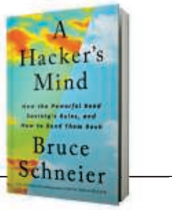
SCIENCE AND SOCIETY

Hacking and the social contract

Although technical fixes can help, solutions must focus on broader societal factors at play

A Hacker's Mind: How the Powerful Bend Society's Rules, and How to Bend Them Back
Bruce Schneier
Norton, 2023. 304 pp.



By **Viktor Mayer-Schönberger**

The concept of "hacking" is not an invention of the digital age. Nor is it a purely technical process, although today it often requires some technical expertise. Humans have always tried to find loopholes in the systems of rules we find ourselves beholden to. When we reach a wall, we try to find a way around it.

Bruce Schneier's *A Hacker's Mind* is a collection of fairly short, often insightful commentaries about hacking. Schneier is one of the nation's most well-known cybersecurity experts, and his prose is clear, jargon-free, and a pleasure to read. A reader might pick up this book for the numerous instructive cases and vignettes it offers, but conceptually, *A Hacker's Mind* advances an important point; and it is hugely revealing that Schneier—a computer scientist—is making it.

People have long sought to hack society's conventions and legal norms—from taking advantage of tax loopholes to creatively evading military drafts—and they do so most often by bending social rules. Hence, Schneier sees hacking as a social rather than a technical phenomenon.

This might sound like a simple reframing, but it has huge consequences. It effectively dispenses with the naïve hope that hacking can be "solved" through technical fixes, although technology can, of course, be a part of the solution. Effective responses, argues Schneier, need to be socially anchored as well.

When we talk about hacks, we often think of their negative consequences, or what economists call "externalities": taxes go unpaid, cars designed to cheat emissions inspections pollute the environment. But some hackers repurpose a social system for their own ends. For instance, a group of kids hacked the prohibition of free-form text communication in Disney's online kids game Club Penguin by using their avatars' body positions to communicate letters. Seen from this perspective, hackers can be social innovators—probing, reinterpreting, circumventing, and even breaking established norms.

Schneier is at his best when he details the balancing act in society between our social systems that ensure rules are followed and the importance of keeping an open mind toward norm innovation–causing hacking. We ought to conceive of hacking as a human behavior that is neither intrinsically dangerous nor inherently laudable, he argues. To judge its value, we need to evaluate a hack along multiple dimensions and in context. The result often highlights complicated trade-offs. We can be impressed, for example, by a hack's effectiveness but loathe its unethical nature, as with the "Double Irish with a Dutch Sandwich," an intricate tax hack that reduced US corporations' tax liability by billions, or find it disruptive, but eventually come to accept it as the new normal, as we did with dunking in basketball, a practice that leagues initially tried to ban but was eventually accepted, as fans liked it.

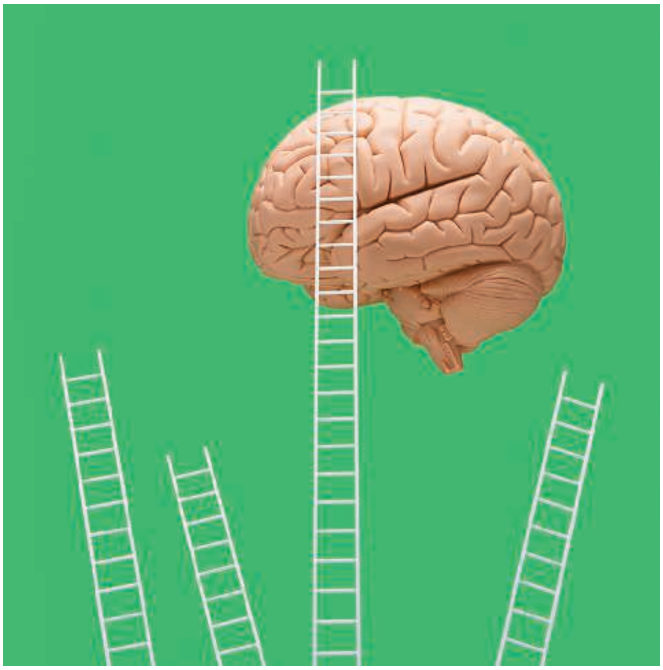


ILLUSTRATION: PM IMAGES/GETTY IMAGES

By giving hacking a social meaning, we link it to the human desire to influence the decisions and behaviors of others and we shift focus to social systems that provide boundaries but are themselves mutable. *A Hacker's Mind* is highly recommended reading, precisely because of the broader context it provides on this point, without which remedies remain elusive.

Perhaps the only limitation of the book is that Schneier does not go far enough in his analysis. For instance, he repeatedly embarks on examinations of the social and technical interplay of a particular case—how Boeing got away with the problematic Maneuvering Characteristics Augmentation System (MCAS) hack in its 737 aircraft, or how banks successfully hacked the Dodd-Frank Act that aimed to regulate derivatives—only to reduce the problem to simple questions of power and wealth. The rich and powerful hack unconstrained, he argues, while the rest of us are forced to follow the rules. As social science research has shown time and again, that is too meek an explanation (*1*).

In other instances, Schneier offers thoughtful descriptions of the social elements of a hack but then advocates a technical fix. He makes clear that such fixes are only one part of a comprehensive solution, but one cannot help but see the computer scientist attempting to fix bugs at such moments. As Schneier seems to have discovered himself, understanding social systems is hard and reverting to trotted paths enticing.

That Schneier has pushed himself beyond his own comfort zone, confronting hacking as something bigger and more multifaceted than simply sand in the machinery of digital systems, is what makes *A Hacker's Mind* unique and valuable. If his message is received, our social systems will soon begin to evolve to interact with hacking with greater agility, nuance, and even—in some instances—appreciation. ■

The reviewer is at the Oxford Internet Institute, University of Oxford, Oxford OX1 3JS, UK. Email: viktor.ms@oii.ox.ac.uk

REFERENCES AND NOTES

1. For example, Lawrence Lessig argues in *Republic, Lost* (Twelve, 2011) that even lobbying Congress is not only about money but also about information.

10.1126/science.adg3002