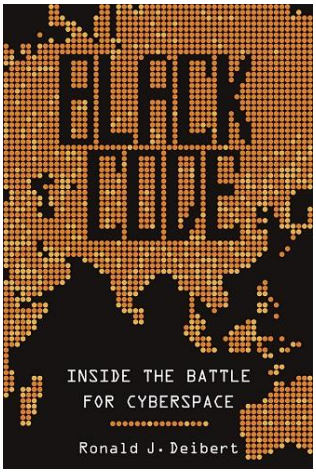
International Journal of Communication 7 (2013), Book Review 2730–2732 1932–8036/2013BKR0009

Ronald J. Deibert, **Black Code: Inside the Battle for Cyberspace**, Signal, 2013, 312 pp., $29.99 (hardcover).

Reviewed by
Sarah Myers
University of Southern California



There is an eerily prescient moment near the beginning of Ronald J. Deibert's ***Black Code: Inside the Battle for Cyberspace***. Deibert describes a program spearheaded by a former admiral and CIA operative that was brought before Congress for approval in the wake of 9/11. The proposed program aimed to integrate all data known to the government about American citizens—credit card transactions, tax documents, flight records, and so on—into a single searchable database. Congress rejected the program, presumably in part because of its sponsor's murky past connections to the Iran-Contra affair. Yet many experts believe the program did not die when it was rejected and instead was subsumed under an intelligence "black budget." This program, perhaps, became the NSA's PRISM program, which was revealed to the public one month after *Black Code* was published.

Black Code focuses on the murky spaces of the Internet that are rarely the subject of deep analysis because they are so difficult to study. Deibert's central argument is that Internet insecurity and the growing imperative to control the Web presents an imminent threat to the openness and dynamism of cyberspace. Deibert, who heads the Citizen Lab at the University of Toronto, seeks to "combine technical interrogation, field research, and social science to lift the lid on the Internet" (p. 5). The book is written for non-experts and serves as a useful primer for the general reader interested in understanding the wide and complex range of issues associated with cyber-security.

Deibert brings clarity to the project of tracking networks of cyber-crime and surveillance. He chronicles Citizen Lab's effort to map out GhostNet, a massive cyber-espionage program that surveilled numerous foreign affairs ministries, state agencies, international organizations, and global media outlets, eventually impacting more than 100 countries. Using the same types of tools as GhostNet's hackers and a sting operation worthy of Hollywood's attention, Deibert and his colleagues traced the origins of GhostNet to a People's Liberation Army compound on Hainan Island in China, leading to a detailed exploration of a cyber-espionage network. He notes, "We are used to our computers being windows onto the world. With GhostNet, we argued that 'it is time to get used to them looking back at us'" (p. 27).

GhostNet is one example of the broader trend toward militarization of cyberspace, which Deibert calls the "cyber-security industrial complex." The key players include government agencies and corporate entities specializing in selling sophisticated tools for cyber-surveillance and cyber-warfare. He describes an underground, massively expanding industry trading on products like FinSpy (a "Remote Monitoring and Infection Solution") that would allow users to break into and secretly monitor Skype conversations, turn

on webcams, and explore the hard disks of the computers of its unwitting targets (p. 196). A 2013 Citizen Lab report found that FinSpy is actively used in at least 25 countries, including Bahrain, Bangladesh, Ethiopia, Germany, India, Mexico, the United Kingdom, and the United States.

North American and European countries traditionally dominated the cyber-surveillance industry, but increasingly its growing client base is located in the Global South. This reflects broader shifts in the makeup of cyberspace that will powerfully affect the Internet, especially the shift in the population of Internet users to emerging economies: "The Internet may have been born in Silicon Valley or Cambridge, Massachusetts, but its destiny lies in Shanghai, Delhi, and the streets of Rio de Janeiro, the places where its next billion users are going to come from" (p. 71).

Internet use is growing most rapidly among the world's failed and most fragile states: the International Telecommunication Union's 2009 Information Society Statistical Profiles found that the 10 fastest Internet-user growth rates since 2004 were in Afghanistan, Myanmar, Vietnam, Albania, Uganda, Nigeria, Liberia, Sudan, Morocco, and the Democratic Republic of the Congo (p. 88). As a result of the lack of state infrastructure, nonstate and noncorporate actors powerfully influence online freedoms. For example, Mexican drug cartels employ sophisticated communication technologies to exert control over the public (p. 98). Members of cartels like the Zetas effectively use YouTube videos to issue threats and intimidate police and the public, posting gruesome images of beheadings as warnings against reporting on cartel activities online. The cartels are not alone—the Taliban, Al-Shabab, and others have gone online to mark their digital turf. These shifts will profoundly impact the texture of cyberspace and further complicate the work of policymakers seeking to shape the Internet's future.

Black Code also suggests that the more imminent threat may come not from cyber-crime or cyber-warfare, but from corporate incursions on user freedoms through end-user license agreements, surveillance of consumers, and the like. Although Internet networks are often presumed to be highly resilient, this is a long-standing myth that obscures the fragility of the Internet's architecture. This becomes more important with the increased use of Internet platforms by the public for deliberative politics, even though they were originally constructed for commercial purposes (p. 107). Moreover, corporations face increasing pressure from activist states that delegate much of their policing to corporations that often fall outside the law—dynamics illustrated within Google's and Twitter's transparency reports. It is especially worrisome that the countries that most frequently use extrajudicial means to police cyberspace are democracies (p. 115). Indeed, "never before have we had such a grand illusion of freedom through technology, when, in fact, that very freedom and technology are constrained by ever-expanding state laws and corporate regulations" (p. 231).

To begin to lift the veil of darkness from this landscape, *Black Code* recommends specific, actionable solutions that are especially timely in the wake of PRISM. Civic groups that aim to protect user rights often associate security with surveillance and censorship, which they view with disdain. Deibert urges civic networks to seek solutions that make the Internet more secure while preserving cyberspace as an open commons of information (p. 237). Greater resources should be devoted to law enforcement to combat cyber-crime—so long as resources come with proper training and equipment and there is judicial oversight and public accountability (p. 243). Finally, Deibert argues that universities should be the

stewards of an open and secure cyberspace. After all, the Internet was born in "the University," and acquired its guiding principles of peer review and transparency there (p. 244). *Black Code* only scratches the surface of the dark waters of the Internet, but it is an accessible volume that describes the broad landscape of cyber-security issues and suggests recommendations for sound policy making and informed advocacy that could help preserve cyberspace as a free and open commons.