Working Groups Proposal – Overview

Active Cyber Defence Alliance

The purpose of this document is to obtain support for the objectives of the ACDA over the next three years and describe how these will be achieved.

The Active Cyber Defence Alliance Inc (ACDA) is a think-tank committed to lifting Australia's cyber resilience through greater awareness, adoption and capability in Active Cyber Defence. Our intent is to draw together leading cyber professionals from both supply and demand sides along with academic, legal and regulatory stakeholders who will jointly support active cyber defence initiatives and to influence policy and practices for the benefit of our community as well as sector, industry and organisational interests.

What we mean by "Active Cyber Defence"

Active Cyber Defence employs cyber intelligence, deception, active threat hunting and lawful countermeasures to expose, elicit and disrupt malicious actors before they impact data and operational capability. An active approach complements current static defences that incorporate security practices such as network hygiene, firewalls, malware filters, identity & access controls, good user behaviour etc. Active Defence can also provide personalised pre-emptive intelligence to inform effective static defences. Active Cyber Defence excludes Offensive cyber actions which are the sole domain of authorised government agencies, although it can include mechanisms to incorporate and coordinate responses of such agencies.

Membership

The Active Cyber Defence Alliance Inc is a not for profit association registered in NSW, Australia. Membership and participation in the Alliance is open to individuals and organisations of good standing who wish to prosecute the aims and intentions of the Alliance. Apply at contact@acda.group

Directors

Andrew Cox – President, John Powell – Treasurer, Duncan Unwin – Secretary,

Helaine Leggat, Robert Deakin, Ben Whitham, Phillip Moore

Public Submissions

The ACDA has contributed submissions on the issue of active defence since it’s inception. Some of these can be reviewed at https://acda.group/submissions/

Working Groups

The ACDA has convened two working groups:

1. **Frameworks** - A working group to lead increased adoption of Active Cyber Defence by developing the operational concepts and methods to adopt active defence and to address the How? and Why? to apply frameworks like MITRE ENGAGE. Using this work, each organisation can evaluate the applicability of Active Cyber Defence to their specific cyber risk tolerance and its contribution to their cyber and business / operational resilience.
2. **Lawful Countermeasures** - A working group to explore and clarify the application of law in the cyber realm, proposing safe guardrails for lawful practice and collaboration with law enforcement and national security.

Lawful Countermeasures Working Group

Active Cyber Defence Alliance

Objectives

The ACDA Lawful Countermeasures working group aims to: clarify the safe boundaries on what counter measures are lawful for civilian organisations to undertake in defending themselves from cyber-attack, what are the consequences of not acting, and to clarify interfaces between industry, law enforcement & national security.

> *"For thousands of years laws in many jurisdictions around the world have recognised the legal defence to the offence of damage and harm caused as a result of action taken in:*
>
> *(a) Self-Defence;*
>
> *(b) Intervening conduct or event;*
>
> *(c) Sudden or extraordinary emergency; and*
>
> *(d) Duress.*
>
> *This right has not yet specifically been recognised to apply in the cyber realm.*

This is only one example of the ambitious scope of work to be undertaken to clarify if and how existing Australian law applies to cyberspace.

Benefits to Cyber Defenders

- Enable organisations to lift their security posture, improve alert fidelity, and acquire customised targeted intelligence.
- Broaden the range of action available to cyber defenders
- Reduce risk by clarifying the benefits and limits of lawful active cyber defence
- Educate practitioners on the efficacy of active defence measures and how to adopt them

Benefits to the Community

- Extend the rule of law in the cyber realm
- Make Australian organisations less attractive because of their robust response
- Increase awareness and adoption of active defence, thus enhancing cyber resilience

Activities and Scope

The initial year's work is designed to demonstrate the feasibility and value of thorough application of law in the cyber realm in selected scenarios in, initially, two Australian jurisdictions and three critical industries. Subsequent work would extend this scope.

Operational Research

- Use MITRE ATT&CK and other MITRE frameworks to define attacker techniques and behaviours and inform the countermeasures in, initially, three critical industries
- Engage CIOs, CISOs and threat hunters to ensure the research is relevant
- Identify adversary behaviours and develop countermeasure scenarios that are industry specific

Legal Research

- Research the regulatory universe for initially three industries and two jurisdictions
- Clarify legal issues raised by the selected scenarios in the selected jurisdictions
- Make recommendations on safe guardrails for lawful active cyber countermeasures

Frameworks Working Group

Active Cyber Defence Alliance

Objectives

Current cyber security framework's underlying philosophy is one of a static/passive defence which has proven to be of limited effectiveness against constantly enhanced and changing capabilities of cyber threat actors. To address this gap and maintain relevance, the current frameworks would be more effective with linkage relationships incorporating both active and passive cyber defence capabilities. The emerging MITRE frameworks: ATT&CK, Engage and Caldera provide a basis for this change. The objective of the working group is to incorporate active defence techniques into the standards.

Benefits to Cyber Defenders

- Enable practitioners to move from passive -> active or NIST -> MITRE thus providing:
  - Earlier detection of malicious activity
  - Improved security posture and alert fidelity
  - Customized, targeted threat intelligence
  - Optimised security practitioner time spent on investigations etc….

Benefits to the Wider Community

- Enable cyber defenders to take and hold the initiative
- Bring active defence into mainstream cyber practice
- Enhance Australia's cyber resilience

Deliverables: Year 1

1. Issues whitepaper incorporating the findings of the Lawful Countermeasures working group
2. Map the MITRE cyber frameworks over NIST CSF frameworks to identify gaps
3. Submit recommendations to the current revision of NIST CSF
4. Submit recommendations to MITRE on the MITRE cyber frameworks

Activities

1. Convene the working group to execute the proposed scope.
2. Engage government and private sector cyber leaders for input and feedback during the progress of the work.
3. Propose recommendations to industry standards in support of active cyber defence.
4. Advocate for adoption of the recommendations.
5. Implement a communications campaign to legitimise active cyber defence.

Future Roadmap

- Extend active defence mapping and recommendations to further frameworks: ISO27000, ISM, PCI-DSS, CPG-236.ISM.
- Develop implementation guides and education for Active Cyber Defence.

Working Groups - Roadmap

Active Cyber Defence Alliance

Future Roadmap

- Extend the work to cover further countermeasure scenarios, jurisdictions, industries and standards
- Implement a communications campaign to legitimise the active-cyber-defence journey.

Budget

Forecast budget (combined in-cash & in-kind)

- First year budget – AU$ 1.5 Million
- Three year budget – AU$10-15 Million

How will the working group be resourced?

Financial contributions

- From ACDA members
- Working group participants
- Grants

In-kind contributions

- Expert staffing of working group tasks
- Intellectual property

Benefits of participation

Contributors to the Lawful Countermeasures group will benefit from:

- Early access to information
- Cross sectorial engagement with greater capacity to influence community outcomes
- Ability to influence priorities in selecting jurisdictions and industry sectors
- Sharing direct contact with other participants to cross pollinate experience
- Recognition of cash and in-kind contributions

How to respond

Please email us at contact@acda.group