Media, War & Conflict
2016, Vol. 9(2) 217–224

DOI: 10.1177/1750635215616718
mwc.sagepub.com

Book reviews

Taylor Owen, *Disruptive Power: The Crisis of the State in the Digital Age*, Oxford University Press: Oxford, 2015; 264 pp.: 978 0199363865, £18.99/$27.95

Shawn M Powers and Michael Jablonski, *The Real Cyber War: The Political Economy of Internet Freedom*, University of Illinois Press: Urbana, 2015; 288 pp.: 978 0252080708, $25.00 (pbk)

Reviewed by: Nathalie Maréchal, University of Southern California, Los Angeles, USA

Taylor Owen's *Disruptive Power* and *The Real Cyber War* by Shawn M Powers and Michael Jablonski both examine the complicated and evolving relationship between actors in the contemporary international system and political uses of the internet. Though each project was initiated before Edward Snowden's landmark 2013 revelations about the pervasiveness and (many would say) wild illegality of the US National Security Administration's domestic and global electronic surveillance programs, both books are essential reading for anyone concerned about the shifting power relations between and among governments and the governed in the wake of the digital revolution – and we should all be concerned.

Disruptive Power is the broadest of the two in scope, providing 'a sweeping look at the way digital technologies are shaking up the workings of the institutions that have traditionally controlled international affairs', as the cover copy puts it. Owen essentially attempts to do in the context of the international system what Bob McChesney did with regard to the political economy of the US media in *Digital Disconnect* (2013): where McChesney points out the ways that media serve as a tool for power, money and influence to accumulate at the top and skewers what he calls the American catechism's doctrinal belief that media capitalism leads to information freedom, Owen explores existing and emerging actors' use of 21st-century communication tools to accumulate and assert power in the international system.

Until the summer of 2013, Owen focused his research on the 'tension' that states face 'as both enablers and targets of disruptive actors', hypothesizing that

> digital technology … was enabling nontraditional international actors to take on and in some important ways replace the capacity of states and large institutions in ways that were both filled with opportunity but also fundamentally destabilizing to the established international order. (Owen, 2015 14)

But, as he (and the world) would soon learn, in the aftermath of the 9/11 terror attacks, the US and other Western governments were so worried about the internet's potential to upend power relations that they became willing to compromise their own values and laws to maintain the status quo. This was made clear by the United States' NSA mass surveillance programs.

Following the Snowden disclosures, Owen's project grew to encompass the use of technology by democratic states and the implications of a 'digital arms race' between the public and the state (Owen, 2015: 15). These implications are far from straightforward, particularly in light of the diametrically opposed goals pursued by different government agencies. As Owen rightly points out regarding the US Internet Freedom agenda, which through ideology and strategic initiatives promotes ostensibly free and open public access to the internet, most stridently in the context of those living under what the US considers repressive regimes:

> The core challenge of the State Department's Internet freedom agenda is not that circumvention tools are a bad idea, or that the censorship and surveillance programs they are meant to counter are not damaging to civil society. It is that at the same time as the 21st century statecraft program was supplying Syrian dissidents with counter-surveillance technology the US government was simultaneously building a large-scale surveillance program of its own. What's more, at the same time the United States was supporting these dissidents to oppose certain regimes, the regimes were often buying their surveillance hardware from American corporations, at the same technology trade fairs as the US intelligence agencies. It is an understatement to say that activists will be suspicious of US efforts going forward. No matter how genuine the intentions, the State Department's Internet freedom agenda cannot be isolated from the wider actions of the US government. (Owen, 2015: 164)

This is fine scholarly analysis, though it risks oversimplifying the matter. The NSA mass surveillance programs were just as much of a surprise to the State Department officials working on the Internet Freedom agenda as they were to the general population (JN Tye, personal communication, March 2015). In addition, restricting exports of dissent-suppressing technology (much less so-called 'dual use' technologies) is a thorny policy problem that continues to thwart the existing export controls regime in spite of ongoing efforts such as the Wassenaar Arrangement, which limits cross-border sales of conventional weapons and other goods that can be used for warfare, including certain software. Moreover, if one accepts the premise that digitally empowered dissident and human rights groups are worthy of support, some may doubt the feasibility of these groups' viability without government funding, especially when there are relatively few other sources of funding that can be accessed without a professional fundraising machine. The US government and digital rights movements doubtless make for strange bedfellows, but it is highly disputable that these groups lack an agenda separate from that of the US government, a sophisticated understanding of the geopolitical stakes, or agency, as certain passages seem to suggest.

Indeed, in places *Disruptive Power* appears to adhere to a common view that diminishes the agency of activist groups who receive government funding, depicting them as mere tools of foreign policy. For example, Owen's discussion of the Global Dialogue on the Future of Iran (ch. 7) is grounded in several factual mistakes, which to his credit he

fully acknowledges (T Owen, personal communication, August 2015). In Owen's account, the event was initiated by the Canadian Department of Foreign Affairs and International Trade (DFAIT), which then 'partnered with the Munk School of Global Affairs at the University of Toronto, specifically researchers from the Citizen Lab and ASL19', described by Owen as 'a research lab that helps Iranians engage with surveillance circumvention technology' (p. 149). In fact, ASL19 is a digital rights group comprising members of the Iranian diaspora as well as contributors based in Iran, founded and headed by University of Toronto PhD student Ali Bangi. It does not work on tools designed to evade surveillance, but to localize existing software for bypassing censorship. ASL19 works closely with, but is distinct from, the Citizen Lab, an interdisciplinary research lab that studies information controls and circumvention technology worldwide. ASL19 does receive grants from the US and Canadian governments, but its staff were rather dismayed by the implied suggestion that they were tools of Canadian foreign policy. Nevertheless, readers would do well to focus on the book's core argument rather than on this oversight, which Owen will hopefully have the chance to rectify in a future edition of the book.

Perhaps the greatest contribution of *Disruptive Power* is the book's deft tackling of a wide range of topics, drawing connections between seemingly mundane developments like the growth of social media or proliferation of internet-connected devices and high-profile phenomena like Anonymous, the 2011 Arab Spring, WikiLeaks, and NSA surveillance. Such media events may seem far removed from the daily lives of casual observers, but Owen makes clear that they are all manifestations of the same trend: the global public sphere's gradual migration from traditional print and broadcast media to the internet, a playing field over which governments are only starting to exert control, and whose technical architecture thumbs its nose at Westphalian notions of national sovereignty (see Mueller, 2010).

Throughout the book Owen highlights the dangers that ICTs, in the hands of the state, can present for free societies, but the author's primary focus is the impact of ICT use by non-state actors on traditional statecraft and national sovereignty. This is the exact opposite of the concerns put forward by many technoskeptics (Deibert, 2013; MacKinnon, 2012; Morozov, 2011) who argue that ICT use by state actors (mediated by the private sector) poses a threat to civil society and individual rights. This difference in the object of analysis is what sets apart *Disruptive Power* – and arguably what allows the author to conclude with more optimism than other researchers in the field. Owen ponders:

> What would a state's policy toward the Internet look like if it were to embrace the voices, values, and attributes of those who live in the networked world? What if a foreign policy were to assertively seek to protect the very foundation of the system that powers the 21st century? (p. 206)

These are vital questions, even if their focus on the nation-state instead of the individual may frustrate the growing international community of digital rights activists.

The Real Cyber War, by Shawn Powers and Michael Jablonski, interrogates further the motivation behind the US Internet Freedom agenda. This book was also begun before the Snowden revelations of 2013, but the NSA's mass surveillance programs are

tangential to its argument. Relying on primary document analysis, Freedom of Information Act requests, and interviews with elites, Powers and Jablonski present a strong case that for the US government, the promotion of internet freedom is primarily about maintaining and extending US economic dominance into the 21st century and beyond. The authors are very clear about their approach:

> Rather than normatively assessing the different Internet policies enacted by states, arguing which is more in line with a particular set of values, this book approaches the topic from a different perspective. It examines the geopolitics of Internet policies, identifying and analyzing why and how states compete to shape policies, technologies, and norms that structure the role of the Internet in society … It aims to facilitate a more pragmatic discussion that eschews the value-laden language of Internet freedom, Orwellian surveillance, globalization and censorship. (p. 5)

Powers and Jablonski are equally clear that they are not rejecting the broad values of internet freedom per se (and even seem to embrace them), and that the book's focus is squarely on the US motives behind the strategy, not on its effects: 'There is certainly humanitarian value to these initiatives, as many in the mainstream media and government have suggested. But the underlying economic and political motivations driving these efforts deserve greater critical inquiry' (p. 6). This is certainly important research, yet it bears repeating that neither the aim nor the conclusion of this book is to undermine the goals, arguments or tactics of the civil society part of the internet freedom equation, despite what net-freedom skeptics on both the right and left may claim.

Geopolitical arguments over information flows fall into two broad camps: those who favor the rights of sovereign states to regulate flows within their borders, and those who champion the right of individuals to seek, receive, and impart whatever information they choose. As Powers and Jablonski describe, on the one hand the onus is on the state to proactively control the flow of bits and bytes, using advanced and evolving technologies. The Chinese Xinhua News Agency has observed, 'The emergence of information technology has posed a great challenge to the traditional concept of national sovereignty, as well as one's ability to safeguard sovereignty' (p. 14). This is why countries like China seek to move internet governance to the United Nations, whose one-state, one-vote rules would (they hope) help ensure the protection of their information sovereignty against the advances of an array of powerful non-state actors. On the other hand, the authors point to scholars like Tim Wu and Milton Mueller, whose work suggests that trying to apply strict interpretations of national sovereignty to the digital space is incompatible with the recognized rights of free expression, access to information, and privacy (Mueller, 2010; Wu, 2011). Powers and Jablonski position their book as filling the gap between these two schools of thought, through a critical examination of the tensions between geopolitics and modern connective technologies. The debate over internet freedom and internet sovereignty is but one – albeit important – manifestation of these tensions.

After tracing the histories of the actors, institutions and norms that oversee the commodification of data, the book addresses the economic drivers of US internet policy, which 'can be boiled down to getting as many people using the network of networks as

possible, while protecting the status quo legal, institutional arrangements governing connectivity online' (p. 23). The status quo, of course, benefits the US as incumbent hegemon. Here the central argument of the book is crystalized:

> The real cyber war is not over offensive capabilities or cybersecurity but rather about legitimizing existing institutions and norms governing Internet industries in order to assure their continued market dominance and profitability … 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. (p. 24)

Subsequent chapters tackle multistakeholderism, the growing trend toward internet fragmentation (such as the creation of national 'intranets'), the friction between cybersecurity policy and the digital rights movement, and the conundrum of anonymous online speech. The conclusion defines the titular real cyber war as 'a competition among different political economies of the information society' (p. 203), in the middle of which civil society struggles to find its own path:

> Turning to civil society, activists and academics alike need to be much more cautious in their use and defense of internet-freedom discourse. This is not to suggest that they should abandon the idea of Internet freedom altogether; quite the contrary. Instead, this analysis shows how the Internet-freedom narrative is used to legitimize a particular geo-strategic vision of the Web that has little to do with the foundational principles of Internet freedom, including freedom of expression and net neutrality. Activists and defenders of the original vision of the Web as a 'fair and humane' cyber-civilization need to avoid lofty 'Internet freedom' declarations and instead champion specific reforms required to protect the values and practices they hold dear. Additional research is also needed to identify how specific corporate policies undermine freedom online, and which institutional arrangements allow for governments and companies to weaken the integrity of the Web. (p. 206)

This is poignant analysis, though one must question whether the digital rights movement should relinquish or feel pressured to abandon its own narrative simply because the US government has appropriated it. Moreover, after Snowden, US officials have stayed away from the lofty language of the first Obama administration, precisely because the contrast between this utopian liberalism and the sinister realities exposed by the former NSA contractor make them look like hypocrites.

Both *Disruptive Power* and *The Real Cyber War* are impressively researched and highly accessible, timely books. Each would be an excellent resource for undergraduate or graduate courses in international communication or international relations. Indeed, these authors demonstrate the degree to which scholars of communication have thus far outstripped their international relations counterparts in grappling with the geopolitical significance of the internet. These books are not limited in reach to the scholarly audience, however: both would also be suited to policy practitioners and to the general public, particularly to anyone engaged in the emergent digital rights movement as a participant, critic or observer.

References

Deibert R (2013) *Black Code: Inside the Battle for Cyberspace*. Toronto: McClelland & Stewart.
MacKinnon R (2012) *Consent of the Networked: The World-Wide Struggle for Internet Freedom*. New York: Basic Books.
McChesney RW (2013) *Digital Disconnect: How Capitalism Is Turning the Internet Against Democracy*. New York: The New Press.
Morozov E (2011) *The Net Delusion: The Dark Side of Internet Freedom*. New York: Public Affairs.
Mueller M (2010) *Networks and States: The Global Politics of Internet Governance*. Boston, MA: MIT Press.
Wu T (2011) *The Master Switch: The Rise and Fall of Information Empires*. New York: Vintage Books.

Beatrice de Graaf, George Dimitriu and Jens Ringsmose (eds), *Strategic Narratives, Public Opinion, and War: Winning Domestic Support for the Afghan War*, Routledge: Abingdon, 2015, xxvii + 380 pp.: ISBN 978 1 138 78042 2 (hbk), ISBN 978 1 315 77073 4 (ebk)

Reviewed by: Thomas Colley, Department of War Studies, King's College London, UK.

Much has been written in the last decade on the importance of narratives in shaping public support for war. Indeed so enthusiastically has the narrative turn been embraced that many consider storytelling the key weapon in contemporary war. Amongst this literature, *Strategic Narratives, Public Opinion, and War* is the most comprehensive volume to date on how narratives can be used to persuade publics to support military interventions. This edited work combines theoretical contributions from some of the leading authors in the field with an impressively broad case study: the efforts of over a dozen states participating in the International Security Assistance Force (ISAF) mission in Afghanistan to persuade their publics to support the war. By providing a comprehensive, comparative account of the 'possibilities and limitations of strategic narratives' (p. 17), the book is invaluable for those looking to better understand how governments seek to convince publics to support military interventions today.

The central argument is that governments can actively shape and sustain public support for war through the strategic construction and deployment of narratives. This may be harder in some political contexts than others, such as when elites disagree on the virtue of the mission or have to persuade particularly cynical publics to accept growing casualties. Nevertheless, by communicating clear, consistent 'storylines' (p. 1) that emphasize progress and future success, governments will be more successful in sustaining public support for war. Having demonstrated this using Afghanistan, the authors offer four 'ideal type arguments' (p. 355) for governments to use, depending on whether the policy goal is immediate or more remote, and whether the mission is driven by moral or national security considerations. Using this framework, they show that while there were significant differences in how administrations 'marketed' Afghanistan, most initially framed it as a national security issue, but then shifted over time to ethical concerns such as helping Afghan civilians.