Cyber Warfare Military Cross Border Computer Network Operations Under International Law

cyber security in transportation sector autonomous vehicles autonomous weapons systems supply chain security military mobility cyber security aspects of 5G and next generation technologies military use of 5G and next generation technology automated operations privacy and human rights in autonomous systems collaboration and information sharing frameworks international organisations cooperation public private partnership in cyber defence artificial intelligence in military operations critical infrastructure protection (incl data diodes, IDS, industrial protocols and smart grids, 4G and 5G networks, traffic and transportation) strategic approaches to emerging and disruptive technologies ripple effect of nation specific approaches to sovereignty and international law crisis management and military civilian cooperation in cyberspace cross border dependencies, trans border access to data the changing role of states in cyberspace state led cyber opera

Just a sample of the contents ... contains over 2,800 total pages .... PROSPECTS FOR THE RULE OF LAW IN CYBERSPACE Cyberwarfare and Operational Art CYBER WARFARE GOVERNANCE: EVALUATION OF CURRENT INTERNATIONAL AGREEMENTS ON THE OFFENSIVE USE OF CYBER Cyber Attacks and the Legal Justification for an Armed Response UNTYING OUR HANDS: RECONSIDERING CYBER AS A SEPARATE INSTRUMENT OF NATIONAL POWER Effects-Based Operations in the Cyber Domain Recommendations for Model-Driven Paradigms for Integrated Approaches to Cyber Defense MILLENNIAL WARFARE IGNORING A REVOLUTION IN MILITARY AFFAIRS: THE NEED TO CREATE A SEPARATE BRANCH OF THE ARMED FORCES FOR CYBER WARFARE SPECIAL OPERATIONS AND CYBER WARFARE LESSONS FROM THE FRONT: A CASE STUDY OF RUSSIAN CYBER WARFARE ADAPTING UNCONVENTIONAL WARFARE DOCTRINE TO CYBERSPACE OPERATIONS: AN EXAMINATION OF HACKTIVIST BASED INSURGENCIES Addressing Human Factors Gaps in Cyber Defense Airpower History and the Cyber Force of the Future How Organization for the Cyber Domain Outpaced Strategic Thinking and Forgot the Lessons of the Past THE COMMAND OF THE TREND: SOCIAL MEDIA AS A WEAPON IN THE INFORMATION AGE SPYING FOR THE RIGHT REASONS: CONTESTED NORMS IN CYBERSPACE AIR FORCE CYBERWORX REPORT: REMODELING AIR FORCE CYBER COMMAND & CONTROL THE CYBER WAR: MAINTAINING AND CONTROLLING THE "KEY CYBER TERRAIN" OF THE CYBERSPACE DOMAIN WHEN NORMS FAIL: NORTH KOREA AND CYBER AS AN ELEMENT OF STATECRAFT AN ANTIFRAGILE APPROACH TO PREPARING FOR CYBER CONFLICT AIR FORCE CYBER MISSION ASSURANCE SOURCES OF MISSION UNCERTAINTY Concurrency Attacks and Defenses Cyber Workforce Retention Airpower Lessons for an Air Force Cyber-Power Targeting ¬Theory IS BRINGING BACK WARRANT OFFICERS THE ANSWER? A LOOK AT HOW THEY COULD WORK IN THE AIR FORCE CYBER OPERATIONS CAREER FIELD NEW TOOLS FOR A NEW TERRAIN AIR FORCE SUPPORT TO SPECIAL OPERATIONS IN THE CYBER ENVIRONMENT Learning to Mow Grass: IDF Adaptations to Hybrid Threats CHINA'S WAR BY OTHER MEANS: UNVEILING CHINA'S QUEST FOR INFORMATION DOMINANCE THE ISLAMIC STATE'S TACTICS IN SYRIA: ROLE OF SOCIAL MEDIA IN SHIFTING A PEACEFUL ARAB SPRING INTO TERRORISM NON-LETHAL WEAPONS: THE KEY TO A MORE AGGRESSIVE STRATEGY TO COMBAT TERRORISM THOUGHTS INVADE US: LEXICAL COGNITION AND CYBERSPACE The Cyber Threat to Military Just-In-Time Logistics: Risk Mitigation and the Return to Forward Basing PROSPECTS FOR THE RULE OF LAW IN CYBERSPACE Cyberwarfare and Operational Art CYBER WARFARE GOVERNANCE: EVALUATION OF CURRENT INTERNATIONAL AGREEMENTS ON THE OFFENSIVE USE OF CYBER Cyber Attacks and the Legal Justification for an Armed Response UNTYING OUR HANDS: RECONSIDERING CYBER AS A SEPARATE INSTRUMENT OF NATIONAL POWER Effects-Based Operations in the Cyber Domain Recommendations for Model-Driven Paradigms for Integrated Approaches to Cyber Defense MILLENNIAL WARFARE IGNORING A REVOLUTION IN MILITARY AFFAIRS: THE NEED TO CREATE A SEPARATE BRANCH OF THE ARMED FORCES FOR CYBER WARFARE SPECIAL OPERATIONS AND CYBER WARFARE LESSONS FROM THE FRONT: A CASE STUDY OF RUSSIAN CYBER WARFARE ADAPTING UNCONVENTIONAL WARFARE DOCTRINE TO CYBERSPACE OPERATIONS: AN EXAMINATION OF HACKTIVIST BASED INSURGENCIES Addressing Human Factors Gaps in Cyber Defense Airpower History and the Cyber Force of the Future How Organization for the Cyber Domain Outpaced Strategic Thinking and Forgot the Lessons of the Past THE COMMAND OF THE TREND: SOCIAL MEDIA AS A WEAPON IN THE INFORMATION AGE SPYING FOR THE RIGHT REASONS: CONTESTED NORMS IN CYBERSPACE AIR FORCE CYBERWORX REPORT: REMODELING AIR FORCE CYBER COMMAND & CONTROL THE CYBER WAR: MAINTAINING AND CONTROLLING THE "KEY CYBER TERRAIN" OF THE CYBERSPACE DOMAIN WHEN NORMS FAIL: NORTH KOREA AND CYBER AS AN ELEMENT OF STATECRAFT AN ANTIFRAGILE APPROACH TO PREPARING FOR CYBER CONFLICT AIR FORCE CYBER MISSION ASSURANCE SOURCES OF MISSION UNCERTAINTY Concurrency Attacks and Defenses Cyber Workforce Retention

This book challenges the traditional approach to international law by concentrating on international hThis book challenges the traditional approach to international law by concentrating on international humanitarian law and placing the focus beyond States: it reflects on current legal, policy and practical issues that concern non-State actors in and around situations of armed conflict. With the emergence of the nation-State, international law was almost entirely focused on inter-State relations, thus excluding - for the most part - non-State entities. In the modern era, such a focus needs to be adjusted, in order to encompass the various types of functions and interactions that those entities perform throughout numerous international decision-making processes. The contributions that comprise this volume are oriented towards a broad readership audience in the academic and professional fields related to international humanitarian law, international criminal law, international human rights law and general public international law. Ezequiel Heffes, LLM, is a Thematic Legal Adviser in the Policy and Legal Unit at Geneva Call in Geneva, Switzerland, Marcos D. Kotlik, LLM, is Academic Coordinator at the Observatory of International Humanitarian Law of the University of Buenos Aires, School of Law and was a Judicial Fellow at the International Court of Justice between 2018-2019, and Manuel J. Ventura, LLM (Hons), is an Associate Legal Officer in the Office of the Prosecutor at the International Residual Mechanism for Criminal Tribunals, an Adjunct Fellow at the School of Law at Western Sydney University, and a Director of The Peace and Justice Initiative.

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

Key Legal Considerations for the Aviation and Space Sectors

The International Law of Economic Warfare

The Law of Armed Conflict and the Dynamics of Modern Warfare

Public International Law of Cyberspace
Not War, Not Peace?

The conduct of warfare is constantly shaped by new forces that create complexities in the battlespace for military operations. As the nature of how and where wars are fought changes, new challenges to the application of the extant body of international law that regulates armed conflicts arise. This inaugural volume of the Lieber Studies Series seeks to address several issues in the confluence of law and armed conflict, with the primary goal of providing the reader with both academic and practitioner perspectives. Featuring chapters from world class scholars, policymakers and other government officials; military and civilian legal practitioners; and other thought leaders, together they examine the role of the law of armed conflict in current and future armed conflicts around the world. Complex Battlespaces also explores several examples of battlespace dynamics through four "lenses of complexity": complexity in legal regimes, governance, technology, and the urbanization of the battlefield.

The role of international organisations, states and non state actors in cyber security and the changing role of states in cyberspace Norms and standards to enhance security in cyberspace Frameworks for collaboration and information sharing Cross border dependencies, trans border access to data Military doctrine development, cyberspace as a domain of warfare Critical information infrastructure and supply chain security Cyber security aspects of 5G technologies and military use of 5G technology Crisis management and military civilian cooperation in cyberspace State led cyber operations, offensive defensive aspects Use of AI technology in state led cyber operations and or in crisis management Malign information campaigns in and through cyberspace Online education and new technologies for cyber exercises and cyber ranges Remote work and its cyber security implications International law responses to crisis situations Electronic surveillance in crisis management

This definitive reference resource on cyber warfare covers all aspects of this headline topic, providing historical context of cyber warfare and an examination its rapid development into a potent technological weapon of the 21st century. • Provides comprehensive coverage of the major individuals, organizations, impacts, and issues related to cyber warfare that enables readers to better understanding of the impact of cyber warfare on modern conflicts • Includes a detailed chronology that documents the evolution and use of cyber warfare over the past few decades • Supplies further readings and a lengthy bibliography that offer a wealth of options to students conducting extensive research on the subject

Cyber WarfareMilitary Cross-Border CCyber WarfareMilitary Cross-border Computer Network Operations Under International Law

Expert Laws of War

Encyclopedia of Cyber Warfare

When the Lights Go Out -- Nation at Risk

Motivating Pakistan to Prevent Cross-Border Terrorism

Research Handbook on International Law and Cyberspace

Cybersecurity

Cyberspace, where information--and hence serious value--is stored and manipulated, is a tempting target. An attacker could be a person, group, or state and may disrupt or corrupt the systems from which cyberspace is built. When states are involved, it is tempting to compare fights to warfare, but there are important differences. The author addresses these differences and ways the United States protect itself in the face of attack.

"What, exactly, is 'National Cyber Security'? The rise of cyberspace as a field of human endeavour is probably nothing less than one of the most significant developments in world history. Cyberspace already directly impacts every facet of human existence including economic, social, cultural and political developments, and the rate of change is not likely to stop anytime soon. However, the socio-political answers to the questions posed by the rise of cyberspace often significantly lag behind the rate of technological change. One of the fields most challenged by this development is that of 'national security'. The National Cyber Security Framework Manual provides detailed background information and in-depth theoretical frameworks to help the reader understand the various facets of National Cyber Security, according to different levels of public policy formulation. The four levels of government--political, strategic, operational and tactical/technical--each have their own perspectives on National Cyber Security, and each is addressed in individual sections within the Manual. Additionally, the Manual gives examples of relevant institutions in National Cyber Security, from top-level policy coordination bodies down to cyber crisis management structures and similar institutions."--Page 4 of cover.

The ever-increasing use of technology is challenging the current status of the law, bringing about new problems and questions. The book addresses this trend from the perspective of International law and European Union law and is divided into three main thematic sections. The first section focuses on the legal implications of the use of technology either for law enforcement purposes or in the context of military activities, and examines how this use adds a new dimension to perennial issues, such as the uneasy balance between security concerns and the protection of individual rights, and defining the exact scope of certain State obligations. In so doing, it takes into account a range of current and potential scenarios at the international, regional and domestic level, including the use of killer robots, databases, drones and technology in general to patrol borders, exchange information on criminal suspects, maintain public order, target suspected terrorists and conduct military activities. In turn, the second section examines the role of institutional and non-institutional actors in establishing

substantive normative standards for the use of high-tech applications. In this respect, it focuses both on the role that European courts have played so far, and on how other actors' initiatives can contribute to the construction of a new legal framework for technology-related activities. Lastly, the third section has a two-fold focus: the first part investigates how the increasing reliance on technology is affecting traditional rules on international responsibility, and is challenging, in particular, the attribution of wrongful conduct to States and international organizations. The second part addresses issues of jurisdiction and justiciability. Given the scope of its coverage, this timely book addresses an important lacuna in the current legal scholarship, exploring some of the most recent applications of technology and the legal issues arising as a result. Readers will gain novel insights into the challenges posed to International law and European law by the growing reliance on technology, taking into account both its uses and misuses.

At no time since the end of the Cold War has interest been higher in Russian security issues and the role played in this by the modernization of Russia's Armed Forces. The continued transformation of its Armed Forces from Cold War legacy towards a modern combat capable force presents many challenges for the Kremlin. Moscow's security concerns domestically, in the turbulent North Caucasus, and internationally linked to the Arab Spring, as well as its complex relations with the US and NATO and its role in the aftermath of the Maidan Revolution in Ukraine in 2014 further raises the need to present an informed analytical survey of the country's military, past, present and future. This collection addresses precisely the nature of the challenges facing Russian policymakers as they struggle to rebuild combat capable military to protect Russian interests in the twenty-first century. This book was based on a special issue of the Journal of Slavic Military Studies.

Conflict in the 21st Century: The Impact of Cyber Warfare, Social Media, and Technology

The Prohibition on the Use of Force in Contemporary International Law

International Law As We Know It

Military Cross-Border C

Law and Ethics for Virtual Conflicts

Self-Defence, Countermeasures, Necessity, and the Question of Attribution

The practice of armed conflict has changed radically in the last decade. With eminent contributors from legal, government and military backgrounds, this Research Handbook addresses the legal implications of remote warfare and its significance for combatants, civilians, policymakers and international lawyers.

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

This book focuses on the PRC ' s cross-border data transfer legislation in recent years, as well as the implications for international trade law. The book addresses the convergence of industries and technologies notably caused by digitization; the issue of conflicts between goods and services; and the General Agreement on Tariffs and Trade (GATT) and General Agreement on Trade in Services (GATS) as well as the difficulty of classifying service sectors under WTO members ' commitments. The book also examines the FTAs that entered into force after 2012 that regulate digital trade beyond the venue of the WTO and analyzes their rules of relevance for cross-border data flows and international trade. It asks whether and how these FTAs have deliberately reacted to the increasing importance of data flows as well as to the trouble of governing them in the context of global governance

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.

Cyber War

Twenty Lost Years

National cyber security : framework manual

Tallinn Manual on the International Law Applicable to Cyber Warfare

2021 13th International Conference on Cyber Conflict (CyCon)

Senior Leadership Roundtable on Military and Defence Aspects of Border Security in South East Europe

Cyberspace governance Norms and standards to enhance security in cyberspace The role of international organisations, states and non state actors in cyber security The new generation of national cyber security strategies The changing role of states in cyberspace Frameworks for collaboration and information sharing Cross border dependencies, trans border access to data The nature of current and future cyber attacks Cyber capabilities, forces and weapons State sponsored operations in cyberspace (incl APTs and proxy actors) Military doctrine development, cyberspace as a domain of warfare Offence, defence and deterrence in cyberspace active responsive cyber defence Attack and defence of military systems Autonomous cyber weapon systems Cyber terrorism The evolution of the Internet of Things and its implications Vulnerability disclosure Cyber physical systems security Critical infrastructure protection (incl data diodes, IDS, industrial protocols

The region of South East Europe (SEE), which is home to both NATO and Partnership for Peace (PfP) countries, serves as an important corridor between Europe and the Middle East, North Africa, and the Caucasus. In recent years, however, SEE has also experienced high levels of cross-border, military and defense-related challenges in the form of migration, smuggling, terrorism, and cyber threats. Furthermore, the use of the new information environment (IE) to further extremism in SEE and elsewhere in NATO and PfP countries has had far-reaching command and control (C2) implications for the Alliance. A collaborative interdisciplinary, international and regional approach is clearly needed to adequately assess and address these hybrid threats. This book presents papers delivered at the NATO Science for Peace and Security

(SPS) event: “Senior Leadership Roundtable on Military and Defense Aspects of Border Security in South East Europe”, held in Berovo, the Former Yugoslav Republic of Macedonia* from 23-30 September 2017. The aim of this special SPS grant was to maximize opportunities for extensive dialogue and collaboration between senior regional members, and the almost 70 distinguished academic and legal experts, as well as current or former senior-level practitioners from various governments, NATO bodies, and international organization that participated. It was the first SPS event of its kind in SEE as well as the first NATO SPS grant to be co-executed by the U.S. Department of Defense via the U.S. National Defense University. Other co-organizers were the C4I and Cyber Center of Excellence at George Mason University and PfP partner institution, the General Mihailo Apostolski Military Academy – Skopje, Associate Member of the University of Goce Del č ev – Stip. The book is divided into five parts: global trends, defining the problem, policy and academic solutions, national and regional case studies, and technological solutions. It will prove an invaluable source of reference for all those with an interest in the SEE region as well as cross-border hybrid threats, in general. * Turkey recognizes the Republic of Macedonia with its constitutional name.

Cybersecurity Key Legal Considerations for the Aviation and Space Sectors Federico Bergamasco, Roberto Cassar, Rada Popova & Benjamyn I. Scott As the aviation and space sectors become ever more connected to cyberspace and reliant on related technology, they become more vulnerable to potential cyberattacks. As a result, cybersecurity is a growing concern that all stakeholders in both sectors must consider. In this forward-looking book, which is the first comprehensive analysis of the relevant facets of cybersecurity in the aviation and space sectors, the authors explore the vast spectrum of relevant international and European Union (EU) law, with specific attention to associated risks, existing legal provisions and the potential development of new rules. Beginning with an overview of the different types of malicious cyber operations, the book proceeds to set the terminological landscape relevant to its core theme. It takes a top-down approach by first analysing general international and EU law related to cybersecurity, then moving to the more specific aspects of the aviation and space sectors, including telecommunications. Finally, the salient features of these analyses are combined with the practical realities in the relevant industries, giving due regard to legal and regulatory initiatives, industry standards and best practices. The broad range of issues and topics covered includes the following and more: whether the various facets of the international law on conflict apply in cyberspace and to cyberattacks; substantial policy and regulatory developments taking place at the EU level, including the activities of its relevant institutions, bodies and entities; jurisdiction and attributability issues relevant to cybersecurity in the aviation and space sectors; vulnerability of space systems, including large constellations, to malicious cyber activities and electromagnetic interference; various challenges for critical infrastructure resulting from, e.g., its interdependency, cross-border nature, public-private ownership and dual civil-military uses; safety and security in international air transportation, with special attention to the Chicago Convention and its Annexes; aviation liability and compensation in cases of cyberattacks, and insurance coverage against cyber risks; review of malicious relevant actors, malicious cyber operations, the typical life cycle of a cyberattack and industry responses. This book clearly responds to the need to elaborate adequate legal rules for ensuring that the multiple inlets for malicious cyber operations and the management of cybersecurity risks are addressed appropriately. It will be welcomed by all parties involved with aviation and space law and policy, including lawyers, governments, regulators, academics, manufacturers, operators, airports, and international governmental and non-governmental organisations.

This reference work examines how sophisticated cyber-attacks and innovative use of social media have changed conflict in the digital realm, while new military technologies such as drones and robotic weaponry continue to have an impact on modern warfare. • Provides fascinating information about cyber weapons that effectively strike through cyberspace to weaken and even cripple its target • Demonstrates how social media is employed in conflicts in innovative ways, including communication, propaganda, and psychological warfare • Explores potential technology avenues related to ensuring the continued military advantages of the United States • Identifies and describes nuclear, precision, and other technological capabilities that have historically been the preserve of superpowers but have been newly acquired by various states

Cross-Border Data Transfers Regulations in the Context of International Trade Law: A PRC Perspective

Understanding Information Security Investigations

Military Thought

2020 12th International Conference on Cyber Conflict (CyCon)

The Law Against War

Cyber Operations and International Law

With over 140 countries fielding nation-state and rouge malious cyber hacking capabilities, it is critical that we are aware of threats and vulnerabilities. Adm. Michael Rogers, director of the National Security Agency warned Congress regarding cyber attacks, "It's only a matter of the 'when, ' not the 'if, ' that we are going to see something dramatic." Cyber Blackout is a warning. It is a chronicle of the cyber threats of which we find ourselves at risk every day. Our power supply is vulnerable. Our food supply. Even the basics of communication. Every facet of our national security is vulnerable to cyber threats, and we are not prepared to defend them all. Cyber Blackout explains how these threats have been building since the Cold War, how they affect us now, and how they are changing the concepts of war and peace as we know them. It is essential knowledge for anyone wishing to understand safety and security in the age of the fifth domain....

The product of a three-year project by twenty renowned international law scholars and practitioners, the Tallinn Manual identifies the international law applicable to cyber warfare and sets out ninety-five 'black-letter rules' governing such conflicts. It addresses topics including sovereignty, State responsibility, the jus ad bellum, international humanitarian law, and the law of neutrality. An extensive commentary accompanies each rule, which sets forth the rule's basis in treaty and customary law, explains how the group of experts interpreted applicable norms in the cyber context, and outlines any disagreements within the group as to each rule's application.

Praise for previous edition: “ ...a comprehensive, meticulously-researched study of contemporary international law governing the use of armed force in international relations...' Andrew Garwood-Gowers, Queensland University of Technology Law Review, Volume 12(2) When this first English language edition of The Law Against War published it quickly established itself as a classic. Detailed, analytically rigorous and comprehensive, it provided an indispensable guide to the legal framework regulating the use of force. Now a decade on the much anticipated new edition brings the work up to date. It looks at new precedents arising from the Arab Spring; the struggle against the "Islamic State" in Iraq and Syria; and the conflicts in Ukraine and Yemen. It also reflects the new doctrinal debates surrounding recent state practice. Previous positions are reconsidered and in some cases revised, notably the question of consensual intervention and the very definition of force, particularly, to accommodate targeted extrajudicial executions and cyber-operations. Finally, the new edition provides detailed coverage of the concept of self-defense, reflecting recent interpretations of the International Court of Justice and the ongoing controversies surrounding its definition and interpretation.

This fourteenth volume of India ’s National Security Annual Review intensively analyses India ’s national security with respect to the changing internal and external dynamics. In the global environment, the situation is characterised by rising tensions between United States and Russia, intensified rivalry between United States (US) and China, and increasing cooperation between China and Russia. For India which seeks peaceful growth to emerge as a major power, this poses severe diplomatic challenges. This volume discusses the complexity of

these challenges and the deftness with which India gets the best out of its strategic partnerships with the US and Russia while warding off the transgressions of a mighty adversary like China. It also studies the impact of internal convulsions and external intrusions on India ' s security from South Asian nations such as Afghanistan, Bangladesh, Nepal and Sri Lanka. Examining the field of internal security, the essays carry rare insights into the causes of expansion of Naxalite violence in tribal areas and the dynamics of conflict resolution in the Northeast, as well as India ' s deep concern as a growing power with its economic slowdown in the recent past, and energy and cyber security. Bringing together contributions from eminent scholars and diplomats, the volume will be indispensable for policymakers, government think tanks, defence and strategic studies experts, as well as students and researchers of international relations, foreign policy and political science.

Contemporary Challenges in International and European Law

Restating and Making Law in Expert Processes

Use and Misuse of New Technologies

Annual Review 2014

Routledge Handbook of International Cybersecurity

Unilateral Remedies to Cyber Operations

This revised and expanded edition of the Research Handbook on International Law and Cyberspace brings together leading scholars and practitioners to examine how international legal rules, concepts and principles apply to cyberspace and the activities occurring within it. In doing so, contributors highlight the difficulties in applying international law to cyberspace, assess the regulatory efficacy of these rules and, where necessary, suggest adjustments and revisions.

The future global environment will still continue to have uncertainty, challenges, and threats to the vital and important interests of the United States. Regional dangers will still be faced with possible large-scale, cross border, attacks against the allies of the United States by hostile states with considerable conventional military power. Additionally, military forces will be required for numerous military operations other than war. The "Total Army" must be prepared for what will happen between now and 2015 with the best forces available in a fiscally constraint world. This document provides a proposal for restructuring the United States Army National Guard Enhanced Brigades for the Future 2010-2015 and beyond. The Force XXI designs and the Army After Next plans for the future fight are of great concern for our leaders. The Reserve Components must also be prepared for the future.

In the last five years the topic of cyber warfare has received much attention due to several so-called "cyber incidents" which have been qualified by many as State-sponsored cyber attacks. This book identifies rules and limits of cross-border computer network operations for which States bear the international responsibility during both peace and war. It consequently addresses questions on jus ad bellum and jus in bello in addition to State responsibility. By reference to treaty and customary international law, actual case studies (Estonia, Georgia, Stuxnet) and the Tallinn Manual, the author illustrates the applicability of current international law and argues for an obligation on the State to prevent malicious operations emanating from networks within their jurisdiction.This book is written for academics in public international law and practitioners from the military and other public security sectors

What people are saying about Inside Cyber Warfare "The necessary handbook for the 21st century." --Lewis Shepherd, Chief Tech Officer and Senior Fellow, Microsoft Institute for Advanced Technology in Governments "A must-read for policy makers and leaders who need to understand the big-picture landscape of cyber war." --Jim Stogdill, CTO, Mission Services Accenture You may have heard about "cyber warfare" in the news, but do you really know what it is? This book provides fascinating and disturbing details on how nations, groups, and individuals throughout the world are using the Internet as an attack platform to gain military, political, and economic advantages over their adversaries. You'll learn how sophisticated hackers working on behalf of states or organized crime patiently play a high-stakes game that could target anyone, regardless of affiliation or nationality. Inside Cyber Warfare goes beyond the headlines of attention-grabbing DDoS attacks and takes a deep look inside multiple cyber-conflicts that occurred from 2002 through summer 2009. Learn how cyber attacks are waged in open conflicts, including recent hostilities between Russia and Georgia, and Israel and Palestine Discover why Twitter, Facebook, LiveJournal, Vkontakte, and other sites on the social web are mined by the intelligence services of many nations Read about China's commitment to penetrate the networks of its technologically superior adversaries as a matter of national survival Find out why many attacks originate from servers in the United States, and who's responsible Learn how hackers are "weaponizing" malware to attack vulnerabilities at the application level

The Transformation of Russia's Armed Forces

Studies Combined: Cyber Warfare In Cyberspace - National Defense, Workforce And Legal Issues

Military Cross-border Computer Network Operations Under International Law

Inside Cyber Warfare

Mapping the Cyber Underworld

Cyberdeterrence and Cyberwar

Addressing both scholars of international law and political science as well as decision makers involved in cybersecurity policy, the book tackles the most important and intricate legal issues that a State faces when considering a reaction to a malicious cyber operation conducted by an adversarial State. While often invoked in political debates and widely analysed in international legal scholarship, self-defence and countermeasures will often remain unavailable to states in situations of cyber emergency due to the pervasive problem of reliable and timely attribution of cyber operations to State actors. Analysing the legal questions surrounding attribution in detail, the book presents the necessity defence as an evidently available alternative. However, the shortcomings of the doctrine as based in customary international law that render it problematic as a remedy for states are examined in-depth. In light of this, the book concludes by outlining a special emergency regime for cyberspace.

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'.

Cyberforensics is a fairly new word in the technology our industry, but one that n- ertheless has immediately recognizable meaning. Although the word forensics may have its origins in formal debates using evidence, it is now most closely associated with investigation into evidence of crime. As the word cyber has become synonymous with the use of electronic technology, the word cyberforensics bears no mystery. It immediately conveys a serious and concentrated endeavor to identify the evidence of crimes or other attacks committed in cyberspace. Nevertheless, the full implications of the word are less well understood. Cyberforensic activities remain a mystery to most people, even those fully immersed in the design and operation of cyber te- nology. This book sheds light on those activities in a way that is comprehensible not only to technology professionals but also to the technology hobbyist and those simply curious about the ?eld. When I started contributing to the ?eld of cybersecurity, it was an obscure ?eld, rarely mentioned in the mainstream media. According to the FBI, by 2009 organized crime syndicates were making more money via cybercrime than in drug traf?- ing. In spite of the rise in cybercrime and the advance of sophisticated threat actors online, the cyber security profession continues to lag behind in its ability to inves- gate cybercrime and understand the root causes of cyber attacks. In the late 1990s I worked to respond to sophisticated attacks as part of the U. S.

Terrorism: Commentary on Security Documents is a series that provides primary source documents and expert commentary on various topics relating to the worldwide effort to combat terrorism, as well as efforts by the United States and other nations to protect their national security interests. Volume 140, The Cyber Threat considers U.S. policy in relation to cybersecurity and cyberterrorism, and examines opposing views on cybersecurity and international law by nations such as Russia and China. The documents in this volume include testimony of FBI officials before Congressional committees, as well as detailed reports from the Strategic Studies Institute/U.S. Army War College Press and from the Congressional Research Service. The detailed studies in this volume tackling the core issues of cybersecurity and cyberterrorism include: Legality in Cyberspace; An Adversary View and Distinguishing Acts of War in Cyberspace; and Assessment Criteria, Policy Considerations, and Response Implications.

2022 14th International Conference on Cyber Conflict Keep Moving (CyCon)

Cyberwar Discourse and the Construction of Knowledge in International Legal Scholarship

CyberForensics

Research Handbook on Remote Warfare

International Humanitarian Law and Non-State Actors

Cyber Warfare

The Mumbai blasts of 1993, the attack on the Indian Parliament in 2001, Mumbai 26/11—cross-border terrorism has continued unabated. What can India do to motivate Pakistan to do more to prevent such attacks? In the nuclear times that we live in, where a military counter-attack could escalate to destruction beyond imagination, overt warfare is clearly not an option. But since outright peace-making seems similarly infeasible, what combination of coercive pressure and bargaining could lead to peace? The authors provide, for the first time, a comprehensive assessment of the violent and non-violent options available to India for compelling Pakistan to take concrete steps towards curbing terrorism originating in its homeland. They draw on extensive interviews with senior Indian and Pakistani officials, in service and retired, to explore the challenges involved in compellence and to show how non-violent coercion combined with clarity on the economic, social and reputational costs of terrorism can better motivate Pakistan to pacify groups involved in cross-border terrorism. Not War, Not Peace? goes beyond the much discussed theories of nuclear deterrence and counterterrorism strategy to explore a new approach to resolving old conflicts.

Explores the role of international legal scholars in the construction of legal knowledge, looking at examples from the cyberwar debate.

The Routledge Handbook of International Cybersecurity examines the development and use of information and communication technologies (ICTs) from the perspective of international peace and security. Acknowledging that the very notion of peace and security has become more complex, the volume seeks to determine which questions of cybersecurity are indeed of relevance for international peace and security and which, while requiring international attention, are simply issues of contemporary governance or development. The Handbook offers a variety of thematic, regional and disciplinary perspectives on the question of international cybersecurity, and the chapters contextualize cybersecurity in the broader contestation over the world order, international law, conflict, human rights, governance and development. The volume is split into four thematic sections: Concepts and frameworks; Challenges to secure and peaceful cyberspace; National and regional perspectives on cybersecurity; Global approaches to cybersecurity. This book will be of much interest to students of cybersecurity, computer science, sociology, international law, defence studies and International Relations in general.

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 analyses 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.

Complex Battlespaces

Military Cross-Border Computer Network Operations Under International Law

The Cyber Threat

Chinese Military Operations in Regional and Global Context

Debates, Law and Practice

United States Army National Guard Enhanced Brigades in the Future

Since the prohibition of the threat or use of force and the resurgence of (economic) nationalism, economic warfare has become an increasingly important substitute for actual hostilities between states. Its manifestations range from medieval sieges to modern day trade wars. Despite its long history, economic warfare remains an elusive term, foreign to international law. This book seeks to identify those portions of international law that are applicable to economic warfare. What is the status quo of regulation? Is there a jus ad bellum oeconomicum? A jus in bello oeconomico? After putting forward its own definition of economic warfare, the book reviews historical case studies – reflecting the three main branches of international economic law: trade, investment and currency – to identify pertinent legal boundaries. While the case studies reveal that numerous rules of international (economic) law regulate (specific measures of) economic warfare, it remains to be seen whether – analogously to the prohibition of the threat or use of force – these selective limitations have the potential to coalesce into a general prohibition of economic warfare in the future.

Cyber Blackout

The PLA Beyond Borders

ICCWS 2017 12th International Conference on Cyber Warfare and Security

India’s National Security