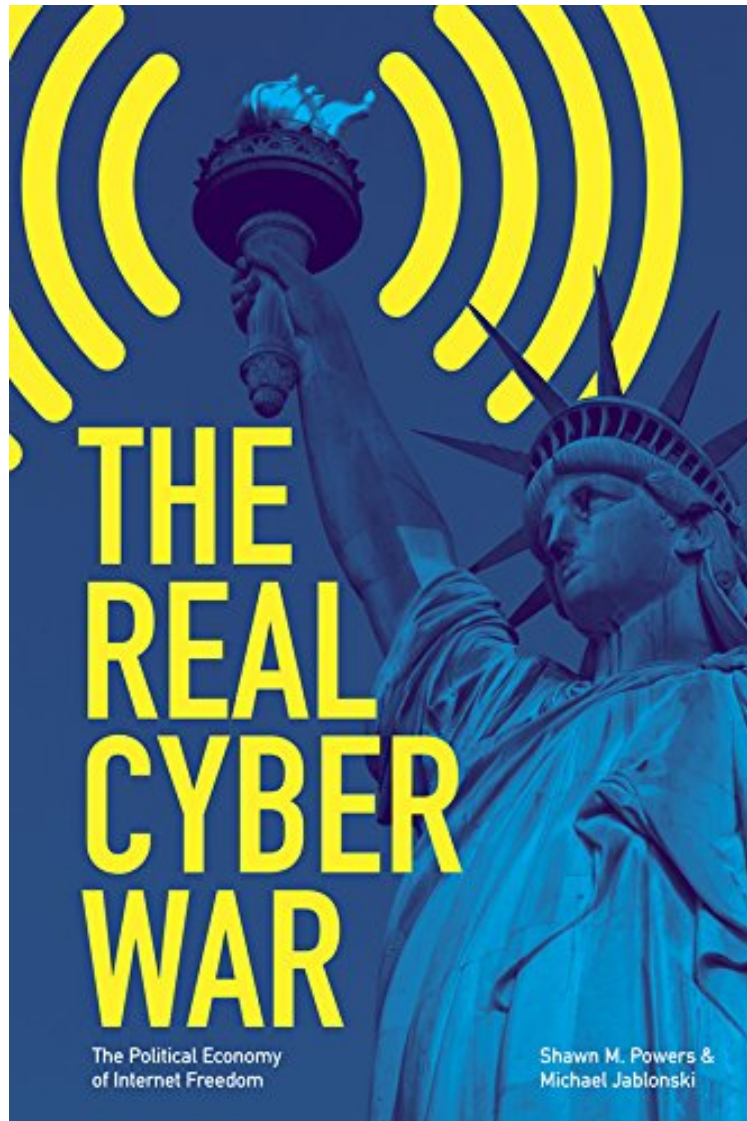


[Free read ebook] The Real Cyber War: The Political Economy of Internet Freedom (History of Communication)

The Real Cyber War: The Political Economy of Internet Freedom (History of Communication)

Shawn M. Powers, Michael Jablonski
DOC | *audiobook | ebooks | Download PDF | ePub



#1047154 in eBooks 2015-03-15 2015-03-15 File Name: B00UGIKUVA | File size: 79.Mb

Shawn M. Powers, Michael Jablonski : The Real Cyber War: The Political Economy of Internet Freedom (History of Communication) before purchasing it in order to gauge whether or not it would be worth my time, and all praised The Real Cyber War: The Political Economy of Internet Freedom (History of Communication):

1 of 1 people found the following review helpful. the depth and breadth of information collation can be amazing. If you don't believe this (and you belong ...By DarrenIngram_dot_comIt is fair to suggest that there are two types

of "cyber war"; affecting our ever-connected society. The first is the most commonly known, whether it is hackers and virus makers, Internet freedoms and identity theft or security issues. The less known form is the actions of nation states, who are seeking to restrict and control access domestically whilst aggressively seeking to ready itself for possible economic and military action by cyber means against future foes. It is the latter that the authors are focussing on in this fairly academic work. On one hand many governments are advocating Internet freedoms and greater connectedness in other countries, yet what are their real motives? Are democracy and humanitarian considerations being overridden by economic, geopolitical and military considerations? It might be easier to say one thing whilst doing something entirely different; U.S. foreign policy is considered along with the information-industrial complex and examination is made about the information-gathering powers of companies such as Google and how our freedom, or perception thereof, is actualised in a surveillance society where recording everything and anything is cheap and joining the dots to build a detailed dossier on a subject is an increasingly trivial task. Whether the information is being gathered by a government against a dissident or by a large corporation about a store customer, the depth and breadth of information collation can be amazing. If you don't believe this (and you belong to the vast majority of people who have not enabled a blocking option) request your search history from Google or your search engine of choice. Each and every line of every search spread over time can reveal a shocking insight into your behaviour. This is just one data point. Government bodies don't necessarily have a check box where you can elect for "no data collection" as well. Naturally the user has to trust the big company if it says that by checking this box, we won't store any data about you. No doubt lawyers could pore over a privacy policy and keep themselves in work for many years. Certainly this was an interesting, thought-provoking read although it is not something you would describe as being a lightweight work. It would have been nice if the book could have been a little more accessible for the average, non-academic reader as it covers a serious subject that deserves a wider audience. For the academic, as you would expect, the book features a very comprehensive index and extensive reference sources. It was an interesting, challenging read that is likely to stand the test of time and become a classic work.

3 of 3 people found the following review helpful. Dissecting "Freedom to Connect" By Richard Hill This review was originally published in boundary 2, at: <http://boundary2.org/2015/04/29/dissecting-the-internet-freedom-agenda/> Disclosure: the author of this review is thanked in the Preface of the reviewed book. Both radical civil society organizations and mainstream defenders of the status quo agree that the free and open Internet is threatened. The threats include government censorship and mass surveillance, but also the failure of governments to control rampant industry concentration and commercial exploitation of personal data, which increasingly takes the form of providing "freed" services in exchange for personal information that is resold at a profit, or used to provide targeted advertising, also at a profit. In *Digital Disconnect*, Robert McChesney has explained how the Internet, which was supposed to be a force for the improvement of human rights and living conditions, has been used to erode privacy and to increase the concentration of economic power, to the point where it is becoming a threat to democracy. In *Digital Depression*, Dan Schiller has documented how US policies regarding the Internet have favored its geo-economic and geo-political goals, in particular the interests of its large private companies that dominate the information and communications technology (ICT) sector worldwide. Shawn M. Powers and Michael Jablonski's seminal book *The Real Cyber War* takes us further down the road of understanding what went wrong, and what might be done to correct the situation. Their objective is to help us understand (citing from p. 19 of the paperback edition) "why states pursue the policies they do". The book "focuses centrally on understanding the numerous ways in which power and control are exerted in cyberspace" (p. 19). Starting from the rather obvious premise that states compete to shape international policies that favor their interests, and using the framework of political economy, the authors outline the geopolitical stakes and show how questions of power, and not human rights, are the real drivers of much of the debate about Internet governance. They show how the United States has deliberately used a human rights discourse to promote policies that further its geo-economic and geo-political interests. And how it has used subsidies and government contracts to help its private companies to acquire or maintain dominant positions in much of the ICT sector. Powers and Jablonski dissect the mechanisms by which vibrant government institutions deliberately transferred power to US corporations in order to further US geo-economical and geo-political goals. In particular, they show how a "freedom to connect" narrative is used by the USA to attempt to transform information and personal data into commercial commodities that should be subject to free trade. Yet all states (including the US) regulate, at least to some extent, the flow of information within and across their borders. If information is the "new oil" of our times, then it is not surprising that states wish to shape the production and flow of information in ways that favor their interests. Thus it is not surprising that states such as China, India, and Russia have started to assert sovereign rights to control some aspect of the production and flow of information within their borders, and that European Union courts have made decisions on the basis of European law that affect global information flows and access. As the authors put the matter (p. 6): "the [US] doctrine of internet freedom... is the realization of a broader [US] strategy promoting a particular conception of networked communication that depends on American companies... supports Western norms... and promotes Western products." (I would personally say that it actually supports US norms and US products and services.) As the authors point out, one can ask (p. 11): "If states have a right to

control the types of people allowed into their territory (immigration), and how its money is exchanged with foreign banks, then why don't they have a right to control information flows from foreign actors? The authors explain how the US military-industrial complex has morphed into an information-industrial complex, with deleterious consequences for both industry and government, consequences such as "weakened oversight, accountability, and industry vitality and competitiveness" (p. 23) that create risks for society and democracy. As the authors say, the shift "from adversarial to cooperative and laissez-faire rule making is a keystone moment in the rise of the information-industrial complex" (p. 61). As a specific example, they focus on Google, showing how it (largely successfully) aims to control and dominate all aspects of the data market, from production, through extraction, refinement, infrastructure and demand. A chapter is devoted to the economics of internet connectivity, showing how US internet policy is basically about getting the largest number of people online, so that US companies can extract ever greater profits from the resulting data flows. They show how the network effects, economies of scale, and externalities that are fundamental features of the internet favor first-movers, which are mostly US companies. The remedy to such situations is well known: government intervention: widely accepted regarding air transport, road transport, pharmaceuticals, etc., and yet unthinkable for many regarding the internet. But why? As the authors put the matter (p. 24): "While heavy-handed government controls over the internet should be resisted, so should a system whereby internet connectivity requires the systematic transfer of wealth from the developing world to the developed." But freedom of information is put forward to justify specific economic practices which would not be easy to justify otherwise, for example "no government taxes companies for data extraction or for data imports/exports, both of which are heavily regulated aspects of markets exchanging other valuable commodities" (p. 97). Thus the authors posit that there are tensions between the US call for "internet freedom" and other states' calls for "information sovereignty", and analyze the 2012 World Conference on International Telecommunications from that point of view. Not surprisingly, the authors conclude that international cooperation, recognizing the legitimate aspirations of all the world's peoples, is the only proper way forward. As the authors put the matter (p. 206): "Activists and defenders of the original vision of the Web as a 'fair and human' cyber-civilization need to avoid lofty 'internet freedom' declarations and instead champion specific reforms required to protect the values and practices they hold dear." And it is with that in mind, as a counterweight to US and US-based corporate power, that a group of civil society organizations have launched the Internet Social Forum. Anybody who is seriously interested in the evolution of internet governance and its impact on society and democracy will enjoy reading this well researched book and its clear exposition of key facts. One can fondly hope that this book will help to inspire a change in course that will restore the internet to what it might become (and what many thought it was supposed to be): an engine for democracy and social and economic progress, justice, and equity. 0 of 0 people found the following review helpful. A Must for those who want to understand diplomacy in a cyber warfare age By Ryan Mixson The most up-to-date and informed work on international diplomacy and business-government relationships in the new cyber landscape, Powers' and Jablonski's book is endlessly informative and meticulously sourced, but never short of utterly engrossing. From espionage to whistleblowers to the emergence of a new world where information is the highest-valued currency, "The Real Cyber War" is a must-read for anyone who expects to stay current on the new fronts of national security and tech-driven economies.

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.

"Shawn M. Powers and Michael Jablonski's seminal new book *The Real Cyber War*. . . will help to inspire a change in course that will restore the internet to what it might become (and what many thought it was supposed to be): an engine for democracy and social and economic progress, justice, and equity." --Boundary 2 "Shawn Powers and Michael Jablonski's book will be of particular use to International Relations scholars and readers eager to place

global digital issues and debates into their geopolitical and geo-economic contextshellip; Bringing together these fields has proved particularly necessary since Edward Snowden's revelations, which have shown that the internet policy has far-reaching implications which go beyond merely technical issues. This is precisely what Powers and Jablonski intend to do in this meticulous book."--International Affairs nbsp;