# Cyberoo.AI Submission

**Horizon 2 (2026–2028) – 2023–2030 Australian Cyber Security Strategy**
**Date:** August 2025

---

## Contents

# Executive Summary

Cyberoo.AI welcomes the opportunity to contribute to the development of Horizon 2 of the Australian Cyber Security Strategy.
Our submission focuses on **scam and fraud disruption**, **public awareness uplift**, **SMB/NFP readiness**, and **regional cooperation**, aligning with the Strategy's goal of making Australia a **world leader in cyber security by 2030**.

**Key Recommendations**

- **Target scam and fraud disruption as a national priority**, integrating near real-time threat intelligence into public alerts, SMB/NFP support, and blocking frameworks.
- **Expand multilingual, culturally accessible awareness programs** supported by structured micro-certifications and community-delivered education.
- **Develop standardised incident evidence formats** to accelerate insurance claims and law enforcement investigations.
- **Strengthen cross-border cooperation** through regional scam intelligence exchanges, harmonised takedown processes, and shared training frameworks.
- **Incorporate scam disruption into critical infrastructure obligations** under the SOCI Act to protect high-trust targets and supply chains.

These recommendations are grounded in operational experience across our product suite and respond directly to gaps and opportunities identified in the Government's Charting New Horizons Discussion Paper, the 2023–2030 Action Plan, and Appendix B – Status of Horizon 1 Initiatives.

## Scam and Fraud Disruption as a Core Component of Cyber Security

While scams and fraud are often treated primarily as consumer protection or financial crime issues, they are delivered through digital infrastructure and adversary tradecraft that fall squarely within the cyber threat landscape. Threats such **as phishing, brand impersonation, malicious websites, and mule account networks** rely on the same infrastructure, exploitation techniques, and cross-border coordination used in broader cybercrime.

Disrupting scams therefore strengthens national cyber security by removing adversary infrastructure, denying them access to financial channels, and reducing opportunities for social engineering at scale. This approach **complements traditional network defence by targeting the operational environment of adversaries** rather than solely focusing on end-user defences.

Our operational experience **in identifying, monitoring, and dismantling** such infrastructure aligns closely with the Strategy's objectives in Shields 1, 2, and 3, particularly in safeguarding businesses and citizens, enhancing technology safety, and enabling world-class threat sharing.

# Shield 1 – Strong Businesses and Citizens

## Q1. What trends or technology developments will shape Australia's cyber threat outlook in Horizon 2?

The Charting New Horizons Discussion Paper (p. 10) notes the increasing sophistication of cyber-enabled crime, with scams and fraud emerging as a major threat vector affecting citizens, small businesses, and critical supply chains. These attacks are increasingly leveraging artificial intelligence, deepfake technologies, and automation to target victims at scale, increasing both the volume and complexity of incidents.

From our operational experience, three developments will be particularly influential in Horizon 2:

1. **Industrialisation of scam operations** – Scam syndicates now operate in highly structured models, often with dedicated infrastructure-as-a-service providers supplying phishing kits, mule accounts, and digital identities.
2. **AI-enabled targeting and impersonation** – The use of generative AI for creating realistic content, including cloned voices and videos, has significantly reduced detection opportunities for end users.
3. **Cross-border mule networks** – The speed at which funds are moved through multi-jurisdictional mule accounts hampers both financial recovery and law enforcement intervention.

**Recommendation:**

- Horizon 2 should prioritise the systematic collection and disruption of scam TTPs (tactics, techniques, and procedures), including mule account harvesting, before funds leave the jurisdiction.
- Invest in AI-driven detection and enrichment pipelines capable of identifying scam campaigns in their early stages, before widespread victim engagement.

## Q5. How can Australia better target and consolidate cyber security awareness messages for citizens and businesses?

Table 1 in the Australian Government's Appendix B – Status of Horizon 1 Initiatives shows that while numerous awareness campaigns have been delivered, message fragmentation remains an issue. Citizens and small-to-medium businesses are exposed to multiple overlapping messages from government, banks, and private industry, often with varying terminology and action advice.

**Recommendation:**

- Establish a national scam and fraud awareness framework with unified terminology, visual identity, and plain-language advice.
- Integrate scam-specific education into mandatory onboarding for high-risk digital services, such as online banking and investment platforms.
- Expand delivery channels to include multilingual, culturally targeted content to reach culturally and linguistically diverse communities, who are disproportionately affected by scams.

## Q6. Which existing programs should be scaled nationally during Horizon 2?

Programs in Horizon 1 that demonstrated measurable impact in reducing victimisation—particularly those involving rapid intelligence sharing between industry and government—should be scaled. Appendix A (p. 12) of the Australian Government's Charting New Horizons materials highlights the importance of coordinated disruption models that integrate reporting, verification, and takedown.

**Recommendation:**

- Expand centralised verification and alerting services to cover not only phishing emails but also scam websites, social media accounts, and investment platforms.
- Ensure all scaled programs are supported by operational intelligence feeds capable of delivering real-time updates.

## Q7. How can we encourage SMBs and NFPs to adopt existing cyber security resources and tools?

The Charting New Horizons Discussion Paper (p. 12) notes low uptake of existing resources among small-to-medium businesses (SMBs) and not-for-profit organisations (NFPs), citing perceived complexity, cost, and a lack of immediate relevance. Scam and fraud disruption capabilities, in particular, need to be delivered in accessible, low-friction formats to gain traction in these sectors.

**Recommendation:**

- Provide turnkey scam disruption packages that combine basic phishing and impersonation detection with standardised incident response templates.
- Leverage industry associations and regional chambers of commerce as trusted delivery partners to extend reach into resource-constrained SMBs and NFPs.

# Shield 2 – Safe Technology

## Q21. How can we strengthen our ability to block threats at scale?

The Charting New Horizons Discussion Paper (p. 18) identifies the need for scalable threat blocking systems that integrate intelligence from both public and private sectors. Table 1 in the Australian Government's Appendix B – Status of Horizon 1 Initiatives notes progress in domain blocking and filtering but highlights gaps in detecting and disrupting scams beyond email-based threats.

**Recommendation:**

- Establish a national scam disruption exchange to receive, validate, and distribute machine-readable indicators, including domains, phone numbers, mule accounts, and social media handles.
- Incorporate scammer-interaction intelligence into blocking decisions to detect and neutralise threats earlier in the attack lifecycle.
- Expand safe browsing protections beyond DNS filtering to include application-layer blocks in online banking and government portals.

## Q22. How can we ensure secure data sharing while promoting economic prosperity?

Secure, privacy-preserving data sharing is essential to ensure that threat intelligence can be used without infringing on privacy or breaching compliance obligations. The Charting New Horizons Discussion Paper (p. 19) calls for interoperable frameworks for cyber data sharing.

**Recommendation:**

- Adopt a federated intelligence-sharing model where enriched scam intelligence remains distributed but is queryable by authorised entities.
- Standardise the data schema for scam intelligence to ensure compatibility with regional partners and financial institutions.

## Q25. How should a proactive cyber security posture be defined for Australia?

Appendix A (p. 22) of the Australian Government's Charting New Horizons materials shows that many initiatives in Horizon 1 were reactive, focusing on post-incident recovery. Horizon 2 should define proactivity as the capacity to detect, verify, and disrupt malicious activity before mass victimisation occurs.

**Recommendation:**

- Include simulated engagement with malicious actors as a recognised proactive measure to identify infrastructure before full deployment.
- Make scam disruption and mule account harvesting a national intelligence priority alongside traditional cyber threat intelligence activities.

## Q26. What are the most effective approaches to blocking threats at scale?

Appendix A of the Australian Government's Charting New Horizons materials notes success in blocking high-risk domains but indicates gaps in coverage for scams propagated via social media, messaging apps, and VoIP.

**Recommendation:**

- Integrate cross-channel blocking into the national framework, including SMS, messaging apps, and VoIP numbers.
- Improve speed-to-block by reducing manual validation delays for high-confidence indicators.

## Q27. How can safe browsing and warning systems be improved?

Current safe browsing measures are underutilised outside mainstream browsers and rely heavily on public reporting.

**Recommendation:**

- Extend safe browsing APIs to mobile banking applications and e-government services, enabling instant flagging of known scam sites.
- Provide multilingual warning pages to ensure accessibility for culturally and linguistically diverse communities.

## Q29. How can we better align and operationalise intelligence sharing for cyber security and scams prevention?

The Charting New Horizons Discussion Paper (p. 22) identifies persistent fragmentation in intelligence sharing, particularly in how scam and fraud disruption data is handled across government, telcos, and financial services. While Horizon 1 advanced sectoral sharing mechanisms, there is no unified framework to operationalise scam-specific intelligence across sectors.

Recommendation:

- Establish a Scam Intelligence Exchange Framework with common data standards covering domains, phone numbers, mule accounts, and social media handles.
- Mandate integration with both public reporting portals and industry sources, ensuring a continuous feed into CERT Australia and the Australian Financial Crimes Exchange (AFCX).
- Create real-time, machine-readable intelligence channels that financial institutions and telcos can act on instantly, reducing delays in takedown and account blocking.
- Incentivise industry participation by enabling liability protections and feedback loops on actioned intelligence.

# Shield 3 – World-Class Threat Sharing and Blocking

## Q33. How can national coordination on cyber threats be improved in Horizon 2?

The Charting New Horizons Discussion Paper (p. 21) notes that while Horizon 1 built stronger threat-sharing frameworks, operational silos remain between law enforcement, financial institutions, telecommunications providers, and government CERTs. Table 1 in the Australian Government's Appendix B – Status of Horizon 1 Initiatives confirms that scam and fraud intelligence is not yet consistently integrated into national coordination models.

**Recommendation:**

- Establish a National Scam Disruption Centre with authority to coordinate scam intelligence sharing across all sectors.
- Mandate the sharing of operational TTPs and mule account data from banks, telecommunications companies, and government agencies into this centre.
- Ensure real-time connectivity with CERT Australia and the Australian Financial Crimes Exchange (AFCX) to accelerate coordinated disruption efforts.

## Q34. Are there risks that current frameworks are not addressing?

Yes. Current frameworks primarily focus on technical indicators such as domains and IP addresses, while underutilising human-sourced intelligence obtained from direct scammer engagement. This results in gaps in:

- Identifying mule account networks.
- Understanding shifts in scammer operational tactics.

- Detecting target lists before large-scale campaigns are launched.

**Recommendation:**

- Expand national frameworks to include active, controlled engagement with scammers as a legitimate and governed intelligence source.
- Establish operational and legal standards to ensure safe, compliant engagement with threat actors.

## Q35. How can we reduce regulatory burden for smaller entities while maintaining security outcomes?

Small businesses and not-for-profit organisations often lack the resources to maintain complex compliance programs. As identified in the *Charting New Horizons* Discussion Paper (p. 12), regulatory requirements need to be streamlined without lowering baseline protection standards.

**Recommendation:**

- Develop compliance starter kits containing standardised policy templates, awareness training modules, and low-cost monitoring tools.
- Use sector-specific intelligence hubs to deliver curated alerts and incident response playbooks to smaller entities.

## Q36. How can we ensure critical infrastructure sectors maintain resilience against emerging threats?

*Table 1 in the Australian Government's Appendix B – Status of Horizon 1 Initiatives* indicates that while critical infrastructure operators maintain strong cyber programs, scam and fraud disruption is not consistently embedded into resilience planning. This represents a risk, as compromise of supply chain vendors through scam-based tactics can have cascading operational impacts.

**Recommendation:**

- Incorporate scam and fraud disruption requirements into the Security of Critical Infrastructure (SOCI) Act obligations.
- Mandate critical infrastructure providers' participation in national scam intelligence exchange initiatives.

# Shield 4 – Skilled, Diverse Cyber Workforce

## Q39. How can we address current and emerging skills shortages in cyber security?

The *Charting New Horizons* Discussion Paper (p. 24) confirms that despite training investments in Horizon 1, Australia faces continuing shortages in specialist fields such as threat intelligence, incident response, and scam disruption. *Table 1 in the Australian Government's Appendix B – Status of Horizon 1 Initiatives* notes that practical, operational training environments remain limited, especially those preparing personnel for live adversary engagement and complex financial crime.

**Recommendation:**

- Expand training programs to include controlled operational intelligence collection, replicating real-world scammer engagement scenarios.
- Partner with industry to build simulation environments where trainees learn to map TTPs, identify mule accounts, and prepare intelligence packages suitable for law enforcement.
- Establish paid industry placements for graduates in operational intelligence roles, ensuring skills are applied in live environments.

## Q40. How can we strengthen diversity in the cyber workforce?

Appendix A (Table 1) shows progress in diversity initiatives but highlights underrepresentation of Culturally and Linguistically Diverse (CALD) communities in advanced technical roles. Horizon 2 should focus on creating targeted entry pathways and culturally inclusive training materials.

**Recommendation:**

- Develop multilingual, accessible training programs to broaden participation from CALD communities.
- Offer micro-certifications as entry points to cyber careers, allowing participants to demonstrate validated skills without committing to lengthy study programs.
- Partner with community organisations to promote cyber career pathways to underrepresented groups.

# Shield 5 – Resilient Region and Global Leadership

## Q41. How can Australia strengthen cyber security cooperation with partners in the Indo-Pacific?

The *Charting New Horizons* Discussion Paper (p. 27) calls for stronger cross-border partnerships to address threats that operate regionally but directly impact Australia. *Appendix B – Status of Horizon 1 Initiatives* confirms that while CERT-to-CERT collaboration has improved, scam and fraud disruption intelligence remains fragmented across jurisdictions.

**Recommendation:**

- Establish a Regional Scam Intelligence Partnership Framework supported by mutual legal assistance treaties (MLATs) that explicitly cover scam disruption data, including mule accounts and infrastructure indicators.
- Form joint operational disruption teams with Indo-Pacific partners to execute coordinated cross-border takedowns.
- Standardise technical indicator formats across the region to speed integration into blocking systems.

## Q42. How can Australia advance its global leadership in emerging cyber security capabilities?

The *Charting New Horizons* Discussion Paper (p. 28) identifies an opportunity for Australia to lead in advanced disruption capabilities, including active intelligence collection integrated into national defence strategies.

**Recommendation:**

- Formalise scam disruption as an exportable capability, supported by a certification framework for trusted providers.
- Lead development of a global scam disruption knowledge base, including TTP profiles, disruption playbooks, and behavioural analysis methodologies accessible to allied governments.

# Shield 6 – Governance, Policy, and Assurance

## Q42. Improving measurement and evaluation of cyber policy outcomes

The Government's proposed *Cyber Security Policy Evaluation Model* is intended to link interventions to outcomes, guiding monitoring and evaluation in Horizon 2. The *Charting New Horizons* framing emphasises the need for timely feedback loops and whole-of-economy data partnerships.

**Recommendation:**

- Define scam-disruption KPIs aligned to the Model's outcome measures (e.g., "cyber attack blocked", "targets supported to respond and recover"), including: mean time-to-takedown for malicious domains/accounts; velocity of mule account identification; blocked-clicks avoided; and victim recovery times.
- Establish secure, structured data contribution pathways so industry can provide de-identified operational telemetry to Government on a regular basis, consistent with the Model's call for longitudinal measurement.

## Q43. Policy alignment across jurisdictions

Horizon 2 emphasises harmonisation across Commonwealth, State, and Territory levels to ensure consistent delivery. The Charting New Horizons Discussion Paper notes the need for simplified, aligned obligations, and Appendix A records continuing work on a Single Reporting Portal to streamline compliance reporting.

**Recommendation:**

- Standardise scam incident definitions, evidence artefacts, and reporting fields across jurisdictions, aligning with the Single Reporting Portal's data model.
- Publish concise, plain-English inter-jurisdictional guidance packs for SMBs and NFPs, building on Horizon 1 governance toolkits in Appendix A.

## Q44. Improving assurance in cyber capabilities

Appendix A documents Horizon 1 progress in compliance monitoring for critical infrastructure, with review powers and crisis-response frameworks now in place. Horizon 2 can extend these assurance models to scam disruption and cyber-fraud capabilities.

**Recommendation:**

- Require funded scam-disruption initiatives to submit quarterly operational impact reports covering takedown metrics, mule account actions, and public-warning reach.
- Conduct independent assurance exercises simulating contemporary scam kill chains to validate end-to-end blocking, takedown, and victim-support functions.

## Conclusion

Cyberoo.AI fully supports the Australian Government's vision to make Australia the most cyber secure nation by 2030. The transition to Horizon 2 presents an opportunity to embed mature, operationally tested scam disruption capabilities into the broader national cyber ecosystem, alongside building workforce expertise and fostering international cooperation.

Through our experience in detecting and dismantling phishing, impersonation, and scam infrastructure, our capabilities in controlled intelligence collection, and our focus on victim protection and recovery, we are well positioned to contribute to the Strategy's six Shields in practical, measurable ways.

We stand ready to collaborate with government, industry, and regional partners on co-design processes, pilot programs, and operational task forces. Our aim is to ensure that scam disruption, intelligence sharing, and victim support remain central pillars of Australia's cyber defence, delivering tangible benefits for businesses, citizens, and the region.

# Appendix A – Cyberoo.AI Capabilities

*This appendix provides descriptions of all Cyberoo.AI capabilities referenced throughout the submission. Each product mentioned in the main document is explained here for clarity and context.*

## About Cyberoo.AI

Cyberoo.AI is an Australian cyber intelligence and disruption provider specialising in scam detection, threat disruption, and victim support. Our capabilities integrate advanced threat intelligence collection with rapid operational disruption to prevent harm at scale. These capabilities directly align with the Strategy's Horizon 2 objectives in threat detection, intelligence sharing, workforce development, and international cooperation.

## Cyberoo.AI Product Suite and Maturity Levels

**Operational**

1. **NothingPhishy** – Brand protection and phishing disruption. Finds impersonation websites, lookalike domains and fraudulent apps, and drives rapid takedown.

2. **Scams.Report** – Public scam verification and reporting. Lets anyone check suspicious links, messages or numbers and receive clear guidance.

3. **ScamIntel** – Controlled engagement with scammers to gather TTPs and identify mule accounts for kill chain disruption and law enforcement use.

4. **Privacore** – Privacy and identity protection platform embedding misuse prevention into digital service workflows.

**Pilot Phase**

5. **FAST$^2$** – Structured knowledge base of scam and fraud tactics, techniques and procedures (TTPs) for analysts and organisations.
6. **MyAiFCA** – Reimbursement evaluation tool to support consistent, fair, and timely assessment of scam-related loss claims.
7. **Frauducation** – Structured micro-certification program delivering short, actionable cyber awareness modules.
8. **MindGuard** – Psychological defence and recovery tool to support individuals after scam victimisation.