Cyber Wars A 21st Century Disease Bringing A New Bdo

Encyclopedia of Cyber Warfare
Conflict in the 21st Century
The Hacker and the State
The Real Cyber War
Operational Lessons of the Wars of 21st Century
Understanding Cyber Conflict
Cyber Warfare in the 21st Century
ICCWS 2022 17th International Conference on Cyber Warfare and Security
Cyber Warfare
Internet Wars
Handbook of Research on War Policies, Strategies, and Cyber Wars
Cyber Security Policies and Strategies of the World's Leading States
Cyber-"War" - Testfall der Staatenverantwortlichkeit
The Handbook of Cyber Wargames
Encyclopedia of Cyber Warfare
Soft War
Cyberspace and the "First Battle" in 21st-century War
Virtual Terror
Nuclear Deterrence in the 21st Century
Cyber Warfare and the Laws of War
The Wires of War
The International Law Concept of Neutrality in the 21st Century
Cyberlibel
Cyber Warfare in the 21st Century
Cyber Warfare
Inside Cyber Warfare
Cyber Warfare in the 21st Century: Threats, Challenges, and Opportunities
Cyber Warfare
Cybersecurity
21st European Conference on Cyber Warfare and Security
International Conflicts in Cyberspace - Battlefield of the 21st Century
2100 Life in the Late 21st Century
Inside Cyber Warfare
Cyberwars in the Middle East
Myths and Realities of Cyber Warfare
Cyber Strategy
21st Century Chinese Cyberwarfare
Cyber Warfare
Cyber Warfare

BENITEZ ATKINSON

Encyclopedia of Cyber Warfare Createspace Independent Publishing Platform
Hackers reported as working on behalf of the Russian Government have attacked a wide variety of American citizens and institutions. They include political organizations of both parties, the Republican National Committee and the Democratic National Committee, as well as prominent Democrat and Republican leaders, as well as civil society groups like various American universities and academic research programs. These attacks started years back, but it continued after the 2016 election. They have been reported as hitting government sites, like the Pentagon's email system, as well as private networks, like U.S. banks. They have also been reported as targeting a wide variety of American allies ranging from government, military, and civilian targets, and states that range from Norway to the United Kingdom, as well as now trying to influence upcoming elections in Germany, France, and the Netherlands. In cyberspace, the malevolent actors presently engaged in attacks on U.S. persons and institutions range from criminals who are stealing personal information or holding ransom valuable corporate data to governments, like China, which have been accused of large-scale intellectual property theft, as well as breaking into government databases like the OPM [Office of Personnel Management] in the cyber version of traditional espionage. What can be done to defend America in this challenging realm? As long as we use the internet, adversaries like Putin's Russia and many others will seek to exploit this technology and our dependence on it in realms that range from politics to business to warfare itself. In response, the United States can build a new set of approaches to deliver true cybersecurity, aiming to better protect ourselves while reshaping adversary attitudes and options, or we can continue to be a victim.
Conflict in the 21st Century e-artnow
Through a wealth of vivid stories, Internet Wars explores the big questions about how the Internet is disrupting the world as we have known it, and how the world must build new understandings in response. A fascinating and compelling argument about a major new global challenge.Hugh White, Professor of Strategic Studies, The Australian National University
Internet Wars thoughtfully portrays how power structures are being twisted, bent and broken by people and institutions who are Internet-smart.Alec Ross, Senior Advisor for Innovation to the then-Secretary of State, Hillary Clinton In the last decade, a radical new network has begun to fully manifest itself; the largest political and economic arena the world has ever known: the internet. For those who can master it the promise of political, economic, and military power is extraordinary. Yet, the dramatic contest for control currently underway is often obscured by our prosaic everyday online activity. At a distance though it is unmistakable. Already, exploitation of this new super-network has helped create the world's most valuable company,

toppled governments, led to the largest wealth transfer in history, and created the most extensive global surveillance system ever known. All of humankind is on track to become linked through this single, universal platform but the full implications for state sovereignty, corporate power and human rights have not yet been grasped. The internet has created daunting challenges that have been allowed to go unaddressed: cyber warfare, industrial online theft, burgeoning monopoly power and eroding privacy. We are fast approaching a turning point where action is needed if the most dynamic features of the internet are to be preserved. There is an urgent need to understand the broad currents of the internet's growth if we are to secure its vitality and promise into the future. Internet Wars is a call to action for a more informed debate about a contest to control the internet that will profoundly affect us all for generations to come. It looks at the three epicentres of online contest: people power, government power, and economic power. Fergus Hanson breaks down the dynamics at play in each of these critical areas and finds the human narratives that tell the emerging story about the internet's transformation of our lives.

The Hacker and the State Oxford University Press

Providing an invaluable introductory resource for students studying cyber warfare, this book highlights the evolution of cyber conflict in modern times through dozens of key primary source documents related to its development and implementation. This meticulously curated primary source collection is designed to offer a broad examination of key documents related to cyber warfare, covering the subject from multiple perspectives. The earliest documents date from the late 20th century, when the concept and possibility of cyber attacks became a reality, while the most recent documents are from 2019. Each document is accompanied by an introduction and analysis written by an expert in the field that provides the necessary context for readers to learn about the complexities of cyber warfare. The title's nearly 100 documents are drawn primarily but not exclusively from government sources and allow readers to understand how policy, strategy, doctrine, and tactics of cyber warfare are created and devised, particularly in the United States. Although the U.S. is the global leader in cyber capabilities and is largely driving the determination of norms within the cyber domain, the title additionally contains a small number of international documents. This invaluable work will serve as an excellent starting point for anyone seeking to understand the nature and character of international cyber warfare.

The Real Cyber War IT Governance Ltd

Wars often start well before main forces engage. In the 19th and early 20th centuries, combat often began when light cavalry units crossed the border. For most of the 20th century, the "first battle" typically involved dawn surprise attacks, usually delivered by air forces. While a few of these attacks were so shattering that they essentially decided the outcome of the struggle or at least dramatically shaped its course -- the

Israeli air force's attack at the opening of the June 1967 Six-Day War comes to mind -- in most cases the defender had sufficient strategic space -- geographic and/or temporal -- to recover and eventually redress the strategic balance to emerge victorious. The opening moments of World War II for Russia and the United States provide two examples. The first battle in the 21st century, however, may well be in cyberspace. Coordinated cyber attacks designed to shape the larger battlespace and influence a wide range of forces and levers of power may become the key feature of the next war. Early forms of this may have already been seen in Estonia and Georgia. Control of cyberspace may thus be as decisive in the network-dependent early 21st century as control of the air was for most of the 20th century. In the future, cyber attacks may be combined with other means to inflict paralyzing damage to a nation's critical infrastructure as well as psychological operations designed to create fear, uncertainty, and doubt, a concept we refer to as "infrastructure and information operations." The cyber sphere itself is, of course, a critical warfighting domain that hosts countless information infrastructures, but the rise of network-based control systems in areas as diverse as the power grid and logistics has widened the threat posed by network attacks on opposing infrastructures. Given the increasing dependence of the U.S. military and society on critical infrastructures, this cyber-based first battle is one that we cannot afford to lose. And yet we might.

Operational Lessons of the Wars of 21st Century Createspace Independent Publishing Platform

Some pundits claim cyber weaponry is the most important military innovation in decades, a transformative new technology that promises a paralyzing first-strike advantage difficult for opponents to deter. Yet, what is cyber strategy? How do actors use cyber capabilities to achieve a position of advantage against rival states? This book examines the emerging art of cyber strategy and its integration as part of a larger approach to coercion by states in the international system between 2000 and 2014. To this end, the book establishes a theoretical framework in the coercion literature for evaluating the efficacy of cyber operations. Cyber coercion represents the use of manipulation, denial, and punishment strategies in the digital frontier to achieve some strategic end. As a contemporary form of covert action and political warfare, cyber operations rarely produce concessions and tend to achieve only limited, signaling objectives. When cyber operations do produce concessions between rival states, they tend to be part of a larger integrated coercive strategy that combines network intrusions with other traditional forms of statecraft such as military threats, economic sanctions, and diplomacy. The books finds that cyber operations rarely produce concessions in isolation. They are additive instruments that complement traditional statecraft and coercive diplomacy. The book combines an analysis of cyber exchanges between rival states and broader event data on political, military, and economic interactions with case

studies on the leading cyber powers: Russia, China, and the United States. The authors investigate cyber strategies in their integrated and isolated contexts, demonstrating that they are useful for maximizing informational asymmetries and disruptions, and thus are important, but limited coercive tools. This empirical foundation allows the authors to explore how leading actors employ cyber strategy and the implications for international relations in the 21st century. While most military plans involving cyber attributes remain highly classified, the authors piece together strategies based on observations of attacks over time and through the policy discussion in unclassified space. The result will be the first broad evaluation of the efficacy of various strategic options in a digital world.

Understanding Cyber Conflict Longueville Books

Cyber warfare in the 21st century : threats, challenges, and opportunities : Committee on Armed Services, House of Representatives, One Hundred Fifteenth Congress, first session, hearing held March 1, 2017.

Cyber Warfare in the 21st Century

Georgetown University Press

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

ICCWS 2022 17th International Conference on Cyber Warfare and Security Academic Conferences and publishing limited

Cyber security is one of the big challenges of the 21st century. Failure to meet the threat can have major consequences for the individual, a company, an NGO or a nation state. The cost of cyber crime is

in the billions of pounds per year. Cyber wargames are an essential part of the training cycle, education and operational analysis needed to rise to meet this threat. This handbook aims to fill a gap in the training for cyber-attacks and cyber warfare. By providing worked examples of different types of manual cyber wargame, including aims and objectives for each, it provides a basis for the reader to understand the potential range of games on offer. It also helps educate clients about the different types of cyber wargame available and can help them procure the right type of game in order to meet their needs. Cyber wargaming combines two complex fields: wargame design and cyber operations. This handbook is full of examples of such manual games. It includes examples of: Network attack and defence exercises Committee games Company and state level games Example of a Matrix Game Analysing the cyber security space using Confrontation Analysis Media Wars: The Battle to Dominate the Information Space Attack Chain modellingThe book is full of additional information for the reader, such as how a cyber conflict might develop or what the key decisions C-Suite leaders need to consider when faced by a sustained cyber attack.

Cyber Warfare Simon and Schuster

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. Today, cyber warfare affects everyone—from governments that need to protect sensitive political and military information, to businesses small and large that stand to collectively lose trillions of dollars each year to cyber crime, to individuals whose privacy, assets, and identities are subject to intrusion and theft. The problem is monumental and growing exponentially. Encyclopedia of Cyber Warfare provides a complete overview of cyber warfare, which has been used with increasing frequency in recent years by such countries as China, Iran, Israel, North Korea, Russia, and the United States. Readers will gain an understanding of the origins and development of cyber warfare and of how it has become a major strategic element in warfare for countries throughout the world. The encyclopedia's entries cover all of the most significant cyber attacks to date, including the Stuxnet worm that successfully disabled centrifuges in Iran's Natanz uranium enrichment facility; the attack on Israel's internet infrastructure during its January 2009 military offensive in the Gaza Strip; the worldwide "Red October" cyber attack that stole information from embassies, research firms, military installations, and nuclear and other energy infrastructures; and cyber attacks on private corporations like Sony.

Internet Wars Bloomsbury Publishing USA

Contemporary discussion surrounding the role of the internet in society is dominated by words like: internet freedom, surveillance, cybersecurity, Edward Snowden and, most prolifically, cyber war. Behind the rhetoric of cyber war is an on-going state-centered battle for control of information resources. Shawn Powers and Michael Jablonski

conceptualize this real cyber war as the utilization of digital networks for geopolitical purposes, including covert attacks against another state's electronic systems, but also, and more importantly, the variety of ways the internet is used to further a state's economic and military agendas. Moving beyond debates on the democratic value of new and emerging information technologies, The Real Cyber War focuses on political, economic, and geopolitical factors driving internet freedom policies, in particular the U.S. State Department's emerging doctrine in support of a universal freedom to connect. They argue that efforts to create a universal internet built upon Western legal, political, and social preferences is driven by economic and geopolitical motivations rather than the humanitarian and democratic ideals that typically accompany related policy discourse. In fact, the freedom-to-connect movement is intertwined with broader efforts to structure global society in ways that favor American and Western cultures, economies, and governments. Thought-provoking and far-seeing, The Real Cyber War reveals how internet policies and governance have emerged as critical sites of geopolitical contestation, with results certain to shape statecraft, diplomacy, and conflict in the twenty-first century.

Handbook of Research on War Policies, Strategies, and Cyber Wars Dike Publishers

Cyberwars in the Middle East argues that hacking is a form of online political disruption whose influence flows vertically in two directions (top-bottom or bottom-up) or horizontally. These hacking activities are performed along three political dimensions: international, regional, and local. Author Ahmed Al-Rawi argues that political hacking is an aggressive and militant form of public communication employed by tech-savvy individuals, regardless of their affiliations, in order to influence politics and policies. Kenneth Waltz's structural realism theory is linked to this argument as it provides a relevant framework to explain why nation-states employ cyber tools against each other. On the one hand, nation-states as well as their affiliated hacking groups like cyber warriors employ hacking as offensive and defensive tools in connection to the cyber activity or inactivity of other nation-states, such as the role of Russian Trolls disseminating disinformation on social media during the US 2016 presidential election. This is regarded as a horizontal flow of political disruption. Sometimes, nation-states, like the UAE, Saudi Arabia, and Bahrain, use hacking and surveillance tactics as a vertical flow (top-bottom) form of online political disruption by targeting their own citizens due to their oppositional or activists' political views. On the other hand, regular hackers who are often politically independent practice a form of bottom-top political disruption to address issues related to the internal politics of their respective nation-states such as the case of a number of Iraqi, Saudi, and Algerian hackers. In some cases, other hackers target ordinary citizens to express opposition to their political or ideological views which is regarded as a horizontal form of online political disruption. This book is the first of its

kind to shine a light on many ways that governments and hackers are perpetrating cyber attacks in the Middle East and beyond, and to show the ripple effect of these attacks.

Cyber Security Policies and Strategies of the World's Leading States 2100 - The Book

In the new world order, conflicts between countries are increasing. Fluctuations in the economy and imbalances in the distribution of scarce resources to developing countries can result in wars. The effect of the recent COVID-19 pandemic and economic crisis has caused changes in the strategies and policies of countries. Technological changes and developments have also triggered cyber wars. Despite this, many countries prefer to fight on the field. The damage to the international economy of wars, which kills civilians and causes serious damage to developing countries, is a current issue. The Handbook of Research on War Policies, Strategies, and Cyber Wars examines the factors that lead to war and the damages caused by war strategies and policies. It is a guide for future generations to develop constructive policies and strategies for living in a peaceful world. Covering topics such as geopolitical consequences, civil liberty, and terrorism, this major reference work is a dynamic resource for policymakers, strategists, government officials, politicians, sociologists, students and educators of higher education, librarians, researchers, and academicians.

Cyber-"War" - Testfall der Staatenverantwortlichkeit Bloomsbury Publishing USA

Even though 'neutrality' - the non-participation of states in international armed conflicts - is a well-known concept of traditional international public law, its value in the 21st century is disputed. Some regard the concept as obsolete, while others still view it as an important contribution to a peaceful world. This book analyzes the contemporary international law concept of neutrality. At the heart lies the question of the present-day value of neutrality for international law. For a deeper understanding of the legal concept, a historical overview of neutrality is followed by a presentation of the different types of neutrality, along with a look at the remaining neutral states of the 21st century. An examination of the sources of neutrality law, its scope of application, as well as the detailed rights and duties of neutral States will answer the question of what it entails nowadays to be neutral in the legal sense. A clear distinction between the law and politics of neutrality is also important. Special attention is given to the traditional problem of exporting war materials, along with the newer developments of private militaries and security companies, as well as cyber warfare. The focus of the book lies on Switzerland as the archetype of a contemporary neutral state. (Series: Dike Law Books) [Subject: Public International Law, Neutrality Law, Swiss Law]

The Handbook of Cyber Wargames Bloomsbury Publishing USA

The information revolution has transformed both modern societies and the way in which they conduct warfare. Cyber Warfare and the Laws of War analyses the status of computer network attacks in international law and examines their treatment under the laws of armed

conflict. The first part of the book deals with the resort to force by states and discusses the threshold issues of force and armed attack by examining the permitted responses against such attacks. The second part offers a comprehensive analysis of the applicability of international humanitarian law to computer network attacks. By examining the legal framework regulating these attacks, Heather Harrison Dinniss addresses the issues associated with this method of attack in terms of the current law and explores the underlying debates which are shaping the modern laws applicable in armed conflict.

Encyclopedia of Cyber Warfare Cambridge University Press

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.

Soft War Routledge

This reference work examines how sophisticated cyber-attacks and innovative use of social media have changed conflict in the digital realm, while new military technologies such as drones and robotic weaponry continue to have an impact on modern warfare. Cyber warfare, social media, and the latest military weapons are transforming the character of modern conflicts. This book explains how, through overview essays written by an award-winning author of military history and technology topics; in addition to more than 200 entries dealing with specific examples of digital and physical technologies, categorized by their relationship to

cyber warfare, social media, and physical technology areas. Individually, these technologies are having a profound impact on modern conflicts; cumulatively, they are dynamically transforming the character of conflicts in the modern world. The book begins with a comprehensive overview essay on cyber warfare and a large section of A–Z reference entries related to this topic. The same detailed coverage is given to both social media and technology as they relate to conflict in the 21st century. Each of the three sections also includes an expansive bibliography that serves as a gateway for further research on these topics. The book ends with a detailed chronology that helps readers place all the key events in these areas.
Cyberspace and the "First Battle" in 21st-century War Oxford University Press
From the former news policy lead at Google, an “informative and often harrowing wake-up call” (Publishers Weekly) that explains the high-stakes global cyberwar brewing between Western democracies and the authoritarian regimes of China and Russia that could potentially crush democracy. From 2016 to 2020, Jacob Helberg led Google’s global internal product policy efforts to combat disinformation and foreign interference. During this time, he found himself in the midst of what can only be described as a quickly escalating two-front technology cold war between democracy and autocracy. On the front-end, we’re fighting to control the software—applications, news information, social media platforms, and more—of what we see on the screens of our computers, tablets, and phones, a clash which started out primarily with Russia but now increasingly includes China and Iran. Even more ominously, we’re also engaged in a hidden back-end battle—largely with China—to control the internet’s hardware, which includes devices like cellular phones, satellites, fiber-optic cables, and 5G networks. This tech-fueled war will shape the world’s balance of power for the coming century as autocracies exploit 21st-century methods to redivide the world into 20th-century-style spheres of influence. Without a firm partnership with the government, Silicon Valley is unable to protect democracy from the autocrats looking to sabotage it from Beijing to Moscow and Tehran. Helberg offers “unnervingly convincing evidence that time is running out in the ‘gray war’ with the enemies of freedom” (Kirkus Reviews) which could affect every meaningful aspect of our lives, including our economy, our infrastructure, our national security, and ultimately, our national sovereignty.

Virtual Terror
Bloomsbury Publishing USA
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.

Irwin Law Incorporated

This illuminating book examines and refines the commonplace "wisdom" about cyber conflict—its effects, character, and implications for national and individual security in the 21st century. "Cyber warfare" evokes different images to different people. This book deals with the technological aspects denoted by "cyber" and also with the information operations connected to social media's role in digital struggle. The author discusses numerous mythologies about cyber warfare, including its presumptively instantaneous speed, that it makes distance and location irrelevant, and that victims of cyber attacks deserve blame for not defending adequately against attacks. The author outlines why several widespread beliefs about cyber weapons need modification and suggests more nuanced and contextualized conclusions about how cyber domain hostility impacts conflict in the modern world. After distinguishing between the nature of warfare and the character of wars, chapters will probe the widespread assumptions about cyber weapons themselves. The second half of the book explores the role of social media and the consequences of the digital realm being a battlespace in 21st-century conflicts. The book also considers how trends in computing and cyber conflict impact security affairs as well as the practicality of people's relationships with institutions and trends, ranging from democracy to the Internet of Things.

Nuclear Deterrence in the 21st Century University of Illinois Press

An authoritative, single-volume introduction to cybersecurity addresses topics ranging from phishing and electrical-grid takedowns to cybercrime and online freedom, sharing illustrative anecdotes to explain how cyberspace security works and what everyday people can do to protect themselves. Simultaneous.