

DEPLOYABLE LOW-ATTRIBUTION COMMUNICATIONS FOR CYBER INCIDENT RESPONSE TEAMS

Context

Defence Defensive Cyber Operations (DCO) teams may deploy at the request of an affected partner nation and under approved Australian Government authorities to assist with a significant cyber incident affecting critical government networks or national infrastructure. A task-organised team may include Cyber Threat Intelligence, Incident Response, Host and Network Analysis, and Terrain Management specialists, supported by secure reach-back to Australian command, intelligence and technical resources.

Within this mission, a small Cyber Intelligence cell may need to produce timely intelligence summaries, threat assessments, indicator reporting, incident updates and other operationally relevant intelligence. Its analysis may draw on open-source information, technical telemetry, intelligence holdings, host-nation reporting, and partner or coalition exchanges.

Existing approved communications systems can provide secure reach-back where available. However, online intelligence research and collection may fall outside the practical or policy constraints of those systems. Cyber Intelligence personnel therefore require a separate environment for authorised Open Source Intelligence (OSINT) and Publicly Available Information (PAI) research across open, deep and dark web sources.

Problem

Cyber threat actors may monitor their profiles, infrastructure, forums and other online environments for signs of investigation. Research activity that can be linked to Defence networks, Defence identities, Defence-procured devices or Australian infrastructure can expose the investigation, degrade collection, and create operational security risks.

The primary capability gap is therefore not secure voice communications. It is reliable, data-focused access to internet-based research environments with a stronger operational security posture and reduced attribution to Defence or Australia. Current access and policy restrictions can limit the effectiveness of available Defence-related solutions.

Desired Solution

The Pilot Project should investigate, design and demonstrate a small, practical low-attribution research environment suitable for use by a Cyber Intelligence cell when deployed or supporting DCO activities from Australia. The concept should enable authorised research while isolating potentially malicious content and reducing identifiable links to Defence and Australia.

The envisaged concept is:

- a cloud-hosted, containerised research image with a defined Standard Operating Environment;
- accessed through a non-Defence commercial network;
- using hardware procured outside Defence channels and not associated with a Defence identity;
- separated from Defence enterprise networks and Defence-related IP ranges;
- capable of accessing authorised open, deep and dark web sources, including social media, breach forums and relevant data repositories;
- designed to support operational security, target-evasion and malware-isolation requirements; and
- focused on dependable data throughput and connectivity. Voice capability is not required.

Research Question

How can an authorised Defence Cyber Intelligence cell conduct effective low-attribution OSINT and PAI research across open, deep and dark web sources using a

practical, isolated and field-usable data-access environment?

Scope of work

1. **Mission workflow.** Refine the supplied DCO scenario into one representative Cyber Intelligence research workflow, including deployed and non-deployed use.
2. **Attribution and operational security requirements.** Identify the principal technical and procedural attribution risks relevant to the scenario, including network, device, account and national attribution.
3. **Architecture.** Design a bounded reference architecture based on a cloud-hosted containerised image, defined SOE, non-Defence hardware and non-Defence commercial connectivity.
4. **Prototype or demonstrator.** Build and demonstrate the proposed research environment in a controlled setting. The activity is intended to establish feasibility, not to produce an accredited operational system.
5. **Evaluation.** Assess the concept against representative research tasks and agreed criteria for connectivity, data throughput, isolation, usability and attribution risk.
6. **Transition advice.** Identify the technical, policy, assurance and procurement work needed to mature a successful concept beyond the Pilot Project.

Expected Outputs

- A documented mission workflow and low-attribution threat model.
- A reference architecture and defined Standard Operating Environment.
- A controlled prototype or demonstrator.
- An evaluation report addressing connectivity, data throughput, usability, malware isolation and attribution risk.
- A practical roadmap for further development, assurance, policy review and transition.

Boundaries and exclusions

- The project is not expected to deliver a production-ready, accredited or fielded Defence capability.
- The project does not require voice communications.

- The project must not conduct unauthorised access, intrusive cyber activity, or operational collection against real targets.
- Testing should use controlled, simulated or otherwise authorised research tasks and environments.
- Named commercial systems are reference points only and do not prescribe a vendor or product solution.

Defence engagement and commercial context

Commercial products including PentenAmio AltoCrypt Stik, AltoCrypt Phone and AltoCrypt Hub, Northrop Grumman SCS-200, and dual-persona phone approaches may be considered as examples of secure mobility or communications design. They are illustrative only and are not mandatory components of the proposed solution.

Problem owner has advised that PentenAmio is a Defence supplier and that Defence can provide an introduction if engagement is sought. Any supplier participation, product access, licensing or technical support would need to be agreed separately and should not be assumed by applicants.

Intended users and broader relevance

The immediate user is a Defence Cyber Intelligence cell supporting Defensive Cyber Operations in deployed and non-deployed settings. If successful, elements of the concept may also inform other authorised Defence or Australian Government teams that require separated, low-attribution internet research environments. Any broader application would be subject to the relevant authorities, policies and security controls.