



**Daniel E. Geer Jr.**  
In-Q-Tel

## More or Less

Two of the gravest general dangers to survival are the desire for comfort and a passive outlook.

—*US Army Ranger Handbook*

**T**he current security situation is unsatisfactory. We either spend too little or too much—too little if we’re on the beam with our security solutions but aren’t giving it enough gas, too much if our security tools can’t be more effective even if we deployed an order of magnitude more of them.

More and less is both feasible. Getting to “more”—diverting a much enlarged percentage of global wealth into digital security—requires a motivating crisis. Getting to “less”—putting on a parachute and leaving the plane—requires the courage to declare defeat. To decisively choose between more or less requires a Presidential Commission with unprecedented resolve.

But none of that matters. In the October *McKinsey Quarterly* ([tinyurl.com/6sg5m5u](http://tinyurl.com/6sg5m5u)), W. Brian Arthur describes the degree to which human work is disappearing into a “second economy” where machines talk to machines:

We don’t have paralegals in the numbers we used to. Or draftsmen, telephone operators, typists, or bookkeeping people. A lot of that work is now done digitally. We do have police and teachers and doctors; where there’s a need for human judgment and human interaction, we still have that. But the primary cause of all of the downsizing we’ve had since the mid-1990s is that a lot of human jobs are disappearing into the second economy. Not to reappear.

Today, we deploy software kits to protect us from other software. The leading edge of that protection is cooperatively networked based on the premise that no one machine can protect itself, that only by massing together is it possible to defeat the opposition. This premise—that self-sufficient point protection is not possible—means that machines must talk to machines. This has implications: the conversation between

machines must be faster than the opposition, no one user can gauge his or her contribution, and this new knowledge is neither in English nor Chinese.

All solutions have side effects. In Arthur’s analysis, a hyperefficient second economy generates a societal conundrum: how do we distribute the wealth that mankind produces? To date, jobs have been the mechanism: everyone takes home a share of the pie earned through their job. But we might soon enter a world where there is enough of everything but no just mechanism to distribute it in any sensible way because a large majority of the population simply might not be needed to do any job they’re skilled to do. Evolutionary population dynamics would then deliver a few super rich kings and many, many serfs.

We security professionals make a claim to the salary we draw because of our “judgment” and “skill.” I suggest that the demand for that judgment, that skill will soon wither in the face of the second economy. We see computers doing things right now—Amazon or Netflix recommendations, Zillow estimates—that a decade ago would have required a human to intervene. The networked security militias of the second economy do not wait for humans, and it’s possible to argue that for the scale and speed at which a networked security collective operates, a human in the loop is not a failsafe but a liability ([tinyurl.com/c7h6x5h](http://tinyurl.com/c7h6x5h)).

What to make of this is a much larger question than this magazine can handle, but I ask you, the infosec professional, which infosec job descriptions are more like typists and draftsmen and which are more like teachers and doctors? Do we need more infosec fighter pilots or more infosec ambulance drivers? Will the salaries of infosec professionals remain high enough for young people to indenture themselves? Will the fact that all security technology is dual use rebalance job growth toward offense? ■

**Daniel E. Geer Jr.** is CISO for In-Q-Tel and past president of the Usenix Association. Contact him at [dan@geer.org](mailto:dan@geer.org).