Polarization

Daniel E. Geer Jr.
In-Q-Tel

There's nothing in the middle of the road except yellow stripes and dead armadillos.
—Jim Hightower

We are living among many trends: polarization, a sharpening impact of our lack of fundamental measures of security, a rising need for prediction, supplier abandonment of code bases still in use, growing interdependence in the digital world, increasing automation of protection, the dual-use nature of most new technologies, a decreasing ability to define "end to end," rising complexity in supply chains, monocultures in components surpassing monocultures in systems, and a growth in attack surface that's outpacing skill growth. I deal here with only the first; for fuller treatment, see tinyurl.com/m7d9ldv.

Much has been written about polarization of American life. The middle is getting smaller whether we're looking at the shrinking middle class, depopulation in the middle of the country, loneliness in the political middle, how farms and banks are now only too small to matter or too big to fail, almost all journalism becoming advocacy journalism, and how middle-tier college education is a ticket to debt.

I submit that polarization has come to cybersecurity. The best skills are now astonishingly good while the great mass of those dependent on cybersecurity are ever less able to even estimate what they don't know, much less act on it. Polarization is driven by the fundamental strategic asymmetry of cybersecurity: the work factor for the offender is the incremental price of finding a new method of attack, but the work factor for the defender is the cumulative cost of forever defending against all attack methods yet discovered. Over time, the curve for the cost of finding a new attack and the curve for the cost of defending against all attacks to date must cross. Once they do, the offender never has to worry about being out of money. That crossing occurred some time ago.

The range of cybersecurity skills between the best and the worst is growing wider. As the worst outnumber the best and always will, we need look no further than the history of empire: empires fall when polarization triumphs. The Internet is an empire. It was built by academics, researchers, and hackers—it embodies the liberal cum libertarian cultural interpretation of "American values," namely, that it's open, nonhierarchical, self-organizing, and leaves essentially no opportunities for governance beyond a few rules of how to keep two parties talking. Anywhere the Internet appears, it brings those values with it. Other governments know that as they adopt the Internet, they become dependent on those strengths and thus on our values as well. A greater challenge to their sovereignty does not exist, which is why the Internet will either be dramatically balkanized or morph into an organ of world government. In either case, the Internet will never again be as free as it is today.

Polarization of cybersecurity within the Internet grows from our willing dependence on the Internet. I don't see us deciding to damp cyber risk by curbing cyber dependence, though to be clear, that's precisely the trajectory that my own life now follows. I don't see the cybersecurity field solving the problem because the problem is getting bigger faster than we (here) are getting better. I see, instead, the probability that legislatures will move to relieve the more numerous incapable of the joint consequences of their dependence and their incapability by assigning liability so as to collectivize the downside risk of cyber insecurity into insurance pools. We're forcibly collectivizing the downside risks of disease, most particularly the self-inflicted kind, into insurance pools; why would we not expect the same of cyber insecurity, most particularly the self-inflicted kind?

Where there are such deep needs and such shallow appreciation of where trend directions lead, the greatest risk is the risk of simplistic solutions carried forward by charismatic fools. ■

Daniel E. Geer Jr. is CISO for In-Q-Tel and past president of the Usenix Association. Contact him at dan@geer.org.