National Maritime Foundation

www.maritimeindia.org

A REVIEW OF THE AUSTRALIAN CYBERSECURITY STRATEGY 2023-2030

Commander Subhash Dutta (Retd)

1. On 22 November 2023, the Australian government released a comprehensive document describing the cybersecurity strategy for the country.[1] The document covers a time frame of 2023-2030 and describes a whole-of-nation approach towards achieving specific cybersecurity goals for its citizens and businesses.

2. The formulation of this strategy document began in December of 2022 with the government appointing an 'Expert Advisory Board' to guide the development of the strategy. The board prepared a discussion paper that solicited comments from individuals and organisations. It received more than 300 public responses. In addition to this discussion paper, the Department of Home Affairs also organised multiple discussions with industry, community leaders, and individuals. These responses were studied, and the final strategy paper was prepared accordingly.

3. The impetus for the promulgation of this strategic guidance appears to be the realisation on the part of the Australian government that with the advancement of internet and information technology [IT] enabled services that have permeated to almost all Australian citizens, there has been a concomitant increase in cyberattacks on Australian individuals and organisations within Australia as well as beyond its shores. Two recent major large-scale incidents occurred in October 2022, when the data of almost 20 million Australian citizens was lost in cyber-attacks on Optus[2] and Medibank[3]. The deleterious effects of these attacks, not just on the companies but also their customers, generated palpable urgency to address this problem on a national scale.

4. The "Australian Cybersecurity Strategy 2023-2030" (hereinafter referred-to as "the Strategy") adopts an approach that emphasises specific actions by the government as well as industry. It highlights the Australian government's commitment to a collaborative effort between government, industry, and individuals to achieve a secure cyberspace for all. It also specifies the goal of Australia becoming a global leader in cybersecurity by 2030. To achieve this this goal, the Strategy calls for a structured and phased approach, which may be summarised as follows:

[1] Australian Government Department of Home Affairs, "2023-2030 Australian Cyber Security Strategy". https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/2023-2030-australian-cyber-security-strategy

[2] *"Singtel Optus Pty Limited is an Australian telecommunications company headquartered in Macquarie Park, a suburb in the Northern Sydney region of Sydney, New South Wales, Australia. It is a wholly owned subsidiary of Singaporean telecommunications company Singtel".* https://en.wikipedia.org/wiki/Optus

[3] Medibank is an Australian company providing private health insurance and health services. https://www.medibank.com.au/about/company/overview/

(a) **Near term activities (2023-2025)**. Strengthen foundational aspects by addressing critical gaps, identify vulnerable citizens and businesses, and work with global partners for cyber maturity.

(b) **Mid Term Activities (2026-2028)**. Scale-up cyber-maturity across all businesses by investments in technology and a diverse cyber workforce.

(c) **Long Term Activities (2029-2030)**. Establish Australia as a global leader in cybersecurity by 2030.

5. The Strategy terms these periods "Horizon 1", "Horizon 2", and "Horizon 3", respectively. The activities of "Horizon 1" would appear to be synchronized with the next general elections that are due in September of 2025, perhaps giving the politicians concerned an achievement that they could use.

6. Some of the factors that have prompted the articulation of the Strategy are:

(a) Like all countries, Australia faces an increasingly hostile cyberspace environment. While businesses and the economy in general have adopted digital transformation to increase productivity and generate wealth, malicious actors have not been idle either. Cyber-attacks have grown in sophistication as well magnitude. In many cases State sponsored, or State-tolerated threat-actors have been relentless in their attempts to cause mayhem across all sectors of the nation's economy.

(b) The acceleration in malicious activity is in many ways due to the fact that most means used to target vulnerabilities are now easily available at minimal cost as compared to the returns that they offer. The "attacker-as-a-service" model also ensures that lack of technical knowledge is no longer a hinderance to successful data breaches by even a novice attacker.

(c) In October 2023, while responding to the Australian Parliament, the Director General of Australian Signals Directorate (ASD) acknowledged Australia's offensive cyber capabilities and the actions that the ASD had taken against cybercriminal syndicates. However, as events have shown this is a short-lived victory as these threat actors quickly regroup under different names and most of them remain beyond the reach of law enforcement agencies.

(d) Australia considers itself to be a trusted partner for other nations in the region for the provision of collective capability as well as a credible leader globally in cybersecurity. Australia has strongly emphasised the rules-based international order and has consistently called out instances of malicious cyber activity by other States.

7. The overall approach of the Strategy is embodied by six interlocking "shields" representing different areas of focus:

(a) **Shield 1: Strong Businesses and Citizens:** Empowering individuals and businesses to defend themselves online.

(b) **Shield 2: Safe Technology:** Ensuring the security of technology products and services used by Australians.

(c) **Shield 3: World-Class Threat-Sharing and Blocking:** Improving information sharing and cyber threat detection capabilities.

(d) **Shield 4: Protected Critical Infrastructure:** Safeguarding essential infrastructure from cyberattacks.

(e) **Shield 5: Sovereign Capabilities:** Developing a strong domestic cyber-security industry and expertise.

(f) **Shield 6: Resilient Region and Global Leadership:** Collaborating with regional and international partners to improve global cyber resilience.

8. Even as the Strategy demonstrates the Australian government's resolve to address challenges posed to its digital economy from threat actors, it is not short on the actual steps the government intends taking to provide protection to its citizens, businesses, and government institutions. Each of the "shields" mentioned above contain specifics of the various actions by the government that would ensure the articulation of desires expressed. For example, the actions that the government would take to ensure a positive outcome of "Shield 1" are:

(a) Advice and guidance to small and medium businesses by way of a free and tailored assessment of cybersecurity maturity. This guidance will be adaptable to keep pace with the growth of this sector of business. A reduction of regulatory compliance requirements would also ensure active participation of small and medium businesses.

(b) Provide support to ensure resilience to this community when faced with cybersecurity incidents. Recovery capability will be provided by dedicated teams of cybersecurity professionals who understand the small business environment.

(c) Building cybersecurity awareness among the citizenry to enable it to embrace the opportunities provided by digital technologies. This awareness campaign is designed to help Australians understand the evolving nature of cyber threats and how to protect themselves. This awareness campaign is also focused on vulnerable communities to provide cyber literacy. Rural and isolated communities that rely on the availability of digitally delivered services comprise one such target group.

(d) Build upon existing domestic law-enforcement and offensive cyber activities to disrupt the activities of threat actors. Currently the Australian Federal Police (AFP) and the ASD use offensive cyber capability as a criminal investigation tool towards prosecution or disruption. The Strategy calls for an expansion of these activities to make Australia a harder target to attack.

(e) On most occasions, under-reporting of ransomware incidents by businesses is due to the punitive actions likely to be faced by victim organisations for failing to protect their data. The Strategy calls for legislating a "no-fault, no-liability" ransomware-reporting obligation for businesses.

(f) Most of cases of payment of ransom do not result in the recovery of encrypted data. The Strategy calls for the government to strongly discourage businesses and individuals from paying ransom to cybercriminals. Along with this advice, the Strategy also advances the development of a "ransomware playbook" that would provide guidance to businesses on preparing, dealing and recovering from a ransomware attack.

(g) To enhance the adoption of the digital economy by businesses, the Australian Government will work with industry to ensure cyber security is appropriately considered in the boardroom and informed by clear guidance on cyber best-practices, and lessons learned from previous cyber incidents. To clarify business expectations of cyber governance, the Australian government will provide corporate obligations for critical infrastructure owners and operators and to collaborate with industry to design best-practice principles to guide good cyber governance.

(h) In a deviation from the current practice being followed elsewhere, the Strategy calls for reducing the need for (1) people to share sensitive personal information with government, and (2) for businesses to access services online. This would help in reducing the risks and impact of identity theft and fraud. Cybersecurity of the Australian Government's "Digital ID "System is recognised in the Strategy as being crucial to this.

(i) In keeping with the theme of working with individuals and organisations the Strategy emphasises the government's desire to support victims of identity theft by increasing funding for this.

9. Recognising the fact that cybercrime is a global threat, the Strategy calls for the Australian government to work with international coalitions to provide effective deterrence and response to cybercrime. The calling out of States that provide safe harbour to threat actors has been emphasised in the Strategy. A case in point is offered by recent public attribution of the attackers responsible for the data breaches at Optus and Medibank in Sept-Oct 2023 being based in Russia.

10. While most national strategy documents are fairly clear on "what" is desired and hence to be articulated, it is the "how" part that is left vague (possibly to cater for evolution of the threat over time) or at best promulgated much later when events have overtaken the premise of the

strategy. What is especially noteworthy in the Australian case is that there is a detailed "Plan of Action" released by the Australian government, as an accompanying document.

11. This "Cyber Security Action Plan" supplements the Strategy and specifies the key initiatives that will be taken over the next two years as detailed in the "Horizon 1" timeframe. This Action Plan describes the implementation details of the measures designated as part of all six Cyber Shields. "Horizon 1", which focuses on strengthening Australia's cyber security foundations, will address the critical gaps in Australia's Cyber Shields to build strong businesses and citizens through deep partnerships across industry and government.

12. The Action Plan will be reviewed every two years, with actions being modified, added, and deleted, as required by changed circumstances or the environment. Even more importantly, the Action Plan designates the leading and supporting government agencies for each action items. This is intended to ensure accountability while providing authority to the concerned agency.

Comparative Analysis vis-à-vis India

13. The details and the expanse of the Strategy and the accompanying Action Plan emphasise the importance of cybersecurity, which is considered essential for the continued development of Australia and to provide a safe and secure digital environment to Australian citizens and businesses. The Strategy provides a focused approach to help realise the Australian Government's vision of becoming a world leader in cybersecurity by 2030. Indeed, there is much to admire and, perhaps, emulate.

14. By way somewhat unflattering contrast, the Indian government's own approach still remains one of a series of disjointed efforts without a single overarching document describing a similar intent. There are multiple agencies each with their niche domain that have promulgated often similar requirements to ensure cybersecurity of their respective constituencies. What is common is that most of these regulatory requirements, instead of providing meaningful guidance or assistance to either the citizens or businesses, simply emphasise punitive measures.

15. Among the bodies that oversee and regulate cybersecurity for Indian entities are the following:

(a) The Ministry of Communications, and the Ministry of Electronics and Information Technology (MeitY) are the two primary ministries that deal with all aspects of cyberspace governance in India. The Department of Telecommunication (DOT) under the Ministry of Communication is responsible for policy, licencing, and coordination, in respect of all matters relating to telecommunications.

(b) The charter of MeitY includes policy matters relating to IT, electronics and the internet, and matters relating to cyber laws as well as other IT related ones. MeitY has three statutory bodies that function under its overarching control, namely, the

"Controller of Certifying Authority "(CCA), the "Indian Computer Emergency Response Team (CERT-In)", and the "Unique Identification Authority of India" (UIDAI).

(c) The "Information Technology Act, 2000" and its companion, the "Information Technology (Amendment) Act, 2008" provide the foundation of India's cyber legal framework. The Regulations issued pursuant to the requirements of these Acts outline the obligations and responsibilities of various authorities and organisations.

(d) The most recent regulation regarding data protection is the "Digital Personal Data Protection Act, 2023", which was passed by the Parliament in August of 2023. However, the regulations and responsibilities of the various designated authorities have yet to be promulgated, leaving the implementation of this Act in limbo. The "National Cyber Security Policy" which sought to provide strategic direction is a document that dates to 2013.

(e) There are, of course, some things to cheer about. Sectoral bodies providing regulatory oversight to their constituents, such as, for example, the Reserve Bank of India (RBI) for the banking (and other financial institutions) sector, do provide guidance in terms of the requirements to address cybersecurity concerns.

(f) In the bulk, however, there is a yawning gap to be bridged. India has a population of almost 900 million internet users with a large ecosystem of digital payments and is firmly committed to sustaining a digital economy. However, it must be admitted that this large population, many of whom lack even the basic education, is left to its own devices when it comes to providing cybersecurity protection and guidance.

16. It is not the intention of this article to list all issues that are missing or not receiving adequate attention from the government. The foregoing paragraphs purports only to highlight that disjointed and desultory efforts will, in all probability, prove inadequate for the provision of strategic guidance on the cybersecurity front. This is especially important now with the growing number of cyber-attacks on citizens and businesses. While India has achieved an enviable level of digital financial inclusion for a large segment of its population, there is still an extremely rudimentary understanding of cybersecurity requirements.

17. What is needed is a comprehensive cybersecurity strategy that gives a timebound action plan with clear authority and accountability assigned — one that provides both, citizens and businesses, with a robust legal framework that can assist them in developing the requisite resilience to recover after a cyberattack. Most importantly, the approach must shift from one centred upon punitive action to one centred upon empathy, guidance, and support. For all these aspirations, the Australian cyber strategy offers an excellent example of a best practice that could and should be adopted and adapted.