Tallinn Manual On The International Law Applicable To Cyber Warfare

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

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

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.

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.

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 Manual provides the most up-to-date restatement of existing international law applicable to the conduct of air and missile warfare.

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.

Frequent instances of intervention in current world affairs have threatened the status of nonintervention as a rule of international relations. Gathering evidence from history, law, sociology, and political science, R. J. Vincent concludes that the principle of nonintervention can and must remain viable. The author approaches the question from several angles, seeking to discover why the principle of nonintervention has been asserted as part of the law of nations; whether states in the past and present have conducted their foreign relations according to the principle of nonintervention; and what function the principle performs in the society formed between states. The author examines the principle of nonintervention through examples taken from contemporary world

politics, focusing on its role in the doctrine and practice of the Soviet Union, the United States, and the United Nations. He argues that, despite the erosion of the order of sovereign states, the arrival of nuclear response weapons, all-enveloping ideological conflict, and transnational relationships that diminish the significance of state frontiers, the principle of nonintervention continues to contribute to the international order. Originally published in 1974. The Princeton Legacy Library uses the latest print-on-demand technology to again make available previously out-of-print books from the distinguished backlist of Princeton University Press. These editions preserve the original texts of these important books while presenting them in durable paperback and hardcover editions. The goal of the Princeton Legacy Library is to vastly increase access to the rich scholarly heritage found in the thousands of books published by Princeton University Press since its founding in 1905.

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 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. 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 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.

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. 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 ofThe 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.

How control over information creation, processing, flows, and use has become the most effective form of power: theoretical foundations and empirical examples of information policy in the U.S., an innovator informational state. As the informational state replaces the bureaucratic welfare state, control over information creation, processing, flows, and use has become the most effective form of power. In Change of State Sandra Braman examines the theoretical and practical ramifications of this "change of state." She looks at the ways in which governments are deliberate, explicit, and consistent in their use of information policy to exercise power, exploring not only such familiar topics as intellectual property rights and privacy but also areas in which

policy is highly effective but little understood. Such lesser-known issues include hybrid citizenship, the use of "functionally equivalent borders" internally to allow exceptions to U.S. law, research funding, census methods, and network interconnection. Trends in information policy, argues Braman, both manifest and trigger change in the nature of governance itself.After laying the theoretical, conceptual, and historical foundations for understanding the informational state, Braman examines 20 information policy principles found in the U.S Constitution. She then explores the effects of U.S. information policy on the identity, structure, borders, and change processes of the state itself and on the individuals, communities, and organizations that make up the state. Looking across the breadth of the legal system, she presents current law as well as trends in and consequences of several information policy issues in each category affected. Change of State introduces information policy on two levels, coupling discussions of specific contemporary problems with more abstract analysis drawing on social theory and empirical research as well as law. Most important, the book provides a way of understanding how information policy brings about the fundamental social changes that come with the transformation to the informational state.

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 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.

Bowett, D.W.Self-Defence in International Law. New York: Praeger, [1958]. xv, 294 pp. Reprinted 2009 by The Lawbook Exchange, Ltd. ISBN-13: 978-1-58477-855-4. ISBN-10: 1-58477-855-5. Cloth. $95.* Bowett observes that the use or threat of force by any state can be a delict, an approved sanction, or a measure taken in self-defense. He examines the evolution of the doctrine in the nineteenth and early twentieth centuries, with the assumption of the existence of a

state's unlimited 'right' to go to war. He then attempts to outline the limited and provisional effects of this right under the U.N. Charter. "Throughout the work there is a refusal to dogmatize or to state in absolute terms any aspect of the 'privilege' of self-defence in its present context. (...) [Bowett] is to be congratulated on producing a timely and scholarly survey of one of the most fundamental, and often abused, sovereign rights known to international law.": K.R. Simmonds, British Year Book of International Law 34 (1958) 432.

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.

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

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?

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.

This book addresses the technological evolution of modern warfare due to unmanned systems and the growing capacity for cyberwarfare. The increasing involvement of unmanned means and methods of warfare can lead to a total removal of humans from the navigation, command and decision-making processes in the control of unmanned systems, and as such away from participation in hostilities – the “dehumanization of warfare.” This raises the question of whether and how today’s law is suitable for governing the dehumanization of warfare effectively. Which rules are relevant? Do interpretations of relevant rules need to be reviewed or is further and adapted regulation necessary? Moreover, ethical reasoning and computer science developments also have to be taken into account in identifying problems. Adopting an interdisciplinary approach the book focuses primarily on international humanitarian law, with related ethics and computer science aspects included in the discussion and the analysis.

Now in a comprehensively updated edition, this indispensable handbook analyzes how international humanitarian law has evolved in the face of these many new challenges. Central concerns include the war on terror, new forms of armed conflict and humanitarian action, the emergence of international criminal justice, and the reshaping of fundamental rules and consensus in a multipolar world. ThePractical Guide to Humanitarian Law provides the precise meaning and content for over 200 terms such as terrorism, refugee, genocide, armed conflict, protection, peacekeeping,

torture, and private military companies—words that the media has introduced into everyday conversation, yet whose legal and political meanings are often obscure. The Guide definitively explains the terms, concepts, and rules of humanitarian law in accessible and reader-friendly alphabetical entries. Written from the perspective of victims and those who provide assistance to them, the Guide outlines the dangers, spells out the law, and points the way toward dealing with violations of the law. Entries are complemented by analysis of the decisions of relevant courts; detailed bibliographic references; addresses, phone numbers, and Internet links to the organizations presented; a thematic index; and an up-to-date list of the status of ratification of more than thirty international conventions and treaties concerning humanitarian law, human rights, refugee law, and international criminal law. This unprecedented work is an invaluable reference for policy makers and opinion leaders, students, relief workers, and members of humanitarian organizations. Published in cooperation with Doctors Without Borders/Médecins Sans Frontières.

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.

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.

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

The 4th edition of Excessive Maritime Claims updates material on state practice of the law of the sea since

publication of the 3rd edition in 2012 and adds new material on islands and other maritime features.

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.

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.

Along with the rest of the U.S. government, the

Department of Defense (DoD) depends on cyberspace to function. DoD operates over 15,000 networks and seven million computing devices across hundreds of installations in dozens of countries around the globe. DoD uses cyberspace to enable its military, intelligence, and business operations, including the movement of personnel and material and the command and control of the full spectrum of military operations. The Department and the nation have vulnerabilities in cyberspace. Our reliance on cyberspace stands in stark contrast to the inadequacy of our cybersecurity -- the security of the technologies that we use each day. Moreover, the continuing growth of networked systems, devices, and platforms means that cyberspace is embedded into an increasing number of capabilities upon which DoD relies to complete its mission. Today, many foreign nations are working to exploit DoD unclassified and classified networks, and some foreign intelligence organizations have already acquired the capacity to disrupt elements of DoD's information infrastructure. Moreover, non-state actors increasingly threaten to penetrate and disrupt DoD networks and systems. DoD, working with its interagency and international partners, seeks to mitigate the risks posed to U.S. and allied cyberspace capabilities, while protecting and respecting the principles of privacy and civil liberties, free expression, and innovation that have made cyberspace an integral part of U.S. prosperity and security. How the Department leverages the opportunities of cyberspace, while managing inherent uncertainties and reducing vulnerabilities, will significantly impact U.S. defensive

readiness and national security for years to come.

Tallinn Manual 2.0 on the International Law Applicable to Cyber OperationsCambridge University Press

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

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.

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 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.