Cyber War Law And Ethics For Virtual Conflicts

Tallinn Manual on the International Law Applicable to Cyber WarfareDefending HumanityCybersecurity EthicsSoft WarConflict in Cyber SpaceCyberethicsTechnology, Ethics and the Protocols of Modern WarThe Basics of Cyber WarfareBinary BulletsMilitary EthicsCyber WarUnderstanding Cyber WarfareCyber Warfare and the Laws of WarCyber WarfareEthics and Policies for Cyber OperationsCybersecurityWar and Political TheoryCyber-Attacks and the Exploitable Imperfections of International LawStrategic Cyber SecurityThe Ethics of Information WarfareCyberdeterrence and CyberwarCyber WarfareCyber WarRoutledge Handbook of Ethics and WarThe Ethics of Cyber Conflicts: An IntroductionDehumanization of WarfareCyberwarfareCyber Warfare – Truth, Tactics, and StrategiesThe Ethics of CybersecurityConfronting Cyberespionage Under International LawCyber War Will Not Take PlaceCyberwarA Better State of WarResearch Handbook on International Law and CyberspaceConflict and Cooperation in CyberspaceEthics and Cyber WarfareInvestigating Cyber Law and Cyber Ethics: Issues, Impacts and PracticesTechnology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack CapabilitiesCybersecurity LawTallinn Manual 2.0 on the International Law Applicable to Cyber Operations

Tallinn Manual on the International Law Applicable to Cyber

Warfare

"Imagine a strategy memo forecasting cyberattacks by Russian hackers, trolls, and bots designed to roil social discontent and damage the electoral prospects of a major party US presidential nominee, or, if she winds up winning, to sabotage her ability to govern by seeding allegations of Democratic voter fraud. Guaranteed payoff. No fingerprints. No keystroke record. No contrails in the cloud. To ensure that Americans would believe that disparaging messages about her were made in the US, use bitcoin to buy space and set up virtual private networks (VPNs) on American servers. Distribute hacked content stolen from the accounts of her staff and associates through an intermediary, WikiLeaks. Use identity theft, stolen Social Security numbers, and appropriated IDs to circumvent Facebook and PayPal's demand for actual names, birth dates, and addresses. On platforms such as Instagram and Twitter, register under assumed names. Diffuse and amplify your attack and advocacy through posts on Facebook, tweets and retweets on Twitter, videos on YouTube, reporting and commentary on RT, blogging on Tumblr, news sharing on Reddit, and viral memes and jokes on 9GAG. Add to the mix a video game called Hilltendo in which a missile-straddling Clinton figure vaporizes classified emails sought by the FBI. Employ "online agitators" and bots to upvote posts from imposter websites such as BlackMattersUS.com to the top of such subreddits as r/The_Donald and r/HillaryForPrison. Drive content to trend. To maximize the impact of your handiwork, use data analytics and search-engine

maximization tools built into the social media platforms. To test and fuel doubts about the security of US voter information, hack the election systems of states. And, throughout the primary and general election season, insinuate the notion that if Hillary Clinton were to win, she would have done so by rigging the election, an outcome that would repay her assaults on the legitimacy of their leader's presidency with doubts about her own. Were she instead to lose, she would no longer be a thistle in the toned torso of the hackers and trolls' boss's likely boss. Every result but one produces desirable results for the Kremlin. Outcome one: Clinton is off the international stage. Outcome two: she wins but can't govern effectively. Outcome three: the former Secretary of State is elected and the country simply moves on, but the sabotage nonetheless has magnified cultural tensions and functioned as a pilot from which to birth later success - perhaps when she runs for a second term. The only eventuality that damages the Russian cybersoldiers and their commander-in-chief is the fourth in which, in real time, the cyberattackers are unmasked by a vigilant intelligence community, condemned by those in both major political parties and around the world, characterized by the media as spies and saboteurs, the Russian messaging is blocked or labeled as Russian propaganda, and, when included in media accounts, the stolen content is relentlessly tied to its Russian origins and sources. None of that happened. Instead, to the surprise of the Russian masterminds as well as both Hillary Clinton and Donald Trump, he won the Electoral College and with it a four-year claim on 1600 Pennsylvania Avenue. Although countrywide she bested him by almost 2.9 million

votes, he unexpectedly captured an Electoral College majority by running the table. By the end of the evening of November 8, Florida as well as Wisconsin, Michigan, and Pennsylvania were in his column. The ways in which Russian hacking and social media messaging altered the content of the electoral dialogue and contributed to Donald Trump's victory are the subjects of this book. To begin my exploration, this overview chapter will highlight key findings of the US intelligence community; preview my focus on the hackers and trolls and the synergies between them; justify casting the Russian machinations as acts of cyberwar; outline ways in which susceptibilities in our system of government and media structures magnified their effects; and note five presuppositions that will shape my analysis of the Russian trolls' work and one that will guide my study of the effects of the hackers."--

Defending Humanity

Part of the Jones & Bartlett Learning Information Systems Security & Assurance Series Cyberwarfare puts students on the real-world battlefield of cyberspace! Students will learn the history of cyberwarfare, techniques used in both offensive and defensive information warfare, and how cyberwarfare is shaping military doctrine. Written by subject matter experts, this book combines accessible explanations with realistic experiences and case studies that make cyberwar evident and understandable. Key Features: - Incorporates hands-on activities,

relevant examples, and realistic exercises to prepare readers for their future careers. - Includes detailed case studies drawn from actual cyberwarfare operations and tactics. - Provides fresh capabilities information drawn from the Snowden NSA leaks

Cybersecurity Ethics

Contemporary security has expanded its meaning, content and structure in response to globalisation and the emergence of greatly improved world-wide communication. The protocols of modern warfare, including targeted killing, enhanced interrogations, mass electronic surveillance and the virtualisation of war have changed the moral landscape and brought diverse new interactions with politics, law, religion, ethics and technology. This book addresses how and why the nature of security has changed and what this means for the security actors involved and the wider society. Offering a crossdisciplinary perspective on concepts, meanings and categories of security, the book brings together scholars and experts from a range of disciplines including political, military studies and security studies, political economy and international relations. Contributors reflect upon new communication methods, postmodern concepts of warfare, technological determinants and cultural preferences to provide new theoretical and analytical insights into a changing security environment and the protocols of war in the 21st century. A useful text for scholars and students of security studies, international

relations, global governance, international law and ethics, foreign policy, comparative studies and contemporary world history.

Soft War

This book offers an overview of the ethical problems posed by Information Warfare, and of the different approaches and methods used to solve them, in order to provide the reader with a better grasp of the ethical conundrums posed by this new form of warfare. The volume is divided into three parts, each comprising four chapters. The first part focuses on issues pertaining to the concept of Information Warfare and the clarifications that need to be made in order to address its ethical implications. The second part collects contributions focusing on Just War Theory and its application to the case of Information Warfare. The third part adopts alternative approaches to Just War Theory for analysing the ethical implications of this phenomenon. Finally, an afterword by Neelie Kroes - Vice President of the European Commission and European Digital Agenda Commissioner - concludes the volume. Her contribution describes the interests and commitments of the European Digital Agenda with respect to research for the development and deployment of robots in various circumstances, including warfare.

Conflict in Cyber Space

This textbook offers an accessible introduction to the historical, technical, and strategic context of cyber conflict. The international relations, policy, doctrine, strategy, and operational issues associated with computer network attack, computer network exploitation, and computer network defense are collectively referred to as cyber warfare. This new textbook provides students with a comprehensive perspective on the technical, strategic, and policy issues associated with cyber conflict as well as an introduction to key state and non-state actors. Specifically, the book provides a comprehensive overview of these key issue areas: the historical emergence and evolution of cyber warfare, including the basic characteristics and methods of computer network attack, exploitation, and defense; a theoretical set of perspectives on conflict in the digital age from the point of view of international relations (IR) and the security studies field; the current national perspectives, policies, doctrines, and strategies relevant to cyber warfare; and an examination of key challenges in international law, norm development, and the potential impact of cyber warfare on future international conflicts. This book will be of much interest to students of cyber conflict and other forms of digital warfare, security studies, strategic studies, defense policy, and, most broadly, international relations.

Cyberethics

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.

Technology, Ethics and the Protocols of Modern War

This book presents 12 essays that focus on the analysis of the problems prompted by cyber operations (COs). It clarifies and discusses the ethical and regulatory problems raised by the deployment of cyber capabilities by a state's army to inflict disruption or damage to an adversary's targets in or through cyberspace. Written by world-leading philosophers, ethicists, policy-makers, and law and military experts, the essays cover such topics as the conceptual novelty of COs and the ethical problems that this engenders; the applicability of existing conceptual and regulatory frameworks to COs deployed in case of conflicts; the definition of deterrence strategies involving COs; and the analysis of models to foster cooperation in managing cyber crises. Each essay is an invited contribution or a revised version of a paper originally presented at the workshop on Ethics and Policies for Cyber Warfare, organized by the NATO Cooperative Cyber Defence Centre of Excellence in collaboration with the University of Oxford. The volume endorses a multi-disciplinary approach, as such it offers a comprehensive overview of the ethical, legal, and policy problems posed by COs and of the different approaches and methods that can be used to solve them. It will appeal to a wide readership, including ethicists, philosophers, military experts, strategy planners, and law- and policy-makers.

The Basics of Cyber Warfare

Cyber-Attacks and the Exploitable Imperfections of International Law reveals

elements of existing jus ad bellum and jus in bello regimes that are unable to accommodate the threats posed by cyber-attacks. It maps out legal gaps, deficiencies, and uncertainties, which international actors may seek to exploit to their political benefit.

Binary Bullets

Cyber weapons and cyber warfare have become one of the most dangerous innovations of recent years, and a significant threat to national security. Cyber weapons can imperil economic, political, and military systems by a single act, or by multifaceted orders of effect, with wide-ranging potential consequences. Unlike past forms of warfare circumscribed by centuries of just war tradition and Law of Armed Conflict prohibitions, cyber warfare occupies a particularly ambiguous status in the conventions of the laws of war. Furthermore, cyber attacks put immense pressure on conventional notions of sovereignty, and the moral and legal doctrines that were developed to regulate them. This book, written by an unrivalled set of experts, assists in proactively addressing the ethical and legal issues that surround cyber warfare by considering, first, whether the Laws of Armed Conflict apply to cyberspace just as they do to traditional warfare, and second, the ethical position of cyber warfare against the background of our generally recognized moral traditions in armed conflict. The book explores these moral and legal issues in three categories. First, it addresses foundational

questions regarding cyber attacks. What are they and what does it mean to talk about a cyber war? The book presents alternative views concerning whether the laws of war should apply, or whether transnational criminal law or some other peacetime framework is more appropriate, or if there is a tipping point that enables the laws of war to be used. Secondly, it examines the key principles of jus in bello to determine how they might be applied to cyber-conflicts, in particular those of proportionality and necessity. It also investigates the distinction between civilian and combatant in this context, and studies the level of causation necessary to elicit a response, looking at the notion of a 'proximate cause'. Finally, it analyzes the specific operational realities implicated by particular regulatory regimes. This book is unmissable reading for anyone interested in the impact of cyber warfare on international law and the laws of war.

Military Ethics

From North Korea's recent attacks on Sony to perpetual news reports of successful hackings and criminal theft, cyber conflict has emerged as a major topic of public concern. Yet even as attacks on military, civilian, and commercial targets have escalated, there is not yet a clear set of ethical guidelines that apply to cyber warfare. Indeed, like terrorism, cyber warfare is commonly believed to be a war without rules. Given the prevalence cyber warfare, developing a practical moral code for this new form of conflict is more important than ever. In Ethics and Cyber

Warfare, internationally-respected ethicist George Lucas delves into the confounding realm of cyber conflict. Comparing "state-sponsored hacktivism" to the transformative impact of "irregular warfare" in conventional armed conflict, Lucas offers a critique of legal approaches to governance, and outlines a new approach to ethics and "just war" reasoning. Lucas draws upon the political philosophies of Alasdair MacIntyre, John Rawls, and Jurgen Habermas to provide a framework for understanding these newly-emerging standards for cyber conflict, and ultimately presents a professional code of ethics for a new generation of "cyber warriors." Lucas concludes with a discussion of whether preemptive self-defense efforts - such as the massive government surveillance programs revealed by Edward Snowden - can ever be justified, addressing controversial topics such as privacy, anonymity, and public trust. Well-reasoned and timely, Ethics and Cyber Warfare is a must-read for anyone with an interest in philosophy, ethics, or cybercrime. "

Cyber War

This new textbook offers an accessible introduction to the topic of cybersecurity ethics. The book is split into three parts. Part I provides an introduction to the field of ethics, philosophy and philosophy of science, three ethical frameworks – virtue ethics, utilitarian ethics and communitarian ethics – and the notion of ethical hacking. Part II applies these frameworks to particular issues within the field of

cybersecurity, including privacy rights, intellectual property and piracy, surveillance, and cyberethics in relation to military affairs. The third part concludes by exploring current codes of ethics used in cybersecurity. The overall aims of the book are to: provide ethical frameworks to aid decision making; present the key ethical issues in relation to computer security; highlight the connection between values and beliefs and the professional code of ethics. The textbook also includes three different features to aid students: 'Going Deeper' provides background information on key individuals and concepts; 'Critical Issues' features contemporary case studies; and 'Applications' examine specific technologies or practices which raise ethical issues. The book will be of much interest to students of cybersecurity, cyberethics, hacking, surveillance studies, ethics and information science.

Understanding Cyber Warfare

This book is a multi-disciplinary analysis of cyber warfare, featuring contributions by leading experts from a mixture of academic and professional backgrounds. Cyber warfare, meaning interstate cyber aggression, is an increasingly important emerging phenomenon in international relations, with state-orchestrated (or apparently state-orchestrated) computer network attacks occurring in Estonia (2007), Georgia (2008) and Iran (2010). This method of waging warfare – given its potential to, for example, make planes fall from the sky or cause nuclear power

plants to melt down – has the capacity to be as devastating as any conventional means of conducting armed conflict. Every state in the world now has a cyber-defence programme and over 120 states also have a cyber-attack programme. While the amount of literature on cyber warfare is growing within disciplines, our understanding of the subject has been limited by a lack of cross-disciplinary engagement. In response, this book, drawn from the fields of computer science, military strategy, international law, political science and military ethics, provides a critical overview of cyber warfare for those approaching the topic from whatever angle. Chapters consider the emergence of the phenomena of cyber warfare in international affairs; what cyber-attacks are from a technological standpoint; the extent to which cyber-attacks can be attributed to state actors; the strategic value and danger posed by cyber conflict; the legal regulation of cyber-attacks, both as international uses of force and as part of an on-going armed conflict, and the ethical implications of cyber warfare. This book will be of great interest to students of cyber warfare, cyber security, military ethics, international law, security studies and IR in general.

Cyber Warfare and the Laws of War

Cyber Warfare

"Cyber war is coming," announced a land-mark RAND report in 1993. In 2005, the U.S. Air Force boasted it would now fly, fight, and win in cyberspace, the "fifth domain" of warfare. This book takes stock, twenty years on: is cyber war really coming? Has war indeed entered the fifth domain? Cyber War Will Not Take Place cuts through the hype and takes a fresh look at cyber security. Thomas Rid argues that the focus on war and winning distracts from the real challenge of cyberspace: non-violent confrontation that may rival or even replace violence in surprising ways. The threat consists of three different vectors: espionage, sabotage, and subversion. The author traces the most significant hacks and attacks, exploring the full spectrum of case studies from the shadowy world of computer espionage and weaponised code. With a mix of technical detail and rigorous political analysis, the book explores some key questions: What are cyber weapons? How have they changed the meaning of violence? How likely and how dangerous is crowd-sourced subversive activity? Why has there never been a lethal cyber attack against a country's critical infrastructure? How serious is the threat of "pure" cyber espionage, of exfiltrating data without infiltrating humans first? And who is most vulnerable: which countries, industries, individuals?

Ethics and Policies for Cyber Operations

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

Cybersecurity

An essential, eye-opening book about cyberterrorism, cyber war, and the next great threat to our national security. “Cyber War may be the most important book about national security policy in the last several years.” –Slate Former presidential advisor and counter-terrorism expert Richard A. Clarke sounds a timely and chilling warning about America’s vulnerability in a terrifying new international conflict. Cyber War is a powerful book about technology, government, and military strategy; about criminals, spies, soldiers, and hackers. It explains clearly and convincingly what cyber war is, and how vulnerable we are as a nation and as individuals to the vast and looming web of cyber criminals. Every concerned American should read this startling and explosive book that offers an insider’s view of White House ‘Situation Room’ operations and carries the reader to the frontlines of our cyber defense. Cyber War exposes a virulent threat to our nation’s security.

War and Political Theory

Conflict and Cooperation in Cyberspace: The Challenge to National Security brings

together some of the world's most distinguished military leaders, scholars, cyber operators, and policymakers in a discussion of current and future challenges that cyberspace poses to the United States and the world. Maintaining a focus on policy-relevant solutions, it offers a well-reasoned study of how to prepare for war, while attempting to keep the peace in the cyberspace domain. The discussion begins with thoughtful contributions concerning the attributes and importance of cyberspace to the American way of life and global prosperity. Examining the truths and myths behind recent headline-grabbing malicious cyber activity, the book spells out the challenges involved with establishing a robust system of monitoring, controls, and sanctions to ensure cooperation amongst all stakeholders. The desire is to create a domain that functions as a trusted and resilient environment that fosters cooperation, collaboration, and commerce. Additionally, the book: Delves into the intricacies and considerations cyber strategists must contemplate before engaging in cyber war Offers a framework for determining the best ways to engage other nations in promoting global norms of behavior Illustrates technologies that can enable cyber arms control agreements Dispels myths surrounding Stuxnet and industrial control systems General Michael V. Hayden, former director of the National Security Agency and the Central Intelligence Agency, begins by explaining why the policymakers, particularly those working on cyber issues, must come to understand the policy implications of a dynamic domain. Expert contributors from the Air Force Research Institute, MIT, the Rand Corporation, Naval Postgraduate School, NSA, USAF, USMC, and others examine the challenges involved with

ensuring improved cyber security. Outlining the larger ethical, legal, and policy challenges facing government, the private sector, civil society, and individual users, the book offers plausible solutions on how to create an environment where there is confidence in the ability to assure national security, conduct military operations, and ensure a vibrant and stable global economy.

Cyber-Attacks and the Exploitable Imperfections of International Law

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.

Strategic Cyber Security

In Defending Humanity, internationally acclaimed legal scholar George P. Fletcher and Jens David Ohlin, a leading expert on international criminal law, tackle one of the most important and controversial questions of our time: When is war justified? When a nation is attacked, few would deny that it has the right to respond with force. But what about preemptive and preventive wars, or crossing another state's border to stop genocide? Was Israel justified in initiating the Six Day War, and was NATO's intervention in Kosovo legal? What about the U.S. invasion of Iraq? In their provocative book, Fletcher and Ohlin offer a groundbreaking theory on the legality of war with clear guidelines for evaluating these interventions. The authors argue that much of the confusion on the subject stems from a persistent misunderstanding of the United Nations Charter. The Charter appears to be very clear on the use of military force: it is only allowed when authorized by the Security Council or in self-defense. Unfortunately, this has led to the problem of justifying force when the Security Council refuses to act or when self-defense is thought not to apply--and to the difficult dilemma of declaring such interventions illegal or ignoring the UN Charter altogether. Fletcher and Ohlin suggest that the answer lies in going back to the domestic criminal law concepts upon which the UN Charter was originally based, in particular, the concept of "legitimate defense," which

encompasses not only self-defense but defense of others. Lost in the English-language version of the Charter but a vital part of the French and other non-English versions, the concept of legitimate defense will enable political leaders, courts, and scholars to see the solid basis under international law for states to intervene with force--not just to protect themselves against an imminent attack but also to defend other national groups.

The Ethics of Information Warfare

We have witnessed a digital revolution that affects the dynamics of existing traditional social, economic, political and legal systems. This revolution has transformed espionage and its features, such as its purpose and targets, methods and means, and actors and incidents, which paves the way for the emergence of the term cyberespionage. This book seeks to address domestic and international legal tools appropriate to adopt in cases of cyberespionage incidents. Cyberespionage operations of state or non-state actors are a kind of cyber attack, which violates certain principles of international law but also constitute wrongful acquisition and misappropriation of the data. Therefore, from the use of force to state responsibility, international law offers a wide array of solutions; likewise, domestic regulations through either specialized laws or general principles stipulate civil and criminal remedies against cyberespionage. Confronting Cyberespionage Under International Law examines how espionage and its applications have

transformed since World War II and how domestic and international legal mechanisms can provide effective legal solutions to this change, hindering the economic development and well-being of individuals, companies and states to the detriment of others. It shows the latest state of knowledge on the topic and will be of interest to researchers, academics, legal practitioners, legal advisors and students in the fields of international law, information technology law and intellectual property law.

Cyberdeterrence and Cyberwar

Completely revised and updated, the new fourth edition of this popular text takes an in-depth look at the social costs and moral problems that have arisen by the ever expanded use of the internet, and offers up-to-date legal and philosophical perspectives. It focuses heavily on content control and free speech, intellectual property, privacy and security, and features new content on blogging and social networking. Case studies throughout offer real-life scenarios and include coverage of numerous hot topics. In the process of examinging current issues, the text identifies some of the legal disputes that will likely set the standard for future cases.

Cyber Warfare

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

Cyber War

This study analyzes the emergent field of cyber warfare through the lens of commonly accepted tenets of ethical warfare. By comparing the foundational understanding of concepts that determine the justice of wars (jus ad bellum) and justice in war (jus en bello) with the capabilities cyber warfare offers, this work highlights both causes for concern and opportunities for betterment. The first chapter introduces important contextual information and definitions that frame the arguments to follow. Chapter 2 presents a theoretical overview of ethical warfare from which to build. This overview presents five core tenets: good faith, proportionality, noncombatant immunity, last resort, and sovereignty. Chapter 3 builds on this framework by analyzing how cyber warfare affects each of the core concepts introduced above. The fourth chapter presents a case study that tests the theoretical assertions presented elsewhere in the work. Finally, the conclusion offers a platform for further exploration and surmises opinions regarding ethics and cyber warfare.Cyber warfare offers both nagging difficulties that complicate existing ethical warfare standards and exciting opportunities to improve how warfare is carried out. Decision makers charged with the authority to carry out acts of cyber warfare must understand the technical limitations of the offensive and defensive components of cyber warfare. Even more importantly, these decision

makers must appreciate how their actions in this burgeoning domain help shape emergent norms and standards that will promulgate through the domain.Cyber warfare has the potential to facilitate effects that were previously only achievable through lethal means. This is an exciting development in terms of ethical warfare. While B. H. Liddell Hart famously proposed the reason for war is to create a better state of peace, cyber warfare offers the potential to create a better state of war

Routledge Handbook of Ethics and War

Just war theory focuses primarily on bodily harm, such as killing, maiming, and torture, while other harms are often largely overlooked. At the same time, contemporary international conflicts increasingly involve the use of unarmed tactics, employing 'softer' alternatives or supplements to kinetic power that have not been sufficiently addressed by the ethics of war or international law. Soft war tactics include cyber-warfare and economic sanctions, media warfare, and propaganda, as well as non-violent resistance as it plays out in civil disobedience, boycotts, and 'lawfare.' While the just war tradition has much to say about 'hard' war - bullets, bombs, and bayonets - it is virtually silent on the subject of 'soft' war. Soft War: The Ethics of Unarmed Conflict illuminates this neglected aspect of international conflict.

The Ethics of Cyber Conflicts: An Introduction

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.

Dehumanization of Warfare

Cyberwarfare

Insights into the true history of cyber warfare, and the strategies, tactics, and cybersecurity tools that can be used to better defend yourself and your organization against cyber threat. Key Features Define and determine a cyber-defence strategy based on current and past real-life examples Understand how future technologies will impact cyber warfare campaigns and society Future-ready yourself and your business against any cyber threat Book Description The era of cyber warfare is now upon us. What we do now and how we determine what we will

do in the future is the difference between whether our businesses live or die and whether our digital self survives the digital battlefield. Cyber Warfare – Truth, Tactics, and Strategies takes you on a journey through the myriad of cyber attacks and threats that are present in a world powered by AI, big data, autonomous vehicles, drones video, and social media. Dr. Chase Cunningham uses his military background to provide you with a unique perspective on cyber security and warfare. Moving away from a reactive stance to one that is forward-looking, he aims to prepare people and organizations to better defend themselves in a world where there are no borders or perimeters. He demonstrates how the cyber landscape is growing infinitely more complex and is continuously evolving at the speed of light. The book not only covers cyber warfare, but it also looks at the political, cultural, and geographical influences that pertain to these attack methods and helps you understand the motivation and impacts that are likely in each scenario. Cyber Warfare – Truth, Tactics, and Strategies is as real-life and up-to-date as cyber can possibly be, with examples of actual attacks and defense techniques, tools. and strategies presented for you to learn how to think about defending your own systems and data. What you will learn Hacking at scale – how machine learning (ML) and artificial intelligence (AI) skew the battlefield Defending a boundaryless enterprise Using video and audio as weapons of influence Uncovering DeepFakes and their associated attack vectors Using voice augmentation for exploitation Defending when there is no perimeter Responding tactically to counter-campaign-based attacks Who this book is for This book is for

any engineer, leader, or professional with either a responsibility for cyber security within their organizations, or an interest in working in this ever-growing field.

Cyber Warfare – Truth, Tactics, and Strategies

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.

The Ethics of Cybersecurity

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

Confronting Cyberespionage Under International Law

The Basics of Cyber Warfare provides readers with fundamental knowledge of cyber war in both theoretical and practical aspects. This book explores the principles of cyber warfare, including military and cyber doctrine, social engineering, and offensive and defensive tools, tactics and procedures, including computer network exploitation (CNE), attack (CNA) and defense (CND). Readers learn the basics of how to defend against espionage, hacking, insider threats, state-sponsored attacks, and non-state actors (such as organized criminals and terrorists). Finally, the book looks ahead to emerging aspects of cyber security technology and trends, including cloud computing, mobile devices, biometrics and nanotechnology. The Basics of Cyber Warfare gives readers a concise overview of these threats and outlines the ethics, laws and consequences of cyber warfare. It is a valuable resource for policy makers, CEOs and CIOs, penetration testers, security administrators, and students and instructors in information security. Provides a sound understanding of the tools and tactics used in cyber warfare. Describes both offensive and defensive tactics from an insider's point of view. Presents doctrine and hands-on techniques to understand as cyber warfare evolves with technology.

Cyber War Will Not Take Place

This open access book provides the first comprehensive collection of papers that provide an integrative view on cybersecurity. It discusses theories, problems and solutions on the relevant ethical issues involved. This work is sorely needed in a

world where cybersecurity has become indispensable to protect trust and confidence in the digital infrastructure whilst respecting fundamental values like equality, fairness, freedom, or privacy. The book has a strong practical focus as it includes case studies outlining ethical issues in cybersecurity and presenting guidelines and other measures to tackle those issues. It is thus not only relevant for academics but also for practitioners in cybersecurity such as providers of security software, governmental CERTs or Chief Security Officers in companies.

Cyberwar

Dependence on computers has had a transformative effect on human society. Cybernetics is now woven into the core functions of virtually every basic institution, including our oldest ones. War is one such institution, and the digital revolution's impact on it has been profound. The American military, which has no peer, is almost completely reliant on high-tech computer systems. Given the Internet's potential for full-spectrum surveillance and information disruption, the marshaling of computer networks represents the next stage of cyberwar. Indeed, it is upon us already. The recent Stuxnet episode, in which Israel fed a malignant computer virus into Iran's nuclear facilities, is one such example. Penetration into US government computer systems by Chinese hackers-presumably sponsored by the Chinese government-is another. Together, they point to a new era in the evolution of human conflict. In Cybersecurity and Cyerbwar: What Everyone Needs

to Know, noted experts Peter W. Singer and Allan Friedman lay out how the revolution in military cybernetics occurred and explain where it is headed. They begin with an explanation of what cyberspace is before moving on to discussions of how it can be exploited and why it is so hard to defend. Throughout, they discuss the latest developments in military and security technology. Singer and Friedman close with a discussion of how people and governments can protect themselves. In sum, Cybersecurity and Cyerbwar is the definitive account on the subject for the educated general reader who wants to know more about the nature of war, conflict, and security in the twenty-first century.

A Better State of War

This new Handbook offers a comprehensive overview of contemporary extensions and alternatives to the just war tradition in the field of the ethics of war. The modern history of just war has typically assumed the primacy of four particular elements: jus ad bellum, jus in bello, the state actor, and the solider. This book will put these four elements under close scrutiny, and will explore how they fare given the following challenges: • What role do the traditional elements of jus ad bellum and jus in bello—and the constituent principles that follow from this distinction—play in modern warfare? Do they adequately account for a normative theory of war? • What is the role of the state in warfare? Is it or should it be the primary actor in just war theory? • Can a just war be understood simply as a

response to territorial aggression between state actors, or should other actions be accommodated under legitimate recourse to armed conflict? • Is the idea of combatant qua state-employed soldier a valid ethical characterization of actors in modern warfare? • What role does the technological backdrop of modern warfare play in understanding and realizing just war theories? Over the course of three key sections, the contributors examine these challenges to the just war tradition in a way that invigorates existing discussions and generates new debate on topical and prospective issues in just war theory. This book will be of great interest to students of just war theory, war and ethics, peace and conflict studies, philosophy and security studies.

Research Handbook on International Law and Cyberspace

Adopting a multidisciplinary perspective, this book explores the key challenges associated with the proliferation of cyber capabilities. Over the past two decades, a new man-made domain of conflict has materialized. Alongside armed conflict in the domains of land, sea, air, and space, hostilities between different types of political actors are now taking place in cyberspace. This volume addresses the challenges posed by cyberspace hostility from theoretical, political, strategic and legal perspectives. In doing so, and in contrast to current literature, cyber-security is analysed through a multidimensional lens, as opposed to being treated solely as a military or criminal issues, for example. The individual chapters map out the

different scholarly and political positions associated with various key aspects of cyber conflict and seek to answer the following questions: do existing theories provide sufficient answers to the current challenges posed by conflict in cyberspace, and, if not, could alternative approaches be developed?; how do states and non-state actors make use of cyber-weapons when pursuing strategic and political aims?; and, how does the advent of conflict in cyberspace challenge our established legal framework? By asking important strategic questions on the theoretical, strategic, ethical and legal implications and challenges of the proliferation of cyber warfare capabilities, the book seeks to stimulate research into an area that has hitherto been neglected. This book will be of much interest to students of cyber-conflict and cyber-warfare, war and conflict studies, international relations, and security studies.

Conflict and Cooperation in Cyberspace

What significance does "ethics" have for the men and women serving in the military forces of nations around the world? What core values and moral principles collectively guide the members of this "military profession?" This book explains these essential moral foundations, along with "just war theory," international relations, and international law. The ethical foundations that define the "Profession of Arms" have developed over millennia from the shared moral values, unique role responsibilities, and occasional reflection by individual members the profession on

their own practices - eventually coming to serve as the basis for the "Law of Armed Conflict" itself. This book focuses upon the ordinary men and women around the world who wear a military uniform and are committed to the defense of their countries and their fellow citizens. It is about what they do, how they do it, what they think about it, how they behave when carrying out their activities, and how they are expected to behave, both on and off the battlefield (whether in, or out of, uniform) - and what everyone (and not just military personnel themselves) needs to know about this. The book also examines how military personnel are treated and regarded by those whom they have sworn to defend and protect, as well as how they treat and regard one another within their respective services and organizational settings. Finally, the book discusses the transformations in military professionalism occasioned by new developments in armed conflict, ranging counterinsurgency warfare and humanitarian military intervention, to cyber conflict, military robotics, and private military contracting. From China to Russia, author George Lucas effectively sheds light on today's military ethics in existence throughout the world. What Everyone Needs to Know® is a registered trademark of Oxford University Press.

Ethics and Cyber Warfare

Cyber Warfare Techniques, Tactics and Tools for Security Practitioners provides a comprehensive look at how and why digital warfare is waged. This book explores

the participants, battlefields, and the tools and techniques used during today's digital conflicts. The concepts discussed will give students of information security a better idea of how cyber conflicts are carried out now, how they will change in the future, and how to detect and defend against espionage, hacktivism, insider threats and non-state actors such as organized criminals and terrorists. Every one of our systems is under attack from multiple vectors - our defenses must be ready all the time and our alert systems must detect the threats every time. This book provides concrete examples and real-world guidance on how to identify and defend a network against malicious attacks. It considers relevant technical and factual information from an insider's point of view, as well as the ethics, laws and consequences of cyber war and how computer criminal law may change as a result. Starting with a definition of cyber warfare, the book’s 15 chapters discuss the following topics: the cyberspace battlefield; cyber doctrine; cyber warriors; logical, physical, and psychological weapons; computer network exploitation; computer network attack and defense; non-state actors in computer network operations; legal system impacts; ethics in cyber warfare; cyberspace challenges; and the future of cyber war. This book is a valuable resource to those involved in cyber warfare activities, including policymakers, penetration testers, security professionals, network and systems administrators, and college instructors. The information provided on cyber tactics and attacks can also be used to assist in developing improved and more efficient procedures and technical defenses. Managers will find the text useful in improving the overall risk management

strategies for their organizations. Provides concrete examples and real-world guidance on how to identify and defend your network against malicious attacks Dives deeply into relevant technical and factual information from an insider's point of view Details the ethics, laws and consequences of cyber war and how computer criminal law may change as a result

Investigating Cyber Law and Cyber Ethics: Issues, Impacts and Practices

The United States is increasingly dependent on information and information technology for both civilian and military purposes, as are many other nations. Although there is a substantial literature on the potential impact of a cyberattack on the societal infrastructure of the United States, little has been written about the use of cyberattack as an instrument of U.S. policy. Cyberattacks--actions intended to damage adversary computer systems or networks--can be used for a variety of military purposes. But they also have application to certain missions of the intelligence community, such as covert action. They may be useful for certain domestic law enforcement purposes, and some analysts believe that they might be useful for certain private sector entities who are themselves under cyberattack. This report considers all of these applications from an integrated perspective that ties together technology, policy, legal, and ethical issues. Focusing on the use of

cyberattack as an instrument of U.S. national policy, Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities explores important characteristics of cyberattack. It describes the current international and domestic legal structure as it might apply to cyberattack, and considers analogies to other domains of conflict to develop relevant insights. Of special interest to the military, intelligence, law enforcement, and homeland security communities, this report is also an essential point of departure for nongovernmental researchers interested in this rarely discussed topic.

Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities

In a world that continues to be riven by armed conflict, the fundamental moral and political questions raised by warfare are as important as ever. Under what circumstances are we justified in going to war? Can conflicts be waged in a 'moral' way? Is war an inevitable feature of a world driven by power politics? What are the new ethical challenges raised by new weapons and technology, from drones to swarming attack robots? This book is an engaging and up-to-date examination of these questions and more, penned by a foremost expert in the field. Using many historical cases, it examines all the core disputes and doctrines, ranging from realism to pacifism, from just war theory and international law, to feminism and

the democratic peace thesis. Its scope stretches from the primordial causes and perennial drivers of war to the cyber-centric space-age future of armed conflict in the 21st century. War and Political Theory is essential reading for anyone, whether advanced expert or undergraduate, who wants to understand the pressing empirical realities and theoretical issues, historical and contemporary, associated with armed conflict.

Cybersecurity Law

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.

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations

Ethical values in computing are essential for understanding and maintaining the relationship between computing professionals and researchers and the users of

their applications and programs. While concerns about cyber ethics and cyber law are constantly changing as technology changes, the intersections of cyber ethics and cyber law are still underexplored. Investigating Cyber Law and Cyber Ethics: Issues, Impacts and Practices discusses the impact of cyber ethics and cyber law on information technologies and society. Featuring current research, theoretical frameworks, and case studies, the book will highlight the ethical and legal practices used in computing technologies, increase the effectiveness of computing students and professionals in applying ethical values and legal statues, and provide insight on ethical and legal discussions of real-world applications.

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