Protecting Critical infrastructure and Systems of National Significance - Consultation Paper

A document developed by the Active Cyber Defence Alliance
Sumission version as at 16 September 2020

Consultation Paper – Protecting Critical infrastructure and Systems of National Significance

Who is the Active Cyber Defence Alliance (ACDA)?

The Active Cyber Defence Alliance (ACDA) is special interest group comprised of industry, academic and government stakeholders whose aim of is to foster awareness, adoption and capability in Active Cyber Defence practices across Australia with the goal of lifting Australia's cyber resilience.

Active Cyber Defence Alliance (ACDA) Cyber Strategy Group:

Andrew Cox
CEO – Avantgard Pty Ltd

Ben Whitham
Founder and Director – Penten Pty Ltd

Debbie Lutter
CEO - AUSCSEC

Duncan Unwin
Managing Director – Tobruk Security

Francis Cox
Compliance Consultant

Helaine Leggat
Attorney at Law – ICT Legal Consulting

John Powell
Principal Consultant for Cyber Security Qld – Telstra Purple

Patrick Fair
Lawyer – Patrick Fair Associates

Phillip Moore
Technical Manager – Avantgard Pty Ltd

Submission from the Active Cyber Defence Alliance (ACDA) to the Australian Government Department of Home Affairs on proposed reforms to **Protecting Critical Infrastructure and Systems of National Significance Consultation Paper (1246KB PDF)**, a key initiative of Australia's **Cyber Security Strategy 2020**.

What is Active Cyber Defence?

Active Cyber Defence employs cyber intelligence, deception, active threat hunting and lawful countermeasures to detect and respond to malicious activity sooner and potentially more effectively than is possible with passive defence. While the tools and techniques of Active Cyber Defence have been employed for decades, they are becoming increasingly popular due to their enablement by technological growth and challenges with traditional approaches.

Active cyber security measures provide a complementary strategy to traditional, passive cyber defence, which relies on conventional cyber security practices such as network hygiene, firewalls, identity and access management, virus filters, good user behaviour, etc. Passive cyber defence has proven difficult to deliver in practice, and by itself, unable to prevent the continued growth in data leakage and intrusions.

While Active Cyber Defence, by its name, prefers a more dynamic set of controls, it excludes offensive cyber actions, which are the sole domain of authorised government agencies, although it could include mechanisms to enable potential responses by such agencies

Summary of Recommendations

1. Holistic cyber resilience obligation

A set-and-forget approach to cyber defence, where inspection of the system is undertaken only during its introduction, is not sustainable. Each party in the supply chain of services provided and acquired, such as sub-contractors must be obliged to maintain their sub-systems in a continuous state of cyber resilience. This should include an obligation to augment and adopt controls to meet the requirements necessary to support other elements of the Critical Infrastructure Asset ("Asset(s)"). Assurance of the resilience of each Asset and its component modules should not be sub-contracted to providers of subsidiary modules but remain the responsibility of each asset owner and or operator.

2. Active Intelligence

The paradox of threat landscape is that one of the only aspects that remains consistent, is that it is continually evolving. Each owner and controller of a Critical Infrastructure asset should be expected to understand the unfolding threat environment as it relates to their specific asset. To accomplish this, effective programmes should include a continuous review of the tools, techniques and actors that are relevant to their systems and assets.

While general, sector-level intelligence feeds is helpful, the challenge is closing the gap on threats that are specific to Australian critical systems. Active Cyber Defence measures have been demonstrated to be effective in providing targeted intelligence and response that is tailored to the Australian ecosystem and local assets, in a way that is complementary to global advice. These activities can easily be undertaken by the asset owner, and/or coordinated at a national level.

3. Situational Awareness

Each owner or controller of a Critical Infrastructure Asset should use the information gleaned from Active Intelligence to maintain a broader cyber situational awareness. Essentially, to ensure that at all times they have an overview of what going on in the immediate proximity and the wider context of the systems they own or control. cyber situational awareness is "knowing what is going on around you".

When applied to Critical Infrastructure, this translates to being able to determine external threat environment as it develops from day to day at both a sectorial and individual asset level as it relates to the health of the asset systems as a whole, in real-time, right down to each of the endpoints.

This task of situational awareness is complicated by the heterogeneous nature of critical infrastructure in general and the significant investments made by each of the parties within the supply chain, often without the context of the interactions between other providers and acquirers of services within the connected systems and networks.

a) Sectorial SOCs

To ensure situational awareness, Security Operations Centres (SOCs) should be established for or, as appropriate, with responsibility allocated for each industry- specific sector. These could take the form of an expanded and better resourced Trusted Information Sharing Network associated directly with the Australian Cyber Security Centre.

This will provide an invaluable uplift to the sector's cyber resilience, especially in securing the Assets of smaller operators who lack resources. It should be noted that countries such as Israel and Estonia that have suffered sustained attacks on their critical infrastructure have already adopted this approach. It does not make sense for Australia to take an evolutionary approach when these best practices are already understood and successful. We can thus leapfrog the learning process to quickly arrive at a high level of resilience in our critical infrastructure.

b) Sectorial (industry specific) threat intelligence sharing

Regardless of whether the responsible regulator establishes sectorial SOCs, sectorial threat intelligence sharing will be fundamental to effective incident response and broader cyber resilience.

We recommend the regulator mandate owners and operators of Critical infrastructure participate in sectorial threat intelligence sharing. Each sector should be required to develop and support automated Intelligence in real-time (or at least near real time) to enable a timely incident

response in the event of sector wide attacks.

The ACDA is committed to developing a data sharing taxonomy that will enable automatic playbook-based response by participants to developing and evolving threats and attacks. The ACDA taxonomy will be developed as creative commons artefacts within the STIX/TAXI framework to build on the Mitre Att@ck framework to enable wide, low friction adoption by Critical Infrastructure operators. These playbooks will incorporate scenarios for lawful response.

4. Continuous Improvement

Threat actors are continuously evolving and so to must defenders. Any national program should include annual Active Cyber Defence and cyber crisis response 'exercises' to test and measure response against the latest threat scenarios. These exercises should entail real intelligence gathering, red teaming, defending teams feeding into crisis response exercises that are not pre-set hypothetical desktop exercises but live interactions. Participation should be mandatory for members of management and staff and be sector specific.

The findings from such exercises would be shared in a prescribed format and without unnecessary security configuration detail, with the responsible regulator, and set minimum standards for continuous enhancement of cyber resilience.

The ACDA has developed a model Cyber Crisis Response and active intelligence gathering methodology for critical infrastructure operators. The exercises cover the spectrum stakeholder engagement, intelligence gathering, cyber deception, active threat hunting and lawful countermeasures in a synthetic live-fire environment. The process is embodied in creative commons artefacts and so is available to the applicable regulator, and the wider critical infrastructure community.

We recommend the regulator mandate similar annual exercises for Critical Infrastructure to operators.

Factual Basis for Recommendations

Structural challenges in securing critical infrastructure

1. Long lead times

A significant challenge with critical infrastructure projects is that they are frequently awarded through tender processes which take years and have multi-year terms. Using Rail or Energy as an example, the control systems (the OT) side, have a 30-year design life with little/no built-in lifecycle planning that sees planned uplift during its operating life. During these extended timeframes the cyber threat landscape evolves significantly and dynamically, with the result that the cyber security standards and controls, proposed during the tender process, become obsolete, sometimes even before the tender is awarded and the project is delivered.

2. Long lifecycles

Critical Infrastructure provided through the private sector will have different financial objectives than those of government-owned Infrastructure. Long asset lifecycles require businesses to achieve a return on investment over the assets lifetime, however, the changing cyber threat landscape will require ongoing but unclear cyber investments to ensure that the Operational Technology (OT) control systems are maintained, secured and protected against the rapidly changing cyber threat landscape.

Ongoing maintenance requires budgeting for cyber Operational Expenses (OpEx) that is extremely difficult to quantify and plan over these long asset lifecycles. Business are unprepared to consider new and emerging cyber risks, that introduce unplanned budgetary OpEx expenses over the forecast shareholder returns.

Further research could indicate an appropriate guideline level of additional expenditure (e.g. a percentage of Capex) introduced into the procurement processes, as part of the asset acquisition process, to be specifically set aside for cyber uplifts on an annual basis.

3. Systemic impediments to cyber resilience

We take cyber resilience to mean the ability to continue to remain in safe functional operation during an attack and the ability to recover quickly if function is impaired. So cyber resilience includes the timely recovery of assets but just as important is having sufficient visibility of adversary activity, footholds, resources, TTPs and capabilities to enable an informed view of whether it is safe to continue to operate during an-ongoing engagement. It is in the second area that intelligence, deception, active threat hunting and continuous systems monitoring capabilities are critical. Even if it is possible to restore systems quickly a prudent operator will not keep operating a train, electricity or water system before safety and security is assured.

Typically, each party in the supply chain of service provision and acquisition has responsibility for securing their own Assets, ICT systems, confidentiality, Intellectual Property, and data privacy. Each party, as part of the connected Critical Infrastructure eco-system also has responsibility for ‘passing the baton’ of resilience to the next participant in the supply chain. No party, however, has the overall context of the cyber threats and impacts across the Critical infrastructure system as a whole.

As an example, Critical Infrastructure rail transportation systems provide a "system of systems" with integration between the different proprietary systems of every party in the supply chain. Typically, Australian rail operators accept agreement between specialist providers for turnkey design, construct, operate and maintain services for substantial and specialised services of the rail system requirements such as Train Management System, Trackside systems and components, Rolling Stock etc. Each of these contract "modules" (Agreements/Statements of Work) will contain requirements for cyber security, with design, implementation and operation of the system resting with the contractor. The rail operator must deploy an integration layer to consolidate a single view for both operations and security. Even when using standards-based integration patterns there are several problems with sustaining cyber resilience in this structure.

The assumption is that, since each element in the Critical Infrastructure of the parties comprising the whole Critical Infrastructure System is secured, the 'system of systems' as a whole, is secure. The assumption, however, is not correct. Effective cyber defence requires a holistic view of the entire Critical Infrastructure eco-system, and the passing of the baton along the supply chain, becomes the weakest link.

OT system components may depart from secure practice in other networks by not encrypting messaging between components or employing other basic firewalling or continuous monitoring & packet inspection. When an entry point is found in the system, malicious code or movement around the network may be undetected and the system could remain compromised and accessible to an adversary, using APT stealth techniques with command and control.

Once requirements are legally agreed, a Critical Infrastructure operator has little or no ability to amend the terms of the agreement dictating further specific system security or other requirements. Furthermore, inconsistencies in approach between participants in the Critical Infrastructure may introduce unforeseen security vulnerabilities in the systems. Also, concessions made to smaller and lower resourced participants in the supply chain may introduce the risk of the weakest point of entry.

The net result is that there is a significant disparity between the term of the agreement, being the number of years over which the service is to be provided on specific agreed terms and conditions between the contracting, and the constantly evolving cyber threat landscape. Changing the underlying security requirements as part of an agreement and implementing new security capabilities is typically a multi-year process, and one that cannot be unilaterally imposed meaning, that this kind of foreseeability needs to be catered for from the outset and on an ongoing basis.

4. Unsuitability of IT sourced cyber defence approaches

Controls should be selected based on their effectiveness to reduce risk, however, this is not the case. Controls are selected for purposes of compliance with external standards. The history of this is that the risk assessment and management practices inside organisations have been immature. The ACDA suggests that Active Defence can lead to a better knowledge of actual threats as they emerge, and lead to a risk-driven control selection culture. In critical systems / operational technology, there is a reluctance to maintain the effectiveness of controls, where doing so (e.g. patching) could compromise safety.

Active Defence provides a strategy where OT systems are not modified, and early detection of threat, allows more informed decision-making about when to prioritise cyber defence controls over operational continuity (i.e. when do we shut down the power plant to patch the SCADA system?).

This condition manifests in the adherence to predefined standards and policies in security architecture and engineering practices and a reactive approach to incident response.

Key Objectives in securing critical infrastructure

Consistent with the 'Objectives' described in the consultation paper on protecting Critical Infrastructure, the ACDA supports:

- Co-developing a scenario-based 'playbook' setting out response arrangements
- Building a near real-time threat picture
- Building the cyber resilience of Systems of National Significance

The ACDA agrees with these objectives and seeks to further expand on how this can be achieved using Active Cyber approaches.

It is our view that the proposed Critical Infrastructure Positive Security Obligation should call out Active Cyber Defence as a critical area for focus and resourcing in Australian cyber defence and resilience.

Today's conventional security strategies mainly focus on passive cyber security approaches using tools, techniques and procedures that seek to prevent and protect against attacks. Although these controls are necessary, they are insufficient against sophisticated adversaries and the demands of rapid response timeframes.

The ACDA believes Critical Infrastructure providers should shift their focus beyond the current passive approach to include Active Cyber defence, detection, response and recovery. This actionable threat intelligence, integrated with existing conventional passive cyber approaches is the best means to quickly detect, respond and recover from a malicious intrusion on an ongoing, relevant and legal basis.

Active Critical Threat Intelligence

As the threat landscape evolves and expands, Critical Infrastructure service providers are facing two factors driving the evolving trends:

1. They deal with highly sensitive control data as well as unpatched, unprotected and unsupported operating systems as ICT systems age. This makes them a target for malicious advanced persistent threat state-sponsored adversaries.
2. The attack surface is increasing because as industries are rapidly moving to Radio Frequency (RF) wireless connected Internet of Things devices for telemetry and automation using the control systems and system of systems, which are currently not adequately secured.

This means, that in order for Critical Infrastructure service providers to protect their digital landscape against threats, they need to maintain their visibility across the whole eco-system as well as to re-evaluate and re-prioritise threat intelligence and provide assurance that threat actors haven't covertly deployed malicious tools within the infrastructure.

Active situational awareness

Deception networks and tools should be leveraged and combined with effective cyber training exercises to accelerate detection using real-world scenarios and well-practiced cyber response drills that are conducted regularly using red teaming playbooks.

With Active Cyber Defence, cyber security teams gain the ability and agility to prioritise vulnerability mitigation by addressing observed vulnerabilities in relation to currently active exploits and/or can provide an assurance that threat actors are not being observed operating within the infrastructure.

Using deception networks and tools will also provide the capability to fully integrate with already-in-place threat feeds and SIEM systems as well as other security tools to maximise existing resources – staff and technology, to mature and build cyber awareness. This provides the prioritisation, contextual awareness and real-time insight necessary to reach achieve the objectives of the proposed reforms to Protecting Critical Infrastructure and Systems of National Significance.

Active Strategies

An Active Cyber Defence strategy will reinforce conventional passive cyber security by leveraging Active Cyber Defence, using deception tools and threat intelligence approaches, in order to:

- Focus beyond conventional protection to include active detection using deception tools to provide intelligence for leading edge response.
- Achieve situational awareness of the entire infrastructure (the on-premises, cloud, IoT, mobile and legacy systems eco-system) by integrating active defence and threat intelligence in the context of actively observing threats and leveraging intelligence for rapid response.
- Proactively hunting for threats and malicious activity which may cause significant damage and loss to critical infrastructure, government, business and society.
- Substantially reduce alert fatigue, by providing context and prioritisation to the observed threat intelligence and enhance the ability to share threat intelligence between all parties in the Critical Infrastructure eco-system.
- Build playbooks for cyber response exercises and regular drills, including to actively pursue adversary attribution and lawful response
- Consolidate external and internal threat intelligence such as Open-source intelligence (OSINT) feeds, conventional passive cyber security information with prioritised Active threat detection into event management (SIEM), and vulnerability data models.
- Accelerate analysis and response to attacks through collaborative threat playbooks to foster a continuous improvement approach, build contextual awareness of the cyber threat landscape, facilitate multi-agency interaction and dramatically improves responses. All of which will raise the bar of Australia's Cyber Security resilience.

Conclusion - Active Cyber Defence Response and Next Steps

What is Required from Government in Protecting Critical Infrastructure and Systems of National Significance

Critical Infrastructure and Systems of National Significance that are owned and controlled by private sector entities operate today on the front lines of cyber conflict, targeted by a variety of hostile actors that seek to steal and misappropriate their intellectual property, degrade their infrastructure and disrupt their business activities. Despite this reality, the options available within the private sector for responding to cyber threats are outdated and constrained. The status quo is reactive in nature land advantages the attacker.

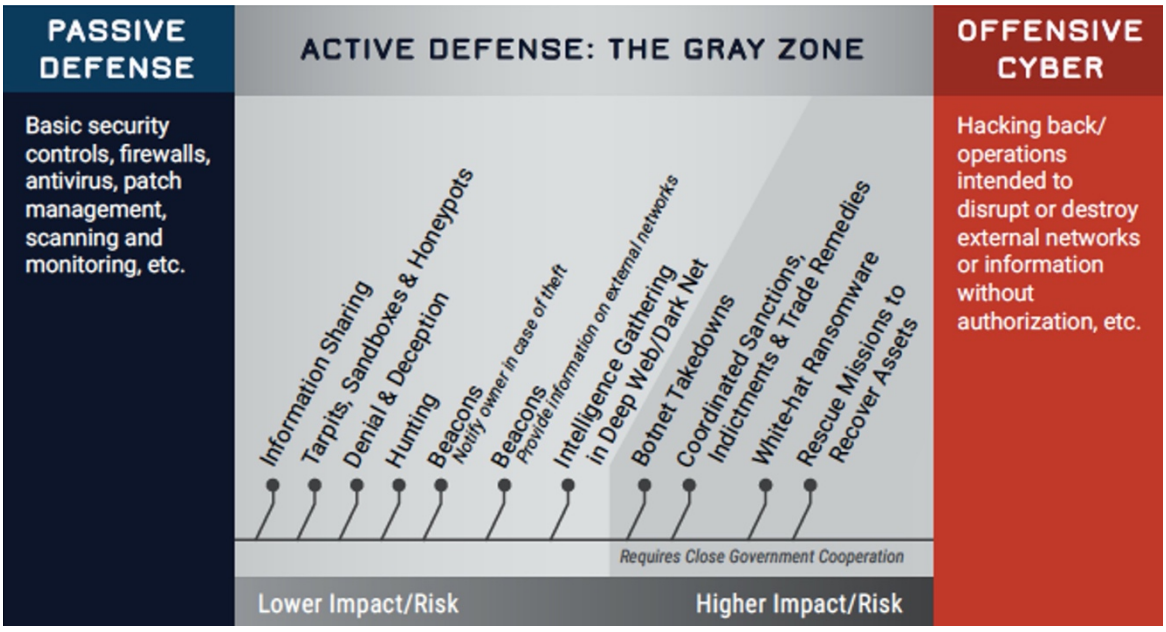
Clarity and the Grey Zone

Active Cyber Defence is not just one thing. It is a range of possible things – behaviours, tools, techniques, and other responses.

The range of Active Cyber Defence is low risk where responses border on passive defence on the left in the diagram below. The risks associated with Active Cyber Defence responses increase towards the right side of the diagram below. Active cyber Defence for the private sector always stops short of offence.

Active Cyber Defence is about addressing the opaqueness of the responses listed in the grey zone in the diagram below. One involves moving from passive to active defence.

The economy is the basis of national security. The economy is underpinned by the digital environment which is largely under the ownership and control of the private sector.



Action Required

The primary objective of this submission is to commence meaningful discussion with Government in relation to the issues raised in this submission, including, but not limited to the steps below:

1	Legislature	– Legislate to allow certain ACD responses to be declared legal or to be legalised. – Appoint or license responsible private sector organisations to act as cyber defence 'affiliates'.
2	Executive	– Formally announce that no prosecutions will arise from certain ACD responses, pending legislative change. – Authorise, advise and provide guidance on ACD. – Coordinate and rationalise the ACD responsibilities to appropriate government agencies.
3	Judiciary	– Interpret and clarify which ACD responses are or should be lawful and will not be prosecuted (an issue of interpretation of existing law). – Provide declaratory relief and advisory opinions on matters of application and interpretation of law to cyberspace. The issue is one needs a contested matter.
4	Department of Foreign Affairs	– Commence discussions with active defence friendly countries. – Lobby the United Nations Commission on International Trade Law for a new model law to adopt active defence to underpin acceptable behaviour in cyberspace and rules-based global order.
5	Each Critical Infrastructure Provider/Acquirer of services in the CI supply chain ("operator")	– Internal engagement and decision making. – Government engagement – through this and similar submission.

Contact Details
Attention: Andrew Cox
Active Cyber Defence Alliance
[redacted]