Tallinn Manual On The International Law Applicable To Cyber Warfare

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.

Provides detailed assessments of law applicable to the most difficult problems encountered during modern armed conflicts and coalitions.

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 book introduces students to the essential questions of the law of armed conflict and international humanitarian law.

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations

Russia has deployed cyber operations to interfere in foreign elections, launch disinformation campaigns, and cripple neighboring states—all while maintaining a thin veneer of deniability and avoiding strikes that cross the line into acts of war. How should a targeted nation respond? In Russian Cyber Operations, Scott Jasper dives into the legal and technical maneuvers of Russian cyber strategies, proposing that nations develop solutions for resilience to withstand future attacks. Jasper examines the place of cyber operations within Russia’s asymmetric arsenal and its use of hybrid and information warfare, considering examples from recent French and US presidential elections and the 2017 NotPetya mock ransomware attack, among others. Jasper shows the international effort to counter these operations through sanctions and indictments has done little to alter Moscow’s behavior and
Instead proposes that nations use data correlation technologies in an integrated security platform to establish a more resilient defense. Russian Cyber Operations provides a critical framework for determining whether Russian cyber campaigns and incidents rise to the level of armed conflict or operate at a lower level as a component of competition. Jasper’s work offers the national security community a robust plan of action critical to effectively mounting a durable defense against Russian cyber campaigns. The result of a three-year project, this manual addresses the entire spectrum of international legal issues raised by cyber warfare. On a global scale, the central tool for responding to complex security challenges is public international law. This handbook provides a comprehensive and systematic overview of the relationship between international law and global security.

State responsibility in international law is considered one of the cornerstones of the field. For a long time it remained the exclusive responsibility system due to the primacy of States as subjects of international law. Its unique position has nonetheless been challenged by several developments both within and outside the international legal order, such as the rise of alternative responsibility ideas and practices, as well as globalization and its consequences. This book adopts a critical and holistic approach to the law of State responsibility and analyzes the functionality of the general rules of State responsibility in a changed international landscape characterized by the fragmentation of responsibility. It is argued that State responsibility is not equally relevant across the broad spectrum of international obligations, and that alternative constructions of responsibility, namely international criminal law and international liability, have increased in standing.

Cyber Mercenaries explores the secretive relationships between states and hackers. As cyberspace has emerged as the new frontier for geopolitics, states have become entrepreneurial in their sponsorship, deployment, and exploitation of hackers as proxies to project power. Such modern-day mercenaries and privateers can impose significant harm undermining global security, stability, and human rights. These state-hacker relationships therefore raise important questions about the control, authority, and use of offensive cyber capabilities. While different countries pursue different models for their proxy relationships, they face the common challenge of balancing the benefits of these relationships with their costs and the potential risks of escalation. This book examines case studies in the United States, Iran, Syria, Russia, and China for the purpose of establishing a framework to better understand and manage the impact and risks of cyber proxies on global politics.

The national security strategy of the United Kingdom is to use all national capabilities to build Britain's prosperity, extend the country's influence in the world and strengthen security. The National Security Council ensures a strategic and co-ordinated approach across the whole of Government to the risks and opportunities the country faces. Parts 1 and 2 of this document outline the Government's analysis of the strategic global context and give an assessment of the UK's place in the world. They also set out the core objectives of the strategy: (i) ensuring a secure and resilient UK by protecting the country from all major risks that can affect us directly, and (ii) shaping a stable world - actions beyond the UK to reduce specific risks to the country or our direct interests overseas. Part 3 identifies and analyses the key security risks the country is likely to face in the future. The National Security Council has prioritised the risks and the current highest priority are: international terrorism; cyber attack; international
military crises; and major accidents or natural hazards. Part 4 describes the ways in which the strategy to prevent and mitigate the specific risks will be achieved. The detailed means to achieve these ends will be set out in the Strategic Defence and Security Review (Cm. 7948, ISBN 9780101794824), due to publish on 19 October 2010.
The protection of civilians is a highly topical issue at the forefront of international discourse, and has taken a prominent role in many international deployments. It has been at the centre of debates on the NATO intervention in Libya, UN deployments in Darfur, South Sudan, and the Democratic Republic of the Congo, and on the failures of the international community in Sri Lanka and Syria. Variously described as a moral responsibility, a legal obligation, a mandated peacekeeping task, and the culmination of humanitarian activity, it has become a high-profile concern of governments, international organisations, and civil society, and a central issue in international peace and security. This book offers a multidisciplinary treatment of this important topic, harnessing perspectives from international law and international relations, traversing academia and practice. Moving from the historical and philosophical development of the civilian protection concept, through relevant bodies of international law and normative underpinnings, and on to politics and practice, the volume presents coherent cross-cutting analysis of the realities of conflict and diplomacy. In doing so, it engages a series of current debates, including on the role of politics in what has often been characterized as a humanitarian endeavour, and the challenges and impacts of the use of force. The work brings together a wide array of eminent academics and respected practitioners, incorporating contributions from legal scholars and ethicists, political commentators, diplomats, UN officials, military commanders, development experts and humanitarian aid workers. As the most comprehensive publication on the subject, this will be a first port of call for anyone studing or working towards a better protection of civilians in conflict.

International law holds a paradoxical position with territory. Most rules of international law are traditionally based on the notion of State territory, and territoriality still significantly shapes our contemporary legal system. At the same time, new developments have challenged territory as the main organising principle in international relations. Three trends in particular have affected the role of territoriality in international law: the move towards functional regimes, the rise of cosmopolitan projects claiming to transgress state boundaries, and the development of technologies resulting in the need to address intangible, non-territorial, phenomena. Yet, notwithstanding some profound changes, it remains impossible to think of international law without a territorial locus. If international law is undergoing changes, this implies a reconfiguration of territory, but not a move beyond it. The Netherlands Yearbook of International Law was first published in 1970. It offers a forum for the publication of scholarly articles of a conceptual nature in a varying thematic area of public international law.
The authoritative manual on the applicable international law and best practice in the planning and conduct of peace operations. This book deals with two areas: Global Commons and Security: inextricably melted together and more relevant than ever in a world which is ever globalized and... with an incognita looming on the horizon: the effects of the Coronavirus pandemic upon the International Relations and globalization. Global Commons have always been relevant. It was Mahan who argued that the first and
most obvious light in which the sea presents itself from the political and social point of view, is that of a great highway; or better, perhaps, of a wide common... Nowadays, this view has been further developed and, in addition to the unique legal implications that the Global Commons introduce, they are viewed, more and more intently, as a common pool of resources. Or perhaps, not that common... Resources, the key word! Which has to be always supplemented by two key words: access and security. And still, another one: data, the cyberspace contribution to the equation.

Explains how existing and proposed law seek to tackle challenges posed by new and emerging technologies in war and peace. The definitive and authoritative international law text, updated to reflect key case law, international practice and treaty developments. The Tallinn Manual on the International Law Applicable to Cyber Warfare, written at the invitation of the Centre by an independent International Group of Experts, is the result of a three-year effort to examine how extant international law norms apply to this new form of warfare. The Tallinn Manual pays particular attention to the jus ad bellum, the international law governing the resort to force by States as an instrument of their national policy, and the jus in bello, the international law regulating the conduct of armed conflict (also labelled the law of war, the law of armed conflict, or international humanitarian law). Related bodies of international law, such as the law of State responsibility and the law of the sea, are dealt within the context of these topics. The Tallinn Manual is not an official document, but instead an expression of opinions of a group of independent experts acting solely in their personal capacity. It does not represent the views of the Centre, our Sponsoring Nations, or NATO. It is also not meant to reflect NATO doctrine. Nor does it reflect the position of any organization or State represented by observers.

International conflict resolution increasingly involves the use of non-military power and non-kinetic capabilities alongside military capabilities in the face of hybrid threats. In this book, counter-measures to those threats are addressed by academics with both practical and theoretical experience and knowledge, providing strategic and operational insights into non-kinetic conflict resolution and on the use of power to influence, affect, deter or coerce states and non-state actors. This volume in the NL ARMS series deals with the non-kinetic capabilities to address international crises and conflicts and as always views matters from a global perspective. Included are chapters on the promise, practice and challenges of non-kinetic instruments of power, the instrumentality of soft power, information as a power instrument and manoeuvring in the information environment, Russia’s use of deception and misinformation in conflict, applying counter-marketing techniques to fight ISIL, using statistics to profile terrorists, and employing tools such as Actor and Audience Analysis. Such diverse subjects as lawfare, the Law of Armed Conflict rules for non-kinetic cyber attacks, navigation warfare, GPS-spoofing, maritime interception operations, and finally, as a prerequisite, innovative ways for intelligence collection in UN Peacekeeping in Mali come up for discussion. The book will provide both professionals such as (foreign) policy makers and those active in the military services, academics at a master level and those with an interest in military law and the law of armed conflict with useful and up-to-date insights into the wide range of subjects that are contained within it.

Paul A.L. Ducheine and Frans P.B. Osinga are General Officers and full professors at the Faculty of Military Sciences of the Netherlands Defence Academy in Breda, The Netherlands.

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 Law of Armed Conflict provides a complete operational scenario and introduction to the operational organization of United States forces. The focus remains on United States law perspective, balanced with exposure to areas where the interpretation of its allied forces diverge. Jus ad bellum and jus in bello issues are addressed at length. The casebook comes to students with stunning authority. All of the authors are active or retired United States Army officers with more than 140 years of collective military operational experience among them. Several have experience in both legal and operational assignments as well. They deliver a comprehensive coverage of all aspects of the law of armed conflict, explaining the difference between law and policy in regulation of military operations.

This book explores the international law framework governing the use of armed force in occupied territory through a rigorous analysis of the interplay between jus ad bellum, international humanitarian law, and international human rights law. Through an examination of state practice and opinio juris, treaty provisions and relevant international and domestic case law, this book offers the first comprehensive study on this topic. This book will be relevant to scholars, practitioners, legal advisors, and students across a range of sub-disciplines of international law, as well as in peace and conflict studies, international relations, and political science. This study will influence the way in which States use armed force in occupied territory, offering guidance and support in litigations before domestic and international courts and tribunals.

A new framework for understanding computing: a coherent set of principles spanning technologies, domains, algorithms, architectures, and designs. Computing is usually viewed as a technology field that advances at the breakneck speed of Moore's Law. If we turn away even for a moment, we might miss a game-changing technological breakthrough or an earthshaking theoretical development. This book takes a different perspective, presenting computing as a science governed by fundamental principles that span all technologies. Computer science is a science of information processes. We need a new language to describe the science, and in this book Peter Denning and Craig Martell offer the great principles framework as just such a language. This is a book about the whole of computing—its algorithms, architectures, and designs. Denning and Martell divide the great principles of computing into six categories: communication, computation, coordination, recollection, evaluation, and design. They begin with an introduction to computing, its history, its many interactions with other fields, its
domains of practice, and the structure of the great principles framework. They go on to examine the great principles in different areas: information, machines, programming, computation, memory, parallelism, queueing, and design. Finally, they apply the great principles to networking, the Internet in particular. Great Principles of Computing will be essential reading for professionals in science and engineering fields with a "computational" branch, for practitioners in computing who want overviews of less familiar areas of computer science, and for non-computer science majors who want an accessible entry way to the field.


This compact, highly engaging book examines the international legal regulation of both the conduct of States among themselves and conduct towards individuals, in relation to the use of cyberspace. Chapters introduce the perspectives of various stakeholders and the challenges for international law. The author discusses State responsibility and key cyberspace rights issues, and takes a detailed look at cyber warfare, espionage, crime and terrorism. The work also covers the situation of non-State actors and quasi-State actors (such as IS, or ISIS, or ISIL) and concludes with a consideration of future prospects for the international law of cyberspace. Readers may explore international rules in the areas of jurisdiction of States in cyberspace, responsibility of States for cyber activities, human rights in the cyber world, permissible responses to cyber attacks, and more. Other topics addressed include the rules of engagement in cyber warfare, suppression of cyber crimes, permissible limits of cyber espionage, and suppression of cyber-related terrorism. Chapters feature explanations of case law from various jurisdictions, against the background of real-life cyber-related incidents across the globe. Written by an internationally recognized practitioner in the field, the book objectively guides readers through on-going debates on cyber-related issues against the background of international law. This book is very accessibly written and is an enlightening read. It will appeal to a wide audience, from international lawyers to students of international law, military strategists, law enforcement officers, policy makers and the lay person.

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.

Over recent decades, international humanitarian law has been shaped by the omnipresence of so-called expert manuals. Astute and engaging, this discerning book provides a comprehensive account of these black letter rules and commentaries produced by private expert groups and demonstrates why the general acceptance of these expert manuals is largely unjustified. The author innovatively links interdisciplinary insights to the needs of military lawyers in practice, showing the pitfalls of relying on private manuals as arguable restatements and interpretations of the law 'as it is'.

“One of the finest books on information security published so far in this century—easily accessible, tightly argued, superbly well-sourced, intimidatingly perceptive.” —Thomas Rid, author of Active Measures “The best examination I have read of how increasingly dramatic developments in cyberspace are defining the ‘new normal’ of geopolitics in the digital age. Buchanan...captures the dynamics of all of this truly brilliantly.” —General David Petraeus, former Director of the CIA and Commander of Coalition Forces in Iraq and Afghanistan Few national-security threats are as potent—or as nebulous—as cyber attacks. Ben Buchanan reveals how hackers are transforming spycraft and statecraft, catching us all in the crossfire, whether we know it or not. Ever since WarGames, we have been bracing for the cyberwar to come, conjuring images of exploding power plants and mass panic. But while cyber attacks are now disturbingly common, they don’t look anything like we thought they would. Packed with insider information based on interviews, declassified files, and forensic analysis of company reports, The Hacker and the State sets aside fantasies of cyber-annihilation to explore the real geopolitical competition of the digital age. Tracing the conflict of wills and interests among modern nations, Ben Buchanan reveals little-known details of how China, Russia, North Korea, Britain, and the United States hack one another in a relentless struggle for dominance. His analysis moves deftly from undersea cable taps to underground nuclear sabotage, from blackouts and data breaches to billion-dollar heists and election interference. Buchanan brings to life this continuous cycle of espionage and deception, attack and counterattack, destabilization and retaliation. He explains why cyber attacks are far less destructive than we anticipated, far more pervasive, and much harder to prevent.
With little fanfare and far less scrutiny, they impact our banks, our tech and health systems, our democracy, and every aspect of our lives. Quietly, insidiously, they have reshaped our national-security priorities and transformed spycraft and statecraft. The contest for geopolitical advantage has moved into cyberspace. The United States and its allies can no longer dominate the way they once did. The nation that hacks best will triumph.

A growing number of states use private military and security companies (PMSCs) for a variety of tasks, which were traditionally fulfilled by soldiers. This book provides a comprehensive analysis of the law that applies to PMSCs active in situations of armed conflict, focusing on international humanitarian law. It examines the limits in international law on how states may use private actors, taking the debate beyond the question of whether PMSCs are mercenaries. The authors delve into issues such as how PMSCs are bound by humanitarian law, whether their staff are civilians or combatants, and how the use of force in self-defence relates to direct participation in hostilities, a key issue for an industry that operates by exploiting the right to use force in self-defence. Throughout, the authors identify how existing legal obligations, including under state and individual criminal responsibility should play a role in the regulation of the industry.

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.

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. This book covers many aspects of cyberspace, emphasizing not only its possible ‘negative’ challenge as a threat to security, but also its positive influence as an efficient tool for defense as well as a welcome new factor for economic and industrial production. Cyberspace is analyzed from quite different and interdisciplinary perspectives, such as: conceptual and legal, military and socio-civil, psychological, commercial, cyber delinquency, cyber intelligence applied to public and private institutions, as well as the nuclear governance.

International Law and New Wars examines how international law fails to address the contemporary experience of what are known as 'new wars' - instances of armed conflict and violence in places such as Syria, Ukraine, Libya, Mali, the Democratic Republic of Congo and South Sudan. International law, largely constructed in the nineteenth and twentieth centuries, rests to a great extent on the outmoded concept of war drawn from European experience - inter-state clashes involving battles between regular and identifiable armed forces. The book shows how different approaches are associated with different interpretations of international law, and, in some cases, this has dangerously weakened the legal restraints on war established after 1945. It puts forward a practical case for what it defines as second generation human security and the implications this carries for international law. A comprehensive analysis of the international law applicable to cyber operations, including a systematic study of attribution, lawfulness and remedies.

‘Child Soldiers and the Lubanga Case’ and ‘The Tallinn Manual on the International Law Applicable to Cyber Warfare’ are the two central themes of this volume. Each of these timely topics is addressed from three different angles, providing a truly comprehensive analysis of the subject. The book also features an article on the duty to investigate civilian casualties during armed conflict and its implementation in practice and an elaborate year in review, discussing developments that occurred in 2012. The Yearbook of International Humanitarian Law is the world's only annual publication devoted to the study of the laws governing armed conflict. It provides a truly international forum for high-quality, peer-reviewed academic articles focusing on this crucial branch of international law. Distinguished by contemporary relevance, the Yearbook of International Humanitarian Law bridges the gap between theory and practice and serves as a useful reference tool for scholars, practitioners, military personnel, civil servants, diplomats, human rights workers and students.

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.

The international law on the use of force is one of the oldest branches of international law. It is an area twinned with the emergence of international law as a concept in itself, and which sees law and politics collide. The number of armed conflicts is equal only to the number of methodological approaches used to describe them. Many violent encounters are well known. The Kosovo Crisis in 1999 and the US-led invasion of Iraq in 2003 spring easily to the minds of most scholars and academics, and gain extensive coverage in this text. Other conflicts, including the Belgian operation in Stanleyville, and the Ethiopian Intervention in Somalia, are often overlooked to our peril. Ruys and Corten's expert-written text compares over sixty different instances of the use of cross border force since the adoption of the UN Charter in 1945, from all out warfare to hostile encounters between individual units, targeted killings, and hostage rescue operations, to ask a complex question. How much authority does the power of precedent really have in the law of the use of force?

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 law. The prohibition of the use of force in international law is one of the major achievements of international law in the past century. The attempt to outlaw war as a means of national policy and to establish a system of collective security after both World Wars resulted in the creation of the United Nations Charter, which remains a principal point of reference for the law on the use of force to this day. There have, however, been considerable challenges to the law on the prohibition of the use of force in international law is one of the major achievements of international law in the past century. The attempt to outlaw war as a means of national policy and to establish a system of collective security after both World Wars resulted in the creation of the United
Nations Charter, which remains a principal point of reference for the law on the use of force to this day. There have, however, been considerable challenges to the law on the prohibition of the use of force over the past two decades. This Oxford Handbook is a comprehensive and authoritative study of the modern law on the use of force. Over seventy experts in the field offer a detailed analysis, and to an extent a restatement, of the law in this area. The Handbook reviews the status of the law on the use of force, and assesses what changes, if any, have occurred in consequence to recent developments. It offers cutting-edge and up-to-date scholarship on all major aspects of the prohibition of the use of force. The work is set in context by an extensive introductory section, reviewing the history of the subject, recent challenges, and addressing major conceptual approaches. Its second part addresses collective security, in particular the law and practice of the United Nations organs, and of regional organizations and arrangements. It then considers the substance of the prohibition of the use of force, and of the right to self-defence and associated doctrines. The next section is devoted to armed action undertaken on behalf of peoples and populations. This includes self-determination conflicts, resistance to armed occupation, and forcible humanitarian and pro-democratic action. The possibility of the revival of classical, expansive justifications for the use of force is then addressed. This is matched by a final section considering new security challenges and the emerging law in relation to them. Finally, the key arguments developed in the book are tied together in a substantive conclusion. The Handbook will be essential reading for scholars and students of international law and the use of force, and legal advisers to both government and NGOs.

Copyright: 5a97beaeb020e778f8ecab5f71bdda23