[nominal delivery draft, 8 February 2012, Rosslyn, Virginia]

People in the Loop: Are They a Failsafe or a Liability?

Daniel E. Geer, Jr., Sc.D.

We are at a cross roads, an inflection point. We will someday look back on this day, this month, or perhaps this year as a turning point. I believe this, but I cannot prove it. Even if I had all the data in the world, I wouldn't be able to detect the inflection beyond all shadow of doubt any more than I can detect the curvature of the earth while standing on the riverbank outside.

Everything about cyberspace is now in a positive feedback loop or, should I say, the positive feedback loop in cyberspace is creating a positive feedback loop within all cutting edge science. That loop includes cybersecurity.

Within the last month, American and Dutch researchers announced that they could make the H5N1 virus transmissible between humans. The World Health Organization and the US Government, arguing that that research has dual use, did their best to direct both the journals Science and Nature to not publish.

Dual use? It is my contention that all cybersecurity technology is dual use, which we can argue later if you are so sanguine as to disagree. That is not my point, however. My point is that there is no world class research in biology or any other speciality that does not involve a plethora of networked computer files, that is to say data in motion. Does anyone in this room think that the computers of, in this case, the University of Wisconsin at Madison or the Erasmus Medical Centre in Rotterdam have not already been plundered for the research we are now trying to suppress? Even if they had not been plundered before, as soon as the "do not publish" directive hit the press those whose job it is to aim cyberattacks at high value targets hit the ground running.

As some of you know, I write a lot and especially about numbers with respect to cyber security. My most recent column in the IEEE's Security and Privacy magazine trivially demonstrated that while the number of addressable nodes on the Internet grows as the cube of elapsed time, the number of systems administrators is growing approximately linearly in time. As such, the fanout per human systems administrator is rising as roughly the square of time. And

that is just the node count. If we were to scale the node count by the effect of Moore's Law, the fanout in human mental capacity versus ability to compute would be even faster a diverging curve.

The amount of money spent in cybersecurity is indeed rising, but as I showed in a different column, investment -- in the sense of putting money to work with entrepreneurs in cybersecurity -- has all but faded away to zero. At least that is so for companies whose mission statement is on the defensive side. Companies whose product is touted primarily for offense are harder to find and to categorize, but not one of them has reached the level where there would be a move to force them into the DIBnet, which I say speaking as someone who by choice foregoes having a Clearance.

No doubt everyone has seen the rate at which data is accumulating. One way to gauge this is to divide the world's total storage by the world's total bandwidth. In 1986, you could fill the world's total storage using the world's total bandwidth in two days. Today, it would take 112 days of the world's total bandwidth to fill the world's total storage, and the measured curve between 1986 and today is all but perfectly exponential. Once again, the amount of human intelligence per unit of, in this case, storage is not just falling but accelerating in its fall.

Access control does not scale economically in the face of this increase simply because the true cost of the access control model is proportional to the product of [the number of entities requesting access] times [the number of things they are able to request access to]. That is a matrix of cost. If there is a finite minimum cost to keeping each cell of that matrix correct, then the access control model has a geometric cost curve. Either the cost of gatekeeping data access rises as fast as data volume rises, or access controls become ever less fine-grained.

If data growth make access control a losing proposition, then accountability is the only fall back, but accountability requires a surveillance regime that is truly pervasive if one is to reach the point where the absence of evidence is likewise the evidence of absence. Event logs at that level of detail are not handle-able by people, which is why large enterprises and the intelligence community alike are struggling and will continue to struggle.

In this we are not talking about doing a better job at cybersecurity, we are talking about not doing a worse job. One can only conclude

that replacing some part of the human cybersecurity worker's job description with automation is necessary. If the threat space is expanding by X to the Y, then the defense has to arm up accordingly. An accelerating share of the total cybersecurity responsibility will have to be automated, will have to be turned over to machines.

I find that conclusion at once inescapable and abhorrent. Harvard's Clayton Christiansen wrote of the "innovator's dilemma" which I suspect many of you have read if not experienced. It says that optimizing the cost structure of an existing product line as a competitive barrier to entry by other like firms eventually assures that your market will be eaten out from under you by low cost entities.

Last October's McKinsey Quarterly spoke of this purely from the societal point of view,

> 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 [at human scale], 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 [digital] economy. Not to reappear.

It is hardly just McKinsey; Martin Ford's _The Lights in the Tunnel_ or Brynjolfsson's and McAfee's _The Race Against the Machine_ also say that the white collar job is the next to go. As one of my colleagues at Goldman Sachs points out, the American white collar job disappears because in a globalized world, even genius is cheap, but what McKinsey, Ford, or Brynjolfsson are talking about is that human genius is soon itself expendable in Taipei as much as Tampa.

But those are economic arguments. Surely cybersecurity is different? I said long ago and I still say it -- cybersecurity is the most intellectually difficult profession on the planet. Surely the core, the purposive adaptability, the drive, the necessary human intelligence is going to be the last to go as the machines take over all the lesser jobs.

I don't think so, and the reason is reaction time. My bot can own your machine in 500 milliseconds; in that time you can set your coffee cup down. My malware can morph with each delivery, a fact

so well known that it is even in legislation, in this case Title F, Section 953 of the Defense Authorization Act for 2012 which directs the DoD to get away from signature-based controls. More importantly still, the attack surface is expanding faster than we can discover its flaws -- think HTML5 or the proliferation of generic Top Level Domains or consumerization.

Now I have said all this not to do the Chicken Little thing once more, but because the question on the table is not really whether a human is a failsafe or a liability -- because the human is going to come out of the loop whether we like it or not. We can do nothing but turn over an increasing percentage of the tasks of cybersecurity to machines. In a sense, they've already won.

The question is under what circumstances that we still control can that turning over be a good thing? How can we put a human back into the loop such that that human *is* a failsafe. Let me give you an example.

I have good relations with a number of the largest banks. One of them has long since made user-level provisioning a completely automated process. This automated provisioning control include de-provisioning -- what you might describe as removing Dan's access within 120 seconds of the time Dan submits his letter of resignation or, for that matter, slugs a Managing Director on the trading floor. Fast, hands off, one-button deprovisioning makes regulators happy. It makes General Counsels happy. But it's a nightmare if it goes into a loop. The bank I'm thinking of has coded for this explicitly; if 50 resignation's have come in within an hour, the deprovisioning system halts and will not proceed until a human gives it authority to proceed. Putting a human back into the loop has saved their bacon at least once.

While some people like to say "Specialization is for insects," tell me that the security field itself is not specializing under the pressure of too wide to master, too deep to know, too fast to photograph. We have people who are expert in forensics on specific operating system localizations, expert in setting up intrusion response, expert in analyzing large sets of firewall rules using non-trivial set theory, expert in designing egress filters for entities that have no ingress filters, expert in steganographically watermarking binaries, and so forth. Generalists are becoming rare, and they are being replaced by specialists. This is speciation in action, and the narrowing of niches. In rough numbers, the expansion

of the computing field is why there are already close to 5,000 technical certifications, and the number of them is growing. Specialization is not just for insects and it will not stop, but the human in the loop is ever less likely to have the big picture.

I ask you to consider a computer to be a life form, subject to evolution just like any other life form. Let's take embedded systems; they are already two orders of magnitude more numerous than keyboards and displays hence the future threat space, which we must lead in the same way one leads the deer when hunting, is a threat space where a computer is not identifiable as such, but is instead inside some nondescript appliance.

So should or should not an embedded system have a remote management interface? If it does not, then a late discovered flaw cannot be fixed without visiting all the embedded systems which is likely to be infeasible both because some will be where you cannot again go and there will be too many of them anyway. If it does have a remote management interface, the opponent of skill focuses on that and, once a break is achieved, will use those self-same management functions to ensure that not only does he retain control over the long interval but, as well, you will be unlikely to know that he is there.

Perhaps what is needed is for at least some computers to be more like humans, and I most assuredly do not mean artificially intelligent. By "more like humans" I mean this: Embedded systems, if having no remote management interface and thus out of reach, are a life form and as the purpose of life is to end, an embedded system without a remote management interface must be so designed as to be certain to die no later than some fixed time. Conversely, an embedded system with a remote management interface must be sufficiently self-protecting that it is capable of refusing a command. Inevitable death and purposive resistance are two aspects of the human condition we need to replicate, not somehow imagine that to overcome them is to make an improvement.

This is perhaps the core of my thesis, that when sentience is available, automation will increase risk whereas when sentience is not available, automation can reduce risk. Note the parsing here, that replacing available sentience with something that is not sentient *will* increase risk but that substituting automation for whatever you have absent sentience *can* make things better. It won't do so necessarily, but it can.

As a child of the hillbilly South, I have nothing against automating drudgery; a 110-year-old woman interviewed for the book _Super Centennarians_ was asked what was the most important invention during her lifetime. Her answer was the washing machine.

But with the spread of computers, we have tended to use automation as soon as it is cheaper than human labor. No single replacement of labor by automation matters, but the sum of it does. Just as it was an epic irony that Linux killed SUN rather than Microsoft, as we sit here today the equation of automation is not that of eliminating drudgery but eliminating the need for sentience.

The complexity of cyberspace makes this an interesting bargain where the question of what value for what cost comes down to asking whether there is enough available sentience to indict cybersecurity automation as risk creating or, alternately, whether there is far too little sentience that is up to the task at hand and therefore automation is essential and risk reducing.

Consider the present trend to silent, automatic upgrade of applications and operating systems. The arguments for automatic upgrade are the same arguments that require first graders to be variously immunized before than are allowed to come to school, that is to say that in the dense interconnections of cyberspace, herd immunity matters. Software companies are coming to see their user base the way the US Public Health Service sees the citizenry -- a clientele that must be pushed around for its own good and better still if it can be done invisibly, like fluoridating the water supply. But in the same way that an accident at the water treatment plant poisons those downstream, the day that a nation state gains control of, say, Windows Update is the last day those downstream control their fate.

The greater share of you in this room are entirely capable of taking care of yourselves and would, I wager, be better off if you did. I say that because cybersecurity people, or the best ones anyway, have a propensity to ask not what some gizmo can do for you but rather what that gizmo can do to you.

Just as genetic diversity is the foundation of resilience, practiced sentience rather than the reliance on automatons is the foundation of longevity. Stretching for an analogy that is not computer related, consider the manual transmission versus the automatic transmission. To describe the manual transmission:

. feedback from engine and road to hand and brain
. can be push started
. get to neutral from any gear directly
. coast hills at no shifting risk (overrunning N -> R)
. solid, not fluid, coupler so no power loss there
. downshift braking including when brakes have faded
. simplicity, per se, including less required repair skill
. focus: one hand on wheel, one on stick, none on {burger,phone,dick}
. still operable if only clutch works but shifting is lost
. still operable if only shift works but clutch is lost
. manual transmissions weigh less
. non-sequential shifting possible
. know what gear you are in, including not having to look to see
. learn neutral thrust by learning to shift clutchless
. parking brake failure is of no concern
. ignorami can't steal your wheels

Now there is no one in this room with insufficient sentience to gain the advantages I just listed. If you prefer the macro view, consider that at the time of its construction, the total energy output of the Trans-Alaska oil pipeline was approximately equal to the efficiency loss due to the then prevalence of automatic transmissions in the US auto fleet of the era.

But, yes, cybersecurity is different. For better or worse, we are all in this together. The dynamic range of cybersecurity sentience is great, enough so that you who are experienced rock climbers might think of "all in this together" as how roping all the amateurs together guarantees the lot of them come off the mountain, taking you with them. You may, in fact, have to be your brother's keeper.

But what would that mean? Those of you who practice self-protection in cyberspace know that it is increasingly tedious, enough so that your own sentience may be challenged. I will bet that a fair fraction of you here today function as the security administrator for your extended family and that the majority of that family is blithely addicted to things they have no hope of understanding.

You may view an infected machine as a weapon. If I do not lock up my guns and they are used for the commission of a crime, then I will have some explaining to do, at the very least. You may simply not choose to drive through an intersection if you know that most of the opposing traffic lacks brakes. I don't believe we will find

the political will to make personal culpability a serious enough matter to effect wide change, but I am at a loss to argue in any other direction. I ask you this, if it is not the responsibility of the end user to avoid being an unwitting accomplice to constant crime, then whose responsibility is it? If you say that it is the ISP's responsibility -- the apparent top likelihood amongst our friends in the Legislature -- then you are flatly giving up on not having your traffic inspected by robots at a fine level of detail. If you say that it is the software manufacturer's responsibility, we will soon need the digital equivalent of the Food & Drug Administration to set standards for efficacy and safety. If you say that it is broadly the government's responsibility, then the mythical Information Superhighway Driver's License must soon follow. To my mind, personal responsibility for Internet safety is the worst choice, except for all the others.

As if we had a choice. We don't. The vox populi demands invisible protection and the invisible protection demands automation. The available domestic human sentience is totally insufficient. You can see this today as the demand for top drawer security expertise so outstrips the supply that the charlatan fraction is rising. The choice before us may well be between, on the one hand, a pool of cybersecurity practitioners that includes "the best minds of my generation" surrounded by infectious camp followers and, on the other hand, a phalanx of machines who must then shoulder the duty of protection. It is time for us all to re-read Asimov's Three Laws of Robotics.

The sentience crisis is coming as sure as I am going. The nose of the camel is the increasingly behavioral aspect embodied in some cybersecurity programs, by which I mean the building up of a model of what is normal by close observation the better to identify the anomalous. In my view, we must preserve a place for human sentience rather than looking for ways to replace human sentience with machine sentience.

Let me give an example. My previous employer was Verdasys where I was Chief Scientist for the product design team. For those with a deep background, my product was a distributed, recording version of the Orange Book's "Reference Monitor" implemented as a rootkit. That said, we could do nearly anything to detect and modify data handling of any sort at any granularity.

We installed at a major hospital. There, the Chief of Medicine

demanded that under no circumstances could our product block access to patient data since who knows what sort of emergency might be in progress. At the same time, the General Counsel demanded that under no circumstances could our product permit a breach of regulatory controls on data handling. The solution to this standoff was that whenever someone asked for data that was nominally forbidden, a popup window would appear which said "Against policy. Click here to proceed." With that, no data was denied but at the same time no person could deny having intent. This finesse represented the well-placed insertion of a tiny bit of sentience in an otherwise fully automated protection regime.

Now it has been said that in a globalized world, genius is cheap. The CEO of Gallup, Jim Clifton, has just published a book that points out that there are three billion people on earth who want a job and no more than 1.2 billion real jobs. That sure sounds like the availability of cheap genius. Might it be a good thing to export jobs rather than automate them? Might this be a good idea for some jobs and not for others? Might it be that cybersecurity jobs ought to be the first to go, or the last?

We make a point of insisting that referees of athletic events not be employed by the teams, the Congress has just decided that it should forbid itself from doing insider trading, and we put TSA x-ray screeners well away from where they could visualize who it is that they are looking at naked. Is it possible to imagine putting our cybersecurity in the hands of the world's unemployed geniuses who are, incidentally, desperate for a job?

In a sense, they already are. Consider the CAPTCHA -- the hard to read image that you, the owner of human sentience, has to decode. Well, in India and elsewhere, there are firms which sell the service of volume decoding of CAPTCHAs. The going rate is $3/thousand. This does not sound like much, but if a CAPTCHA decoder works 8 hours per day, 6 days per week, spending 8 seconds per CAPTCHA, then that person makes median world income. If he or she can get it down to 6 seconds, the decoder is at the 68th percentile. That is a cybersecurity job which absolutely no one in the US would take because the median US welfare payment is 4X the median world income.

For a while I worked with Trudy Wasenaar, a Dutch bacteriologist working in Germany but publishing in English in the online-only publication of the US Centers for Disease Control on how a bacteriologist sees computer viri and the like. Many things we

discussed amounted to her teaching me the facts of Life. One of her telling observations was this: In Life, the further up the ladder you go, the greater the percentage of the species total metabolic capacity is spent on self-preservation culminating in we humans spending twenty years raising our children. She asked why, with Moore's Law accelerating everything, we cybersecurity people weren't spending an increasing fraction of the total available computing horsepower on protection?

That is a good question because "we" are doing precisely the opposite. How many times have I been told that if my security product costs the customer 5% of throughput then I should just leave because there is nothing worth talking about? Folks, +5% is 45 days of Moore's Law.

These leaves us at a three-way fork in the road.

(1) We can accumulate risk by continuing to build shiny new toys and bet that the trouble comes on someone else's watch if ever

(2) We can turn over our protection to machines that consume a serious, increasing percentage of the Moore's Law dividend on programs that we had better be sure can never turn on us

(3) We can figure out how to harness the world's cheap genius for cybersecurity even though that means putting our eggs in baskets that are not under our jurisdiction

There is never enough time. Thank you for yours.