DOI:10.1145/3073731

Moshe Y. Vardi

Cyber Insecurity and Cyber Libertarianism

ONE CAN GET a good picture of what is “hot” in technology by attending a Tech Summit. Such events are now held regularly in places trying to compete with Silicon Valley. I attended such a summit a few weeks ago. So what’s hot? FinTech (financial technology), MedTech (medical technology), IoT (Internet of Things), and autonomous cars are all hot. These areas attract a high level of venture capital, and one can expect them to grow and reshape the financial, medical, and transportation industries. Underlying these technologies is, of course, the Internet—our “network of insecurity”—so we can expect cyber insecurity to spread across more and more aspects of our lives.

Cyber insecurity seems to be the normal state of affairs these days. In June 2015, the U.S. Office of Personnel Management announced it had been the target of a data breach targeting the records of as many as 18 million people. In late 2016, we learned about two data breaches at Yahoo! Inc., which compromised over one billion accounts. Lastly, during 2016, close to 20,000 email messages from the U.S. Democratic National Committee were leaked via WikiLeaks. U.S. intelligence agencies argued that the Russian government directed the breaches in an attempt to interfere with the U.S. election process. Furthermore, cyber insecurity goes way beyond data breaches. In October 2016, for example, emergency centers in at least 12 U.S. states had been hit by a deluge of fake emergency calls. What cyber disaster is going to happen next?

So here we are, 70 years into the computer age and after three ACM Turing Awards in the area of cryptog-

raphy (but none in cybersecurity), and we still do not seem to know how to build secure information systems. This state of affairs was bemoaned in 2005 by then ACM President David Patterson, who argued (<https://goo.gl/9QbuZc>), “We must protect the security and privacy of computer and communication users from criminals and terrorists while preventing the Orwellian vision of Big Brother.” Yet here we are, over a decade later, and Patterson’s passionate appeal is as relevant as ever! That is not to say we have not made significant progress in the development of security-enhancing techniques, but we have not really succeeded in making information-technology infrastructure more secure. As information technology permeates more and more aspects of our lives, the stakes are getting higher and higher. The risk is no longer merely about compromised privacy. We must worry now about the integrity of vital infrastructure components, including the electrical-power grid, the telecommunication system, the financial system, and the transportation system. And yet, our community marches forward with no special sense of urgency.

The basic problem, I believe, is that security never gets a high-enough priority. We build a computing system for certain functionality, and functionality sells. Then we discover security vulnerabilities and fix them, and security of the system does improve. Microsoft Windows 10 is much, much better security-wise than Windows XP. The question is whether we are eliminating old vulnerabilities faster than we are creating new ones. Judging by the number of publicized security breaches and attacks, the answer to that question seems to be negative.

This raises some very fundamental questions about our field. Are we investing enough in cybersecurity research? Has the research yielded solid scientific foundations as well as useful solutions? Has industry failed to adopt these solutions due to cost/benefit? More fundamentally, how do we change the trajectory in a fundamental way, so the cybersecurity derivative goes from being negative to being positive?

We can draw an analogy to car safety. Over the past 100 years, the amount of vehicle miles traveled has been steadily increasing, but fatalities with respect to vehicle miles traveled have been decreasing. Car safety has been increasing mostly due to government regulation. For example, the U.S. Congress established the National Transportation Safety Board in 1926. Why is there no National Cyber Security Board?

Cyber libertarianism refers to the belief that individuals should be at liberty to pursue their own tastes and interests online. Cyber libertarianism is a common attitude in the tech community; “regulation stifles innovation” is the prevailing mantra. One could imagine a similar attitude being applied to the car industry, but history has shown that regulation and innovation can co-exist. The tech community has not been able to address the cybersecurity situation on its own; it is time to get governments involved, via laws and regulations. Numerous issues will have to be debated and resolved, but we must accept, I believe, that the cybersecurity problem will not be resolved by the market.

Follow me on Facebook, Google+, and Twitter.

Moshe Y. Vardi, EDITOR-IN-CHIEF

Copyright held by author.