Submission: 2020 Cybersecurity Strategy

Dr Lesley Seebeck
CEO Cyber Institute
1 November 2019

I welcome the opportunity to provide some thoughts on the proposed cybersecurity strategy.

The number of questions in the discussion paper illustrates the complex, contested, and changeable nature of cyber and cyber security. A subset addresses larger issues, such as the role of government. Given that cyber is a wicked problem, without a broader conceptual framework, the danger is that fragmented approach and point solutions are not likely to meet the challenge.

How are we doing

Cyber is not simply technology, nor is it simply security. Assuming that it is a technology, and that security should be our only concern, has reinforced the parlous situation of our systems, networks, and the threat environment.

There is a reasonable argument that too much emphasis has been placed on the national security aspects of cyber, such that it is tending to trump other considerations, including community well-being, individual rights, free speech, business opportunity, collaboration and creativity. Balance, and greater transparency and debate, is needed. Provisions—and technologies—sought to prevent the prospect of terrorism, or child exploitation, are too easily extended to other use cases. Without redress, such trends risk Australia's geopolitical position and opportunity to build a robust and resilient digital economy and society. Perhaps for each security measure, we should consider a measure supporting and bolstering liberty and opportunity, and apply offset rules and sunset clauses to security measures.

Similarly, reliance on a single source of authority, or over-reach into other jurisdictions and areas where local or deep technical knowledge underpins the health and adaptiveness of systems and community, builds fragility, not strength.

Judging success is not simply ticking off an activity from a past strategy. As Russell Ackoff, argues, quoting Peter Drucker, there is a difference between doing things right, or doing the right things. There's a strong case that we have fallen into the trap of seeking to do the former—doing things right.

Yes, a number of activities have occurred. But the purpose of the strategy is not to simply to do things—outputs—but to achieve outcomes. By that measure, efforts so far have not resolved the challenge posed by cyber, whether geopolitically, nationally, economically, organisationally or at the level of the individual. Yes, in part that may be because the threat environment has worsened—but arguably the trend, if not specifics, should have been foreseeable. The discussion paper itself makes the case of increasing cost and impairment.

And the costs go further than simply financial. Restricting the ability of individuals and organisations to secure their interests and identity, to ensure their privacy and freedom to express themselves, and to control their own data, not simply undermines the cyber resilience of individuals, organisation and society, it risks our credibility as a Western, liberal democracy. And too great a reliance on legislative instruments as a quick fix for constraints and control—or signalling intent—adds to the thicket, generating complexity and uncertainty.

Any weakening of Australia's geopolitical position—and community, economic and individual welfare—means we have to do much more than focussing on existing internal cyber controls and activities. Yes, we are under increasing attack by non-state actors and illiberal and authoritarian regimes, including their proxies. But we need to build societal resilience, civic society, and the strength of individuals and communities to withstand incursions and to 'bounce forward', should they occur.

Reasons for a rethink

Cyber is a significant—but not the only—driver of the trends and concerns. Efforts thus far have not withstood events and trends—and given the ubiquity of digital technologies and our reliance on networks and data, the need to improve is increasingly urgent. There is reason to believe that doubling down on the current approach will exacerbate the problems and the deterioration of our position.

We are dealing with wicked problems and complex adaptive systems. Such systems typically elude efforts to tightly control them—or at least, without fundamentally altering their nature. Government by itself has little hope of assuring safety and security for all—again, at least to levels acceptable in democratic societies. Indeed, in such systems, government has few instruments available to it to manage change well in the short-term. The usual tools, typically budgetary and legislative, tend to be blunt, misdirected (not deliberately) and often too slow for fast-changing problems. The strength of Western liberal democratic systems lies in the initiative and adaptiveness of individuals and small groups, the contestability of ideas, and the productivity of free markets. And to make best use of that, the slower, more careful work of strategy, statecraft, subtlety and an understanding of complex socio-technical systems is needed.

To illustrate: amongst the many features of the complex socio-technical system we inhabit, there are definitional issues. In other words, what we see often depends on where we stand. For example, variety and diversity are the hallmarks of a democracy and resilient society: what may constitute 'safety' for one individual may offer insight, experience and acceptable risk for another. Without local knowledge, and the ability to differentiate between types, it is easier for government to apply one perspective, and overly constrain variety and diversity. That, naturally, limits adaptability and responsiveness.

Then there is the intransparency of complex systems. Triggering events, causal chains, interdependencies are generally hidden—and may only be surfaced under particular conditions. Thus it is hard to act with certainty—and there are often unintended consequences, which may not emerge for some time. It is also hard to establish

accountability, or to provide adequate support or the necessary variety in tools to manage the problem. In the face of uncertainty, government tends to respond with increased levels of risk aversion, not least because decisions to act themselves imply risk.

Last, given the pace of change, and the disruption in formerly stable systems, it is easy to misapply efforts to exert control, to protect components, and to constrain actors as a means of risk management. Technological fixes will be quickly overtaken, generating orphaned systems and increased vulnerability, especially without the skills, systems and funding to resolve issues quickly. Social fixes, including legislation, tend to be reactive and if aimed more at control than enabling individuals and the community, risk slowing adaptiveness and impeding initiative.

Suggested approach

Rather than simply a defensive approach, and one that shifts risk from decision-makers onto individuals, we have the opportunity to rethink and do things better, and in such a way that strengthens Australia.

First, **a return to the fundamentals of Western, liberal democracy**. A fundamental strength of democracies is that, by investing in individuals and giving them the freedom, and ability, to create, build, prosper and take a large measure of responsibility for their own well-being, they build both legitimacy and resilience that authoritarian societies lack. Increasingly, in a digital society, that'll include their online activities as well. It also lets Western liberal democracies play to their strengths.

Changing the narrative around cyber will help. We cannot afford cyber to be seen simply through the lens of national security: that's too restrictive. Legal provisions should offer rails supporting freedom and prosperity, the protection of citizen data, as well as limiting the prospect of government over-reach, particularly as data accumulates and digital technologies are easily extendable. Cyber should be seen as an enabler, not something that impedes growth, change, investment, and exchange. As Singapore is showing, promoting cyber research and technology can be a competitive advantage.

Second, invest in people. Ultimately, cyber is about people. People make mistakes; they can act with malicious intent. They are also part of the solution: they are creative, capable and they care. Building capability—improving their knowledge and awareness, providing them with the access to tools to help protect themselves, their family and workplace—will help build trust. Enabling people to control their own data gives them an investment in their own security, in the same way that home ownership gives them an investment to looking after and protecting their own property.

More people with skills are also needed. Technical skills, of course, are short, and much needed. But just as cyber is not about technology, we need people who understand cyber and prioritise and build the policy, financial, cultural, economic and social systems around it as well—something of particular interest to the Cyber Institute.

Third, simply invest. It is a truism of business strategy that both intent and effect follow the money. The government cannot expect any real outcomes or substantive improvements if it is not prepared to put real, sufficient and sustained funding and other incentives behind a new strategy. Assigning an agency with a broad remit to tackle a wicked problem—if it must—without matching resources is setting it up to fail. That represents an exploitable vulnerability all of its own.

Government also needs to invest not in point solutions, but in building the ecosystem around cyber. That requires considerably more support for research and development—and not just in science, engineering and technology, but also where these technologies have applications (for example, in archaeology, finance, international relations, the humanities and Asian studies) and in interdisciplinary fields, to broaden the base. Australia needs a strong R&D and technical capability so as to secure its own destiny, including in cyber.

Fourth, adopt a systems-level approach. Drawing on complex systems theory, I would emphasise resilience and adaptiveness—there will be failures, there will be breaches despite our best efforts, and government will not always get it right.

In a changeable contested world, we need options and so we need to invest in resilience, diversity and redundancy over efficiency. As what might fit today may be less than optimal tomorrow, we need to hedge our bets and open the aperture to new ideas and insights, that is, exploring science, technologies and different approaches.

Systems, people and technology interact and as they do, they co-evolve. That means any assessment of critical infrastructure, for example, has to take such change into account. As I found when doing some research on the 2001 UK foot and mouth outbreak, assumptions about agricultural systems were based on the earlier outbreaks in the late 1960s. In the time since, transport systems, demographics, industry consolidation and global trade had changed the underlying structure of British agriculture, so that the outbreak did not behave as expected. I expect we will find similar issues in Australia, whether it be a similar disease outbreak or a major cyber event (as currently in the health system in Victoria).

Provide individuals with broad guidance and strengthen local communities, including through distributed such as social media, user groups, and professional organisations. And enable adaptive responses, and ensure openness and transparency so that different communities, government and the provide sector can share lessons as well as threat information and remediations. ANU has made a start on the latter, with its report on its data breach. It would be great for government agencies to follow its lead.

I am happy to discuss further,

Dr Lesley Seebeck
CEO
Cyber Institute
The Australian National University