Cyber Risk Quant

15 September 2020

Dear Sir or Madam,

Re: Submission to Department of Home Affairs, Protecting Critical National Infrastructure and Systems of National Significance.

Thank you for the decision to make this an open, public and inclusive consultation exercise. I gratefully appreciate this opportunity to participate in providing feedback for your further consideration. Please find herein my considered comments and I standby if you require clarification or additional information. I have concentrated on those questions from which I can provide qualified constructive comment and have provided a general synopsis of the matters as I see them.

The General Synopsis

The wellspring of infrastructure risk is dependence, and specifically the dependence on the expectation of a stable and consistent service when you need it the most. This dependency is additive in the sense that we regularly add additional dependencies to our portfolio, but rarely remove or decommission others. In the time since national infrastructure became a thing, each passing year has meant that we rely on that infrastructure for *more and more* things, and I don't expect that will change in the future. It is Australian societies willingness to adopt, and therefore instantiate the dependencies that makes the infrastructure 'critical' as soon as it is widely enough adopted. *And if rate of adoption is the metric then does that mean cloud computing service providers are critical national infrastructure too?*

The reality is that Australia's collective attack surface is growing quickly in volume, complexity and in interlocking dependencies. There comes a point with this trifecta when the growth of scale, scope and complexity mean that it is no longer possible to be fully aware of all failure modes and be able to make informed decisions of the human sort. *Perhaps we have reached the state of being 'too interconnected to fail'?*

And when the problem domain changes as fast as it does the hardest problem is not applying mitigations to the attack surface but rather understanding, and then deciding how to spend our inherently finite resources. By default, there will always be too much to do, and there will always be an insatiable top-down demand for perfection. Inevitably there will be infrastructure failure from time to time, mitigating all failure modes is no longer financially or technically feasible or sustainable.

Melbourne, Victoria 3141, Australia
Tel +61 3 9028 4143

Cambridge, MA 02142, USA
Tel +1 617 682 9377

In the above there is an implicit assumption that common failure is a singular event. Alas, in an interdependent and complex environment it is more likely to be plural, or in other words cascading multiple failures that are correlated together. If the risk is realised by dependency and connectedness, then a logical approach would be to either be deliberately disconnected or perhaps more realistic to mitigate the risk. It is the later option that becomes even more challenging over time as complexity compounds and underappreciated, or unrecognised correlated risks become further embedded and opaque.

So, what is to be done? At the most strategic level we must do our best to either drive the mean time between failures towards time infinity or drive the mean time between repair towards time zero.

At the operational level we need an environmental surveillance network with instrumentation capable of showing changes to risk leading indicators in near real time, enabling the infrastructure to respond and make adjustments as necessary. The characteristics of good instrumentation would include:

It is consistently measured;

It is cheap to gather;

It has units of measure;

It is expressed as a number rather than an adjective;

It is relevant to decision making.

As you decide what you're going to measure, please keep these points in mind.

Thank you for the opportunity to contribute to this important subject for the security of Australia. For clarification or further information in relation to this submission, please do not hesitate to contact me.

Yours sincerely,

Duncan Hart MSc (Lond)
Cyber Risk Quant' & Managing Partner
StartHere@CyberRiskQuant.com