This book provides an up-to-date, accessible guide to the growing threats in cyberspace that affects everyone from private individuals to businesses to national governments. This volume provides an authoritative, cutting-edge resource on the characteristics of both technological and social change in warfare in the twenty-first century, and the challenges such change presents to international law. The character of contemporary warfare has recently undergone significant transformation in several important respects: the nature of the actors, the changing technological capabilities available to them, and the sites and spaces in which war is fought. These changes have augmented the phenomenon of non-obvious warfare, making understanding warfare one of the key challenges. Such developments have been accompanied by significant flux and uncertainty in the international legal sphere. This handbook brings together a unique blend of expertise, combining scholars and practitioners in science and technology, international law, strategy and policy, in order properly to understand and identify the chief characteristics and features of a range of innovative developments, means and processes in the context of obvious and non-obvious warfare. The handbook has six thematic sections: Law, war and technology Cyber warfare Autonomy, robotics and drones Synthetic biology New frontiers International perspectives. This interdisciplinary blend and the novel, rich and insightful contribution that it makes across various fields will make this volume a crucial research tool and guide for practitioners, scholars and students of war studies, security studies, technology and design, ethics, international relations and international law.
Cyber warfare has become more pervasive and more complex in recent years. It is difficult to regulate, as it holds an ambiguous position within the laws of war. This book investigates the legal and ethical ramifications of cyber war, considering which sets of laws apply to it, and how it fits into traditional ideas of armed conflict.
The result of a three-year project, this manual addresses the entire spectrum of international legal issues raised by 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...
Access Free Field Manual Cyber War

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.

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.
This book offers an introduction to Information Technology with regard to peace, conflict, and security research, a topic that it approaches from natural science, technical and computer science perspectives. Following an initial review of the fundamental roles of IT in connection with peace, conflict and security, the contributing authors address
the rise of cyber conflicts via information warfare, cyber espionage, cyber defence and Darknets. The book subsequently explores recent examples of cyber warfare, including: • The Stuxnet attack on Iran’s uranium refining capability • The hacking of the German Federal Parliament’s internal communication system • The Wannacry malware campaign, which used software stolen from a US security agency to launch ransomware attacks worldwide The book then introduces readers to the concept of cyber peace, including a discussion of confidence and security-building measures. A section on Cyber Arms Control draws comparisons to global efforts to control chemical warfare, to reduce the risk of nuclear war, and to prevent the militarization of space. Additional topics include the security of critical information infrastructures, and cultural violence and peace in social media. The book concludes with an outlook on the future role of IT in peace and security. Information Technology for Peace and Security breaks new ground in a largely unexplored field of study, and offers a valuable asset for a broad readership including students, educators and working professionals in computer science, IT security, peace and conflict studies, and political science. In 2011, Nasser Al-Awlaki, a terrorist on the US 'kill list' in Yemen, was targeted by the CIA. A week later, a military strike killed his son. The following year, the US Ambassador to Pakistan resigned, undermined by
CIA-conducted drone strikes of which he had no knowledge or control. The demands of the new, borderless 'gray area' conflict have cast civilians and military into unaccustomed roles with inadequate legal underpinning. As the Department of Homeland Security defends against cyber threats and civilian contractors work in paramilitary roles abroad, the legal boundaries of war demand to be outlined. In this book, former Under Secretary of the Air Force Antonia Chayes examines these new 'gray areas' in counterinsurgency, counter-terrorism and cyber warfare. Her innovative solutions for role definition and transparency will establish new guidelines in a rapidly evolving military-legal environment.

These proceedings represent the work of contributors to the 19th European Conference on Cyber Warfare and Security (ECCWS 2020), supported by University of Chester, UK on 25-26 June 2020. The Conference Co-chairs are Dr Thaddeus Eze and Dr Lee Speakman, both from University of Chester and the Programme Chair is Dr Cyril Onwubiko from IEEE and Director, Cyber Security Intelligence at Research Series Limited. ECCWS is a well-established event on the academic research calendar and now in its 19th year the key aim remains the opportunity for participants to share ideas and meet. The conference was due to be held at University of Chester, UK, but due to the global Covid-19 pandemic it was moved online to be held as a virtual event. The scope of
papers will ensure an interesting conference. The subjects covered illustrate the wide range of topics that fall into this important and ever-growing area of research. This volume looks at current and emerging technologies of war and some of the ethical issues surrounding their use. Although the nature and politics of war never change, the weapons and technologies used in war do change and are always undergoing development. Because of that, the arsenal of weapons for twenty-first century conflict is different from previous centuries. Weapons in today’s world include an array of instruments of war that include, robotics, cyber war capabilities, human performance enhancement for warriors, and the proliferation of an entire spectrum of unmanned weapons systems and platforms. Tactical weapons now have the potential of strategic results and have changed the understanding of the battle space creating ethical, legal, and political issues unknown in the pre-9/11 world. What do these technologies mean for things such as contemporary international relations, the just-war tradition, and civil-military relations? Directed at readers in the academic, scientific, military, and public policy communities, this volume offers current thought on ethics and emerging technologies from internationally-recognized scholars addressing the full spectrum of issues in present warfare technology. It includes current and ongoing topics of multi-discipline and
international interest, such as ethics, law, international relations, war studies, public policy, science and technology. This book was originally published in various issues and volumes of the Journal of Military Ethics.

A finalist for the Pulitzer Prize The inside story of the small group of soldier-scholars who—against fierce resistance from within their own ranks—changed the way the Pentagon does business and the American military fights wars. The Insurgents is the inside story of the small group of soldier-scholars, led by General David Petraeus, who plotted to revolutionize one of the largest, oldest, and most hidebound institutions—the United States military. Their aim was to build a new Army that could fight the new kind of war in the post–Cold War age: not massive wars on vast battlefields, but “small wars” in cities and villages, against insurgents and terrorists. These would be wars not only of fighting but of “nation building,” often not of necessity but of choice. Based on secret documents, private emails, and interviews with more than one hundred key characters, including Petraeus, the tale unfolds against the backdrop of the wars against insurgents in Iraq and Afghanistan. But the main insurgency is the one mounted at home by ambitious, self-consciously intellectual officers—Petraeus, John Nagl, H. R. McMaster, and others—many of them classmates or colleagues in West Point’s Social Science Department who rose
through the ranks, seized with an idea of how to fight these wars better. Amid the crisis, they forged a community (some of them called it a cabal or mafia) and adapted their enemies’ techniques to overhaul the culture and institutions of their own Army. Fred Kaplan describes how these men and women maneuvered the idea through the bureaucracy and made it official policy. This is a story of power, politics, ideas, and personalities—and how they converged to reshape the twenty-first-century American military. But it is also a cautionary tale about how creative doctrine can harden into dogma, how smart strategists—today’s “best and brightest”—can win the battles at home but not the wars abroad. Petraeus and his fellow insurgents made the US military more adaptive to the conflicts of the modern era, but they also created the tools—and made it more tempting—for political leaders to wade into wars that they would be wise to avoid.

Field Manual FM 3-38 Cyber Electromagnetic Activities provides overarching doctrinal guidance and direction for conducting cyber electromagnetic activities (CEMA). This manual describes the importance of cyberspace and the electromagnetic spectrum (EMS) to Army forces and provides the tactics and procedures commanders and staffs use in planning, integrating, and synchronizing CEMA. This manual provides the information necessary for Army forces to conduct CEMA that enable them to shape
their operational environment and conduct unified land operations. It provides enough guidance for commanders and their staffs to develop innovative approaches to seize, retain, and exploit advantages throughout an operational environment. CEMA enable the Army to achieve desired effects in support of the commander’s objectives and intent. The principal audience for FM 3-38 is all members of the profession of arms. Commanders and staffs of Army headquarters serving as joint task force or multinational headquarters should see applicable joint or multinational doctrine concerning cyberspace operations, electronic warfare (EW), and spectrum management operations (SMO). Trainers and educators throughout the Army will also use this manual. United States (U.S.) forces operate in an increasingly network-based world. The proliferation of information technologies is changing the way humans interact with each other and their environment, including interactions during military operations. This broad and rapidly changing operational environment requires that today’s Army must operate in cyberspace and leverage an electromagnetic spectrum that is increasingly competitive, congested, and contested. FM 3-38, Cyber Electromagnetic Activities, is the first doctrinal field manual of its kind. The integration and synchronization of cyber electromagnetic activities (CEMA) is a new concept. The Army codified the concept of CEMA in Army
Doctrine Publication (ADP) 3-0, Unified Land Operations, and ADP 6-0, Mission Command. The mission command warfighting function now includes four primary staff tasks: conduct the operations process (plan, prepare, execute, assess), conduct knowledge management and information management, conduct inform and influence activities (IIA), and conduct CEMA. The purpose of FM 3-38 is to provide an overview of principles, tactics, and procedures on Army integration of CEMA as part of unified land operations. At its heart, CEMA are designed to posture the Army to address the increasing importance of cyberspace and the electromagnetic spectrum (EMS) and their role in unified land operations. CEMA are implemented via the integration and synchronization of cyberspace operations, electronic warfare (EW), and spectrum management operations (SMO). FM 3-38 contains seven chapters: Chapter 1 defines CEMA and provides an understanding of the fundamentals of the CEMA staff tasks. It briefly describes each activity and provides a framework for the emerging operational environment that includes cyberspace. Chapter 2 begins with a discussion of the commander’s role in the conduct of CEMA. It then describes the CEMA element, its role in the operations process, and how it interacts with, supports, and receives support from other staff members. Chapter 3 provides tactics and procedures specific to
cyberspace operations. Chapter 4 provides tactics and procedures specific to EW. Chapter 5 provides tactics and procedures specific to SMO and the functions executed by the spectrum manager. Chapter 6 describes how CEMA are executed through the operations processes, including other integrating processes. Chapter 7 describes considerations unique to CEMA when conducting operations with unified action partners. Appendix A provides guidance on CEMA input to operations orders and plans.

This timely handbook traces the development of cyber capabilities from their roots in information warfare and cryptology to their potential military application in combat. • Incorporates expertise from diverse viewpoints from the military, government agencies, industry, and academia • Provides an informative timeline of key events in the development of cyber warfare capabilities • Highlights the most prominent and effective cyber attacks in history as well as legal attempts to curb them

Cyber technology gives states the ability to accomplish effects that once required kinetic action. These effects can now be achieved with cyber means in a manner that is covert, deniable, cheap, and technologically feasible for many governments. In some cases, cyber means are morally preferable to conventional military operations, but in other cases, cyber’s unique qualities can lead to greater mischief than governments would have chanced using kinetic
means. This volume addresses the applicability of traditional military ethics to cyber operations, jus ad vim (an emerging sub-field governing grey zone or soft war operations), the rights of the targets of cyber operations, cyber sabotage, cyber surveillance, phase zero operations, psychological operations, artificial intelligence, and algorithmic ethics. Uniquely, it includes a number of cyber incidents that do not currently exist as case studies and have not received much public attention. This volume has been designed to work as a handbook for cyber warriors, drone pilots and military professionals involved in cyber training and teaching. Provides information on the ways individuals, nations, and groups are using the Internet as an attack platform.

David Petraeus and the Plot to Change the American Way of War
Encyclopedia of Cyber Warfare
Cyber Warfare Ethics
The Ethics of Cyberwarfare
Surviving Cyberwar
Field Manual FM 3-38 Cyber Electromagnetic Activities February 2014
Inside Cyber Warfare
Computer and Information Security Handbook
Journal of Law & Cyber Warfare: The New Frontier of Warfare
Routledge Handbook of War, Law and Technology

Over the past two decades, Cyber space and her tools have entered all important spheres of human lives including armed conflicts and have reached there dimensions that were privy to imagination when the current Laws of War in particular the International Humanitarian Law (IHL) were created. Hitherto, these rules designed for a kinetic Cyber-free world are currently regulating them. The purpose of this term paper is to highlight the legal vacuum governing the Cyber warfare, Cyber weapons and their use in an armed conflict and to advocate for a new IHL convention dedicated to Cyber warfare and Cyber weapons. It is done so using the qualitative method and legal analysis of the current legal framework including international treaties, customary law and work of the leading instances of international justice as well as writings of judicial scholars and legal and Cyber experts. The Researcher of the term paper presents the topic "CYBER ATTACK IN INTERNATIONAL WARFARE: ANOTHER USE OF FORCE?", hitherto has started to take shape by the turn of the decade in the field of Cyber-warfare. This research proposes particular Cyber concepts and examines the impacts of defining these concepts in the legal field. The term paper aims to introduce the
grounds of application of the law of armed combat to Cyberspace. This research is a theoretical approach based on scientific texts written by the legal professionals. Applying the principles of International Humanitarian Law to Cyber-warfare is complicated, and it raises more questions than solutions. This term paper reaches a conclusion where the law of armed conflict may be applied to Cyber-warfare if it reaches the threshold of armed combat, but if the threshold is not reached, then the law of armed conflict should not apply and the battle field is the Cyber space for such a case. As a result, the Researcher finds that more attention should be paid to define the crucial concepts of the topic and provide guidelines on their application in legal context.

International humanitarian law is the law that governs the conduct of participants during armed conflict. This branch of law aims to regulate the means and methods of warfare as well as to provide protections to those who do not, or who no longer, take part in the hostilities. It is one of the oldest branches of international law and one of enduring relevance today. The Oxford Guide to International Humanitarian Law provides a practical yet sophisticated overview of this important area of law. Written by a stellar line up of contributors, drawn from those who not only have extensive practical experience but who are also regarded as leading scholars of the subject, the text offers a
comprehensive and authoritative exposition of the field. The Guide provides professionals and advanced students with information and analysis of sufficient depth to enable them to perform their tasks with understanding and confidence. Each chapter illuminates how the law applies in practice, but does not shy away from the important conceptual issues that underpin how the law has developed. It will serve as a first port of call and a regular reference work for those interested in international humanitarian law.

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.

Cyber Warfare, Second Edition, takes a comprehensive look at how and why digital warfare is waged. The book explores the participants, battlefields, and the tools and techniques used in today's digital conflicts. The concepts discussed gives 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. This book provides concrete examples and real-world guidance on how to identify and defend a network against malicious attacks. It probes 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. Logical,
physical, and psychological weapons used in cyber warfare are discussed. This text will appeal to information security practitioners, network security administrators, computer system administrators, and security analysts. 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 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
Diese Einführung stellt die naturwissenschaftlichen Grundlagen für die Friedens- und Konfliktforschung einleitend und verständlich dar. Damit wird Studierenden die Möglichkeit geboten, wichtiges

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

Computer and Information Security Handbook, Third Edition, provides the most current and complete reference on computer security available in one volume. The book offers deep coverage of an extremely wide range of issues in computer and
cybersecurity theory, applications, and best practices, offering the latest insights into established and emerging technologies and advancements. With new parts devoted to such current topics as Cloud Security, Cyber-Physical Security, and Critical Infrastructure Security, the book now has 100 chapters written by leading experts in their fields, as well as 12 updated appendices and an expanded glossary. It continues its successful format of offering problem-solving techniques that use real-life case studies, checklists, hands-on exercises, question and answers, and summaries. Chapters new to this edition include such timely topics as Cyber Warfare, Endpoint Security, Ethical Hacking, Internet of Things Security, Nanoscale Networking and Communications Security, Social Engineering, System Forensics, Wireless Sensor Network Security, Verifying User and Host Identity, Detecting System Intrusions, Insider Threats, Security Certification and Standards Implementation, Metadata Forensics, Hard Drive Imaging, Context-Aware Multi-Factor Authentication, Cloud Security, Protecting Virtual Infrastructure, Penetration Testing, and much more. Written by leaders in the field Comprehensive and up-to-date coverage of the latest security technologies, issues, and best practices Presents methods for analysis, along with problem-solving techniques for implementing practical solutions
Cyber Attack in International Warfare: Another Use of Force
Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations
Law and Ethics for Virtual Conflicts
Tallinn Manual on the International Law Applicable to Cyber Warfare
Cyber Warfare - Truth, Tactics, and Strategies
ECCWS 2015
ECCWS 2020 20th European Conference on Cyber Warfare and Security
Commentary and Critique
Redefining Information Warfare Boundaries for an Army in a Wireless World
Informationskrieg. Über den Zusammenhang von militärischen Konzepten mit Informationen und Medien
21st Century Chinese Cyberwarfare
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.

Inhaltsangabe:
Access Free Field Manual Cyber War


Inhaltsverzeichnis
1. Einleitung
   1.1 Themenbegründung
   1.2 Forschungsstand
   1.3 Problemstellung
   1.4 Was kann diese Arbeit leisten?
   1.5 Gliederung
   1.6 Methodik
2. Kriegskommunikation
   2.1 Das Wesen von Kriegskommunikation
   2.2 Kontrolle und Instrumentalisierung von Medien
   2.3 Behördliches Informationsmanagement
   2.4 Geheimhaltung
   2.5 Täuschung
   2.6 Zensur
   2.7 Psychologische Kriegsführung
   2.8 Propaganda
   2.9 Desinformation
   2.11 Zusammenfassung
3. Darstellung: Konzept Information Warfare
The new edition of the highly influential Tallinn Manual, which outlines public international law as it applies to cyber operations.

Complete proceedings of the 14th European Conference on Cyber Warfare and Security Hatfield UK

Published by Academic Conferences and Publishing International Limited

Field Manual FM 3-12 (FM 3-38) Cyberspace and Electronic Warfare Operations April 2017

Over the past decade of conflict, the U.S. Army has deployed the most capable communications systems in its history. U.S. forces dominated cyberspace and the electromagnetic spectrum (EMS) in Afghanistan and Iraq against enemies and adversaries lacking the technical capabilities to challenge our superiority in cyberspace. However, regional peers have since demonstrated impressive capabilities in a hybrid operational environment that threaten the Army's dominance in cyberspace and the EMS. The Department of Defense information network-Army (DODIN-A) is an essential warfighting platform foundational to the success of all unified land operations. Effectively operating, securing, and defending this network and associated data is...
Access Free Field Manual Cyber War

essential to the success of commanders at all echelons. We must anticipate that future enemies and adversaries will persistently attempt to infiltrate, exploit, and degrade access to our networks and data. A commander who loses the ability to access mission command systems, or whose operational data is compromised, risks the loss of lives and critical resources, or mission failure. In the future, as adversary and enemy capabilities grow, our ability to dominate cyberspace and the EMS will become more complex and critical to mission success. Incorporating cyberspace electromagnetic activities (CEMA) throughout all phases of an operation is key to obtaining and maintaining freedom of maneuver in cyberspace and the EMS while denying the same to enemies and adversaries. CEMA synchronizes capabilities across domains and warfighting functions and maximizes complementary effects in and through cyberspace and the EMS. Intelligence, signal, information operations (IO), cyberspace, space, and fires operations are critical to planning, synchronizing, and executing cyberspace and electronic warfare (EW) operations. CEMA optimizes cyberspace and EW effects when integrated throughout Army operations. FM 3-12 defines and describes the tactics to address future challenges while providing an overview of cyberspace and EW operations, planning, integration, and synchronization through CEMA. It describes how CEMA supports operations and the accomplishment of commander's objectives, and identifies the units that conduct these operations. Due to the rapidly revolving
Through the rise of big data and the internet of things, terrorist organizations have been freed from geographic and logistical confines and now have more power than ever before to strike the average citizen directly at home. This, coupled with the inherently asymmetrical nature of cyberwarfare, which grants great advantage to the attacker, has created an unprecedented national security risk that both governments and their citizens are woefully ill-prepared to face. Examining cyber warfare and terrorism through a critical and academic perspective can lead to a better understanding of its foundations and implications. Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications is an essential reference for the latest research on the utilization of online tools by terrorist organizations to communicate with and recruit potential extremists and examines effective countermeasures employed by law enforcement agencies to defend against such threats. Highlighting a range of topics such as cyber threats, digital intelligence, and counterterrorism, this multi-volume book is ideally designed for law enforcement, government officials, lawmakers, security analysts, IT specialists, software developers, intelligence and security practitioners, students, educators, and researchers.
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.

21st Century Chinese Cyberwarfare draws from a combination of business, cultural, historical and linguistic sources, as well as the author's personal experience, to attempt to explain China to the uninitiated. The objective of the book is to present the salient information regarding the use of cyber warfare doctrine by the People's
Republic of China to promote its own interests and enforce its political, military and economic will on other nation states. The threat of Chinese Cyberwarfare can no longer be ignored. It is a clear and present danger to the experienced and innocent alike and will be economically, societally and culturally changing and damaging for the nations that are targeted. This electronic warfare (EW) doctrine is a key element in the Army's ongoing effort to rebuild and modernize its EW capability. This publication, FM 3-36, the first Army EW doctrine to be issued in nearly a decade, is as timely as it is essential. In addition to directly supporting traditional EW operations, FM 3-36 is moving the Army's EW strategy into cyberspace and the electromagnetic environment and is a great start in providing guidance to commanders and ultimately our national decision makers. It provides commanders clear concepts and doctrine that maximize operational effectiveness across the electromagnetic spectrum in both traditional and evolving technologies. The global proliferation of electronics and wireless transmissions has evolved into a significant technological advantage for our nation while simultaneously creating a greater dependence on technology. This dependence also presents challenges, as our adversaries are constantly developing the means to use these same wireless networks, electronics, computer networks, and electronic warfare capabilities to launch attacks against us. To meet these challenges, the Army is implementing and integrating network and electronic warfare capabilities to counter the hostile use of cyberspace, space, and the electromagnetic
spectrum. FM 3-36 provides Army commanders and their staff guidance on how the electromagnetic spectrum can impact their operations and how friendly EW operations can be used to gain an advantage. This manual describes the application of EW in support of full spectrum operations and provides a baseline for ensuring a common understanding and operational consistency. Although new equipment, tactics, techniques, and procedures continue to be developed, the physics of electromagnetic energy remains constant. So, as new strategies and tactics are devised to meet the cyberspace environment of the 21st century, electronic warfare remains a critical component of our national defense. This updated doctrine and other modifications to the Army's operational strategies are testimony to the innovation and vision on which our nation relies in this era of the Cyber Revolution. The U.S. Army is studying ways to apply its cyber power and is reconsidering doctrinally defined areas that are integral to cyberspace operations. An examination of network operations, information operations, and several other, more focused areas across the U.S. military found significant overlap and potential boundary progression that could inform the development of future Army doctrine. The turn of the century was accompanied by two historically significant phenomena. One was the emergence of computer networks as a vital component of advanced militaries and interdependent global economic systems. The second concerned China’s rise on the global stage through economic reforms that led to
sustained growth and military modernization. At the same time, Chinese government policies and actions have drawn international criticisms including persistent allegations of online espionage, domestic Internet censorship, and an increased military capability, all of which utilize computer networks. These threat perceptions are heightened by a lack of transparency. Unlike the United States or the North Atlantic Treaty Organization, China does not articulate its strategic doctrine. Further, open source material on this topic is often contradictory, cursory, and unclear due, in part, to the absence of consensus on cyber-related terminology and the infancy of this field. With a focus on the period 1998 to 2016, this book identifies and analyzes the strategic context, conceptual framework, and historical evolution of China’s cyber warfare doctrine.

A Multidisciplinary Analysis
A Special Analysis in the Light of the Tallinn Manual
Mapping the Cyber Underworld
Field Manual FM 3-36 Electronic Warfare in Operations
February 2009
Borderless Wars
How Conflicts in Cyberspace are Challenging America and Changing the World
Routledge Handbook of Ethics and War
The United States Department of Defense Law of War Manual
Cyber War Will Not Take Place
Information Technology for Peace and Security