FY2020 Cyber Security Strategy Submission

By Jasmine Rodet

13/10/2019

The FY2020 Cyber Security Strategy appears to exclude ADF requirements. Given that;

- cyber human capital can be shared across civilian and military domains, and there is a shortfall in cyber skills nationally and likely globally, our FY2020 cyber security strategy should include a cyber human capital approach that will provide the people we need in both the non-military and military domains. It would be wasteful to have separate strategies for these domains given the skills for cyber defence and non-technical cyber skills are similar.
- an all of economy approach to the FY2020 cyber strategy should not ignore the convergence between the military domain and the non-military domain. The two are converging every day in cyber space, given attacks to our national security can be initiated by non-state actors. Additionally, a cyber-attack on Australia's critical infrastructure is the responsibility of the ADF to respond to, an attack of which would likely impact all of economy.

If you do intend to keep cyber strategy for the ADF separate from the FY2020 Cyber Security Strategy, there needs to be some comment to this effect, the reasons why and how will the cyber human capital issue be resolved (for both domains)?