Tallinn Manual International Law

The Use of Force against Ukraine and International LawRisk and the Regulation of Uncertainty in International LawA strong Britain in an age of uncertaintyTerrorism, War and International LawNew Technologies and the Law in War and PeaceResearch Handbook on International Law and CyberspaceThe Oxford Handbook of the Use of Force in International LawCustomary International Humanitarian LawTallinn Manual 2.0 on the International Law Applicable to Cyber OperationsLeuven Manual on the International Law Applicable to Peace OperationsOslo Manual on Select Topics of the Law of Armed ConflictComparative International LawYearbook of International Humanitarian LawThe Epochs of International LawCyber BlockadesCyber Operations and International LawCyber WarfareManaging Cyber Attacks in International Law, Business, and RelationsThe Use of Armed Force in Occupied TerritoryProspects for the Rule of Law in CyberspaceCyber Operations and the Use of Force in International LawThe Law of Armed ConflictStriking PowerInternational Law and New WarsThe Use of Force in International LawPublic International Law of CyberspacePrivatizing WarCybersecurity LawTallinn Manual on the International Law Applicable to Cyber WarfareBinary BulletsCyber Warfare and the Laws of WarThe Conduct of Hostilities under the Law of International Armed ConflictCyber WarCyberspaceNetherlands Yearbook of International Law 2016The Law of Armed ConflictCyber

MercenariesPeacetime Regime for State Activities in CyberspaceDeconstruction Machines

The Use of Force against Ukraine and International Law

A bold new theory of cyberwar argues that militarized hacking is best understood as a form of deconstruction From shadowy attempts to steal state secrets to the explosive destruction of Iranian centrifuges, cyberwar has been a vital part of statecraft for nearly thirty years. But although computer-based warfare has been with us for decades, it has changed dramatically since its emergence in the 1990s, and the pace of change is accelerating. In Deconstruction Machines, Justin Joque inquires into the fundamental nature of cyberwar through a detailed investigation of what happens at the crisis points when cybersecurity systems break down and reveal their internal contradictions. He concludes that cyberwar is best envisioned as a series of networks whose constantly shifting connections shape its very possibilities. He ultimately envisions cyberwar as a form of writing, advancing the innovative thesis that cyber attacks should be seen as a militarized form of deconstruction in which computer programs are systems that operate within the broader world of texts. Throughout, Joque addresses hot-button subjects such as technological social control and cyber-resistance entities like Anonymous and Wikileaks while also providing a rich, detailed history of cyberwar. Deconstruction Machines

provides a necessary new interpretation of deconstruction and timely analysis of media, war, and technology.

Risk and the Regulation of Uncertainty in International Law

Increasingly, international legal arrangements imagine future worlds or create space for experts to articulate how the future can be conceptualized and managed. With the increased specialization of international law, a series of functional regimes and sub-regimes has emerged, each with their own imageries, vocabularies, expert-knowledge, and rules to translate our hopes and fears for the future into action in the present. At issue in the development of these regimes are not just competing predictions of the future based on what we know about what has happened in the past and what we know is happening in the present. Rather, these regimes seek to deal with futures about which we know very little or nothing at all; futures that are inherently uncertain and even potentially catastrophic; futures for which we need to find ways to identify, conceptualise, manage, and regulate risks the existence of which we can possibly only speculate about. This book explores how the future is imagined, articulated, and managed across the various fields of international law, including the use of force, maritime security, international economic and environmental law, and human rights. It investigates how the future is construed in these various areas; how the costs of risk, risk regulation, risk assessment, and risk management are distributed

in international law; the effect of uncertain futures on the subjects of international law; and the way in which international law operates when faced with catastrophic or existential risk.

A strong Britain in an age of uncertainty

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.

Terrorism, War and International Law

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.

New Technologies and the Law in War and Peace

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

Research Handbook on International Law and Cyberspace

The Oxford Handbook of the Use of Force in International Law

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.

Customary International Humanitarian 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 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.

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations

By definition, international law, once agreed upon and consented to, applies to all parties equally. It is perhaps the one area of law where cross-country comparison seems inappropriate, because all parties are governed by the same rules. However, as this book explains, states sometimes adhere to similar, and at other times, adopt different interpretations of the same international norms and standards. International legal rules are not a monolithic whole, but are the basis for ongoing contestation in which states set forth competing interpretations.

International norms are interpreted and redefined by national executives, legislatures, and judiciaries. These varying and evolving interpretations can, in turn, change and impact the international rules themselves. These similarities and differences make for an important, but thus far, largely unexamined object of comparison. This is the premise for this book, and for what the editors call "comparative international law." This book achieves three objectives. The first is to show that international law is not a monolith. The second is to map the cross-country similarities and differences in international legal norms in different fields of international law, as well as their application and interpretation with regards to geographic differences. The third is to make a first and preliminary attempt to explain these differences. It is organized into three broad thematic sections, exploring: conceptual matters, domestic institutions and comparative international law, and comparing approaches across issue-areas. The chapters are authored by contributors who include leading international law and comparative law scholars with diverse backgrounds, experience, and perspectives.

Leuven Manual on the International Law Applicable to Peace Operations

Written by a team of international lawyers from Europe, Asia, Africa, and the Caribbean, this book analyses some of the most significant aspects of the ongoing armed conflict between the Russian Federation and Ukraine. As challenging as this conflict

is for the international legal order, it also offers lessons to be learned by the States concerned, and by other States alike. The book analyses the application of international law in this conflict, and suggests ways for this law's progressive development. It will be useful to practitioners of international law working at national Ministries of Defence, Justice, and Foreign Affairs, as well as in Parliaments, to lawyers of international organizations, and to national and international judges dealing with matters of public international law, international humanitarian law and criminal law. It will also be of interest to scholars and students of international law, and to historians of international relations. Sergey Sayapin is Assistant Professor in International and Criminal Law at the School of Law of the KIMEP University in Almaty, Kazakhstan. Evhen Tsybulenko is Professor of Law at the Department of Law of the Tallinn University of Technology in Tallinn, Estonia.

Oslo Manual on Select Topics of the Law of Armed Conflict

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

Comparative International Law

Yearbook of International Humanitarian Law

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.

The Epochs of International Law

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

laws apply to it, and how it fits into traditional ideas of armed conflict.

Cyber Blockades

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.

Cyber Operations and 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.

Cyber Warfare

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.

Managing Cyber Attacks in International Law, Business, and Relations

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.

The Use of Armed Force in Occupied Territory

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.

Prospects for the Rule of Law in Cyberspace

The application of international law and legal principles in cyberspace is a topic that has caused confusion, doubt, and interminable discussions between lawyers since the earliest days of the internationalization of the Internet. The still unresolved debate over whether cyberspace constitutes a fundamentally new domain that requires fundamentally new laws to govern it reveals basic ideological divides. On the one hand, the Euro-Atlantic community led by the United States believes, in broad terms, that activities in cyberspace require no new legislation, and existing legal obligations are sufficient. On the other, a large number of other states led by Russia and China believe that new international legal instruments are essential in order to govern information security overall, including those expressed through the evolving domain of cyberspace. Russia in particular argues that the challenges presented by cyberspace are too urgent to wait for customary law to develop as it has done in other domains; instead, urgent action is needed. This Letort Paper will provide an overview of moves toward establishing norms and the rule of law in cyberspace, and the potential for establishing further international norms of behavior. Strategic Studies Institute recommends this Letort Paper not only to policymakers, legislative leaders, and researchers focusing on law and policy in the cyber field, but also more broadly to those engaged in protecting the United States against other forms of information operations, including subversion, destabilization, and disinformation. As shown in this Letort Paper, legislative initiatives by potential adversaries provide important insights into the conceptual framework

within which they consider and plan unfriendly actions. Attorneys within the information security arena and cyber professionals may also be interested in this text. Undergraduate and Graduate Students studying national and global security with an emphasis on information cyber security coursework may be interested in this text for additional research for classes, such as: Ethics, law and policy, network security, IT Security Defense Countermeasures; Cyber Investigation, Cybersecurity Law and Policy, Introduction to Cyber Conflict, Cyber Defense Strategies, Information Sharing and Safeguarding, Globalization and Threats and International Security, Intelligence and Strategic Analysis, Security and Civil Liberties, Methods of Strategic Analysis, and more. Related products: Infrastructure and Electronic Security resources collection can be found here: https: //bookstore.gpo.gov/catalog/security-defense-law-enforcement/infrastructure-electronic-security Mail & Communications Security resources collection is available here: https: //bookstore.gpo.gov/catalog/security-defense-law-enforcement/mail-communications-security Military, Logistics, Engineering & Technology collection is available here: https: //bookstore.gpo.gov/catalog/security-defense-law-enforcement/military-logistics-engineering-technology

Cyber Operations and the Use of Force in International Law

This book analyzes the legality of the use of force by the US, the UK and their NATO allies against

Afghanistan in 2001. The work challenges the main ground for resorting to force, namely, self-defence under Article 51 of the United Nations' Charter, by examining each element of Article 51 that ought to have been satisfied in order to legitimise the use of force. It also examines the wider context, including comparable Security Council resolutions in historic situations as well as modern instances where force has been used, such as against Iraq in 2003 and against Lebanon in 2006. As well as making the case against the legality of the use of force, the book addresses wider questions such as the meaning of 'terrorism' in international law, the changing nature of conflict in the twentieth and twenty-first centuries including the impact of non-state actors and an overview of terrorism trends as well as the evolution of limitations on the resort to force from the League of Nations through to 2001. The book concludes with some insight into the possible future implications for the use of force by states, particularly when force is purportedly justified on the grounds of self-defence.

The Law of Armed Conflict

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.

Striking Power

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

International Law and New Wars

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?

The Use of Force in International Law

Newly revised and expanded, The Law of Armed Conflict, 2nd edition introduces law students and undergraduates to the law of war in an age of terrorism. What law of armed conflict (LOAC), or its civilian counterpart, international humanitarian law (IHL), applies in a particular armed conflict? Are terrorists legally bound by that law? What constitutes a war crime? What (or who) is a lawful target and how are targeting decisions made? What are 'rules of

engagement' and who formulates them? How can an autonomous weapon system be bound by the law of armed conflict? Why were the Guantánamo military commissions a failure? This book takes students through these LOACIHL questions and more, employing real-world examples and legal opinions from the US and abroad. From Nuremberg to 9/11, from courts-martial to the US Supreme Court, from the nineteenth century to the twenty-first, the law of war is explained, interpreted, and applied.

Public International Law of Cyberspace

Philosophical and ethical discussions of warfare are often tied to emerging technologies and techniques. Today we are presented with what many believe is a radical shift in the nature of war-the realization of conflict in the cyber-realm, the so-called "fifth domain" of warfare. Does an aggressive act in the cyber-realm constitute an act of war? If so, what rules should govern such warfare? Are the standard theories of just war capable of analyzing and assessing this mode of conflict? These changing circumstances present us with a series of questions demanding serious attention. Is there such a thing as cyberwarfare? How do the existing rules of engagement and theories from the just war tradition apply to cyberwarfare? How should we assess a cyber-attack conducted by a state agency against private enterprise and vice versa? Furthermore, how should actors behave in the cyber-realm? Are there ethical norms that can be applied to the cyber-realm? Are the classic just war constraints of non-combatant

immunity and proportionality possible in this realm? Especially given the idea that events that are constrained within the cyber-realm do not directly physically harm anyone, what do traditional ethics of war conventions say about this new space? These questions strike at the very center of contemporary intellectual discussion over the ethics of war. In twelve original essays, plus a foreword from John Arquilla and an introduction, Binary Bullets: The Ethics of Cyberwarfare, engages these questions head on with contributions from the top scholars working in this field today.

Privatizing War

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

Cybersecurity Law

Originally presented as author's thesis (doctoral)--University of Hamburg, 2013.

Tallinn Manual on the International Law Applicable to Cyber Warfare

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.

Binary Bullets

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.

The authoritative manual on the applicable international law and best practice in the planning and conduct of peace operations.

Cyber Warfare and the Laws of War

Threats to international peace and security include the proliferation of weapons of mass destructions, rogue nations, and international terrorism. The United States must respond to these challenges to its national security and to world stability by embracing new military technologies such as drones, autonomous robots, and cyber weapons. These weapons can provide more precise, less destructive means to coerce opponents to stop WMD proliferation, clamp down on terrorism, or end humanitarian disasters. Efforts to constrain new military technologies are not only doomed, but dangerous. Most weapons in themselves are not good or evil; their morality turns on the motives and purposes for the war itself. These new weapons can send a strong message without cause death or severe personal injury, and as a result can make war less, rather than more, destructive.

The Conduct of Hostilities under the Law of International Armed Conflict

Cyber War

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

Cyberspace

This open access book provides a valuable restatement of the current law of armed conflict regarding hostilities in a diverse range of contexts: outer space, cyber operations, remote and autonomous weapons, undersea systems and devices, submarine cables, civilians participating in unmanned operations, military objectives by nature, civilian airliners, destruction of property, surrender, search and rescue, humanitarian assistance, cultural property, the natural environment, and more. The book was prepared by a group of experts after consultation with a number of key governments. It is intended to offer guidance for practitioners (mainly commanding officers); facilitate training at military colleges; and inform both instructors and graduate students of international law on the current state of the law.

Netherlands Yearbook of International Law 2016

'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.

The Law of Armed Conflict

This is the first book to examine cyber blockades, which are large-scale attacks on infrastructure or systems that prevent a state from accessing cyberspace, thus preventing the transmission (ingress/egress) of data. The attack can take place through digital, physical, and/or electromagnetic means, and it can be conducted by another state or a sub-state group. The purpose of this book is to understand how cyber blockades can shut down or otherwise render cyberspace useless for an entire country, and Russell also seeks to understand the implications of cyber blockades for international relations. A cyber blockade can be either a legitimate or illegitimate tool depending on the circumstances.

What is certain is that the state on the receiving end faces a serious threat to its political, military, economic, and social stability. The book includes two in-depth case studies of cyber blockades, Estonia in 2007 and Georgia in 2008, both of which suffered cyber attacks from Russia. Russell compares cyber blockades with those in other domains (sea, land, air, and space) and offers recommendations for policymakers and for further academic study.

Cyber Mercenaries

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.

Peacetime Regime for State Activities in

Cyberspace

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.

Deconstruction Machines

Wilhelm G. Grewe's "Epochen der Völkerrechtsgeschichte", published in 1984, is widely regarded as one of the classic twentieth century works of international law. This revised translation by Michael Byers of Duke University, Durham, North Carolina, makes this important book available to non-German readers for the first time. "The Epocs of International Law" provides a theoretical overview and detailed analysis of the history of international

law from the Middle Ages, to the Age of Discovery and the Thirty Years War, from Napoleon Bonaparte to the Treaty of Versailles, the Cold War and the Age of the Single Superpower, and does so in a way that reflects Grewe's own experience as one of Germany's leading diplomats and professors of international law. A new chapter, written by Wilhelm G. Grewe and Michael Byers, updates the book to October 1998, making the revised translation of interest to German international layers, international relations scholars and historians as well. Wilhelm G. Grewe was one of Germany's leading diplomats, serving as West German ambassador to Washington, Tokyo and NATO, and was a member of the International Court of Arbitration in The Hague. Subsequently professor of International Law at the University of Freiburg, he remains one of Germany's most famous academic lawyers. Wilhelm G. Grewe died in January 2000. Professor Dr. Michael Byers, Duke University, School of Law, Durham, North Carolina, formerly a Fellow of Jesus College, Oxford, and a visiting Fellow of the Max-Planck-Institute for Comparative Public Law and International Law, Heidelberg.

ROMANCE ACTION & ADVENTURE MYSTERY & THRILLER BIOGRAPHIES & HISTORY CHILDREN'S YOUNG ADULT FANTASY HISTORICAL FICTION HORROR LITERARY FICTION NON-FICTION SCIENCE FICTION