

For Good Measure Cyberjobsecurity

DAN GEER



Dan Geer is the CISO for In-Q-Tel and a security researcher with a quantitative bent. He has a long history with the USENIX Association, including officer positions, program committees, etc. dan@geer.org

When you see something that is technically sweet, you go ahead and do it and you argue about what to do about it only after you have had your technical success. That is the way it was with the atomic bomb.—*Julius Robert Oppenheimer*

Automation exists to remove costs. Some costs are measured in money lost. Some costs are measured in inaccurate results. Some costs are measured in risk taken on. For any cost, however, the first question to ask is, from whose vantage point is such and such a cost a cost? Is it the person shelling out money that could have been saved? Is it the person receiving inaccurate outputs that drove needlessly poor decisions? Is it the person trading short-term convenience for long-term risk? Or is it the counterparties to each of those persons?

The best, most careful observers are now singing the same chorus, that automation is moving beyond the routinizable to the non-routine by way of the tsunami of ever bigger data. As such, it is not the fraction of people who are unemployed that matters; it is the fraction of people who will soon be unemployable. Machines that are cheaper than you, that make fewer mistakes than you, that can accept any drudgery that risk avoidance imposes are coming.

What does that have to do with cybersecurity and its measurement? Cybersecurity is perhaps the most challenging intellectual profession on the planet both because of the rate of change and because your failure is the intentional work product of sentient opponents. Can automation help with that? Of course and it already is, as you well know regardless of your misgivings about whether anomaly detection will work in an ever more “personalized” Internet—one man’s personalization is another man’s targeting.

The U.S. Bureau of Labor Statistics reports [1] that the five occupations with the best outlook for new jobs over the next 10 years are personal care aides, registered nurses, retail salespersons, home health aides, and food preparers/servers, with an aggregate 10-year employment growth of 2,388,400 at \$30,048 average income. Accepting that it takes 125,000 new jobs/month to hold unemployment steady, those five occupations can cover 19 of the next 120 months. On the world scale, those are good jobs—\$30,048 and you’re in the world’s top 6% [2].

High-paying jobs are precisely the ones that automation wants to take. Turning to BLS data for “information security analysts” [3], there are 75,000 of those with mean income of \$86,070 per year, putting ISAs in the top 0.5% on the world scale. The growth in that occupation for the coming decade is 37% (3.5% per year, the 16th best of all U.S. occupations), and of the 20 jobs with the fastest growth, only physicians’ assistants have a higher mean salary than ISAs. *Computerworld’s* survey [4] confirms the pinnacle status of information security practitioners, putting a CSO in the world top 0.2%.

So is automation gunning for the ISA role? If not, is it because ISAs are too few to bother with or is it that the job is too hard to automate (yet)? Shosana Zuboff’s [5] three laws bear repeating:

- ◆ Everything that can be automated will be automated.
- ◆ Everything that can be informed will be informed.
- ◆ Every digital application that can be used for surveillance and control will be used for surveillance and control.

Universities and the White House argue that as machines take over existing jobs, new opportunities are created for those who “invest in themselves.” As Federico Pistono argues [6] with clear numbers, that is not true. Ranking U.S. jobs by how many people hold them, computer software engineer is the only job created in the last 50 years with over a million job holders. It is #33 on the list; there are twice as many janitors. The most numerous job, delivery driver, is being automated out of existence as we speak. If cybersecurity jobs are safe from automation, should we be retraining all the truck drivers who are about to be unemployed as information security analysts? Are we lucky that our jobs come with sentient opponents? Are sentient opponents our job security—the source of both our pain and our power?

We cybersecurity folk are not the best paid. All but one of the 15 best paying jobs are in medicine (that one is CEO at #11), but as C.G.P. Grey [7] points out, once electronic health records really take hold, most of health care can be automated—at least the parts for diagnosis, prescribing, monitoring, timing, and keeping up with the literature.

But if it is true that all cybersecurity technology is dual use, then what about offense? Chris Inglis, recently retired NSA deputy director, remarked that if we were to score cyber the way we score soccer, the tally would be 462-456 twenty minutes into the game [8], i.e., all offense. I will take his remark as confirming at the highest level not only the dual use nature of cybersecurity but also confirming that offense is where the innovations that only Nation States can afford is going on. Put differently, is cybersecurity as a job moving away from defense toward offense insofar as the defense side is easier to automate? That won't show up in any statistics that you or I are likely to find; offense does not publish.

In sum, everything I see in the security literature and/or the blogosphere argues for automating cybersecurity. One must then ask if, in truth, our job description is to work ourselves out of a job. Or do we say that with a wink and a nod [9]?

References

- [1] Occupational Outlook Handbook: www.bls.gov/ooh/most-new-jobs.htm.
- [2] Wealth calculator (adjusted for purchasing parity) <http://www.worldwealthcalculator.org/results>.
- [3] Information Security Analysts: www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm.
- [4] IT Salary Survey: www.computerworld.com/category/salariesurvey2014/.
- [5] “Skilled workers historically have been ambivalent toward automation, knowing that the bodies it would augment or replace were the occasion for both their pain and their power.” *In the Age of the Smart Machine (Basic Books, 1988)*, p. 56.
- [6] *Robots Will Steal Your Job, But That's OK* (CreateSpace, 2012), Chapter 9: www.robotswillstealyourjob.com/read/part1/ch9-unemployment-tomorrow.
- [7] “Humans Need Not Apply”: www.youtube.com/watch?v=7Pq-S557XQU.
- [8] Chris Inglis, confirmed by personal communication.
- [9] “Never write if you can speak; never speak if you can nod; never nod if you can wink.”—Martin Lomasney, Ward Boss, Boston.