2023-2030 Australian Cyber Security Strategy Discussion Paper: Submission

Framework for Evaluating National Cyber Security Policy

Co-founder of the Social Cyber Group

14 April 2023

Government Invitation

In 2023, the government released a Discussion Paper which called, alongside many other things, for 'a transparent, meaningful evaluation framework to ensure the Australian Government's vision is realised, and the Strategy is fit-for-purpose now and into the future'.[1]

This submission, based on a longer research paper by the author for the Social Cyber Group, addresses that call for an evaluation framework.

Basic Principles

1. The federal government should align its evaluation processes with the appropriate strategic focal points, especially the prevention of cyber harms to the country, its businesses, and its citizens.
2. The evaluations must be independent and therefore led by an eminent social scientist, expert in policy evaluation and policy reform, who as 'evaluation leader' reports to the Department of Prime Minister and Cabinet.
3. The mechanism of evaluation should include several distinct panels specialising in sub-elements of national cyber policy (countering cybercrime, protection of citizens' rights, technical aspects of cyber security, education and workforce development).
4. The evaluation criteria and terms of reference can be set once the mechanisms of evaluation are in place since the criteria and performance indicators would need to be determined by the expert panels under the guidance of the evaluation leader.
5. The evaluations must be highly transparent and open to public scrutiny (subject to the content detail not offering sensitive information to cyber-criminals or hostile governments).
6. The overall policy should be evaluated by this independent process every four years, with all sub-components evaluated at least every two years, bearing in mind that the Department of Finance has advised that evaluation should be a continuing and permanent element of policy delivery.
7. The government must commit to the best standards of evaluation eg not those currently practised by the Department of home Affairs in its annual reporting on cyber security performance which are assessed as poorer than those conducted by other government departments, such as the Department of Industry.
8. Given the importance of cyber security to national security, the federal government should commit at least 3% of all cyber security component spending to evaluation of their execution.

Key features of the implementation of these principles should be :

Strategic Focus on Cyber Harms: Australia's cyber security policy must be assessed against its reduction of cyber harms, the mitigation of cyber harms, and the prevention of cyber harms.

These harms, by source, include:

- Hostile state activity.

[1] Australian Government, '2023-2030 Australian Cyber Security Strategy Discussion Paper', 2023, p. 25, https://www.homeaffairs.gov.au/reports-and-pubs/files/2023-2030_australian_cyber_security_strategy_discussion_paper.pdf.

- Criminal activity in cyberspace.
- Anti-social but lawful practices.
- Incompetence by users or operators.
- Unforeseeable effects created by coincidence of negative events.

To address cyber harms from these sources is the most urgent purpose of cyber security policy. The prioritization in evaluation of urgent purposes over non-urgent purposes is an essential departure point.

Non-urgent purposes, though very important, would be those designed to create social or economic value for its own welfare gains and have less to do with protection in cyberspace. Such welfare gains include:

- Improved ICT knowledge and skills
- Improved economic gains
- More creative uses of cyberspace.

Strategic Focus on Outcomes: Reduction in Cyber Harms

The evaluation of cyber security policy must have a laser-like focus on outcomes: a measurable reduction in cyber harms and a measurable growth in national confidence that cyberspace is more secure and productive and less threatening as a result of national cyber policy.

Strategic Focus on Whole of Society

The evaluation must be rooted in the reality that improved cyber security outcomes in Australia need to be delivered by many actors working in close coordination, and the outcomes shaped by these actors should be focal points of evaluation:

- National security agencies and their international partners capable of preventing or mitigating cyber harms.
- Domestic police forces and their international partners capable of successful prosecutions for cyber crime and related prevention activities.
- National, state-based, local and international actors whose mission is mitigation of the most serious cyber effects.
- A vibrant and responsive system of laws and regulations.
- A highly developed research ecosystem focused on national cyber security outcomes.
- Domestic and international news media that act responsibly and are well-informed.
- Civil society actors, in Australia and internationally, mobilised around the goal of improved protection in cyber space.

Strategic Focus on Rights and Obligations

An overarching approach to evaluation must include assessment of impacts on citizens' rights and obligations. In particular, there needs to be much more attention paid to privacy issues arising from breaches of sensitive personal data.

Individual Program Evaluations

The framework should allow for individual program evaluations, of which the federal government's formal 'Cyber Security Strategy' is but one program, not the totality of national effort in cyber security policy that needs to be evaluated.

The government has identified four pillars of the forthcoming strategy, but these cannot be allowed to dominate the evaluation because that would seriously degrade the strategic focus described on the preceding page. These four pillars identified by the government are:

- A secure economy and thriving cyber ecosystem.
- A secure and resilient critical infrastructure and government sector.
- A sovereign and assured capability to counter cyber threats.
- Australia as a trusted and influential global cyber leader, working in partnership with our neighbours to lift cyber security and build a cyber resilient region.

The way they government organises its cyber security strategy around these four themes blurs fundamental priorities, such as security and business growth, that deserve much sharper articulation separately. These four policy themes appear to overlook others which have very high priority (such as reducing cybercrime). Australia's policies for countering and mitigating cybercrime are one of its weakest areas of performance in cyber security policy.