ISSUES IN SCIENCE AND TECHNOLOGY

NATIONAL ACADEMIES OF SCIENCES,
ENGINEERING, AND MEDICINE
THE UNIVERSITY OF TEXAS AT DALLAS
ARIZONA STATE UNIVERSITY
SPRING 2016

Summit on Human Gene Editing

David Baltimore,
R. Alta Charo,
Daniel J. Kevles,
Ruha Benjamin

The case for rapid use of gene-editing technology

The rise of the platform economy

Rethinking society's active orientation

Data-driven science policy

Super-muscly pigs: Trading ethics for efficiency

USA $12.00 / CAN $13.00
6 1>
0 56698 57433 0

BOOKS

A Tangled Web

The Internet of Things

by Samuel Greengard. Cambridge, MA: MIT Press Essential Knowledge series, 2015, 232 pp.

Cybersecurity and Cyberwar: What Everyone Needs to Know

by P. W. Singer and Allan Friedman. New York, NY: Oxford University Press, 2014, 320 pp.

Nigel Cameron

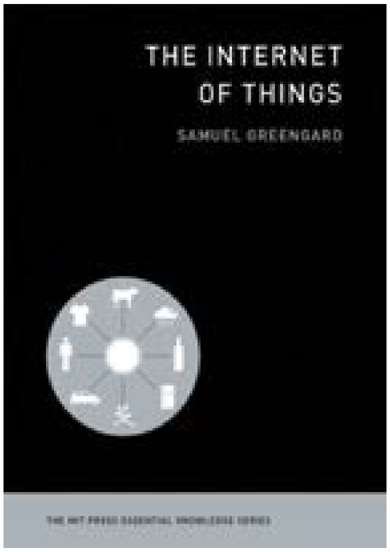
The Internet certainly seemed a good idea at the time. What's wrong with linking top academics through their computers so they can share big thoughts? And in these democratic times, extending those messaging facilities to the hoi polloi so they can share their tedious little thoughts, too? Yet one thing has led to another, and another, and the Internet of 2016 is a vast and ever-vaster entity. We don't need to be techno-skeptics such as Andrew Keen and Sherry Turkle to wonder if one day we may question our wisdom. Because we didn't just sit back and watch the Internet infiltrate every aspect of our lives; we cheered it on like Blackhawks fans at the Stanley Cup Final. The highly mixed results of which lead grumpy academics to organize another seminar on Collingridge's famous dilemma (we can't accurately predict the impact of a new technology until it is fully developed, and by then it is too late to do anything about it); heady Silicon Valley optimists to conjure Ned Ludd and tell us to sit down and shut up while technology solves its own problems; and those who are thinking hardest about cybersecurity to pour another Scotch.

These were among my preliminary thoughts as I approached these two very readable books, addressed to generalists. Samuel Greengard's *The Internet of Things* comes from MIT Press's Essential Knowledge series—small books on big subjects. In the case of P. W. Singer and Allan Friedman's *Cybersecurity and Cyberwar*, they write out of a mission to alert both specialists and the public to rising and disturbingly underestimated threats, a theme that is also reaching a broad audience through Ted Koppel's new book.

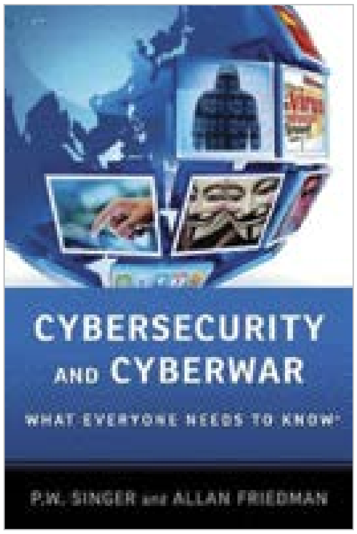
Cybersecurity is without doubt a threat inadequately recognized, perhaps vastly so, as I am reminded every time Microsoft Word flags it as a misspelling. (Word does not recognize what may yet prove the most consequential word of the twenty-first century, though it also continues to evade germline, which with CRISPR technology may prove the biggest boost or threat to *Homo sapiens*, qua species, since fire.) Similarly, the Internet of Things must be the least-noted of all developments in history at the human-machine interface. Its obscure name has certainly helped maintain an almost unbelievable opaqueness in a transparency-driven digital world.

Even generally well-informed people (including many tech people) have little notion what the Internet of Things signifies, let alone how revolutionary it promises to be. An Internet that has created its own new (and often bizarre) economy of cat pics and unicorns elbowing its improbable way into the Fortune 500 is suddenly refurbished as the new driver of value for General Electric and John Deere? It's almost as if Beanie Babies had kept on going up in value until they underpinned the global economy in place of gold. How on earth can this be? My homespun summary: It's where the new economy buttons itself to the old.

Greengard's *Internet of Things* is a Dummies book without the horrible design that for some reason the Dummies people find sells books. An MIT Press watermark sits curiously on a book intended to be a primer—and dragooned from a writer rather than a technology specialist. (Though to be fair, although Greengard's website pushes his American Association of Retired Persons book on finding the job you love in later life, he has long and expertly followed technology.) That itself is interesting, and perhaps a positive indication that the IoT (as we call it, partly because it sounds less silly) is, despite its unfamiliar name, moving mainstream. On the other hand, for all its handiness as a Dummies guide, this little book does somewhat lack the "here's the scoop" enthusiasm that insiders tend to evince, and feels a little like reading Wikipedia.



Singer and Friedman, by contrast, are content gurus commandeered by a publisher to dumb down cybersecurity issues. Their blow-by-blow, Dummies-level prose is the result of gargantuan effort, and succeeds. If you really don't know more about the Internet than that it is a system of pipes akin to the Paris *petit bleu* system of compressed-air telegrams that served late nineteenth century elites rather well (which is actually not a bad starting point), then there is no better place to begin your education. The downside, of course, is that if you do know your Internet onions, the Dummies lingo can get tedious. But it's worth plowing through because the book is full of insight.


CYBERSECURITY AND CYBERWAR
WHAT EVERYONE NEEDS TO KNOW
P.W. SINGER and ALLAN FRIEDMAN

In short: the IoT is linking every object of any economic significance with every other such object. And increasingly, it's doing so with standards that enable interoperability and Internet connectivity. Whereas some of this goes way back (RFID was the pioneer technology), some is already rather prosaic (those home heating systems you can operate from your phone if you really want to), and some is densely engineering-focused (think drilling, pumps, airplane engines, etc.), the frontiers include sensors in your bloodstream and vital organs, and of course, the end of driving.

The history of cybersecurity is well illustrated by the old saw, trotted out by intelligence chiefs when they want new money or are caught red-faced, that the manifold successes of cybersecurity remain a secret, while the bad guys need to score only one time to hit the headlines. The deceptive and self-serving nature of this rhetoric is plain when one considers that, like safety in an elevator, only 100% success is actually acceptable; anything less denominates the entire system as a disaster.

The history of efforts in cybersecurity, laid out in extraordinarily helpful detail by Singer and Friedman, amounts to millions of successfully resisted attacks punctuated by a succession of enormous disasters—from the hacking of Target stores to the federal government's Office of Personnel Management (OPM). There have been dozens of major consumer (and some government) hacks, many releasing tens of millions of records either to the public domain or the private databases of criminals, foreign powers, or others whom we have begun to call "bad actors."

Information hacks are not merely annoying and potentially costly in dollar terms; they can have all manner of real-world implications. The OPM hack stands out because it included not merely up to 20 million federal employee personnel records, but umpteen thousands of security clearance applications. If this was the work of the Chinese or some other foreign power, as has been suggested, then those individuals could be subject to phishing attacks for the rest of their careers. The ridiculous fact that the intelligence community permitted those records to remain with clunky old OPM in the first place has excited little scrutiny. But who expects actual career-losing accountability among federal employees?

What neither of these books addresses is the step change in the significance of cyberattacks that is heralded by the incessant rise of the IoT. Not many months back, the news media was briefly fixated with the tale of the hacked Jeep Cherokee. In fact, it was a friendly hack: "white hat" hackers, who seek to help plug rather than exploit security holes, had prearranged to take over the car of a *Wired* magazine journalist. They broke in through the entertainment system, messed with the music options, then moved to the power controls—and ended up nearly killing the journalist as he had a truck on his tail. Fiat-Chrysler, under the leadership of its larger-than-life boss Sergio Marchionne, responded vigorously and fast, and all's well that ends well for the future of the auto industry.

Except that it's not. For a start, the fact that one of the world's leading engineering companies could have its signature product compromised by a

couple of guys in a basement should have sent shivers down the spines of every global executive—and every shareholder. It's one thing to compromise financial data, the stigma of which has diminished with every gross breach and the harm of which is papered over with companies' letters of apology to their 10 million or 20 million affected customers offering free credit reports, identity theft insurance, and other feel-good benefits. It is quite another to compromise cyber-physical systems that tie the Internet to real-world activity.

As the Jeep hack demonstrated, in the IoT age, a major hack to a connected car system could direct a million vehicles to stop at 5:30 p.m. eastern time. Or turn left. Or speed up. As I stated recently when I was chairing the annual information technology expo GITEX in Dubai, all it will take is two or three cyber-attacks on cyber-physical systems that cause large numbers of casualties, and the IoT will be a dead letter. One hundred dead here, 1,000 there, and the rush hour will be back to analog.

Singer and Friedman list a series of developments that are needed to raise the status and effectiveness of cybersecurity in corporate and government contexts. It's plain that we don't have a moment to lose. After the Jeep hack, I speculated that the famously hands-on Marchionne would have the company's cybersecurity guy reporting directly to him the day after the breach. If top companies don't elevate this role to an office leading into that of the CEO, giving proper priority to the integrity of code and the protection of valuable databases, it's hard to see how the promised IoT revolution will safely succeed. Can this happen when so few corporate leaders (and board members) can follow, let alone lead, a conversation such as this one? We need to attend to the cybersecurity sirens or we shall be swiftly moving back to an analog future. They say the Kremlin is buying typewriters.

Nigel Cameron is president and CEO of the Center for Policy on Emerging Technologies in Washington, DC.

Chemical Solutions

Chemicals Without Harm: Policies for a Sustainable World

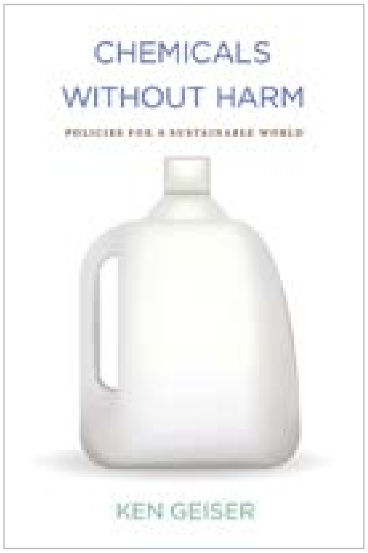
by Ken Geiser, Cambridge, MA: MIT Press, 2015, 440 pp.

Richard Clapp

Ken Geiser, professor emeritus at the University of Massachusetts, Lowell, and founder of the Lowell Center for Sustainable Production, has written another excellent book, *Chemicals Without Harm: Policies for a Sustainable World*, which follows and extends a book he wrote 14 years ago. That book, *Materials Matter: Toward a Sustainable Materials Policy*, was framed by the Bhopal chemical plant disaster in India and the lessons learned from that experience. Geiser said that the chief lesson of Bhopal was that the materials used were highly toxic and hazardous and the production process itself was inherently problematic.

The earlier book had a foreword by the ecologist Barry Commoner in which he described a hypothetical business decision about whether to produce acrylic grass for use on athletic fields; the company in this example decided not to produce the grass because of the injuries athletes suffered when they fell or slid on artificial turf. The example could now be updated to include the potential hazards of crumb rubber from recycled tires that is spread on artificial turf to cushion falls, and the growing concerns about health problems the new materials may be causing. Paul Anastas, the director of the Center for Green Chemistry and Green Engineering at Yale University, said recently in response to these concerns, "Tires were not designed to be playgrounds. They were designed to be tires." The point, as before, is that materials matter.

Chemicals Without Harm takes the reader beyond the previous lessons and proposes a re-framing of the dilemmas created by manufacturing products made of hazardous materials. To get to the re-framing, however, Geiser takes us on a deep dive into current federal and state policies, current synthetic chemical science, industrial infrastructure, advocacy organizations, and politics regarding chemicals production. He focuses primarily on the United States, although he references important developments in the European Union, East Asia, and international organizations, such as the United Nations Environment Program. He states the central argument of the book at the outset: "We can develop and use safer alternatives to the chemicals that threaten our health and environment; however, this will require a new chemical strategy focused on broad changes in science, the chemical economy, and government policy."



In the early chapters, Geiser traces the origins of the current U.S. legal and regulatory framework, and the gaps, loopholes, and weaknesses that have reduced the effectiveness of even the most well-intentioned chemical policies. On a more fundamental level, he notes that by reducing the problem to the regulation of "a few bad actors," this system avoided addressing the production and consumption systems that created the hazards in the first place. He also notes that the U.S. regulatory