Dr Frank Rossi
Business Consultant
[redacted]

18/4/2023

Dear Expert Advisory Committee,

Apologies for the lateness of my submission regarding the Discussion Paper on the Australian Cyber Security Strategy. I really only became aware of it just after the closure date. I believe Australia's response to the threats in cyber space is crucial to all our well-being. I hope you will still consider my initial thoughts.

My own experience of transformation programs as an IT business consultant over the last 30 years is that they take a long time for both the technology and the cultural change. Along the way there is usually resistance to change. Almost invariably, there is a shift in the premises that the program was founded upon. This leaves us wondering at the end if we could have approached our goals differently. Was our passionate effort well spent? Could we have anticipated the shifts? Should we have pursued different goals?

I've noticed a pleasing shift in the Australian Government from a purely defensive posture to include an offensive one against the threat agents as they currently present. But my concern is that we are in a threat environment that will evolve more quickly than the proposed strategy from 2023 to 2030. Experience shows all too often that such large programs of work do not always respond with agility, in spite of the best intents.

So, my question is: how can we mitigate this risk and anticipate and work to the threat landscape as it will appear in 2030, without the benefit of a time machine?

I think that a quick response from those closest to these plans would be that of course we will adjust our approach to the evolving landscape. Or that we can only plan based on our current understanding. But I think that the history of technological and cultural change over the last 50 or so years has shown that keeping up with, or ideally ahead of the change, proves too difficult. We are usually on the back foot with such rapid and unpredictable change.

I pose these questions not because I have all the answers, but because I believe that thinking creatively about that future threat landscape, rather than purely analytically and linearly, offers us the best chance to anticipate that future. After all, this point is where we have the most leverage on our future success.

So, what I am suggesting is that we think carefully about how we go about creating a strategy. The Minister's Foreword on page 4 of the Discussion Paper lists four points that describe a great vision for Australia's cyber security by 2030. But as someone once noted, "Change is not a destination, just as hope is not a strategy" (Rudy Giuliani).

In 2001, Donald C. Hambrick and James W. Fredrickson authored a paper[1] "Are you sure you have a strategy?". Their key point is that what actually constitutes a strategy isn't generally well understood and articulated. They argue that a strategy has five elements, providing answers to five questions - arenas: where will we be active? vehicles: how will we get there? differentiators: how will we win in

[1] https://carpenterstrategytoolbox.files.wordpress.com/2013/10/strategydiamond-hambrickfredricksoname01.pdf

the marketplace? staging: what will be our speed and sequence of moves? economic logic: how will we obtain our returns?

While this may seem like just more business jargon for private companies trying to make a profit in their marketplace, I believe the approach could facilitate a creative discussion for cyberspace. After all, the vision articulated by the Minister is also an economic one. My experience of using it with business stakeholders is that the questions do get them thinking, not always with immediate answers. And that sets the stage for creative responses.

Sincerely, Frank Rossi