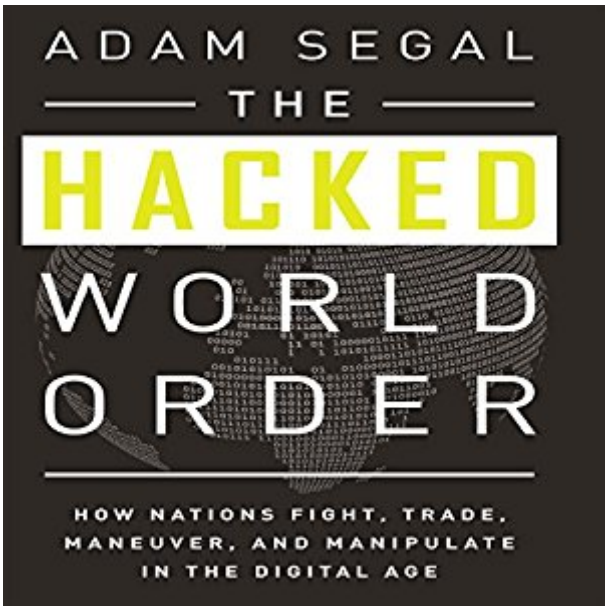
The Hacked World Order: How Nations Fight, Trade, Maneuver, And Manipulate In The Digital Age



Synopsis

The Internet today connects roughly 2.7 billion people around the world, and booming interest in the "Internet of things" could result in 75 billion devices connected to the web by 2020. The myth of cyberspace as a digital utopia has long been put to rest. Governments are increasingly developing smarter ways of asserting their national authority in cyberspace in an effort to control the flow, organization, and ownership of information. In The Hacked World Order, Adam Segal shows how governments use the web to wage war and spy on, coerce, and damage each other. Israel is intent on derailing the Iranian nuclear weapons program. India wants to prevent Pakistani terrorists from using their Blackberries to coordinate attacks. Brazil has plans to lay new fiber cables and develop satellite links so its Internet traffic no longer has to pass through Miami. China does not want to be dependent on the West for its technology needs. These new digital conflicts have as yet posed no physical threat - no one has ever died from a cyberattack - but they serve to undermine the integrity of complex systems like power grids, financial institutions, and security networks. Segal describes how cyberattacks have the potential to produce unintended and unimaginable problems for anyone with an Internet connection and an email account. State-backed hacking initiatives can sabotage trade strategies, steal intellectual property, sow economic chaos, and paralyze whole countries. The Hacked World Order exposes how the Internet has ushered in a new era of geopolitical maneuvering and reveals its tremendous and terrifying implications for our economic livelihood, security, and personal identity.

Book Information

Audible Audio Edition
Listening Length: 10 hoursÂ andÂ 40 minutes
Program Type: Audiobook
Version: Unabridged
Publisher: Gildan Media, LLC
Audible.com Release Date: February 18, 2016
Whispersync for Voice: Ready
Language: English
ASIN: B01BUJAYPA
Best Sellers Rank: #138 inÂ Books > Audible Audiobooks > Politics & Current Events > International Relations #229 inÂ Books > Computers & Technology > Security & Encryption > Privacy & Online Safety #282 inÂ Books > Computers & Technology > Internet & Social Media >

Hacking

Customer Reviews

War, Clausewitz taught us, is a fight to the extreme. Left to itself, absolute war leads to maximum use of force, total disarmament of the enemy, and maximum exertion of power. Of course, many factors prevent war to reach its logical extreme. Wars donÃ¢Â Â™t happen in a vacuum: like any human activity, it is constrained by material elements, and governed by formal and informal rules. In the contemporary era, absolute war was contained by the destructive power of the atomic bomb and the concept of nuclear deterrence. This great moderation is what saved mankind from annihilation. But with cyberwar and robot weapons, absolute war is looming again on the horizon. The forces of restraint imposed by politics and society, not to mention the practical constraints of time and space, are no longer operative. The war of the machines as envisaged by science-fiction writers will be a war to the extremes, whereby all technological forces are thrown into the battle. There are already signs that we are entering a new era of absolute warfare. In the cyber world, everything that can technologically be done, ultimately will be. Cyberwar is a war without borders, without the limitations due to distance and to space. It is also a war without end: there is no declaration of war, no cessation of hostilities, only a succession of more or less covert operations with variable intensity. It is a war of all against all: non-state actors like terrorist groups, criminal gangs, and individual hackers, are also entering the fray.And yet states have so far have used considerable restraint in the use of cyber weapons. Predictions of a cyber Pearl Harbor, or a September 11 in cyberspace, never materialized. Cyber conflicts have been kept at low intensity. What is often described in terms of war or aggression can more aptly be characterized as public disturbance, spying on secrets, or commercial theft. Distributed denial-of-service (DDoS) attacks, the most common type of aggression on the web, are a bit like protesters blocking access to a government office: obviously a nuisance for the public, but not the stuff treated in war rooms and military headquarters. Even the worst cases of cyber warfare described by Adam Segal in his bookÃ¢Â Â”the Stuxnet attack on IranÃ¢Â Â™s nuclear program, the Shaman malware directed at Saudi Aramco, the hacking of Sony Pictures in retaliation of its movie on the North Korean leader, the paralyzation of EstoniaÃ¢Â Â™s electronic infrastructure, the war of propaganda directed at Georgia or waged between Israel and its enemies, did not cause death or physical destruction. The lasting impact of the attacks was minimal: Estonia did not reverse its decision to tear down the statue of Stalin that had caused the ire of Russian patriots, Georgia upheld the disruption in its communication infrastructure by rerouting its data transfers through the United States, and the Stuxnet virus delayed the development of

IranÃ¢Â Â™s nuclear program for only a few months at best. On the whole, states have refrained from engaging in an all-out war on the Internet.There are several reasons for this restraint. First, only a handful of states have full cyber capabilities. According to Adam Segal, China and the United States are the only true cyber superpowers, with Russia standing just in the wings. He identifies four criteria that define power in the cyber age: size of the economy, a shared mission between the private and the public, inventive military and intelligence agencies, and an attractive narrative on the governance of cyberspace. Some middle powers or emerging actors are strong on only one or two of these aspects. European states, and the European Union as a whole, have a vision of Internet governance that emphasizes the rights to privacy and the regulating role of the state. Brazil has leveraged domestic experience into international influence by passing the first Internet bill of rights and by presenting Internet as a global public good that should be managed by states and international organizations. Small, technologically advanced states like Israel or Estonia consider cyberspace as crucial for their development and security, and have a dense community of Internet experts who all know each other very well and collaborate with security and defense agencies. ISIS, a non-state actor, has also developed a cadre of cybernetics experts who fuel its propaganda and maintain its communication channels. Although malware and spying software are readily available on the dark web or sold by commercial enterprises, only technologically advanced states can use cyber offensive and defensive tools to their full capabilities.Second, there is a natural tendency to exaggerate cyber threats. The IT sector is an industry where hype reins master. Business executives and technology pundits are used to inflating the growth potential and disruptive power of the latest innovation. They insist on market disruption, technological breakthrough, and paradigm shift, less so on continuity, path dependency, and incremental change. It is therefore no wonder than the news of imminent cyber warfare has been grossly exaggerated. No one has ever died from cyberwar, no facility was ever destroyed, no territory was ever lost. Pundits point the new vulnerabilities emerging as the Internet of Things spreads to every sector of the economy, but this new threat remains very hypothetical. The Internet backbone of our modern economy has so far proved its robustness. Similarly, there is a feeling in the general public that most of cyber warfare is kept secret. Hence the popularity of books that claim to reveal what is hidden. In reality, there is very little in The Hacked World Order that the attentive reader doesnÃ¢Â Â™t already know from reading the columns of tech magazines or the newspaper accounts of the Snowden revelations. Adam SegalÃ¢Â Â™s book is not exempt from this type of exaggeration and hyperbole found in media reports and business presentations. Labelling the period from June 2012 to June 2013 as Year Zero in the battle over cyberspace makes good headlines, but the succession of events that

marked these twelve monthsÃ¢Â Â”the attack on IranÃ¢Â Â™s nuclear program, IranÃ¢Â Â™s retaliation through a DDoS campaign, SnowdenÃ¢Â Â™s revelations and the Obama-Xi summitÃ¢Â Â”were neither the first nor the last episodes of Internet skirmishes.Third, putting a figure on the economic loss due to cyber espionnage and theft of intellectual property rights serves a well-defined constituency. A whole sector is dependent on exposing the actual cost and potential risk of computer hacking to fuel demand for security solutions and technological firewalls. Cyber security firms and IT consultants have a strong incentive to maximize the threat, putting figures as high as $300 billion a yearÃ¢Â Â”approximately the current annual level of US exports to Asia. The story of the Millennium Bug should warn us of dire predictions or end-of-the-world narratives that only serve to fill the pockets of computer consultants and system providers. In the end, the Y2K time bomb didnÃ¢Â Â™t even tick, and countries like South Korea that invested very little in Y2K remediation had the same negligible problems as countries that spent enormous sums of money. Inflating the cost of cyberattacks also serves to pass on the bill to the government. It is hoped that the public sector will ultimately step in to protect private firms from vulnerabilities. Claims of property theft also provide an excuse for the loss of competitiveness vis-a-vis foreign competitors. Meanwhile, the low level invested by companies in their own protection is a sure sign that this threat is not taken as seriously as pundits would advance.As a fourth factor, states have an interest in keeping Internet warfare at bay and in avoiding overt attacks on other statesÃ¢Â Â™ network infrastructure. Once set loose, malware can be examined, repurposed, and used by the targeted country or by someone else. For instance, websites on the dark web now make Stuxnet available for download. It is said that the US government keeps several zero-day vulnerabilities in check in order to prevent hackers from using them. Until the Snowden revelations, Washington denied it had any cyber offensive capabilities, and now only acknowledges them grudgingly. What makes the US vulnerable is also its greatest strength. The United States is a city built upon a hill, its government a house of glass that is transparent to all. As a technology specialist put it, Ã¢Â Âœif you are in the glass house, you should not be the one initiating throwing rocks at each other.Ã¢Â Â• Internet warfare operates under a veil of ignorance; the fog of war is made thicker by technology. The most difficult problem of cyber protection is that you may not actually know who is attacking you or what the assailant is planning. Even when an attack can be traced to a country, there is usually uncertainty about its ultimate origin. Aggressors can also mount Ã¢Â Âœfalse flagÃ¢Â Â• operations designed to look like they are coming from another group or nation-state. But this cloak-and-dagger game can only lead you so far: once exposed, states risk massive retaliation, and even the United States are not exempt from the sanctioning power of public opinion. Even staunch allies like

Germany have reacted strongly to the revelations put forth by Wikileaks and Edward Snowden. Silicon Valley companies also have an interest in limiting diversion of the information they collect: they all operate globally, and donÃ¢Â Â™t want to be perceived as pawns in the hands of warmongers in the Pentagon or at Fort Meade.As Adam Segal puts it, Ã¢Â Âœsuccessful policymaking in cyberspace requires an understanding of technology, economics, anthropology, sociology, and international relations.Ã¢Â Â• In other words, it calls for a new synthesis or convergence of disciplines that have each gone their separate ways. It also requires a perspective that takes into account the multipolarity of the new world order. The approach needed to sustain policymaking in the digital age should be interdisciplinary and intercultural. This raises a rare challenge for policy advisers, scholars and students alike. Interdisciplinarity is more often invoked than practiced. Acknowledging that there are several viewpoints and perspectives on a single phenomenon goes against the traditional approach of scholarly disciplines, which all claim exclusive competence on their object. In addition, disciplines are shaped by the phenomenon that they study. They were constituted in an age when there were no Internet, when non-state actors were relegated at the margin, and when globalization was still in its infancy. Adapting to this brand new world needs more than just turning old lenses to new topics.To what extend does this book succeed in producing the new synthesis needed to study the new international order? Compared to other essays like Fred KaplanÃ¢Â Â™s Dark Territory (which I reviewed on this website), it is more global in its reach and takes the emerging multipolarity seriously. The cyber policies of China, Russia, and Brazil are reviewed in some detail, and there are also interesting highlights on Israel, Estonia, Georgia, Iran, and North Korea. The book is not a WhoÃ¢Â Â™s Who in CyberdefenceÃ¢Â Â”by some estimates, 29 countries have formal military or intelligence units dedicated to offensive operations online, and a variety of skilled non-state actors can also launch digital assaults. But at least, it is not exclusively focused on the United States. As for disciplinary advancement, the book doesnÃ¢Â Â™t claim to make an academic contribution to the field of International Relations theory. It is a journalistic survey, not a scholarly work. The hacked world order it describes is not a new international system where the laws of war and peace would no longer apply. The new synthesis of disciplines and methodologies that is deemed necessary for effective policymaking in the twenty-first century is still waiting for its Machiavelli, its Clausewitz, its Hans Morgenthau or its Kenneth Waltz.

Segal details how the internet has evolved from its academic roots to another frontier in the international power struggle between nation-states. Fair and uncompromising in its analysis, Hacked World Order lets no country off the hook, least of all the United States. Dark in its realistic

appraisal of how countries have entered the business of hacking in support of their own interests, the book also suggests a framework for establishing the rules of future cyberwarfare, in order to ensure that the relative stability inherent in the balance of power in the physical world has its counterpart in the virtual world. A fascinating, illuminating, and compelling read.

There are a number of books out regarding cyber security. This one does a pretty good job of remaining grounded in the real world problems of the politics and cultural impacts of a rapidly changing vector of man and technology. Unfortunately there are not enough people interested enough to understand the implications of cybersec and dare I cyber safety. The takeaway is that there are real opportunities in the cybersecurity industry for clever people and clever machines...

Excellent book. A must read for everyone.

It was a very interesting read.

Great Info- Hard read!

The Information Age or, as this author describes it, the Digital Age, dominates the early 21st Century. Change, brought about by computers, sensors, the internet, and the exponential interconnection of the globe because of our implementation of these technologies, races ever faster forcing individuals and societies to adjust at an ever increasing pace. I set out to explore these phenomena through 3 books: Information - A Very Short Introduction; The Hacked World Order; and, Only Humans Need Apply. This is the second of those 3 books. It met my expectations.Adam Segal, the author, is, among other roles, the Director of the Program on Digital and Cyberspace Policy at the Council on Foreign Relations. In this role, he has been a close observer of the political, military, economic and social effects of the global expansion of cyberspace. His interest, as is perhaps not surprising, is in the effect of governmental policy on the changes wrought by the Digital Age. If this is an interest of yours, you will be rewarded; but even if not, his focus on policy is not so exclusive that you can’t come away with new insights.As frequently occurs in such a review, Stuxnet provides an early example of the changed nature of the competition between nations. To his credit the author does not dwell excessively on Stuxnet perhaps in the expectation that his readers are already familiar with this event. His analysis also looks at the rise of other powers to challenge U.S. dominance of the internet. China and Russia clearly seed to usurp dominance, but Brazil does as

well. If you’re interested in how this is occurring, the book provides guidance.The impact of Edward Snowden’s revelations courses throughout the book. The effect of these disclosures on diminishing American moral authority cannot be discounted. The book examines this effect carefully and, I think, fairly so. It is not an America is bad and I’ll show you how hatchet job. I appreciated the, what appeared to me, fair treatment of a complex issue. Balancing moral values and national interest (with national interest being affected by the soft power conferred by morality) is not simple.Another matter that I was somewhat aware of, but insufficiently understood, is the difficult relationship between American national interests and U.S. based multinationals such as Facebook, Google, Microsoft, IBM and others. Trying to run one a dynamic technology-focused company doing business across the globe (and Europe can be as challenging as China) with the U.S. government seeking to use your company for its purposes undoubtedly challenges these companies’ management. Read the book to see how.In my mind Mr. Segal provided some useful takeaways for the Digital Age. The U.S. cannot expect to dictate the architecture of the internet; it will greatly affect the architecture, but other players will affect this architecture as well. China and Russia will continue to hack into U.S. information systems no matter what they say. Defenses against this must be undertaken and will be ever evolving. On page 226 of the hardback he quotes Jessica Mathews, the former president of the Carnegie Endowment for International Peace, saying "Absolutes of the Westphalian system - territorially fixed states where everything of value lies within some state’s borders; a single, secular authority governing each territory and representing it outside its borders and no authority above states - are all dissolving." This may be the most important takeaway.The book met my expectations for this part of my investigation of the Information Age. I recommend it highly.

Age of Order: Book 1 of the Age of Order Saga Hacked: The Bundle HACKED Manipulation: 12 Dangerous Persuasion Secrets Used by The World's Most Powerful Men to Manipulate, Persuade & Influence People (Manipulation Series) Mail Order Bride: The Mail Order Bride and the Hunted Man: Sweet, and Inspirational Western Historical Romance (Mail Order Brides and the Marriage Agent Book 4) Stephen King Series Reading Order: Series List - In Order: The Dark Tower series, Shining series, Talisman series, The Green Mile series, stand-alone novels, ... (Listastik Series Reading Order Book 30) Anne McCaffrey Series Reading Order: Series List - In Order: Dragonriders of Pern series, Acorna series, Catteni sequence, Brainships, The Talent series, ... (Listastik Series Reading Order Book 21) SERIES READING ORDER: DIANA GABALDON: Reading Order of Entire Outlander universe in reading order, Outlander series only, Lord John Grey series, short stories, novellas W.E.B. Griffin Series Reading Order: Series List - In Order: Presidential Agent series, Badge of Honor series, The Corps series, Honor Bound series, Brotherhood ... (Listastik Series Reading Order Book 14) Dale Brown Series Reading Order: Series List - In Order: Patrick McLanahan series, Acts of War series, Independent series, Dreamland series (Listastik Series Reading Order Book 24) J.A. Jance Series Reading Order: Series List - In Order: J.P. Beaumont series, Joana Brady Mysteries series, Ali Reynolds series, Walker Family series (Listastik Series Reading Order Book 13) Robert Ludlum Series Reading Order: Series List - In Order: Jason Bourne series, Covert-One series, Janson series, Stand-alone novels (Listastik Series Reading Order Book 15) Alexander McCall Smith Series Reading Order: Series List - In Order: No. 1 LadiesÃ¢â ¬â„¢ Detective Agency, 44 Scotland Street, Isabel Dalhousie, Portuguese Irregular ... (Listastik Series Reading Order Book 31) This Is Your Brain on Parasites: How Tiny Creatures Manipulate Our Behavior and Shape Society