# For Good Measure

## Why Speculate?

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

The late Michael Crichton was many things. He had both extraordinary imagination and unquivering analytic clarity. In this column, I borrow the title and more from his magnificent essay, "Why Speculate?" given in La Jolla, California, at the International Leadership Forum on April 26, 2002 [1].

Boiled down, Crichton simply said that no one knows the future and that those who pretend to do so are self-serving, delusional, or something else equivalently uncomplimentary. So are the people who believe what the predictors say. He notes how big the prediction industry really is, singling out media especially, and he reminds us all that the track record for sweeping predictions is pretty poor. He coins a clinical term, and I might as well copy his text where he does so:

> Media carries with it a credibility that is totally undeserved. You have all experienced this in what I call the Murray Gell-Mann Amnesia effect. (I refer to it by this name because I once discussed it with Murray Gell-Mann, and by dropping a famous name I imply greater importance to myself, and to the effect, than it would otherwise have.)
>
> Briefly stated, the Gell-Mann Amnesia effect is as follows. You open the newspaper to an article on some subject you know well. In Murray's case, physics. In mine, show business. You read the article and see the journalist has absolutely no understanding of either the facts or the issues. Often, the article is so wrong it actually presents the story backward—reversing cause and effect. I call these the "wet streets cause rain" stories. Paper's full of them.
>
> In any case, you read with exasperation or amusement the multiple errors in a story, and then turn the page to national or international affairs, and read as if the rest of the newspaper was somehow more accurate about Palestine than the baloney you just read. You turn the page, and forget what you know.
>
> That is the Gell-Mann Amnesia effect. I'd point out it does not operate in other arenas of life. In ordinary life, if somebody consistently exaggerates or lies to you, you soon discount everything they say. In court, there is the legal doctrine of falsus in uno, falsus in omnibus, which means untruthful in one part, untruthful in all. But when it comes to the media, we believe against evidence that it is probably worth our time to read other parts of the paper. When, in fact, it almost certainly isn't. The only possible explanation for our behavior is amnesia.

Everyone reading this article knows precisely what Crichton is talking about (or was, 13 years ago): what is written about cybersecurity for the general audience is often counterfactual and/or counterlogical. Unfortunately, what is written for specific audiences like legislatures and regulatory agencies is also counterfactual and/or counterlogical. And all of this finds an audience because of an actual need that I argue is acutely important for cybersecurity—we need to predict the future if our tools are to intersect our problems on target and in time.

That is the theme here—that the fast-moving nature and, yes, the unpredictability of the cybersecurity regime are such that were it occasionally possible to make useful predictions, we would be better off, better able to accomplish our security plans while those plans were still relevant. At the same time, and especially in cybersecurity, no one can predict the future. We desperately need prediction, we know it, and it is impossible to do and increasingly so.

I am, myself, entirely guilty of trying to do prediction in cybersecurity. I give speeches on this precisely [2]. I am working on a personal project right now whose only point is prediction. With a quant colleague, I've long run another. I work on the periphery of the intelligence community, and the intelligence community is entirely about prediction—constantly speculating on what is our actual position and what is our actual velocity. If your very job is security in any sense, then you want all the prediction you can get.

Yet, at the same time, surprises happen. If he were still with us, Crichton would remind us that "[T]he problem with speculation is that it piggybacks on the Gell-Mann effect of unwarranted credibility, making the speculation look more useful than it is." One can argue that compliance is a predictive exercise, based on the idea that "if you do this thing, then you can approach the future with less to fear." I buy that train of thought wholeheartedly, but what if the rules to be complied with cannot keep up with the rate of change? If they cannot, then whatever the prediction of outcome that compliance promises is prediction made relative to conditions that no longer hold. That can't be good. Or useful.

Unpredictability is so true in cybersecurity that we have a special name for when prediction fails: zero-day. We accept that a genuine 0day is an attack that no one could have seen coming. We so very often imply that failing to handle that 0day is blameless since, after all, it was not predicted. Yet every time a particularly lurid 0day shows up, I find myself thinking, "Could I have predicted that? How?"

In my last column [3], I leaned on Nassim Taleb's writing to relate how "the fat tails of power law distributions enlarge the variance of our estimates leading to less frequent but more severe failures (*The Black Swan*). The best one could say is that most days will be better and better but some will be worse than ever. Everything with a power law underneath has that property, and cyberspace's interconnectivity and interdependence are inherently power law phenomena." A fat-tailed setting inherently resists prediction, but for that very reason makes prediction ever more attractive to pursue.

So we get published predictions. Lots of them. Many of them hedge their bets by phrasing their prediction as a question, but that only invokes Betteridge's Law of Headlines ("Any headline that ends in a question mark can be answered by the word no").

It's a quandary. Fast change means tool sets for protection always trail the need unless the need can be forecast. Fast change makes forecasts hard if that fast change is one of adding mechanisms, not just scale, to the equation. We've got both scale (IoT with a 35% compound annual growth rate) and mechanism (afterthought interconnection of sundry gizmos runs on the proliferation of mechanism).

To be deadly serious about cybersecurity requires that *either* we damp down the rate of change, slowing it enough to give prediction operational validity—OR—we purposely increase unpredictability so that opposition targeting grows too hard for them to do. In the former, we give up various sorts of progress. In the latter, we give up various sorts of freedom as it would be the machines then in charge, not us.

But look at that; I can't even talk about prediction without making a prediction…

### *References*

[1] Michael Crichton's 2002 speech: http://geer.tinho.net/crichton.why.speculate.txt.

[2] Dan Geer, "What Does the Future Hold for Cyber Security?" Suits and Spooks: http://geer.tinho.net/geer.suitsandspooks.19vi15.txt.

[3] Dan Geer, "The Denominator," *;login:*, vol. 40, no. 5, October 2015: https://www.usenix.org/publications/login/oct15/geer.