In this essay, convergence is the idea of merging the duties and responsibilities of physical security with that of digital security to make them part of a common reporting structure—to employ tools and techniques that are parallel if not collinear. It’s a widespread idea in larger businesses, and thanks to 9/11-driven expansion of “security” training programs, convergence has developed an academic panache.

So what to make of this convergence? Is it a good thing? Is it efficient? Does it make a newly converged security department more or less likely to succeed in solving its problem statement than its nonconverged predecessors? Do physical security and digital security have enough in common to be able to teach each other anything?

They’re certainly different, so which aphorism applies: do opposites still attract, or do birds of a feather still flock together?

This observer says convergence is a mirage. The reason is time. Everything about digital security has time constants that are three orders of magnitude different from the time constants of physical security: break into my computer in 500 milliseconds but into my house in 5 to 10 minutes. Drive a gigabyte of data per second over a wire (full of books) or a convoy of pickup trucks at 60 miles per hour, 88 feet on center. Spend man-months on a million-dollar heist from one bank or lift $1 from one million individuals with automation. Physically speaking, the bigger the threat, the less warning you get (0day attacks).

Human-scale time and rate constants underlie the law enforcement model of security. The crime happens and the wheels of detection, analysis, pursuit, apprehension, jurisprudence, and, perhaps, penal servitude then, paraphrasing Longfellow, “grind slowly, yet they grind exceeding fine.” In other words, law enforcement generally has all the time in the world, and its opponent, the criminal, thus must commit the perfect crime to cleanly profit from that crime.

There’s nothing human-scale about the digital world’s time constants; automation alone dismisses any such thought. In the digital world, crime must be prevented; once committed, it’s likely never ameliorable—data is never unexposed, for example. It’s not the criminal who must commit the perfect crime but rather the defender who must commit the perfect defense.

Time is the reason.

Consequently, the physical world strategies of law enforcement are of limited value in the digital sphere. Law enforcement officials (or the military) are not our natural allies or even mentors. Who is? Is anyone left?

When your enemy can strike with no warning, from anywhere (or everywhere at once), with no need for coordination, and with no danger of harm to self, perhaps not even with the danger of self-identification, then your only answer is preemption. Preemption requires intelligence. Intelligence requires surveillance. If, as digital security people, we have any natural allies or even mentors, they’re to be found in the intelligence model of security, not the law enforcement model where this talk of “convergence” has itself converged.

If the physics of digital space and digital time mean we ally ourselves with the intelligence world view and not the law enforcement world view, we have to ask ourselves two things: is the price of digital surveillance a bearable price for the benefit of digital safety? And, if so, what is the unit of digital surveillance? What do we watch—people or bits?

If we depend ever more on the digital world, whether for its convenience or for its wealth, then we accept surveillance both within that world and, by spillover, in the physical world, too. There’s no stopping history, but it is time for some wise choices that are anything but wishful. It’s time to decide what risks are worth what other risks. Not to decide is to decide.

Daniel E. Geer Jr. is chief scientist for Verdasys and in that role wrestles with the questions of surveillance and control every day; he only hopes there is still time to get it right. Contact him at dan@geer.org.