In Cybersecurity, Decentralization and Diversity are Strength

The US Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), the *New York Times* reports, fears "ransomware" attacks against America's voter registration systems in the run-up to the 2020 presidential election. In response, it's launching a program that "narrowly focuses" on protecting those systems.

A laudable goal, to be sure, but should we accept the premise? It goes almost without saying that CISA, created only late last year, is casting about for ways to justify its existence and its $3.3 billion annual budget. Is this a real problem? And is CISA the organization to solve it?

Yes, "ransomware" and other types of cyberattacks are real problems. They threaten the integrity of any computer systems they target, which means any systems connected to the Internet or even accepting data from external sources like potentially contaminated flash drives (most early microcomputer viruses reached their targets when users inserted contaminated floppy disks; no Internet needed).

On the other hand, the federal government's track record on securing its own systems, let alone anyone else's, is remarkably poor. Millions of Americans have had their personal information exposed in hacks of the Office of Personnel Management and other government agencies.

And on the third hand, the worst way to respond to a diffuse set of threats against a large number of systems is to centralize that response, especially in terms of requiring or encouraging the operators of all those systems to adopt the same systems and the same security measures.

Suppose that every front door of every building in the world was secured by one model of lock, made by one company. A flaw in that model of lock would be a flaw in every front door. Anyone who could exploit that flaw at a building down the street or across the country could exploit that flaw at your house too.

Or suppose that every variety of vegetable had one genetic weakness that allowed a particular blight to infect it. Once that blight hit your neighbor's tomatoes, it could easily jump to your bell peppers and your neighbor's cucumbers.

The world's computing power is already far less diverse than you might think. It's dominated by a few processor architectures, a few operating systems, a few server software packages, a few browser engines.

That’s convenient, even necessary, to the increasingly automated and interconnected world we’ve created over the last 30 years or so. But it’s also a source of vulnerability — vulnerability we shouldn’t compound by centralizing cybersecurity solutions under a federal agency’s leaky umbrella.

Our state and local election systems are safer to the extent that an attacker has to find 50 or 500 different ways to hack 50 or 500 of those systems, instead of one way to hack them all.