Three policies

1. Rustproof the undercarriage

Some fraction of Internet backbone traffic is unidentifiable as to protocol; some\(^1\) say 10%. Regardless of the perfect figure, that raises a question: What is that 10%? Is that 10% attack traffic? Is it nation state black comms? What is it (besides routable)? Do we actually care that it is being carried at all, or do we care about endpoints?

The thinking man’s answer is "endpoints" as is reflected in the end-to-end principle and, indeed, the entire Internet as it now exists. Adding policy to carriage is like adding salt to roadways; you can go marginally faster in marginally bad weather, but the car rots out from under you and salt is no solution to snow drifts. The Internet undercarriage that we have is a spectacular serendipity; concentrate on endpoints you care about,\(^2\) and, while you are at it, ring up the ISPs to say this and this explicitly:

Hello, Uncle Sam here.

You can charge whatever you like based on the contents of what you are carrying, but you are responsible for that content if it is illegal; inspecting brings with it a responsibility for what you learn.

-or-

You can enjoy common carrier protections at all times, but you cannot inspect nor act on the contents of what you are carrying and can only charge for carriage itself. Bits are bits.

Choose wisely. No refunds or exchanges at this window.

---

\(^1\) John Quarterman, Internet Perils, \textit{e.g.}

\(^2\) geer.tinho.net/ieee/ieee.sp.geer.1101b.pdf
As a matter of policy, just straightforwardly acknowledge that it is (proven) impossible to design a network that is, at the same time, maximally resistant to random faults and maximally resistant to targeted faults. The scale-free character of the Internet is naturally occurring, and as such naturally resistant to random faults, which conveniently works out in practice to mean resilient to incompetence and bad luck. The Internet is not and cannot be made resistant to targeted faults without asserting micromanagerial (re)configuration control over the interconnection fabric down to the individual node, and the result would then be vulnerable to incompetence and bad luck, just not to bad guys. It is just what it is.

2. Corner the market

The good news: Finding vulnerabilities is now too hard to do as a hobby, it has to be a job. The bad news: People who do it for a job don’t share their spoils. The effect: Whatever the count of exploitable vulnerabilities, the ones known to the public are a falling fraction — a fraction that will continue to fall the harder finding vulnerabilities becomes.

This means that found vulnerabilities have mercantile value, and as you know vulnerabilities are bought and sold. If a couple of Texas brothers could corner the world silver market, there is no doubt that the USG could corner the world vulnerability market. Simply announce "Show us a competing bid, and we’ll give you 10x." Sure, there are some who will say "I hate Americans; I only sell to Ukrainians," but because vulnerability finding is increasingly automation-assisted, the seller who won’t sell to the Americans knows that his vulns can be rediscovered in due course by someone who will sell to the Americans, thus his

need to sell his product before it outdates is irresistible.

Noto bene: Do not corner the market unless you are going to make all the vulns you buy public. If you believe in critical infrastructure as a concept, then amassing secret hoards of vulns is lunacy — yes, by making them public you zero out the investment cost of buying the vulns but anyone else who holds those vulns gets zeroed out at the same time and you don’t have to go find them. Buy-All-and-Make-Public, it’s the cheapest win you’ll ever get.

3. Buy the future

While we’re buying things, buy the future itself. If there is anything I know, it is that the purpose of risk management is to change the future, not to explain the past. The more rapid the change, the more explaining the past is irrelevant. Given that that is where we are and seem likely to remain, prediction is the heart of risk management. Again, the more rapid the rate of change, the more prediction matters. Enter cybersecurity.

Prediction markets need no introduction for anyone who has training in decision theory, has read *The Wisdom of Crowds*, or has looked at the scientific literature.⁵ The regulator, the squeamish, the timid, and the perfectionist will all find something to hate because a market is a market is a market. That is the beauty of a prediction market: it is messy, unmanageable, and it trades money for knowledge such that the most knowledgeable get rich, the merely prideful get poor, and all the bystanders get smarter. That is what evolution is made of, and to get evolution to run faster you have no choice but to increase the flux of reward and shorten the lifetime of dumb. The present author does, in fact, have a cybersecurity

³⁵ hanson.gmu.edu/promisepredmkt.pdf
prediction market defined and ready to go, were it not for those selfsame regulation-happy, squeamish, timid, and perfectionist folks who have managed to prevent real prediction markets from taking hold, it would be running today (notwithstanding the various toy markets running variously, including inside the ODNI).

There’s more where this came from, but the best must not be the enemy of the good.

Let’s roll.