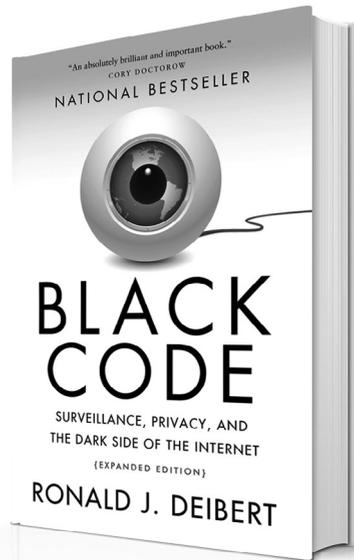


Black Code: Surveillance,  
Privacy, and the Dark  
Side of the Internet  
by Dr. Ronald J. Deibert

Reviewed by CDT Monte Ho  
and Dr. Jan Kallberg



Dr. Ronald J. Deibert’s book *Black Code: Surveillance, Privacy, and the Dark Side of the Internet* addresses growing concerns regarding international cyber threats and argues against current countries’ methods of responding to these threats. Deibert presents a solid, well-rounded argument, with intriguing evidence to support his assertions regarding our flawed cybersecurity environment, and closes *Black Code* with personal recommendations to secure and regulate the cyberspace domain. Readers receive a broad spectrum analysis of cyberspace and cybersecurity and are provided specific information on the actions and interactions of hackers, international governments, and related cyber industries. *Black Code* reads like a cyber novel; brilliantly crafted with a strong foundation and argument against current cybersecurity techniques and practices. Dr. Deibert is Professor of Political Science, and Director of the Citizen Lab at the Munk School of Global Affairs, University of Toronto. The Citizen Lab is described as “an interdisciplinary research and development laboratory working at the intersection of the digital technologies, global security, and human rights.”

Dr. Deibert opens *Black Code* with a revealing description of his background as a researcher at the Citizen Lab and a detailed accounting of how modern cyberspace is defined. The first few chapters give readers a baseline knowledge of the physical and theoretical components of cyberspace, and how these pieces, functioning together, provide the entirety of the Internet. He then provides compelling facts and in-depth analysis of cyber threats ranging from Internet pranksters to violent terrorist groups

and even nation-backed cybercriminals. Readers learn about metadata and how much data they surrender to their online accounts, which are increasingly vulnerable to attacks from international hackers operating outside of national jurisdiction. Dr. Deibert moves between referencing cybercrimes such as GhostNet and Stuxnet and the masterminds behind them to the role companies like Google and Facebook play in securing user information, not only from cyber criminals but also from governments around the world. He believes private industry has too much power in policing cyberspace and that governments are trying to use these giant corporations to regulate cyber freedom and invade netizens' privacy.

Stylistically, this author is very descriptive with lengthy paragraphs that contain technical information, which some new cyber readers might find difficult to understand. His arguments are strong and have substantial supporting evidence, but are sometimes hidden within multiple layers of text. However, his broad range of evidence from different situations and locations from around the world make his argument nearly impenetrable. It would be difficult to find a hole in his arguments with the logical and convincing conclusions he presents to readers. Dr. Deibert also stresses the seriousness of cybersecurity, citing cyberwarfare and government involvement in cyberattacks against other nations as an indictment of the current state of cyberspace.

Dr. Deibert considers cybersecurity from many different perspectives and presents arguments both for and against the tightening of cybersecurity despite his personal belief in the latter. His arguments have an abundance of evidence and examples, making *Black Code* a must-read for cyber practitioners. Though his writing is at an advanced level and requires some knowledge of the cyberspace domain, readers will be captivated by his arguments' applicability and importance to their everyday lives as well as global affairs. It is an intriguing and captivating work that provides an insider perspective of the cyberspace domain with its contentious issues. The author's solutions to these global cybersecurity challenges deserve a broad audience. 🛡️

*Black Code: Surveillance, Privacy, and the Dark Side of the Internet*

Author: Ronald J. Deibert

Publisher: Signal/McClelland & Stewart/Random House (November 19, 2013)

Paperback: 336 pages

Language: English

ISBN-10: 0771025351

ISBN-13: 978-0771025358

Price: \$8.00 Paperback

\$14.00 Kindle Edition



**Cadet Monte Ho** studies Computer Science at West Point and is a rising Cow. She is also the cadet executive officer of the Army West Point Cycling team, which is nationally ranked first by USA Cycling in Division II for 2016-2017. She is originally from Los Angeles, California and participated in an AIAD last summer, through the USC Institute for Creative Technologies in Playa Vista, involving the design of a Military Intelligence role tutorial. Upon graduation, she hopes to branch Cyber.



**Dr. Jan Kallberg** is Assistant Professor of American Politics in the Department of Social Sciences and Cyber Policy Fellow at the Army Cyber Institute at West Point. He holds a Ph.D. in Public Affairs and a Master's of Political Science from the University of Texas at Dallas; and a JD/LL.M. from Stockholm University. Prior to joining the West Point faculty, Jan was a researcher and Post-Doc at the Cyber Security Research and Education Institute, Erik Jonsson School of Engineering and Computer Science, at the University of Texas at Dallas under Dr. Bhavani Thuraisingham. Dr. Kallberg's research interest is the intersection between public leadership and cyber capabilities; especially offensive cyber operations as an alternative policy option. His personal website is [www.cyberdefense.com](http://www.cyberdefense.com).