Conceptual Model: Two-Layer IDR

- National level (NOE – National Operations/Observation Environment)
- Organization level (enterprise, agency, critical infrastructure operator)

Summary: Two-Layer IDR Conceptual Model

National and Organization-Level Cyber Defence

The document outlines a conceptual model for incident detection and response (IDR) across two layers: the national level (NOE) and the organization level (enterprise, agency, or critical infrastructure operator).

At the national level, the system is operated by government cyber centers (like ACSC, National CERT, and Fusion Cells) and aggregates sanitized telemetry from participating organizations spanning critical infrastructure, telecommunications, government, and finance.

Key functions include:

- Cross-sector correlation to identify threats impacting multiple sectors (e.g., malware affecting several energy providers)
- Fusion of threat intelligence from ACSC advisories, Five Eyes partners, and commercial sources, distributed back to organizations
- Big-data analytics and AI for detecting nationwide patterns such as botnets, DDoS attacks, and advanced persistent threats (APTs)
- Coordinated response guidance, including takedown requests, law enforcement actions, infrastructure blocking, national DNS filtering, and emergency security uplifts
- Compliance monitoring for SOCI Act reporting and government security policy frameworks
- Deployment of network IDS/NDR sensors at international gateways

This model aims to strengthen national cyber resilience by enabling integrated visibility, intelligence sharing, and rapid, coordinated responses to threats across both national and organizational levels.

First Layer of Defence – National Level (NOE)

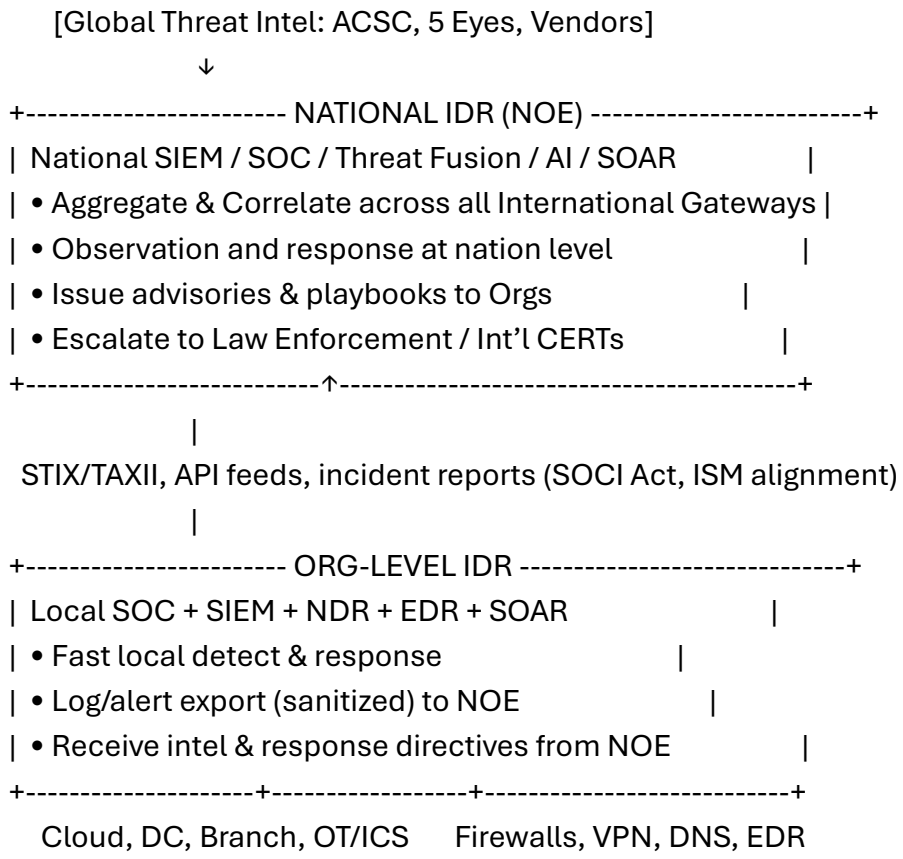
- Operated by ACSC / Gov Cyber Centre / National CERT / Fusion Cell.
- Aggregates sanitized telemetry from all participating orgs (critical infra, telcos, govt, finance).
- Provides:
  - Cross-sector correlation (e.g., same malware across multiple energy providers).
  - Threat intel fusion: ACSC advisories, Five Eyes, commercial TI → distributed back to orgs.
  - Big-data analytics & AI for nationwide patterns (botnets, DDoS, APT campaigns).
  - Coordinated response guidance (takedown requests, law enforcement actions, blocking C2 infra, national DNS filtering, emergency Essential Eight uplift).
  - Compliance monitoring for SOCI Act reporting, Gov Protective Security Policy Framework (PSPF).
  - Network IDS/NDR sensors at international gateways.
  - SIEM + SOAR for correlation and response.
  - Automated response at National control points (firewalls, EDR, DNS).

- Responsibility:
  - Protect the national digital estate.
  - Coordinate multi-org responses.
  - Interface with international CERTs, law enforcement, defence.

Second Layer of Defence – Organization Level

- Each org (government department, bank, utility, ISP, etc.) deploys its own IDR stack:
  - Network IDS/NDR sensors at gateways, branches, cloud, OT zones.
  - SIEM + SOAR for correlation and response.
  - Threat intel ingestion (global + national feeds).
  - Automated response at local control points (firewalls, EDR, DNS, email).
  - Incident logs standardized (e.g., STIX 2.1 / TAXII, CEF, JSON).
- Responsibility:
  - Fastest detection/response to local threats.
  - Protects business, maintains compliance (ISM, Essential Eight).
  - Escalates serious or novel incidents to National level.

Architecture Overview



Data & Control Flows

Downstream (NOE → Org):

- Enriched threat intel (curated, de-duplicated, prioritized).
- Detection signatures & YARA/Suricata rules.
- Coordinated response instructions (block infra, patch directives, emergency MFA mandate).
- Nationwide situational awareness dashboards.

Challenges to Two-Layer Approach

Technical Challenges

Data Volume & Scale

- National NOE aggregating logs/events from hundreds of orgs → petabytes of data.
- Need filtering (IOC-level, metadata, flow logs) instead of raw pcaps.

Standardisation

- Different orgs use different SIEMs (Splunk, Sentinel, Elastic), formats (CEF, JSON, syslog).
- Without STIX/TAXII or common schema, data fusion becomes unreliable.

Real-time correlation

- Detecting campaigns across multiple industries requires ultra-low-latency pipelines and powerful analytics (ML/NLP for patterns).

Encrypted Traffic Visibility

- TLS 1.3, DoH/DoQ, QUIC: limits packet inspection at both org and national level.

Organizational Challenges

Maturity Gaps

- Some orgs (e.g., big banks) already have mature SOCs; others (regional hospitals, small utilities) may have minimal detection.
- NOE has to support both without slowing down.

Response Authority

- Who has the final say in containment? The org's SOC, or national NOE?
- Legal/contractual authority must be clear.

Legal & Policy Challenges (AU context)

Privacy & Interception Laws

- Sharing raw network traffic may violate Telecommunications (Interception and Access) Act 1979.
- Must stick to metadata/indicators unless explicitly authorized.

Liability & Accountability

- If the NOE directs an org to block traffic and it disrupts business, who is liable?

Operational Challenges

False Positives at Scale

- Even a 1% FP rate becomes unmanageable when correlating thousands of org feeds.

Resource Constraints

- Smaller orgs may lack staff to integrate with NOE feeds or run a full IDR stack.

Incident Coordination

- Multi-org campaign requires synchronized response. If one org lags, adversaries pivot.

Redundancy & Availability

- NOE becomes a critical "single point of failure." Needs strong resilience (active-active SOCs, multi-region cloud).

Benefits of the Two-Layer Approach

1. National Cyber Resilience

- Early Warning System: National NOE sees cross-sector anomalies → can detect large-scale campaigns (APT, ransomware, DDoS) before they escalate.
    - National visibility (detect campaign-level attacks spanning sectors).
    - National Controls in case of cyber WAR.
    - Threat intel multiplier (each org's detection → feeds the nation → feeds all orgs).
- Rapid Containment: Coordinated response prevents "domino effect" (e.g., ransomware spreading across hospitals or power grids).
- Resilient Critical Infrastructure: Protects energy, water, transport, healthcare, comms — the backbone of sovereignty.

2. Strategic Threat Visibility

- Campaign-level Detection: Even if each org only sees fragments, NOE assembles the "big picture" of adversary TTPs (MITRE ATT&CK mapping).
- Nationwide Situational Awareness: Government can track which sectors are being targeted (e.g., energy sector hit by hostile APTs).
- Intelligence Fusion: Combines commercial TI, Five Eyes feeds, and org-level telemetry → gives a clearer national threat landscape.

3. Enhanced Deterrence

- Signal to Adversaries: Knowing Australia has a federated, fast-response IDR capability raises the cost for foreign actors.
- Legal & Diplomatic Action: National-level attribution enables sanctions, public exposure, or international countermeasures.

- Active Defense: Coordinated disruption of C2 infrastructure (sinkholes, takedowns) at scale.

4. Faster National Incident Response

- Coordinated Playbooks: NOE issues standard response steps → all affected orgs act in sync.
- Reduced Recovery Time: Unified approach lowers MTTR (Mean Time to Respond) across the whole country.
- Emergency Directives: In crisis (e.g., election interference, nation-state attack), ACSC can push rapid mitigation instructions nationwide.

5. Regulatory & Policy Advantages

- SOCI Act Compliance: Streamlined reporting → less chaos during major incidents.
- Evidence for Policy: Aggregated data informs risk assessments, critical infrastructure policy, defense posture.
- Public Trust: Citizens see gov actively protecting national digital borders.

6. Economic & Strategic Security

- Protects Economy: Prevents massive losses from coordinated cyber campaigns (financial sector, trade systems, supply chains).
- Safeguards Sovereignty: Maintains control over Australia's information space → reduces foreign manipulation, espionage, disinformation.
- Boosts Alliances: Enables richer intel sharing with Five Eyes & regional partners (e.g., ASEAN), strengthening Australia's geopolitical role.

7. Long-Term Benefits

- Shared Learning Loop: Each org's detection improves national defence; national intel improves each org's resilience → virtuous cycle.
- Uplifts Cyber Maturity: Smaller orgs benefit from intelligence and tooling they could never afford alone.
- National Security as Deterrence: Builds Australia's reputation as a "hard target", discouraging opportunistic and state-sponsored attacks.

Two-Layer IDR: Challenges vs. Benefits Matrix

Category	Challenges	National Security Benefits
Visibility & Data	- Massive data volumes (petabytes if all logs shared)- Different formats (CEF, JSON, syslog)- Encrypted traffic (TLS 1.3, QUIC) reduces inspection	- Nationwide situational awareness of threats- Early detection of campaigns across multiple sectors- Unified threat landscape for decision makers
Operational	- False positives scale up quickly- Incident coordination across orgs is complex- Smaller orgs lack mature SOC/IDR teams	- Faster national response (synchronized playbooks)- Reduced MTTR across all sectors- Uplifts less mature orgs with shared intel & directives
Legal & Policy	- Privacy and interception limits under TIAA 1979- Data sharing sensitivities (fear of exposure/liability)- Ambiguity over response authority	- SOCI Act compliance streamlined (single reporting channel)- Evidence base for policy making- Public trust in government-led defense
Trust & Governance	- Private orgs may hesitate to share incidents- Risk of over-centralisation (NOE dictating org actions)- Liability if NOE advice disrupts operations	- Builds public-private cyber defense partnership- Shared learning loop (org → NOE → org)- National-level attribution & deterrence capability
Technology & Scale	- High cost of SIEM/analytics at national scale- Integration with OT/ICS is fragile- Ensuring 24/7 resilience of NOE (avoid single point of failure)	- Central fusion centre can afford advanced analytics & AI- Detect APTs, disinformation ops, systemic risks- Strengthened resilience of critical infrastructure
Strategic & Geopolitical	- Coordination across industries/sectors with different priorities- International data sharing constrained by sovereignty laws	- Strengthens Five Eyes & ASEAN partnerships- Enables sanctions, diplomatic responses, cyber deterrence- Protects economy & sovereignty from hostile actors