Active Cyber Defence Alliance

Submission on Security Legislation Amendment Bill 2020

Parliamentary Joint Committee for Intelligence and Security

A document developed by the Active Cyber Defence Alliance
Final version as of 12 February 2021

ACDA Submission to PJCIS – Submission on Security Legislation Amendment Bill 2020

Disclaimer

The statements in this submission are the opinions of the authors as members of the Active Cyber Defence Alliance and do not necessarily reflect the views of their individual employers

Executive Summary

The Active Cyber Defence Alliance (**ACDA**) is providing this submission to the Parliamentary Joint Committee for Intelligence and Security to address the Security Legislation Amendment Bill 2020 (**Bill**) and also to address issues of cyber security for Australia's critical infrastructure.

We have developed a structured commentary of cyber security issues rather than providing direct commentary to each part and section of the Bill because we considered there to be substantial gaps in the text of the Bill to achieve the robust cyber security outcome suitable for critical infrastructure assets. Recommendations have been included at the end of each section with an index of recommendations included after the table of contents.

The promise of adding cyber security specific sections and sub-sections to legislation has been welcomed by many in the information and cyber security sector. Recognition of the necessity to secure environments from adversaries and build robust and mature cyber security methods and mechanisms into critical infrastructure, with the hope that eventually we will see cyber security requirements for the broader business community also added to legislation for the protection of all business and personal sensitive information. But the Bill provides no robustness of cyber security, no mention of cyber maturity, no requirement for a system to manage information security but a limited list of specific controls.

In summary, the changes proposed in the Bill to amend the Security of Critical Infrastructure Act 2018 do not go nearly far enough in developing cyber resiliency of critical infrastructure operation. This may be best articulated by paraphrasing Sean Connery from one of his movie roles and saying that the cyber security controls mandated by this bill to protect against a cyber-attack are like bringing a knife to a gunfight.

Table of Contents

Recommendations

Legislative Recommendations

Executive Recommendations

Judicial Recommendations

1 Who is the Active Cyber Defence Alliance?

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

1.1 Active Cyber Defence Alliance - Cyber Strategy Group

Andrew Cox CEO Avantgard Pty Ltd	Ben Whitham CEO Penten Pty Ltd
Debbie Lutter CEO AUSCSEC Pty Ltd	Duncan Unwin Managing Director Tobruk Security
Francis Cox Compliance Consultant	Helaine Leggat Attorney at Law ICT Legal Consulting
John Powell Principal Security Consultant Telstra Purple	Rob Deakin Director Cyber Security ACCC
Phillip Moore Technical Manager Avantgard Pty Ltd	

1.2 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 (Passive cyber defence relies on conventional cyber security practices such as network hygiene, firewalls, identity and access management, virus filters, good user behaviour etc.)
- leverages the foundation provided by passive cyber defence to provide greater visibility of the contextualised threat landscape
- seeks to grasp the initiative with attendant negotiating power and assurance by leveraging intelligence and indicators of compromise to identify an attack, respond to, or against the capability to give the defender the ability to adapt quickly in a proactive way
- excludes offensive cyber actions which are the sole domain of authorised government agencies, although it could include mechanisms to coordinate potential responses by such agencies

2 Cyber Security Threats

Evolving and expanding threat landscape

The interconnectedness of the modern world means that our critical infrastructure assets face a threat landscape that is evolving and expanding at a rate that is both hard to fathom and hard to defend against. The responsibility of securing any information environment gets more difficult as the threat landscape grows but critical infrastructure service providers are facing additional unique factors.

Soft targets

Unpatched and unsecured

They deal with highly sensitive control data destined for devices that convert control command data into kinetic activity. The bytes of data may have no direct impact on humans, but the resulting kinetic activity from a hacked control command has the potential for fatal consequences so safety is a primary concern. The systems delivering and receiving these control commands are often unpatched and unprotected due to long lead times, long lifecycle and obstacles to cyber resilience (this is explained further in Section 9). They also become unsupported as they age. This combination of sensitive control data on systems that are unpatched and unsecured makes them a target for malicious adversaries including criminal and state-sponsored advanced persistent threat groups.

Increased attack surface

Wireless / RF

The attack surface is increasing as many sectors move to radio frequency or wireless connectivity to provide underlying communications layers for control and monitoring systems, which are currently not adequately secured as described in the point above. This can improve flexibility and effectiveness but removes a layer of physical security and provides the opportunity for an attack to originate from the beyond the immediate proximity of the critical infrastructure effectively making critical infrastructure an easier opportunity for threat actors of every motivation.

Convergence and commoditisation

Connecting IT & OT

The connection of information technology and operational technology networks (e.g., Corporate office to manufacturing plant) can have operational and security benefits. The architectural model for connecting these two disparate networks will include blocking all communication between the networks by default with explicit exemptions to allow controlled access.

Converged through lack of security

It is unfortunate that this architectural model is often not implemented properly or not implemented at all and the security posture of the operational technology environment is compromised rather than enhanced because the operation technology network is now converged with the information technology network and easier to access from outside the organisation.

Vulnerabilities and weaknesses in commodity software

The widespread use of commoditised software on information technology networks provides multiple footholds through software vulnerabilities and configuration weaknesses for a malicious actor to attack the operational technology devices that are potentially unpatched and unsecured. The mere existence of an operational executive dashboard sharing updates of the success or failure of patching cycles overnight can provide leads for adversaries to start to plan for opportunities to cause long lasting harm and destruction.

3 Threat Intelligence

Capability
Intention
Activities

To contextualise the intelligence that has been called out in the Bill, we have referenced the Intelligence Services Act 2001 where sections 6(1)(a), 6B(1)(a) and 7(a) state "to obtain … intelligence about the capability, intention and activities of people or organisations …". While these sections of the Intelligence Services Act deal with intelligence services obtaining intelligence about people and organisation from outside Australia (i.e., the subject of the statements), we are focused on the object of the statements, and that is the intelligence about the capability, intention and activities of the adversaries. Being specific about the intelligence to be gathered and shared allows us to be specific in our comments about this intelligence.

Analyst must be law-abiding

For a security analyst to gather intelligence about an adversary, the analyst must be able to identify where and how the adversary is acting within the systems that the analyst is authorised to access. There are two key issues here. One is that the analyst must know that the adversary is active, and secondly, the analyst must abide by the law and only collect intelligence from systems that they are authorised to access and for the purpose for which it was intended. Currently, this leaves the analyst at a disadvantage and the amount of intelligence that can be obtained will be limited to attacks in progress – often detected weeks or months after the attacker's initial infiltration.

Why does detection take so long?

This is largely due to inadequate resources afforded to identifying the high value alert amid a sea of thousands of alerts per hour, both true positive and false positive. As well as collecting the right alert to collect, the analyst must also understand what is the known verses the unknown in the intelligence gathering process.

This scenario, faced by most security analysts, is the quintessential needle in a haystack.

When considering the time that it takes to identify a breach it is important to note that every minute counts. As soon as the breach occurs the clock is ticking and every minute between the breach and the expulsion, the adversary is moving throughout the environment. Discovering and compromising.

Where is the adversary acting?
Authorised access only

Gaps in the cyber resilience of the critical infrastructure eco-system are inevitably created by analysts being limited in movement through the cyber-sphere (i.e., following the legal and ethical limitations of authorised access). The sharing of intelligence will help to fill in some of these gaps, but it will not assist in an analyst knowing where the adversary is currently active within their environment

Immediately expel adversaries from production

If an adversary is known to be active on a production system within a critical infrastructure asset, expulsion of the adversary and restoration of the system will be the top priority. The detected indicators of compromise can be shared and the intelligence about the

immediate activities of the adversary on the system can be shared but the intelligence regarding the capability and intention of the adversary will only be circumstantial because they no longer have access to the system. The only information about such a breach that has been properly answered is "what" happened and the need to restore critical service delivery often conflicts with ongoing collection of intelligence for detailed analysis and long-term remediation.

The use of active cyber defence technology, including traps and synthetic systems designed to gather this needed intelligence, will provide several benefits in the coordinated defence of critical infrastructure.

Delayed expulsion

Adversary can stay in a synthetic environment

Active cyber defence consists of synthetic systems and traps configured to appear genuine, interesting and easier to compromise than any 'real' systems. The adversary can be detected more easily, and expulsion delayed while their attack techniques are monitored and analysed within a controlled environment where the security analyst is authorised to act without impact on critical service delivery. This gives confidence to management and allows for containment of the incident at no loss to business as usual.

Thorough intelligence

Why and How

The ability to monitor the adversary provides the opportunity to collect intelligence about capability and intention. Understanding the 'who', helps answer the questions of 'why' and 'how', rather than just the question of 'what'.

Seed for disruption

Surveillance Devices Act

The additional value of this intelligence, collected using active cyber defence, will be realised with the proposed amendments to the Surveillance Devices Act 2004 as defined in the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020.

Monitor the adversary
Data disruption warrant

As soon as an adversary scans or attempts to access a synthetic system or a trap the analyst responsible for that system will be notified. The analyst can monitor the activity of the adversary, measure their capability and determine their intent to understand what they are doing, why they are doing it and how they are doing it. Assuming the successful passage of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020, and specifically the addition of Division 5 – Data Disruption Warrants to the Surveillance

Devices Act 2004, this information can be passed on to the appropriate law enforcement agency who can then apply for a data disruption warrant to act against the adversary.

4 Situational Awareness and Visibility

Understand the pending threats

Cyber Situational Awareness is about knowing what is going on around you in the cyber-sphere. When applied to critical infrastructure, this translates to being able to monitor the threat environment as it develops from day to day at both a sectorial and individual asset level and as it relates to the health of asset systems as a whole, in real-time (or near real-time), right down to each of the endpoints. It also includes having visibility of all digital devices within the asset environment.

Interconnection between assets

This task of maintaining cyber 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.

Sectorial Security Operations Centres

Learn from other countries

To ensure situational awareness, Security Operations Centres (SOCs) should be established for each critical infrastructure sector. This will provide an invaluable uplift to the sector's cyber resilience through real time threat sharing of attacks against the sector such as those noted by ASD against the health and aged care sector in 2020. This is especially effective in supporting protection of the assets of smaller operators who lack cyber 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 leapfrog the learning process to quickly improve the resilience in our critical infrastructure.

Active Situational Awareness

Deception AND response drills

Combining deception networks and tools with well-practiced cyber response drills that are conducted regularly using red teaming approaches will accelerate detection in real-world scenarios. Such cyber response drills can be conducted against the active cyber defence infrastructure removing a major risk to service delivery from conducting drills against the critical infrastructure itself.

Prioritise remediation

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 observed operating within the production infrastructure.

Deception AND security tools
Context and real-time insight

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

How important is the human capital?

The technology is only half the story. The security analysts that are required to operate Security Operations Centres are highly skilled resources, who require substantial training and experience to provide value directly and make the most of the technology. The training and development of security analysts is a significant undertaking.

Staff need good technology and technology needs good staff.

Legislative Recommendation 1: Establish sector specific Security Operations Centres

Include a requirement for each sector regulator to provide security operation centre services to coordinate threat intelligence visibility across the sector and support for smaller operators.

5 Threat Intelligence Sharing

If the critical infrastructure community is to collaborate in securing the critical infrastructure assets of this country, then the intelligence sharing mandated in the Bill is vital for a coordinated response.

Vital for coordinated responses

Sectorial Threat Intelligence Sharing

Sectorial threat intelligence sharing will be fundamental to effective incident response and broader cyber resilience. The sharing of threat intelligence within a sector should leverage the threat intelligence sharing across the entire critical infrastructure community, but also have a focus on highlighting sector specific threats and alerting other owners and operators in the sector of threat intelligence as it comes to light.

Threat sharing PLUS sectorial threat sharing

However, there is a pressing need for a framework to define how this intelligence is to be shared. This is an area where the intelligence community can both lead and provide a service to the critical infrastructure community with the possibility of intelligence sharing to the broader business community.

Intelligence sharing framework

Threat intelligence sharing across all critical infrastructure sectors should be automated and operate in real-time (or at least near real time) to enable a timely incident response in the event of attacks across multiple critical infrastructure assets.

Automated intelligence sharing
Real-time intelligence sharing

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 leveraging existing threat and threat sharing frameworks to enable wide, low friction adoption by critical infrastructure operators. These playbooks will incorporate scenarios for lawful response.

Resources available under creative commons

Legislative Recommendation 2: Threat intelligence sharing

Include a requirement for critical infrastructure asset owners/operators to share near-real-time threat intelligence sharing across the critical infrastructure eco-system. If there is an inability to implement threat sharing across the whole critical infrastructure community then threat sharing across each critical infrastructure sector should be included as a minimum requirement.

6 Standards, Frameworks and Controls

Risk driven approach

The use of risk management to drive the selection of appropriate security controls has long been supported by the information security industry and the inclusion of a risk management program for critical infrastructure assets is welcome in this bill. It is unfortunate that this legislation does not go further in defining an approach for securing these assets.

Drive standards adoption

An opportunity currently exists for legislation to drive the adoption of standards across the critical infrastructure landscape and unify the efforts to defend against the growing and changing threat landscape.

Skills shortage
Structure/guidance all orgs

The shortage of cyber security capability both in Australia and across the world means that we cannot simply hire more cyber security analysts to implement more controls to defend the critical infrastructure. Instead, we need to take a smarter approach to securing our country and this includes centralising the development of frameworks and guidelines that all organisations can use to help build and mature their security posture. Ideally, the Security of Critical Infrastructure Act 2018 would provide the structure and guidance for information and cyber security that all Australian organisations can use, but the critical infrastructure assets would be held to account including all of the service and product suppliers in the supply chain eco-system of the asset.

US Executive Order
NIST
Cyber Security Framework

A similar situation existed in the United States of America where Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," was issued on February 12, 2013, which established that "[i]t is the Policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties." (Framework for Improving Critical Infrastructure Cybersecurity, 2021). This framework is often referred to as the NIST Cyber Security Framework or NIST CSF because it was developed by the National Institute for Science and Technology (NIST) in response to the Executive Order. It is a framework for all critical infrastructure assets that is also used by non-critical infrastructure entities because it has been recognised as comprehensive, robust and efficient.

ISO/IEC 27001

While there will be nuances in the security requirements for each of the 11 sectors defined in the bill, all organisations share many of the controls recommended in cyber security standards. This is demonstrated by the adoption of the NIST Cybersecurity Framework and

the international standard for information security management systems (ISO/IEC 27001) by organisations across many sectors. In fact, both the NIST Cybersecurity Framework and ISO/IEC 27001 call for the use of a risk management system to drive the selection of the controls that will reduce the information risks of the organisation. The nuances in the security requirements that differentiate each sector listed in the bill can be accommodated within one framework because of the optionality of including controls based on risk. Further reason to create a single framework rather than adding similar workload to multiple sector regulators.

Disparate frameworks

If the intent of the bill is to have each sector build their own information security framework, then the result will be disparate frameworks as each sector regulator (or similar) is left to set their own direction and agenda when collaboratively they will be responsible for the protection of critical infrastructure of this country. The disparity between guides or frameworks as one critical infrastructure asset supplies to or consumes from another critical infrastructure asset will likely provide the weak points that threat actors will exploit.

3 controls in this bill

This bill articulates the requirement for three information security controls that have also been defined in information security standards or frameworks, and all three are from the Enhanced Security Obligation. These controls are incident response planning, cyber security exercises and vulnerability assessments.

More clarity required

There needs to be more clarity in the purpose of the legislation, and this does not appear to be provided by this bill. It is still unclear whether the legislation is mandating control, outcomes, standards, frameworks or processes. It is worth comparing the Security of Critical Infrastructure Act with the Security Legislation Amendment Bill applied in its current form to other information security guidance.

ACSC Essential 8

Essential 8 – 8 controls

This is a compilation of the most significant 8 controls to provide improvement to cyber security posture. This is not a comprehensive list of controls but a necessary starting point to remediate against malware delivery and execution, limiting the extent of cyber security incidents, and enabling the ability to recover data and system availability to ensure information can be accessed following a cyber security incident (e.g., ransomware).

ISO/IEC 27001

ISO27001 – 114 controls

ISO/IEC 27001 has 35 security objectives and 114 security controls. Being an international standard, organisations can gain certification against this standard to demonstrate their security posture to suppliers, partners or consumers.

NIST Cyber Security Framework

NIST CSF – No controls
108 sub-categories for controls

NIST Cybersecurity Framework has 108 sub-categories for controls. This is a framework mandated for use by critical infrastructure entities in the United States of America. There are no security controls listed in this framework. It is up to each entity to implement the cyber security controls necessary to remediate the cyber risks of the organisation and then align each control to the sub-category in the framework that is most suitable.

NIST have also published a catalogue of controls for US federal systems (*Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations*) and two smaller controls catalogues for non-federal systems with Controlled Unclassified Information (*Special Publications 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organisations, and Special Publication 800-172 Enhanced Security Requirements for Protecting Controlled Unclassified Information*).

NIST SP800-53 – 827 controls
NIST SP800-171 – 109 controls
NIST SP800-172 – 33 controls

Special Publication 800-53 includes 827 controls and control enhancements that can be selected based on the level of security required and the specific risks to be mitigated. A number of these controls are mapped to sub-categories of the NIST cyber security framework. Special Publication 800-171 has 109 controls and Special Publication 800-172, both applicable to unclassified data for non-federal organisations, has 33 controls. These are an only a few of the information security guides available from NIST.

In early February of this year (2021) NIST released special publication 800-172. Enhanced control 3.13.1e in this publication addresses the need for the active cyber defence capability that the ACDA has been promoting since its inception. Quoting directly from this publication, "There are many techniques and approaches that can be used to confuse and mislead adversaries, including misdirection, tainting, disinformation, or a combination thereof. Deception is used to confuse and mislead adversaries regarding the information that the adversaries use for decision making, the value and authenticity of the information that the adversaries attempt to exfiltrate, or the environment in which the adversaries desire or need to operate. Such actions can impede the adversary's ability to conduct meaningful reconnaissance of the targeted organization, delay or degrade an adversary's ability to move laterally through a system or from one system to another system, divert the adversary away from systems or system components containing CUI, and increase observability of the adversary to the defender—revealing the presence of the adversary along with its TTPs [(i.e., Tools, Techniques and Procedures)]"

Special Publication 800-160 Volume 2 also addresses deception techniques (an element of active cyber defence) as part of cyber resiliency engineering (refer Appendix E).

These two publications from the National Institute of Science and Technology (United States Department of Commerce) concur with and back up the call for active cyber defence measures by the Active Cyber Defence Alliance

Information Security Manual

AusGov ISM – 779 controls

The Australian Government Information Security Manual (ISM) has 779 controls. The selection of these controls is driven by the official classification of the data being stored, transmitted or processed as well as the mitigation of risk.

Minimum effort

The mandating of only three controls in the Bill leaves open the very real possibility that critical infrastructure entities that do not have a strong cyber security posture will only do enough to meet the legislation and leave serious vulnerabilities and weaknesses unaddressed. This may not even be deliberate. An organisation that does not implement vulnerability management or control assessment processes may never know about the vulnerabilities or weaknesses that leave them exposed to the risk of an information security breach.

Controls vs No controls

APRA CPS234

For consistency, the Act should stipulate a comprehensive structure of security controls or no controls at all. This is where the Australian Prudential Regulatory Authority struck the right balance when they published Prudential Standard 234 (CPS234). This standard called for the implementation of an information Security Management System that was properly maintained and notification of breaches to the regulator. They did not specify any information security controls but mandated that each regulated entity develop a system for applying controls according to the risks of the organisation. A similar standard could be mandated within the Act for critical infrastructure.

Sovereign control set

If a comprehensive sovereign set of controls is required, then the Act could leverage the Australian Government Information Security Manual and define an applicability to critical infrastructure for each control rather than define a completely new standard.

Legislative Recommendation 3: Remove specific controls from the legislation

Remove the requirement for specific controls from the Bill to avoid the appearance those listed controls being viewed as the complete list of security requirements.

Legislative Recommendation 4: Mandate an information security management system

Include the requirement for an information security management system driven by risk with periodic reporting to regulators on the state of the management system including the rate at which findings are remediated and risks mitigated.

Legislative Recommendation 5: Recommend active cyber defence measure

Include a recommendation in the bill for asset owners to consider the use of active cyber defence measures in line with the latest cyber security industry guidance.

7 Holistic cyber resilience

Clear responsibility required

Legislation should make clear the responsibility of each party in the critical infrastructure eco-system to provide assurance that the assets under their ownership and/or control are cyber safe and operationally resilient as a 'system of systems' in the context of the unfolding threat environment over the operating life of the asset.

Safety and resilience

A set-and-forget approach to cyber defence is not feasible. Each party in the supply chain of services provided and acquired, such as operators, contractors, sub-contractors, managed service providers, etc., must be obliged to maintain their sub-systems in a continuous state of cyber safety and operational resilience and be obliged to augment and adopt controls from time of time to meet the requirement for holistic cyber resilience of each party's entire critical infrastructure asset. Assurance of the safety and resilience of each critical infrastructure 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.

Legislative Recommendation 6: Define clear lines of accountability for cyber security

Include a requirement for each owner to provide assurances in regard to the safety and resilience of the services that they provide. An operator or sub-contractor may develop the assurance report, but the owner must provide sign-off on delivery of the report to the regulator.

8 Continuous Compliance

To provide a benchmark of cyber defence measures and facilitate the continuous measurement of compliance to match the unfolding threat environment, annual cyber crisis response 'exercises' should be mandated for all regulated operators of critical infrastructure. These exercises should entail real intelligence gathering, red teaming (attacking) and blue teaming (defending) all feeding into crisis response exercises that are not pre-set hypothetical desktop exercises but live interactions. Participation should be mandatory for all asset owners and operators, be sector specific and coordinated by the sector regulator.

Response exercises
Red teaming
Blue teaming
Live interactions

The findings from such exercises should be shared with the responsible regulator in a prescribed format and without unnecessary security configuration detail. The regulator should set minimum standards for continuous enhancement of cyber resilience and be funded to provide assistance to smaller owners or operators, so that the sector improves security posture holistically rather than on an asset-by-asset basis.

Shared findings
Assistance for small operators

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

Resources available under creative commons

Legislative Recommendation 7: Crisis response exercises

Include a requirement in the Bill for all critical infrastructure operators to run (at least) annual crisis response exercises that require live interactions between internal system owners and live interactions with other external entities. A recommendation should be added to this requirement to promote the use of live-fire environments where possible to improve realism and learning opportunities.

9 Structural challenges in securing critical infrastructure

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 operational technology (control systems), 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, resulting in the cyber security requirements proposed during the tender process becoming outdated, sometimes before the tender is awarded and the project is delivered.

Little/No uplift during lifetime

the critical order and priority of the mitigation strategies are changed regularly to focus on the changing cyber threats and cyber events

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 control systems are maintained, secured and protected against the rapidly changing cyber threat landscape.

Unclear cyber investment over lifetime

Ongoing maintenance requires budgeting for operational expenditure that is extremely difficult to quantify and plan over these long asset lifecycles. Businesses are often unprepared to consider new and emerging cyber risks that introduce unplanned operational expenditure and diminish the shareholder returns from forecast.

Unplanned operational expenditure for cyber risks

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

Ongoing security spend considered in acquisition

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

Visibility of adversary activity

sufficient visibility of adversary activity, footholds, resources, tools, techniques, procedures and capabilities to enable an informed view of whether it is safe to continue to operate during an-ongoing attack. It is in the second area that intelligence, deception, active threat hunting and continuous systems monitoring capabilities are critical. Even if you can restore broken systems quickly you can't keep operating a train, electricity or water system if you're not sure it is safe.

Passing the baton of resilience

Typically, each party in the supply chain of service provision and acquisition has responsibility for securing their own assets, 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.

Rail example of whole system resilience

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 Systems, 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.

Integration layer

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.

Holistic view required

The assumption is that, since each element in the critical infrastructure of the parties comprising the whole critical infrastructure eco-system is secured, the 'system of systems' as a whole, is secure. This 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.

Inconsistent approaches
Concessions to small operators

Once requirements are legally agreed, a critical infrastructure operator has little or no ability to amend the terms of the contract to dictate further specific system security or other requirements. Furthermore, inconsistencies in approach between participants in the critical infrastructure eco-system 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.

Threats change faster than contracts

The net result is that the disparity between the terms of the agreement, and the constantly evolving cyber threat landscape grows more significant over the life of the contract. 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.

Unsuitability of IT sourced cyber defence approaches

Immature risk practices
Resistance to change in OT environments

Active defence facilitates informed decision-making

Controls should be selected based on their effectiveness to reduce risk; however, this is often 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 ADCA suggests that active cyber defence can lead to a better knowledge of actual threats as they emerge, and lead to a risk-driven control selection culture. In operational technology, there is a reluctance to maintain the effectiveness of controls, where doing so (e.g., patching) could compromise safety. Active cyber defence provides a strategy where OT systems are not modified, and early detection of threats, 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?)

Key Objectives in securing critical infrastructure

Playbooks, real-time response and resilience

The Bill outlines the following Key 'Objectives' identified through a process of industry consultation and discussion workshops.

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

Call out active cyber defence

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 Positive Security Obligation should call out active cyber defence as a critical area for focus and resourcing in Australian cyber defence and resilience.

More than passive defence

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.

Active defence
Active detection
Active response

The ACDA believes critical infrastructure providers should shift their focus beyond the current passive approach to include active cyber defence, detection, response and recovery. The actionable threat intelligence gathered from active cyber defence measures, 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.

Legislative Recommendation 8: Include inter-asset security requirements

Include a requirement for operators to report to the regulator on risks associated with the transfer or access of information to/from another operator to show that they have considered the risks associated with data entering or leaving their domain of control.

10 Active Strategies

Deception, traps and threat intelligence

An active cyber defence strategy will reinforce and compliment conventional passive cyber security by leveraging 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 eco-system (the on-premises, cloud, IoT, mobile and legacy systems) by integrating active cyber defence and threat intelligence in the context of actively observing cyber 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 actively pursuing 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 cyber incident management, 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 improve responses. All of which will raise the bar of Australia's cyber security resilience.

Legislative Recommendation 9: Callout lawful defensive responses

Include provisions in legislation to allow certain active cyber defence responses to be declared legal or to be legalised. In spite of the advantages of employing active cyber defence techniques with an environment owned and/or controlled by an asset operator, there is reluctance to use these tools and techniques because of a concern that any engagement with an adversary may not be legal. A declaration of the active cyber defence actions and response that are legal will provide greater certainty for information security practitioners.

Legislative Recommendation 10: Private sector cyber defence affiliates

Include provisions in legislation to appoint or license responsible private sector organisations to act as cyber defence 'affiliates'. This resource pool of cyber security consultants and subject matter experts will be available to supplement government agencies in responding to cyber defence issues.

Executive Recommendation 1: No prosecution against active cyber defence

Formally announce that no prosecutions will arise from certain active cyber defence responses, pending legislative change. This will provide certainty to organisations that have already implemented active cyber defence measures.

Executive Recommendation 2: Provide guidance on active cyber defence

Clearly define the active cyber defence actions and responses that are authorised and provide advice/guidance on the application of active cyber defence.

Executive Recommendation 3: Communication active cyber defence responsibilities

Coordinate and rationalise the active cyber defence responsibilities to appropriate government agencies.

Executive Recommendation 4: Active cyber defence discussion with other countries

Commence discussions with active cyber defence friendly countries to develop a charter of the acceptable actions and responses for active cyber defence.

Executive Recommendation 5: Lobbying United Nations Commission

Lobby the United Nations Commission on International Trade Law for a new model law to adopt active cyber defence to underpin acceptable behaviour in cyberspace and rules-based global order.

Judicial Recommendation 1: Advisory opinions

Interpret and clarify which active cyber defence responses are or should be lawful and will not be prosecuted by interpreting existing federal and state law.

Judicial Recommendation 2: Interpretation and Clarification

Where there is a contested matter, provide declaratory relief and advisory opinions on matters of application and interpretation of law to cyberspace.

11 Conclusion

Given the assessment that we have provided in the preceding pages, there is no silver bullet solution that can protect organisations from all threats. An adversary who is motivated to breach a system will do so given the resources and time, however, an active cyber defence approach provides a higher fidelity understanding of the threats and threat actors and provides assurance that the adversary is not operating within the asset infrastructure.

The application of active cyber defence on top of mature passive cyber defence will provide the security posture that will make it difficult for adversaries to get a persistent foothold in an environment.

The Bill that has been presented does not define or promote this outcome and is materially lacking in content to do so. The intent to limit the regulatory burden on operators indicates a focus on compliance rather than security. The recommendations throughout this submission will provide improvements to the security posture of critical infrastructure assets and the critical infrastructure eco-system, however we would suggest the Bill be reconsidered in its entirety because of the material shortcomings in its current form.

While legislation is often viewed as placing boundaries on what actions are allowed to meet with social expectations and defining a list of metrics or actions to which we must comply, legislation regarding the cyber security of systems, assets and society should be presented as enabling and defining how far each asset owner or operator may go to defend their systems and asset.

Our adversaries will not be constrained by what is allowed or what is compliant. Therefore, we need to be active in the defence of our systems, assets and country.

Contact Details

Attention: Andrew Cox
Active Cyber Defence Alliance
c/o Avantgard Pty Ltd
[redacted]
Australia

Lead Author

John Powell
Principal Security Consultant
Telstra Purple

Contributing Authors

Duncan Unwin
Managing Director
Tobruk Security

Debbie Lutter
CEO
AUSCSEC Pty Ltd

Andrew Cox
CEO
Avantgard

Helaine Legget
Attorney at Law
ICT Legal Consulting

Phillip Moore
Technical Manager
Avantgard

Bruce Dawson
Managing Security Consultant
Telstra Purple