fellow physicist Leo Szilard's work on Maxwell's demon, a thought experiment that revealed how entropic disorder could be undone by making use of molecular-level information that looks like mere statistical noise at the macroscopic level.

What's more, Schrödinger gave his code-script too much agency by imagining that its readout was mapped directly onto the phenotype. This isn't how it works: you can't read the arrangement of the body's organs in the genome. The information functions as a resource, not a step-by-step guide. To acquire meaning, it must have context: a cell's history and environment. Tracing how the phenotype emerges from interactions of genes with each other and with their environment is the key puzzle of modern genomics.

What is Life? helped to make influential biologists out of several physicists: Crick, Seymour Benzer and Maurice Wilkins, among others. But there's no indication from contemporary reviews that many biologists grasped the real significance of Schrödinger's code-script as a kind of active program for the organism. Some in the emerging science of molecular biology were critical. Linus Pauling and Max Perutz were both damning about the book in 1987, on the centenary of Schrödinger's birth. Pauling considered negative entropy a "negative contribution" to biology, and castigated Schrödinger for a "vague and superficial" treatment of life's thermodynamics. Perutz grumbled that "what was true in his book was not original, and most of what was original was known not to be true even when the book was written".

Although these judgements are uncharitable, they are not without substance. Why, then, was the book so influential? Rhetorical theorist Leah Ceccarelli argues that it was down to Schrödinger's writing style: he managed to bridge physics and biology without privileging either. But today, we can find more than that. Schrödinger's thoughts on the entropic balance of life can be regarded as precursors to studies of how biological prerogatives such as replication, memory, ageing, epigenetic modification and self-regulation must be understood as processes of non-equilibrium complexity that cannot ignore the environment. It is intriguing that similar considerations of environment and contingency are now seen to be central in quantum mechanics, with its ideas of entanglement, decoherence and contextuality. Whether this is more than coincidence, we can't yet say. ■

Philip Ball *is a writer based in London. His latest book, on quantum physics, is* Beyond Weird.
e-mail: p.ball@btinternet.com

SECURITY

How smart connectivity is stupider by design

Steven Aftergood assesses a warning about the future of the Internet.

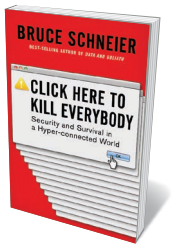
Hardly a day now passes without reports of a massive breach of computer security and the theft or compromise of confidential data. That digital nightmare is about to get much worse, asserts security technologist Bruce Schneier in *Click Here to Kill Everybody*, his critique of government inertia on Internet security.

The burgeoning threat, writes Schneier, arises from the rapid expansion of online connectivity to billions of unsecured nodes. The Internet of Things, in which physical objects and devices are networked together, is well on its way to becoming an Internet of Everything. Over the past decade or so, a growing number of products have been sold with embedded software and communications capacity: household appliances, cars, medical instruments and even clothing can now be monitored and controlled from afar. More of the same is on the way, as smart homes yield to smart cities and automated systems assume a larger role in the management of critical infrastructure. The Stuxnet computer worm used to attack Iran's uranium-enrichment programme remotely in 2010 was an early, audacious indicator of the threat.

Enhanced global connectivity has many advantages for knowledge sharing, commerce and convenience. Securing it, however, is a daunting prospect. The all-too-familiar vulnerability of computer networks — their susceptibility to failure, disruption and interference by malware, viruses and other factors — is amplified as practically everything becomes computerized. That relentless expansion of cyberspace into the physical domain brings with it new threats to power systems, mass transportation, public health and safety, and even political institutions, as effectively demonstrated by the Russian information operations that targeted the 2016 US presidential election.

> ***"When the Internet starts killing people it will be regulated."***

Despite its lurid title, Schneier's book is sober, lucid and often wise in diagnosing how the security challenges posed by the expanding Internet came about, and in proposing what should (but probably won't) be done about them.



Click Here to Kill Everybody: Security and Survival in a Hyper-connected World
BRUCE SCHNEIER
W. W. Norton (2018)

As he notes, security was not a primary concern in the early design of the Internet in the mid to late twentieth century. Developers of early efforts, from the US Department of Defense's ARPANET onwards, did not anticipate the Internet's explosive growth or coming role in global commerce and communication. Even today, there is little incentive to prioritize security above other concerns — so, for example, e-mails may or may not be from the sender named.

SURVEILLANCE CAPITALISM

Surprisingly to some, much of the business of the Internet is predicated on insecurity. 'Surveillance capitalism' — the collection of user data and its sale to advertisers and others — depends on vulnerable Internet practices, as does intelligence collection for national security and law enforcement. Governments act as if their need to monitor the Internet can be satisfied without any larger compromise of security. That, writes Schneier, is not so.

In principle, he explains, securing the Internet is straightforward, but it would demand concerted government action at each step. Financial incentives should be realigned to promote security and penalize failure by mandating that manufacturers disclose defects in commercial software, making them legally liable for defects. Security should be required in new devices, and rewarded through subsidies and tax breaks. Data should be encrypted to secure them against unwanted collection. Critical infrastructure — power grids, communications and transportation — should be protected by bolstering network security or disconnecting them from the network altogether.

Government agencies are fully aware that the expanding Internet "will create

Airline systems, like all networks, are vulnerable to hacking.

MICHAEL H/GETTY

an incalculably larger exploitation space for cyber threat actors", as the US National Counterintelligence and Security Center noted in a 2018 report, *Foreign Economic Espionage in Cyberspace*. Yet Schneier's views on security differ sharply from those of many government officials in the United States and elsewhere. For instance, Schneier considers strong encryption to be indispensable for personal and network security. The US Department of Justice sees it as "a serious challenge to effective law enforcement".

Similarly, Schneier advocates ruling out 'back doors' — design features that enable users, authorized or not, to bypass security and to decipher encrypted communications. He reasons that they render entire systems more vulnerable. But as then-UK home secretary Amber Rudd said last year, lack of access to encrypted data "in specific and targeted instances is right now severely limiting our agencies' ability to stop terrorist attacks and bring criminals to justice". Schneier also feels that it would be unfeasible and inappropriate to ban anonymity online. But the US Department of Justice insists that impenetrable anonymity "poses a unique and significant threat to public safety" in criminal contexts.

PRIORITY CLASH

Because Schneier and his opponents in law-enforcement agencies are responding to different problems on different timescales — solving a crime today versus fixing the whole Internet for the foreseeable future — it is difficult to say categorically that one side is right and the other wrong. But Schneier argues his position well. And to compensate for the admitted loss of collection capability that would follow from improved Internet security, he proposes to "make law enforcement smarter" through security research, enhanced computer forensics and new career paths.

Although cybersecurity is a hot-button issue in policy circles, progress is hindered by bureaucratic lethargy, especially on fundamental questions. In July, the US Government Accountability Office reported that 1,000 of its recommendations for addressing cyber threats have yet to be implemented, placing government information systems increasingly at risk. Governance seems to be an even harder problem than cybersecurity, leaving Schneier to predict that the United States "will do nothing soon".

At some point action will become imperative — perhaps sooner in the European Union, which has demonstrated a willingness to act on data-protection issues. "Governments regulate things that kill people," Schneier notes, citing vehicles, airlines and power plants. He adds: "when the Internet starts killing people it will be regulated".

Not just any regulations will do. To help devise a sensible response, he says, scientists and engineers need to get more involved in the policy process. And the challenges posed by the advancing online world go beyond security. If the question is what sort of Internet is compatible with a humane and enlightened society, technologists are not the only ones who will need a seat at the table. ■

Steven Aftergood *directs the Federation of American Scientists Project on Government Secrecy in Washington DC.*
e-mail: saftergood@fas.org