disasters across the world. This Research Handbook examines a broad range of legal regimes directly and indirectly relevant to disaster prevention, mitigation and reconstruction across a spectrum of natural and manmade disasters, including armed conflict.

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

"This workshop, Complex Battlespaces: The Law of Armed Conflict and the Dynamics of Modern Warfare, was held at West Point on October 24-26, 2016. It marked the official opening of the Lieber Institute." -- ECIP forword.

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.

Cyber weapons and cyber warfare have become one of the most dangerous innovations of recent years, and a significant threat to national security. Cyber weapons can imperil economic, political, and military systems by a single act, or by multifaceted orders of effect, with wide-ranging potential consequences. Unlike past forms of warfare circumscribed by centuries of just war tradition and Law of Armed Conflict prohibitions, cyber warfare occupies a particularly ambiguous status in the conventions of the laws of war. Furthermore, cyber attacks put immense pressure on conventional notions of sovereignty, and the moral and legal doctrines that were developed to regulate them. This book, written by an unrivalled set of experts, assists in proactively addressing the ethical and legal issues that surround cyber warfare by considering, first, whether the Laws of Armed Conflict apply to cyberspace just as they do to traditional warfare, and second, the ethical position of cyber warfare against the background of our generally recognized moral traditions in armed conflict. The book explores these moral and legal issues in three categories. First, it addresses foundational questions regarding cyber attacks. What are they and what does it mean to talk about a cyber war? The book presents alternative views concerning whether the laws of war should apply, or whether transnational criminal law or some other peacetime framework is more appropriate, or if there is a tipping point that enables the laws of war to be used. Secondly, it examines the key principles of jus in bello to determine how they might be applied to cyber-conflicts, in particular those of proportionality and necessity. It also investigates the distinction between civilian and combatant in this context, and studies the level of causation necessary to elicit a response, looking at the notion of a 'proximate cause'. Finally, it analyzes the specific operational realities implicated by particular regulatory regimes. This book is unmissable reading for anyone interested in the impact of cyber warfare on international law and the laws of war.

This is the seminal textbook on the law of international armed conflict, written by a leading commentator on the subject. The second edition has been thoroughly revised and updated, taking into account new developments in combat, numerous recent judicial cases (especially decisions rendered by the International Criminal Tribunal for the Former Yugoslavia), as well as topical studies and instruments. The text clarifies complex issues, offering solutions to practical combat dilemmas that have emerged in present-day battlefield situations. Several current (and controversial) subjects are examined in depth, including direct participation in hostilities, human shields, and air and missile warfare. Useful definitions and explanations have been added, making intricate problems easier to comprehend. The book is designed not only for students of international law, but also as a tool for the instruction of military officers.

This timely Research Handbook contains an analysis of various legal questions concerning cyberspace and cyber activities and provides a critical account of their effectiveness. Expert contributors examine the application of fundamental international la

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.

A gripping behind-the-scenes account of the dramatic legal fight to hold leaders personally responsible for aggressive war On July 17, 2018, starting an unjust war became a prosecutable international crime alongside genocide, crimes against humanity, and war crimes. Instead of collective state responsibility, our leaders are now personally subject to indictment for crimes of aggression, from invasions and preemptions to drone strikes and cyberattacks. The Crime of Aggression is Noah Weisbord's riveting insider's account of the high-stakes legal fight to enact this historic legislation and hold politicians accountable for the wars they start. Weisbord, a key drafter of the law for the International Criminal Court, takes readers behind the scenes of one of the most consequential legal dramas in modern international diplomacy. Drawing on in-depth interviews and his own invaluable insights, he sheds critical light on the motivations of the prosecutors, diplomats, and military strategists who championed the fledgling prohibition on unjust war—and those who tried to sink it. He untangles the complex history behind the measure, tracing how the crime of aggression was born at the Nuremberg trials only to fall dormant during the Cold War, and he draws lessons from such pivotal events as the collapse of the League of Nations, the rise of the United Nations, September 11, and the war on terror. The power to try leaders for unjust war holds untold promise for the international order, but also great risk. In this incisive and vitally important book, Weisbord explains how judges in such cases can balance the imperatives of justice and peace, and how the fair prosecution of aggression can humanize modern statecraft.

This open access volume surveys the state of the field to examine whether a fifth wave of deterrence theory is emerging. Bringing together insights from world-leading experts from three continents, the volume identifies the most pressing strategic challenges, frames theoretical concepts, and describes new strategies. The use and utility of deterrence in today's strategic environment is a topic of paramount concern to scholars, strategists and policymakers. Ours is a period of considerable strategic turbulence, which in recent years has featured a renewed emphasis on nuclear weapons used in defence postures across different theatres; a dramatic growth in the scale of military cyber capabilities and the frequency with which these are used; and rapid technological progress including the proliferation of long-range strike and unmanned systems. These military-strategic developments occur in a polarized international system, where cooperation between leading powers on arms control regimes is breaking down, states widely make use of hybrid conflict strategies, and the number of internationalized intrastate proxy conflicts has quintupled over the past two decades. Contemporary conflict actors exploit a wider gamut of coercive instruments, which they apply across a wider range of domains. The prevalence of multi-domain coercion across but also beyond traditional dimensions of armed conflict raises an important question: what does effective deterrence look like in the 21st century? Answering that question requires a re-appraisal of key theoretical concepts and dominant strategies of Western and non-Western actors in order to assess how they hold up in today's world. Air Commodore Professor Dr. Frans Osinga is the Chair of the War Studies Department of the Netherlands Defence Academy and the Special Chair in War Studies at the University Leiden. Dr. Tim Sweijs is the Director of Research at The Hague Centre for Strategic Studies and a Research Fellow at the Faculty of Military Sciences of the Netherlands Defence Academy in Breda.

This updated edition of a well-known comprehensive analysis of the criminalization of cyberattacks adds important new guidance to the legal framework on cybercrime, reflecting new legislation, technological developments, and the changing nature of cybercrime itself. The focus is not only on criminal law aspects but also on issues of data protection, jurisdiction, electronic evidence, enforcement, and digital forensics. It provides a thorough analysis of the legal regulation of attacks against information systems in the European, international, and comparative law contexts. Among the new and continuing aspects of cybersecurity covered are the following: the conflict of cybercrime investigation and prosecution with fundamental rights to privacy and freedom of expression; the 2016 Directive on security of network and information systems (NIS Directive); the General Data Protection Regulation (GDPR); the role of national computer security incident response teams (CSIRTs); the European Union (EU) response to new technologies involving payment instruments, including virtual currencies and digital wallets; the EU Commission's legislative proposals to enhance cross-border gathering of electronic evidence; internet service providers' role in fighting cybercrime; measures combatting identity theft, spyware, and malware; states and legal persons as perpetrators of cybercrime; and the security and data breach notification as a compliance and transparency tool. Technical definitions, case laws, and analysis of both substantive law and procedural law contribute to a comprehensive understanding of cybercrime regulation and its current evolution in practice. Addressing a topic of growing importance in unprecedented detail, this new edition of a much-relied-upon resource will be welcomed by professionals and authorities dealing with cybercrime, including lawyers, judges, academics, security professionals, information technology experts, and law enforcement agencies.