In the book's denouement, Venter imagines futures when biology can shuttle seamlessly between the material and the informatic. Drawing examples from Star Trek and Doctor Who, he speculates that DNA sequencing and synthesis are paired technologies for dematerializing, digitizing, and subsequently rematerializing life. He's confident that soon "we will be able [to] send a robotically controlled genome-sequencing unit in a probe to other planets to read the DNA sequence of any alien microbe life that may be there." If such a sequence is beamed back from Mars, "we should be able to reconstruct the genome. The synthetic version of the Martian genome could then be used to re-create Martian life."

Although fantastic, such scenarios proffer one answer to Schrödinger's question. What was life in 1943, what is it in 2013, and what will it become next? Despite staggering developments in molecular biology since the 1940s, I'm struck by how little has changed. If Venter is to be believed, life itself has been recreated, yet the same hoary debates are still being aired: mechanism versus vitalism, form versus substance, experimental deduction versus proof by synthesis. Life, it seems, moves more slowly than Venter supposes.

References

1. J. C. Venter, *A Life Decoded: My Genome: My Life* (Viking, New York, 2007).
2. E. Schrödinger, *What Is Life? The Physical Aspect of the Living Cell* (Cambridge Univ. Press, Cambridge, 1944).

10.1126/science.1243547

THE INTERNET

The Cyber-Espionage X-Files

Laura DeNardis

Former U.S. Secretary of State Hillary Clinton once delivered a soaring speech on Internet freedom urging American media corporations to challenge "foreign governments' demands for censorship and surveillance." Three years later, Internet-freedom advocates experienced the cognitive dissonance of juxtaposing this rhetoric with revelations about the U.S. National Security Agency's (NSA's) expansive digital surveillance practices. These disclosures came as no surprise to those who have read Ron Deibert's *Black Code*.

Although the Internet's exosphere of content and applications is visible to users, the majority of the network's technical and material architecture lies deeply concealed beneath this surface. The structure and governance of the Internet's underlying infrastructure—comprising code, hardware, protocols, switches, and other virtual and physical resources—is hardly neutral but rather constrains behavior through technical design, direct governance, and private contractual agreements. The multivariate metaphor "black code" refers to this hidden nature of cyberspace infrastructure and also to the clandestine sphere of nation-state intelligence gathering and warfare in cyberspace (invoking Black Ops) and more nefarious online criminal practices (invoking Black Hat hacking).

Many readers will find *Black Code* both illuminating and terrifying. State power over the Internet is escalating, with the exact same technologies that provide unprecedented opportunities for free expression being used to enact surveillance and censorship of citizens by authoritarian governments and liberal democracies alike. In a book researched and penned prior to Edward Snowden's whistleblowing on NSA surveillance, Deibert (a political scientist at the University of Toronto) cites a former NSA employee who estimated that "billions" of phone calls and "voluminous" quantities of e-mails are electronically processed every day.

Black Code
Inside the Battle for Cyberspace

by Ronald J. Deibert
Signal (McClelland and Stewart), Toronto, 2013.
320 pp. $29.99, C$32.99.
ISBN 9780771025334.

Government surveillance does not happen sui generis but requires cooperation from the private companies—social media platforms, search engines, and transactional sites—that serve as information intermediaries. Big data gathered around routine Internet use through these private intermediaries fuel the online advertising business models enabling free and unprecedented access to knowledge. But collecting these data (including metadata such as geographical location, phone number, and unique technical identifiers) creates unprecedented challenges to individual privacy and opportunities for surveillance. As Deibert graphically portrays private industry data capture, "Like a giant python that has consumed a rat, Facebook captures, swallows, and slowly digests its users."

One of *Black Code*'s contributions is to illumine the privatized political architecture of the Internet's core technologies. Deibert once toured a Toronto Internet Exchange Point, a shared switching facility at which networks conjoin to collectively compose the global Internet. A tour guide's response to his query about "hundreds of what appeared to be randomly distributed red tags attached to the equipment" was "Oh, those are the wiretaps."

Deibert also unearths the subterranean battles at the Internet's core via his account of the investigative work of the University of Toronto's Citizen Lab, which he founded in the spring of 2001 to "lift the lid on the Internet" and research global security issues in cyberspace. Using a combination of technical forensic analysis and social science research methods, Citizen Lab exposed a disturbing world of digital subterfuge, including "GhostNet," a global cyber-espionage network that had compromised computers operated by ministries of foreign affairs, major news outlets, embassies, and numerous global institutions. The Dalai Lama's computers having been infiltrated, his administration granted Citizen Lab unrestricted access to them. Citizen Lab analysts infiltrated a cyber-espionage operation for months, discovering that the attackers used the freely available open-source cyber-intrusion tool Ghost RAT.

The book also conveys examples of the Internet's vulnerability to inadvertent problems, such as when Internet access in the nation state of Georgia "went dark" for 12 hours after an elderly woman with a shovel accidentally severed a critical fiber-optic cable. Basic societal structures of financial flows, energy infrastructures, social interactions, and commerce depend on the Internet, an infrastructure whose technical architecture and governance are in constant flux.

Black Code ties together usually disparate subject matter—big data, new business models based on online advertising, cybercrime, infrastructure vulnerability, and geopolitical power struggles—into a coherent exposé of what is at stake in how the Internet is designed, governed, and infiltrated. In it, Deibert uncovers more problems than solutions (which he addresses elsewhere), but this is a refreshing change from prevailing narratives about social media–driven democratic revolutions. In reality, the Internet's architecture is now ground zero for geopolitical conflict, rising state power, and the future of what counts as basic civil liberties in the digital era.

10.1126/science.1244722

The reviewer, the author of *The Global War for Internet Governance*, is at the School of Communication, American University, 4400 Massachusetts Avenue NW, Washington, DC 20016, USA. E-mail: denardis@american.edu

Published by AAAS