CRITICAL NEXUS: The role of policy and cybersecurity in critical infrastructure resilience.

Lauren Veenstra, Charles Sturt University.

Abstract

Reliable access to energy, water, transport, finance, and communications are inextricably linked to societal stability, economic output, and ultimately, national security. Governments worldwide are acutely aware of the role these essential services play in underpinning the function of contemporary society. Nevertheless, despite more than two decades of working to address critical infrastructure protection, recent cyber-attacks such as those impacting Colonial Pipeline, the Amsterdam-Rotterdam-Antwerp refining hub, and more recently DP World Australia, attest to critical infrastructure resilience remaining a formidable challenge; moreover, one with potentially far-reaching and dire consequences should regulators and industry fall short in combating increasingly sophisticated and capable adversaries. This research paper explores the critical infrastructure policy landscape, cataloguing characteristic elements from various jurisdictions and identifying those with the potential to realise material uplift in cybersecurity posture and maturity. Australia's approach is analysed in the context of the broader policy landscape and research findings, with a discussion on government and industry's role in securing critical infrastructure assets. The research concludes with recommendations on additional policy and strategic elements to further progress critical infrastructure resilience.

1. Introduction

From ransomware syndicates targeting medical facilities with time-critical risk-to-life consequences to nation-state actors engaging in grey zone activities for geopolitical advantage, critical infrastructure is a high-value target across multiple threat actor categories. While such scenarios may be reminiscent of dystopian futures portrayed in fiction, they are, in fact, occurring in the here and now. The 2017 attacks on the UK National Health System [1] and the ongoing campaign of Russian cyber-attacks on Ukrainian infrastructure [2] serve as high-profile examples of significant societal disruption.

Addressing critical infrastructure protection presents multifaceted challenges for policymakers and asset owners alike. Contemporary Western policy development has to a large extent been contextualised by post 9/11 security agendas [3], with varying degrees of success, or otherwise, in addressing security and resilience in highly digitised critical infrastructure networks. Governments face navigating complex legislative structures and regulatory bodies with overlapping responsibilities whilst endeavouring to harmonise diverse stakeholder interests in formulating strategies that balance efficacy against the burden of regulatory impost foisted upon asset owners [4].

Further complexity is found in the array of technologies deployed in critical infrastructure domains, from commodity information technology to specialised industrial controllers manipulating the physical environment. Many such devices deployed in industrial control have lifecycles measured in decades [5], having been designed and installed well before cyber risks arising from converged information technology and operational technology environments were considered. Subsequently, standard information security practices are often ill-suited or overly hazardous in operational technology settings such as power stations, nuclear reactors, oil refineries, etc.

Moreover, the highly interconnected nature of the contemporary critical infrastructure ecosystem brings about the spectre of cascading consequences, whereby the failure of an asset(s) in one sector, such as electricity transmission, precipitates service disruptions or failures in downstream critical infrastructure with widespread societal impacts. Such cascading consequences were evidenced on December 23, 2015, when a cyber-attack targeting Ukrainian distribution company Kyivoblenergo propagated to three energy companies, ultimately impacting 225,000 customers [6]. The potential for realisation of such scenarios is not lost on policymakers, with an emerging trend of mandating additional protections to lessen the likelihood and mitigate the impacts of cascading consequences, as is the case in Australia's definition and treatment of systems of national significance [7].

When examining research in cybersecurity, one can posit two categories of research problems worthy of pursuit: problems lacking sufficient consideration, and problems lacking focused perspective. The nexus between critical infrastructure policy and cybersecurity is arguably both. Despite the importance of safeguarding critical infrastructure and the essential services provided, there remains an observable gap in scholarly investigation specifically focused on the intersection of policy and

cybersecurity within the context of critical infrastructure resilience. To address that gap, this research initiative investigates how policy influences critical infrastructure cyber resilience and Australia's comparative standing among its peers.

The two sub-questions to be addressed by the investigative process are:

What commonalities and differentiators characterise the policy landscape addressing critical infrastructure cyber resilience, and which elements are indicative of policy success?

How does Australia's policy position drive advancements in cyber posture and maturity for critical infrastructure assets within the national context?

This collision of highly complex challenges and high-consequence outcomes at the national scale makes for a critical nexus warranting investigation.

2. Methodology

The broadly recognised literature review methodology [8] is combined with comparative study [9] delivering a hybrid approach to addressing the problem domain and associated sub-questions. Literature critique of scholarly articles, government documents, and industry sources informs analysis and comparative study. Linguistic, systematic, and teleological interpretation techniques serve as the primary mode of analysis applied to critical infrastructure policy comparative study for the Australian (AU), the European Union (EU), and United States of America (US) jurisdictions. These review and analysis techniques collectively provide a comprehensive understanding of the problem domain, facilitating a nuanced and insightful response to research questions. By integrating a diversity of methodologies, the synthesis achieved affords a deeper understanding and a highly informed perspective, giving rise to robust research outcomes that support policymakers and guide future research studies.

3. The Policy Landscape

Understanding the critical infrastructure policy landscape requires a comparative analysis of the approaches adopted by Australia, the European Union, and the United States, each of which have developed distinct frameworks addressing critical infrastructure security within their respective jurisdictions. Policy evolution in Australia and the EU has moved towards a largely centralised model, whereby policy is articulated across a small number of legislative instruments with logical linkages serving to provide for a largely cohesive whole [10, 11]. These centralised approaches facilitate coordinated and consistent regulation across critical infrastructure sectors.

In contrast, US policy evolution has resulted in a more diffuse strategy, characterised by a complex patchwork of regulation with overlapping mandates at federal and state levels [12]. Further complexities arise from both civil and defence agency involvement in the regulatory landscape, with blurred lines of responsibility diminishing the overall effectiveness of governance practices [4]. While it may be argued this decentralised approach affords the opportunity for flexibility in sectorial adaptation, it raises questions as to accessibility and uniformity of efficacy across critical infrastructure sectors.

Divergence in policy approaches underscores the influence of economic paradigms, socio-political context, and governance structures, combining to present unique pressures and constraints for policymakers across these jurisdictions.

3.1 Australia

Within the Australian jurisdiction, the policy framework consists of:

1 Security of Critical Infrastructure (SoCI) Act 2018 [13],

2 Security of Critical Infrastructure (Definitions) Rules (LIN 21/039) 2021 [14],

3 Security of Critical Infrastructure (Application) Rules (LIN 22/026) 2022 [15],

4 Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023 [16],

5 Security of Critical Infrastructure (Naval shipbuilding precinct) Rules (LIN 23/007) 2023 [17], and

6 Security of Critical Infrastructure (Australian National University) Rules (LIN 22/041) 2022 [18].

The Act is the overarching regulatory document, with the Rules being legislative instruments operationalising various elements of the Act. During the legislative reform processes of 2020 through 2021, Government adopted a staged approach in operationalising new legislative requirements to expedite compliance against certain elements of the Act, such as asset registration against an expanded definition of critical infrastructure assets spanning 11 sectors and 22 asset classes, and mandatory cyber incident reporting. Remaining elements, including risk management obligations, progressed through industry stakeholder consultation and parliamentary review committees, being operationalised in 2022. Figure 1 provides an overview of the framework.

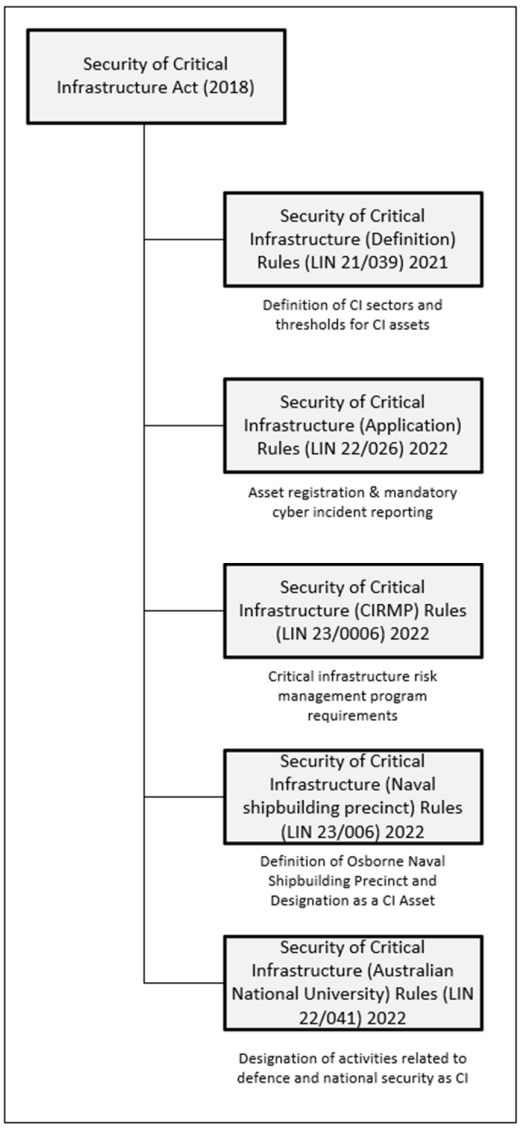

Figure 1 Australian Legislative Instruments

Australian policymakers applied an all-hazards approach to critical infrastructure security, categorising hazards into four domains, namely personnel, supply chain, physical and natural, and cyber. Organisations are obliged to develop a Critical Infrastructure Risk Management Program (CIRMP) to deliver a formalised and structured approach to risk management and treatment, with governance oversight in the form of mandatory annual board attestation of CRIMP effectiveness submitted to Government.

Four elements underpin cyber and information security risk management:

1 Mandatory notification of cybersecurity incidents, designed to afford Government timely situational awareness of threat actor activities impacting critical infrastructure assets with a view to both supporting the operators of CI assets under attack, and sharing threat actor intelligence with the CI asset operator community through mechanisms including the Trusted Information Sharing Network (TSIN), Joint Cyber Security Center (JCSC) briefings, Australian Cyber Security Center (ACSC) advisories, and direct contact.

2 Government response to serious cybersecurity incidents. This may take the form of providing confidential intelligence including threat actor tactics, techniques, and protocols (TTPs), remediation assistance, and other support. In circumstances where an incident is, or is likely to seriously prejudice societal or economic stability, defence, or national security, the Act empowers the Minister for Home Affairs to authorise directives obliging CI operators to participate in information gathering activities, undertake actions specified by the Secretary or their delegate, or facilitate direct intervention by Government. Ministerial directives are reserved for circumstances when a CI operator is either unwilling or unable to take all reasonable steps to respond to an incident, and there exists no other state for federal regulatory framework under which such actions can be taken.

3 Enhanced cybersecurity obligations for Systems of National Significance (SoNS) for improved preparedness and response capabilities. Obligations include statutory incident response planning and compliance, undertaking of cybersecurity exercises and vulnerability assessments observable by designated officers. Further, these obligations extend to providing the Australian Signals Directorate (ASD) with periodic or event-based system information or reports, and installation of Government software that transmits system information to ASD.

4 Cybersecurity framework compliance. CI operators must elect, and comply with, one of ISO/IEC 27001:2015, ASD's Essential 8 Maturity Model maturity level 1, NIST CSF, C2M2 maturity indicator level 1, Australian Energy Sector Cybersecurity Framework Cor security profile 1, or an equivalent thereof.

3.2 European Union

The European policy framework consists of:

1 Directive 2022/2557 on the Resilience of Critical Entities (CER) [19],

2 Directive 2022/2555 on Measures for a High Common Level of Cybersecurity Across the EU (NIS2) [20], and

3 Regulation 2022/2554 on Digital Operational

Resilience for the Financial Sector (DORA) [21].

Policies are largely complementary in nature, with the CER directive being similar to the Australian SoCI act, adopting a comprehensive all-hazards framework addressing the resilience of critical entities to natural, man-made, accidental, and intentional threats. Drafting activities for CER, NIS2, and DORA have been closely coordinated so as to produce a comprehensive and cohesive policy suite with synergetic benefits to be realised through parallel implementation across EU Member States. CER clause 9 [19] explicitly excludes cybersecurity risk management practices in preference to such provisions being prescribed in the NIS2 directive. Though segregated, CER calls for a collaborative approach between the Critical Entities Resilience Group established under CER, with that of the Cooperation Group established under NIS2, so as to promote cooperation and coordination of competent authorities in discharging responsibilities. Figure 2 provides an overview of policy relationships.

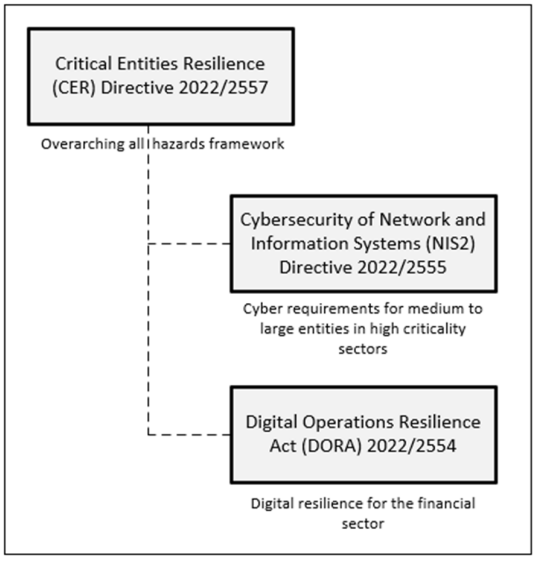

Figure 2 European Legislative Instruments

Primary cybersecurity requirements of NIS2 are articulated in articles 20 through 25 of chapter IV of the directive:

1 Governance (art. 20) – management bodies of CI assets are required to undertake training in cyber risk management practices, and sign off against the adequacy of the CI assets' cybersecurity risk management practices,

2 Cyber risk management (art. 21) – organisations are to implement an all-of-hazards cyber risk management program, adhering to relevant standards and delivering technical, operational, and organisational controls commensurate to risk, including the severity of societal and economic impacts. Control measures are to include risk analysis, incident response, business continuity, supply chain security, identity and access management, and security education and awareness training.

3 Supply chain risk assessment (art.22) – the Cooperation Group, in collaboration with the Commission and the European Agency for Cybersecurity (ENISA) may conduct coordinated security risk assessments of critical services, systems, or supply chains.

4 Reporting obligations (art.23) – CI asset operators are obliged to provide Member State Computer Security Incident Response Teams (CSIRT) or competent authorities timely situational awareness of threat actor activities impacting assets. Upon request, CSIRTs or competent authorities are to provide organisations guidance and operational advice on potential mitigations. Further, organisations are obliged to inform recipients of their services of significant incidents that are likely to adversely impact provision of services. In instances where cross-border impacts are likely, CSIRTs or competent authorities are to inform affected Member States and ENISA such that coordinated incident response activities may be undertaken.

5 EU Cyber certification (art 24.) – To support Article 21 compliance, Member States may require organisations to use products, services, and processes certified under the European cybersecurity certification scheme. The certification scheme is designed to establish and maintain trust in information communications technology (ICT) supply chains [22]. Although voluntary, speculation exists as to the potential for future mandates prescribing the use of certified products, services, and processes [23].

6 Standardisation (art. 25) – To foster consistent implementation of Article 21 across Member States and CI operators, ENISA in cooperation with stakeholders will develop advice and guidance regarding technical standards for information security.

With DORA being solely focused on the financial sector, it serves as an adjunct to CER and NIS2 and, as such, falls outside of the review scope.

3.3 United States

Section 213 of the Homeland Security Act 2002 [24] designates The President, or The Secretary of Homeland Security, responsible for critical infrastructure protection. President Obama exercised this authority via Presidential Policy Directive 21 (PDP-21) of 2013 [25], mandating the 2009 National

Table 1 Sector Specific Agencies

Critical Infrastructure Sector	Sector Specific Agency
Chemical	Department of Homeland Security
Commercial Facilities	
Communications	
Critical Manufacturing	
Dams	
Emergency Services	
Information Technology	
Nuclear Reactors, Materials, and Waste	
Food and Agriculture	Department of Agriculture, Department of Health, and Human Services
Defence Industrial Base	Department of Defence
Energy	Department of Energy
Healthcare and Public Health	Department of Health and Human Services
Financial Services	Department of the Treasury
Water and Wastewater	Environmental Protection Agency
Government Facilities	Department of Homeland Security, General Services Administration
Transport Systems	Department of Homeland Security, Department of Transportation

Infrastructure Protection Plan be updated to align with national preparedness goals. Further, PDP-21 identified 16 CI sectors, delegating governance and oversight functions to a range of sector-specific agencies (SAAs), as shown in Table 1. Pursuant to PDP-21, this sectorial structure carried forward into the 2013 National Infrastructure Protection Plan [26], and remains in place supported by Sector Coordinating Councils, Government Coordinating Councils and Regional Consortia, under the purview of the Critical Infrastructure Advisory Council.

Focusing on the energy sector for the purpose of review, early iterations of the Federal Power Act failed to address reliability and security. Section 1211 of the Energy Policy Act 2005 [27] redressed this shortcoming, amending the Federal Power Act to include Section 215 [28], directing the Federal Energy Regulatory Commission (FERC) to certify an Electric Reliability Organisation (ERO) for the purpose of developing mandatory enforceable reliability standards applicable across the electricity sector [29]. Following successful review and performance evaluation, the North American Electricity Reliability Corporation (NERC) was subsequently designated ERO under the auspices of FERC Order Number 672 [29, 30].

NERC has established and maintains a framework of critical infrastructure protection standards, commonly termed NERC CIP, designed to manage cybersecurity risks, and mitigate impacts within the electricity sector, predominately focused on generation and transmission systems. The NERC CIP framework includes 12 cyber-specific standards [31]:

1 CIP-002 Cyber System Categorisation – risk-based identification of systems critical to maintaining transmission and generation asset reliability.

2 CIP-003 Security Management Controls – mandates minimum requirements for security management controls protecting critical assets.

3 CIP-004 Personnel and Training – ensuring personnel with logical or physical access to assets are suitable vetted, trained, and security aware.

4 CIP-005 Electronic Perimeter(s) – identification and protection of logical electronic perimeters to ensure confidentiality, integrity, and availability of digital assets.

5 CIP-006 Physical Security of Cyber Systems – definition of physical security strategy and implementation of controls commensurate with risk.

6 CIP-007 System Security Management – details methods, processes, and procedures for protecting critical, and non-critical digital assets within logical perimeter.

7 CIP-008 Incident Reporting and Response Planning – identification, classification, response, and reporting.

8 CIP-009 Recovery Plans for Cyber Systems – ensuring adequate disaster recovery plans are

established.

9 CIP-010 Configuration Change Management and Vulnerability Assessments – prevention and detection of unauthorised change, and implementation of systematic vulnerability management practices.

10 CIP-011 Information Protection – establish and maintain controls to ensure the confidentiality, integrity, and availability of information assets.

11 CIP-012 Communications Between Control Centres – protection of real-time monitoring and control data in transit between control centres and similar such facilities.

12 CIP-013 Supply Chain Risk Management – prevention of supply chain initiated cyber disruption to generation and transmission assets.

Review of the electricity sector highlights the complexity of serpentine delegation pathways linking policy directives to regulatory controls, with numerous agencies and bodies intertwined in policy formulation and execution. Similarly, other critical infrastructure sectors exhibit equally convoluted delegation and discharge pathways with diffuse policy and regulatory processes seeing blurred lines of responsibility diminish the effectiveness of overall governance practices [4, 12].

Despite the disparate nature of critical infrastructure governance and oversight in the US jurisdiction, the approach to cybersecurity regulation across the balance of CI sectors is fundamentally similar in nature due to Presidential Executive Order 13636 issued in 2013 under the Obama administration. This order tasked the National Institute of Standards and Technology (NIST) with developing a cybersecurity framework (CSF) to reduce cyber risk to CI assets [32]. Further, section 10 of the order established requirements for designated CI regulatory agencies regarding adoption of NIST CSF in sectors falling within their remit. Consequently, guidance and direction for NIST CSF implementation appears in all sector-specific plans.

Policy evolution remains ongoing in the US. As recently as April 30th 2024, the Biden Administration released the National Security Memorandum-22 (NSM) on Critical Infrastructure Security and Resilience [33], which sees a pivot from protection to risk management, similar to that of the Australian and EU jurisdictions.

4. Security, Resilience, and Cyber Frameworks

Security and resilience are often conflated terms. The Oxford English Dictionary defines security as "the state or condition of being protected from, or not exposed to danger; safety" [34], with resilience being "the quality or fact of being able to recover quickly or easily from, or resist being affected by, a misfortune, shock, illness, etc.; robustness" [35]. Building upon this, cybersecurity and cyber resilience are two areas of endeavour critical to maintaining the confidentiality, integrity, and availability of digital assets. Cybersecurity is primarily focused on threat prevention and protection, whereas cyber resilience is concerned with the ability to withstand, recover, and adapt to cyber incidents [36-38]. The US National Academy of Sciences definition of resilience, that being "the ability to prepare and plan for, absorb, recover from, and more successfully adapt to adverse events" [39], features prevalently in industry and academic sources. Connelly et al. [40] expand upon this, articulating resilience features across socio-ecology, psychological, organisational, and engineering domains as shown in Table 2.

In Figure 3 Panteli and Mancarella [41] provide a visualisation of resilience as a factor of time with a resilience feature overlay, demonstrating key resilience features necessary for contemporary power systems to cope with disruptive events, including cyber incidents.

In order to withstand the initial shock of a disruptive event, it is necessary to be operating in a robust/resilient state, R0. Following an event, the system transitions to a degraded state R*pr* where resilience is significantly compromised. The magnitude of the event is largely determined by the extent to which assortative resilience features such as resourcefulness, redundancy, and adaptive organisation are able to dampen impacts (R*pe*). Further, these features provide the corrective flexibility necessary to adapt to new conditions, minimising the resilience differential (R0 - Rpe).

During the restorative state, recovery resilience features need be sufficiently capable to afford the system a rapid return to the resilient state, that being minimising the t*pr* – tr differential. The post-restoration state returns the system to an operational state with resilience level R*pr*, affording limited resilience through until full restoration operational resilience at R0 at t*pir*.

In exploring the relationship between security and resilience, bow tie analysis, a common industrial risk management technique, provides a readily accessible visual representation of the relationship between threats, preventative controls, mitigating controls and consequential outcomes, centred around realisation of a hazardous scenario [42]. Figure 4 depicts a simplistic representation where external adversaries pose a threat to the loss of confidentiality for sensitive data holdings, with perimeter firewall defences shown as a security control, and data loss prevention systems a risk mitigant for data breach. Here, elements to the left of the hazardous scenario,

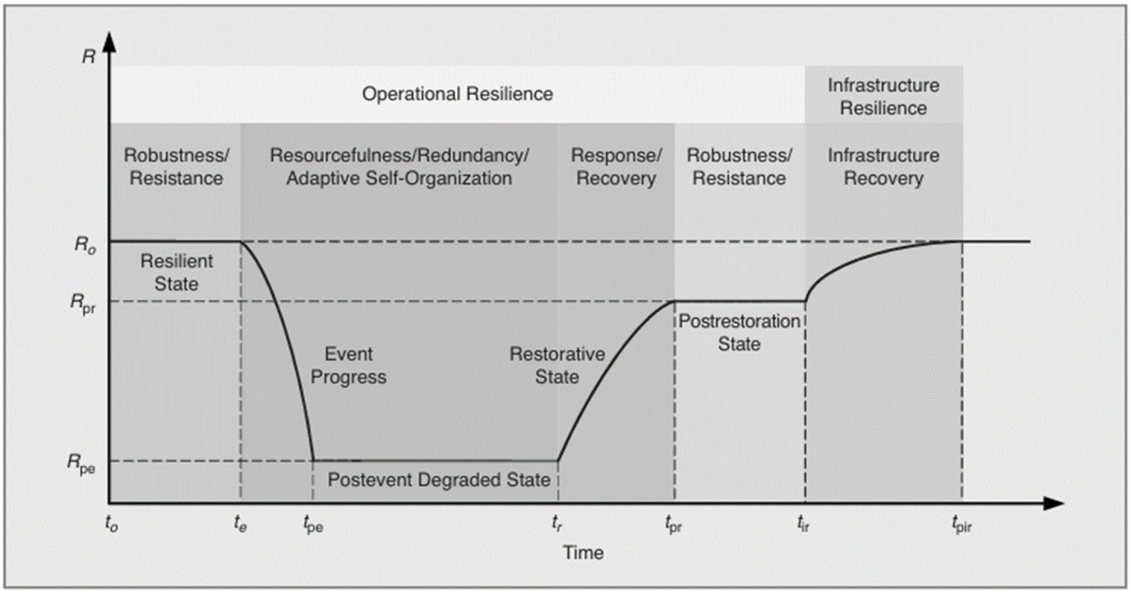

Figure 3 Conceptual Resilience Curve, Panteli and Mancarella [41]

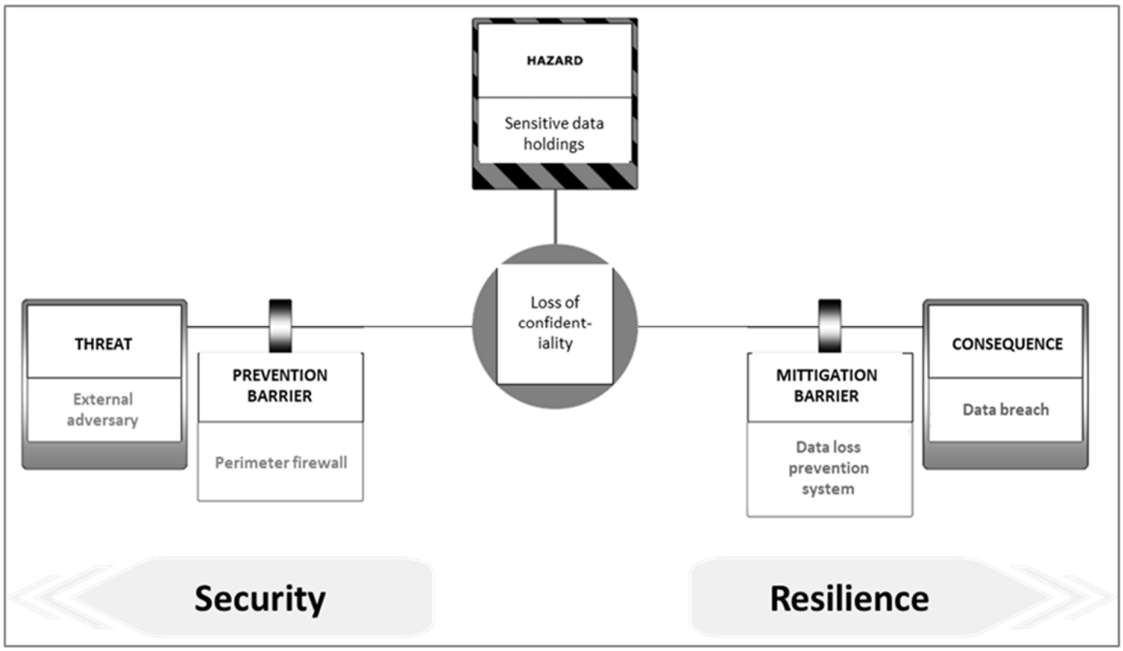

Figure 4 Simplified Bow Tie, Data Breach Scenario

loss of confidentiality, can be considered contributing to security, and those to the right contributing to resilience. Hatch and Geddes have systematically adapted bow tie techniques in their Hazards Australasia conference paper of 2019 [43] titled of Computer Hazard and Security Evaluation (CHASE) to combine bow tie analysis with the rigours of HAZOP and CHAZOP in visualising cybersecurity risks and vulnerabilities in operational technology environments; the paper is commended to interested readers in the critical infrastructure domain. Further, these features provide the corrective flexibility necessary to adapt to new conditions, minimising the resilience differential (R0 - R*pe*).

Table 2 Resilience features, Connelly et al. [40]

		Description by application domain			
NAS phase of resilience	Resilience feature	Socioecological	Psychological	Organizational	Engineering and infrastructure
Plan	Critical functions (services)	A system function identified by stakeholders as an important dimension by which to assess system performance			
		Ecosystem services provided to society	Human psychological well-being	Goods and services provided to society	Services provided by physical and technical engineered systems
Absorb	Thresholds	Intrinsic tolerance to stress or changes in conditions where exceeding a threshold perpetuates a regime shift			
		Used to identify natural breaks in scale	Based on sense of community and personal attributes	Linked to organizational adaptive capacity and to brittleness when close to threshold	Based on sensitivity of system functioning to changes in input variables
Recover	Time (& scale)	Duration of degraded system performance			
		Emphasis on dynamics over time	Emphasis on time of disruption (i.e., developmental stage: childhood vs adulthood)	Emphasis on time until recovery	Emphasis on time until recovery
Adapt	Memory / adaptive management	Change in management approach or other responses in anticipation of or enabled by learning from previous disruptions, events, or experiences			
		Ecological memory guides how ecosystem reorganises after a disruption, which is maintained if the system has high modularity	Human and social memory can enhance (through learning) or diminish (e.g., posttraumatic stress) psychological resilience	Corporate memory of challenges posed to the organization and management that enable modification and building of responsiveness to events	Redesigning of engineering systems designs based on past and potential future stressors

Critical infrastructure policy and associated regulatory control measures demonstrate broad acknowledgement of the complementary nature of cybersecurity and cyber resilience, with integration providing a more comprehensive approach to risk management. This is evidenced by policymakers across the Australian, European, and US jurisdictions pivoting from a security-orientated focus to the adoption of risk-based principles and risk management practices in more recent iterations of policy and regulatory controls. However, the extent to which cybersecurity frameworks associated with regulatory controls address resilience factors varies considerably.

NIST CSF demonstrates a notable balance between security and resilience objectives. The framework is based on a series of practices structured into five domains [44]:

1 Identify – Understanding of operational context, sources, and risks to facilitate effective management and mitigation,

2 Protect – Implement safeguards commensurate with risk to limit exposure to cyber threats and limit consequential damage,

3 Detect – Establish means to provide situational awareness of security incidents to support timely intervention activities,

4 Respond – Development and operationalisation

of incident response plans to support the execution of appropriate action in the event of a cyber incident,

5 Recover – Plans and strategies for resilience to limit the impact of cyber incidents and facilitate recovery activities for restoring business processes and outputs following a cyber incident.

An additional governance domain was added in 2024 with the release of NIST CSF 2.0 [45]. The Respond and Recover domains exhibit strong alignment with resilience characteristics, emphasising the capability to manage and restore operations following disruptive events. Similarly, the detect domain contributes to resilience by promoting situational awareness, thereby enabling timely incident response and mitigating incident impacts.

The Cybersecurity Capability Maturity Model (C2M2), developed by the US Department of Energy in collaboration with industry, has likewise undergone recent revisions with version 2.1 released in June of 2022 [46]. C2M2 2.1 has been aligned with Government strategic guidance focused on improving US cyber posture and contains practices addressing both security and resilience characteristics [47]. Structured across 10 domains, C2M2 balances security and resilience, arguably favouring the former. Nevertheless, elements analogous to those of NIST CSF's Detect, Respond, and Recover domains provide comparable mechanisms, enhancing organisations' capability to identify, address, and recover from cybersecurity incidents.

Founded on C2M2, and maintaining alignment with its ongoing development, The Australian Energy Sector Cyber Security Framework (AESCSF) has been tailored for the Australian context, incorporating local frameworks and legislative obligations such as the Information Security Manual, the Australian Cyber Security Center Essential 8, the Privacy Act, and energy regulation [48]. AESCSF builds upon C2M2's cybersecurity practices by introducing 42 anti-patterns, that being behaviours and practices indicative of cyber insecurity. With a shared foundation, both AESCSF and C2M2 are equally adept at balancing security and resilience objectives.

By way of contrast, the widely adopted ISO/IEC 27001:2023 standard for Information Security Management Systems [49], primarily focuses on establishing and maintaining a systematic approach to managing and mitigating risk associated with information assets. While ISO/IEC27001 provides a robust framework for implementing security controls and safeguarding the confidentiality, integrity, and availability of information assets, its scope is inherently confined to information security risk and prevention [50]. Consequently, it falls short in fostering the full suite of resilience characteristics necessary to support the mission critical nature of critical infrastructure assets, in particular those with a heavy reliance on operational technology. This limitation raises questions as to the inclusion of ISO/IEC 27001 as one of the approved cybersecurity frameworks for critical infrastructure in Australian legislation.

Comparative analysis of frameworks such as NIST CSF, C2M2, AESCSF, and ISO/IEC 27001 reveals not all are equally suited to addressing the demands of critical infrastructure assets and their potential for cascading consequences. Frameworks demonstrating an integrated approach to balancing security and resilience characteristics, such as NIST CSF, C2M2, and AESCSF, are well suited to ensuring systems can absorb, respond, recover, and adapt to disruptive events, thus maximising the likelihood of assets maintaining the provision of critical services under adverse conditions. Conversely, frameworks focused on the prevention of information risk, such as ISO/IEC 27001, are ill-suited to critical infrastructure assets. This disparity highlights the necessity for policymakers to be cognisant of the need for a balanced approach to security and resilience, commensurate to the unique risk and consequence profiles associated with critical infrastructure. Moreover, policy formulation needs to afford this adequate consideration so that ensuing regulatory frameworks encompass the robust resilience measures vital for safeguarding the critical infrastructure assets that underpin societal stability, economic prosperity, and, ultimately, national security.

5. The Gordian Knot of Policy, Cybersecurity, and Resilience

The formulation of public policy requires policymakers to navigate competing interests, diverse stakeholders, and complex regulatory landscapes to create legislation that advances national interests and serves the public good. In the realm of critical infrastructure protection, this challenge is amplified as policymakers contend with geopolitical instability, strategic alliances, varying economic models, national security imperatives, and the dynamics of public-private partnerships. Additionally, governments need to reconcile the financial implications of policy such that effective controls can be realised without placing undue regulatory impost on private sector critical infrastructure asset owners and operators. Consequently, achieving a balanced and effective critical infrastructure protection policy demands a nuanced approach that integrates multiple perspectives and addresses both national and global challenges.

The emergence of cyber as a fifth domain in international relations and warfare underscores the relationship between critical infrastructure protection and national security. The prevalence of private ownership and operation of these essential assets further complicates these challenges, particularly in cases involving foreign ownership, which introduces risks of geopolitical coercion, espionage, sabotage, or other activities contrary to national security interests [51]. In the Australian jurisdiction, mandatory obligations exist under the SoCI Act [13], and powers afforded the Foreign Investment Review Board (FIRB), to provide Government visibility of foreign ownership and influence, with FIRB authorised to call in for review actions of foreign owners that pose a potential national security risk, and when such risk arise, to exercise powers of last resort in undertaking actions necessary to eliminate or reduce such risks [52].

Despite this, foreign ownership and influence in critical infrastructure remains contentious. In submissions to the Senate Economics Reference Committee into the Foreign Investment Review Framework [53], the Australian Strategic Policy Institute (ASPI) content that issues with state owned enterprises (SOEs), such as State Grid, a Chinese SOE bidder who sought interests in distribution network operator Transgrid, pose serious risk. ASPI argues that the close relationship between Chinese SOEs and the Peoples Republic of China (PRC) makes these entities instruments of the PRC when operating in extraterritorial markets. China Light and Power's ownership of Energy Australia, and more recently a 99-year lease of the Port of Darwin to Chinese owned Landbridge Group, has seen debate in the public forum as to the adequacy of Australian foreign investment controls, particularly in the case of critical infrastructure.

Aside from foreign ownership and influence, ASPI note that Australia's electricity networks are vulnerable to various forms of cyber intrusion and manipulation, with transmission and distribution networks operators being particularly strategic targets in an environment that has seen an ongoing increase in the number and scale of cyber-attacks directed at critical infrastructure, including major electricity networks. As recently as February 2024, Five Eyes Alliance partners Australia, Canada, New Zealand, the United Kingdom, and the United States have issued guidance to critical infrastructure operators in the energy sector regarding the PRC state-sponsored threat actor dubbed Volt Typhoon deploying covert living of the land techniques to gain a foothold and pre-position in critical infrastructure assets, with long term persistence observed in some instances [54]. These developments underscore the importance of well-defined and resilient critical infrastructure policy to safeguard against sophisticated cross boarder threats and raise questions regarding international efforts in critical infrastructure protection.

In seeking to redress the lack of international consensus on critical infrastructure protection the UN Group of Government Experts (UNGGE) and the UN Office for Disarmament Affairs Open-ended Working Group (UNOEWG) have compiled cyber norms of responsible state behaviour in cyberspace [55] that include protections for critical infrastructure. Analysing the undertakings of the UNGGE and UNOEWG, challenges arise in formulating such norms due to issues stemming from divergent interpretations and the inherently non-binding nature of cyber norms. Moreover, it is observed that non-territorial aspects of the cyber domain further encumber state accountabilities and obligations in regard to cyber norms. In acknowledging the UN's endeavour to link cyber norms to both the UN Charter and international law, it must be noted that in the absence of formal due diligence obligations linked to hard law, the powers afforded by cyber norms remain, in essence, voluntary and non-binding [56]. One could contend that such an arrangement is to the benefit of nation-states seeking to include cyber operations targeting critical infrastructure in their arsenal of offensive capabilities, as it provides a cover of legal ambiguity for such operations. With international consensus and cyber norms less than effective in facilitating enforceable and substantive protections for critical infrastructure now, and for the foreseeable future, the burden of doing so lies clearly with national policymakers, and in the case of the EU, the European Commission and its subordinates.

Further to international aspects of critical infrastructure policy, diversity of economic governance models among nations necessitates that policymakers adapt their approach to align with the degree of state control inherent in each economic paradigm. Within the contexts of the Australian, EU, and US jurisdictions, economic models can be broadly categorised into state-capitalist and market-capitalist systems. France exemplifies the state-capitalist model where significant state intervention shapes economic activities, while Australia serves as an example of a market-capital model characterised by minimal state interference and a predominance of market driven economic decisions.

Academic sources recommend critical infrastructure policy engagements in state-capital economies leverage hierarchical capability through rules-based regulation with top-down enforcement, whereas market-capital models are better suited to principles-based contractual obligations supported by non-binding guidance [57]. Contrary to the prevailing differentiation in economic paradigms and national policy approaches among EU Member States, emergence of the European Union NIS Directive [58], and its successor NIS2 [20],

represents convergence in management of diffuse cyber risk across disparate economic models. Convergence at the EU level provides the common framework necessary for articulating agreed objectives and control specifics, while affording Member States the flexibility to operationalise EU critical infrastructure cybersecurity mandates within national legislation tailored to their specific economic and political contexts.

EU Cybersecurity Strategy advocates a multifaceted approach to cyber resilience, including the cultivation of an enhanced public-private collaboration model. Key to this model is the development of normative regulation aimed at defining minimum requirements for network and information security and establishing coordinated prevention and response mechanisms [59], as is manifestly evident in the current NIS2 directive. While NIS2 represents notable progress in enhancing European critical infrastructure cybersecurity and resilience, challenges remain, particularly concerning reporting obligations and peer review feedback for Member States' policies.

Likewise, some observers question efficacy of risk management requirements applicable to the detect, analyse, and contain components of incident handling obligations [60]. However, it can be argued that adoption of frameworks that deliver a balanced approach to security and resilience, such as NIST and C2M2, serves to address these concerns through their structured and systemic approach to incident response. Others cite a lack of standardised methods and indicators for assessing resilience across differing sectors and nations as a major issue yet to be addressed, along with CER's reliance on conventional ISO31000-based risk methodologies that are primarily focused on risk prevention and mitigation [61]. Such criticism parallel concerns related to incident response, highlighting the need to identify an optimal balance between security and resilience characteristics.

Governance and regulatory harmonisation at Union scale presents significant challenges, as does integration of cyber resilience into Member States' policy agendas. Nonetheless, NIS2 represents a positive step in the evolution of robust and responsive critical infrastructure cyber policy, promoting a unified yet flexible approach across the EU.

Pivoting to the US, decentralisation features as a headline characteristic common to governance and regulation alike. The Department for Homeland Security (DHS) leads critical infrastructure protection providing overarching governance and oversight, supported by Department of Defence National Security Agency (NSA), Defence Cyber Command (CYBERCOM), and the Cyber and Infrastructure Security Agency (CISA) providing operational and intelligence support at the federal level, with sectorial governance and oversight provided by the 9 SSAs noted in Table 1.

Defence sector agencies CYBERCOM and NSA have the capacity to contribute significant human resources and technical capabilities that can greatly contribute to critical infrastructure protection. However, legal constraints limit the extent to which these agencies can engage with civilian entities, including critical infrastructure, during peacetime. Consequently, DHS, CISA, and SSAs are tasked with bridging capacity and capability gaps, a role for which some argue they are not optimally positioned; a sentiment likely contributing to the Defence Science Board's recommendation that CYBERCOM actively support private sector critical infrastructure through the provision of monitoring services, tools, and information sharing [4]. The blurred lines of responsibility and overlapping remits among these agencies impede the realisation of high-level policy objectives. Moreover, this fragmentation hinders cohesive strategy implementation and challenges the ability of agencies to exercise agile regulatory responses in the highly dynamic cybersecurity domain.

While further leveraging military capability for peacetime critical infrastructure protection could yield substantial advantages, it also presents notable risks. As an example, there may arise scenarios whereby defence agencies identify previously unknown technical vulnerabilities in critical infrastructure systems, precipitating conflicting priorities and the ethical dilemma of whether to remediate or exploit for strategic advantage. At a more fundamental level, one could question if the militarisation of civil cybersecurity runs counter to the philosophical ethos of liberal, democratic, market-capitalist society or if it is a justified measure to safeguard sovereign interests in the face of evermore sophisticated technological brinkmanship.

Conversely, it can be argued that private industry will mitigate operational risk within the bounds of organisational risk appetite, which is inherently linked to commercial imperatives in a market-capitalist paradigm. However, challenges arise where the societal, economic, or national security costs of critical infrastructure disruption far exceed those borne by the asset owner/operator. This disparity was highlighted in the response to the 2023-30 Australian Cyber Security Strategy Legislative Reform Consultation Paper by Australian transmission and distribution network operator, Ausgrid. In March of 2024, Head of Network Strategy and Future Grid, Murray Chandler, emphasised the significant impact imbalance. Noting their networks service an area that generates 20% of the nation's GDP, Chandler stated "a cyber-attack on our network, even for a few hours, would severely disrupt lives and livelihoods […] the economic impact from a complete shutdown of our

infrastructure may be as high as $120 million per hour or over $2.9 billion per day" [62]. This clear disparity in impact consequence gives rise to questions as to what constitutes adequate security and resilience measures for such organisations, and how the financial burden of implementing these measures should be apportioned.

6. Burden Bearers or Burden Sharers?

Analysis has yielded insights into the complex interplay of various economic, governance, engagement, and enforcement models. Amidst these complexities, three thematic elements emerged specific to the relationship between public and private entities:

1. Neither a solely government-led nor industry-led approach can realise critical infrastructure cyber resilience in contemporary economies where significant private asset ownership is prevalent; cyber resilience is a shared responsibility. Government-led approaches, while beneficial in providing policy and regulatory oversight aligned to political, economic, and national security interests, frequently lack the agility required to respond to technological disruption and the rapidly evolving cyber landscape [12]. Conversely, industry-led approaches driven by market forces are inherently focused on organisations' economic imperatives and consequently lack alignment with government agendas. Therefore, a shared responsibility model, founded on genuine consultation and active collaboration, is essential in harmonising competing interests such that policy and regulatory controls are sufficiently robust to meet government objectives, yet drafted in a manner sensitive to the operational context of critical infrastructure asset owners, and suitably pragmatic in approach to support real-world implementation.
2. Establishing and maintaining a public-private engagement model contextualised to national economic and market conditions is an essential requisite for success. The success of public-private collaboration is heavily influenced by the specific political and market conditions in each jurisdiction. Engagement models that are suitable in one context may not be suitable in another due to differing regulatory environments, technological maturity, existing public-private dynamics, and other region-specific factors. Tailoring the public-private engagement model to national conditions involves consideration of factors including the level of government intervention in the market, the readiness and capability of private sector operators to implement cybersecurity measures that may exceed the needs of organisational risk appetite, and existing legal and policy frameworks. By aligning engagement models with contextual factors, public-private cooperation can more effectively address specific challenges and foster mutual trust and effective collaboration in moving towards the realisation of critical infrastructure policy objectives.
3. While there exists scholarly consensus as to the criticality of public-private collaboration, defining what constitutes an effective engagement model remains contentious. The elements commonly considered essential for an effective engagement model include clear communication channels, well-defined roles and responsibilities, agreed shared objectives, mutual trust, and mechanisms fostering accountability and transparency for government and industry alike. However, there exists less agreement as to the balance between stringent regulation and market flexibility. Proponents of the former argue such measures are necessary to ensure compliance and uniformity across all critical infrastructure sectors, whereas those supporting a more adaptable approach content that flexibility better accommodates the particulars of differing sectorial and organisational needs, allows for more timely adaptation to changing conditions, and breaks down adversarial roles instead fostering cooperative relationships. The challenge lies in designing engagement models that leverage the strengths of both perspectives, delivering sufficient regulatory oversight to ensure baseline security and resilience compliance while affording asset owners the flexibility to pursue innovative and responsive means of achieving security and resilience objectives.

Underpinning these thematic elements is equitable sharing of financial burden. Irrespective of economic paradigm, sector maturity, threat landscape, or any other jurisdiction-specific factor, obliging organisations to implement cybersecurity and resilience measures exceeding those necessary to meet corporate risk appetite is a regulatory impost counter to commercial and business objectives, requiring organisations to realign capital plans to accommodate what may be a significant cost of compliance in some instances. Such concerns are particularly pronounced in regulated markets, where pricing controls limit the extent to which asset

owners can pass on costs to customers. It could be argued that if the government is sincere in its commitment to safeguard the contributions of critical infrastructure to social stability, economic prosperity, and national security, it is incumbent upon them to engage in equitable sharing of the financial burden to achieve these goals. Tax incentives, subsidies, program sponsorship and the like, directly linked to demonstrable uplift in critical infrastructure security and resilience at the sectoral level is an additional policy consideration warranting further investigation, and one with the potential to strengthen the public-private model of shared responsibility.

7. The Australian Perspective

As has been discussed thus far, Australia has adopted an all-of-hazards approach to critical infrastructure security and resilience that is multifaceted in nature, encompassing strategic policy, legislative frameworks, and an established public-private stakeholder engagement model. The central tenet of Australia's approach is the SoCI Act, which has been designed as a comprehensive and cohesive set of measures applicable across all 11 critical infrastructure sectors within the Act's definition, and of equal relevance to all 11 sectors. The Act delineates between systems of national significance (SoNS), and the balance of critical infrastructure asset categories, with additional rigour afforded to SoNS with their potential to trigger high impact cascading consequences as articulated in Ausgrid's submission on regulatory reforms [62]. Australia's approach in this regard bears similarities to that of the EU, with NIS2 Annex 1 designation of high-criticality entities [20]. To aid in further developing strategies for managing sectorial interdependencies and cascading consequences, Australia has engaged the national science body, the Commonwealth Scientific and Industrial Research Organisation (CSIRO), to undertake research in collaboration with industry stakeholders. Integration of research serves to provide policymakers and the critical infrastructure community with a more fulsome understanding of complexities to inform subsequent policy and regulatory direction.

While the SoCI Act provides largely comprehensive sectorial coverage, the chemical sector is a notable omission compared to EU and US regulations. The manufacture of gaseous chlorine serves as a case in point to underscore the consequence of such omissions. Chlorine gas is critical to the purification of drinking water for urban and regional communities, and with Australia reliant upon a single manufacturing facility, and there being no import market, a national shortage of chlorine will result within one to three weeks of a cyber incident disrupting production [63]. A thorough examination of chemical sector interdependencies is recommended, with results to inform asset inclusion definitions under the SoCI Act.

Forward policy direction is supported by the Critical Infrastructure Resilience Strategy [64] and 2023-2030 Australian Cybersecurity Strategy [63], developed in consultation with industry, government, and academic stakeholders. These strategy documents aim to guide adjustment of regulatory settings, with a notable uplift in regulatory compliance provisions. The compliance evaluation and monitoring framework included in Shield 4 of the Cybersecurity Strategy is a necessary adjustment to remedy currently limited audit and correction provisions which are lacking in contrast to EU and US regulation. The Cyber and Infrastructure Security Centre (CISC) has announced a change in posture in keeping with this, with trial audits of critical infrastructure asset compliance across Q3 and Q4 of 2024, ahead of pivoting from current the education and awareness focus to balancing collaboration and enforcement agendas.

When considering cybersecurity frameworks in legislative instruments, it is prudent policymakers aim to promote frameworks that exhibit a balanced approach to security and resilience. While ISO27001 is a widely recognised and adopted information security standard, it is recommended that it not be included due to comparative weakness in addressing resilience factors in comparison to other frameworks such as NIST, C2M2, and AESCSF. As mentioned previously, frameworks focused on information protection are ill-suited to critical infrastructure assets, particularly those dependent on operational technology. Therefore, adopting more robust frameworks is necessary for ensuring a comprehensive and balanced approach to security and resilience.

The Trusted Information Sharing Network (TISN), established in 2003, has been the primary stakeholder engagement platform between government and industry, consisting of sector groups that facilitate information sharing and collaboration, along with cross-sectorial sharing and collaboration. While TISN aims to promote an open and trusted environment, concerns among participants as to regulator involvement may limit the efficacy of the platform in achieving its objectives. Such reservations may lead to reluctance among participants in sharing of information, undermining the collaborative and transparent environment TISN aims to foster, ultimately impeding the network's ability to facilitate effective risk management and resilience building across sectors.

In sum, Australia's approach to critical infrastructure security and resilience is characterised by a comprehensive integration of legislative mandates, strategic frameworks, and stakeholder engagement aimed at ensuring the robustness and

adaptability of the nation's critical infrastructure in the face of geopolitical destabilisation and evolving sophisticated threats. However, addressing TSIN challenges and closing legislative gaps, such as chemical sector assets, are an essential step forward in enhancing the effectiveness and comprehensiveness of this approach. The mandatory reporting obligations of SoCI, coupled with the capabilities of ASD Assist, significantly bolster Australia's capacity to provide timely and effective support of critical infrastructure assets under attack. Nevertheless, the efficacy of existing compliance measures and government's ability to critically evaluate compliance requires improvement. Planned compliance activities by the CISC in FY24-25 represent a significant step in addressing these gaps and ensuring a more secure and resilient network of critical infrastructure assets.

Although later in adoption of mature critical infrastructure policy and regulation, Australia has developed a regulatory landscape that offers protections comparable to its EU and US counterparts. Notable strengths include the clarity and accessibility of Australian policy, strategy, and regulatory instruments, as well as integration of advanced research activities. The overall maturity of Australia's critical infrastructure will benefit from enhanced compliance activities, with the inclusion of competent assessment authorities highly recommended. The 2023-2030 Cybersecurity Strategy acknowledges opportunities for improvement and proposed remedies reflecting an ongoing commitment to the development of a robust policy and regulatory framework.

8. Research Directions

This paper serves as an interim report, outlining the current state and future directions for enhancing the resilience of Australia's critical infrastructure, informed by the strategic approach of other leading jurisdictions. Further research will aid progress towards quantitative analysis of factors contributing to a demonstrable uplift in critical infrastructure cyber resilience. This includes interviews with government and industry stakeholders, particularly leading Chief Information Security Officers (CISOs) of critical infrastructure sectors, and data collection across critical infrastructure assets.

Further research will benefit from engaging with policy think tanks such as ASPI, and exploring collaboration opportunities with academics and researchers active in the field. Establishing such relationships will aid in developing robust methodologies for assessing security and resilience and ensuring policy recommendations are grounded in empirical evidence that reflects the complexities of managing interdependencies and cross-sectorial cascading consequences. Focus needs to be afforded to identification and quantification of effective strategies for enhancing resilience through stakeholder feedback and integration of ongoing research in the field.

9. Conclusion

Critical Nexus underscores the complex relationships between policy, cybersecurity, and the resilience of critical infrastructure. Research has identified that despite the ongoing efforts of policymakers over the past two decades, critical infrastructure cybersecurity and resilience remains a formidable challenge, with policy and regulatory environments needing to respond and adapt to the fast-paced cyber threat landscape, IT and OT convergence, and technological disruption.

Through comparative analysis of policy frameworks in Australia, the EU, and US, research has identified key factors contributing critical infrastructure cyber security and resilience uplift as being:

- Comprehensive legislative frameworks,
- Mandatory reporting and information sharing,
- Government-assisted incident response,
- Sector-specific guidance and standards,
- Cyber frameworks balancing security and resilience,
- Effective and ongoing stakeholder engagement,
- Compliance evaluation and monitoring, and
- Integration of research activities.

Australia's policy position drives significant advancements in cyber posture and maturity for critical infrastructure assets, with SoCI extending obligations to a broader range of critical infrastructure assets. The nation's approach is characterised by a comprehensive suite of legislative measures, stakeholder engagement, and integration of research and reform activities, placing it on par with its EU and US counterparts. The clarity and accessibility of Australia's policy, strategy, and regulatory instruments, alongside active government assistance through mechanisms like ASD Assist, demonstrate notable strengths.

This research initiative covers a broad spectrum of critical infrastructure cyber security and resilience, presenting findings that will be foundational in supporting further detailed research. A thorough literature review has informed comprehensive discussion, serving as a basis for future engagement with policy think tanks, academia, and senior

industry stakeholders in furthering efforts in this space.

In conclusion, Australia's critical infrastructure resilience efforts are commendable and largely aligned with global best practices. There is clear recognition of existing gaps, and an appetite to progress gap closure. The ongoing enhancement of critical infrastructure security and resilience through responsive policy is imperative for maintaining societal stability, economic prosperity, and national security in times of growing geo-political instability, adversarial grey zone activities, and a dynamic threat environment.

References

[1] Argaw, S. T. *et al.*,(2020), "Cybersecurity of Hospitals: Discussing the challenges and working towards mitigating the risks," *BMC medical informatics and decision making,* vol. 20, no. 1, pp. 146-146, doi:10.1186/s12911-020-01161-7.

[2] Kozak, P., Klaban, I., & Slajs, T., "Industroyer cyber-attacks on Ukraine's critical infrastructure," 2023: IEEE, pp. 1-6, doi:10.1109/ICMT58149.2023.10171308

[3] The Organization for Economic Cooperation and Development (OECD), "Good Governance for Critical Infrastructure Resilience, OECD Reviews of Risk Management Policies," OECD Publishing, 2019.

[4] Bronk, C. & Conklin, W. A.,(2022), "Who's in charge and how does it work? US cybersecurity of critical infrastructure," *Journal of cyber policy,* vol. 7, no. 2, pp. 155-174, doi:10.1080/23738871.2022.2116346.

[5] Semenkov, K., Mengazetdinov, N., & Poletykin, A., "Extending Operation Lifespan of Instrumentation and Control Systems with Virtualization Technologies," 2019: IEEE, pp. 1-5, doi:10.1109/RUSAUTOCON.2019.8867595

[6] Lee, R. M., Assante, M. J., & Conway, T., "Analysis of the Cyber Attack on the Ukrainian Power Grid," 2016. [Online]. Available: https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf

[7] Australia. Department of Home Affairs, *Protecting Critical Infrastructure and Systems of National Significance Consultation Paper*, (2020) [Online] Available: https://www.homeaffairs.gov.au/reports-and-pubs/files/protecting-critical-infrastructure-systems-consultation-paper.pdf [Accessed: Jun. 1,2024]

[8] Furlong, D. E. & Lester, J. N.,(2023), "Toward a Practice of Qualitative Methodological Literature Reviewing," *Qualitative inquiry,* vol. 29, no. 6, pp. 669-677, doi:10.1177/10778004221131028.

[9] Mbanaso, U. M., Abrahams, L., & Okafor, K. C.,(2023), *Research Techniques for Computer Science, Information Systems and Cybersecurity*, 1 ed. Cham: Springer, ISBN: 9783031300301

[10] Warren, M.,(2021), "Australia Critical Infrastructure Protection: A Twenty-Year Journey," *Journal of Information Warfare,* vol. 20, no. 4, pp. 45-56.

[11] European Parliament, 2013. *Cybersecurity Strategy of the European Union*. [Online] Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52013JC0001 [Accessed: May 22,2024]

[12] Atkins, S. & Lawson, C.,(2021), "An Improvised Patchwork: Success and Failure in Cybersecurity Policy for Critical Infrastructure," *Public administration review,* vol. 81, no. 5, pp. 847-861, doi:10.1111/puar.13322.

[13] *Security of Critical Infrastructure Act 2018 (Cth)*. [Online] Available: https://www.legislation.gov.au/C2018A00029 [Accessed: May 22,2024]

[14] *Security of Critical Infrastructure (Definitions) Rules (LIN 21/039)*. [Online] Available: https://www.legislation.gov.au/F2021L01769 [Accessed: May 22,2024]

[15] *Security of Critical Infrastructure (Application) Rules (LIN 22/026)*. [Online] Available: https://www.legislation.gov.au/F2022L00562 [Accessed: May 22,2024]

[16] *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006)*. [Online] Available: https://www.legislation.gov.au/F2023L00112 [Accessed: May 22,2024]

[17] *Security of Critical Infrastructure (Naval shipbuilding precinct) Rules (LIN 23/007)*. [Online] Available: https://www.legislation.gov.au/F2023L00113 [Accessed: May 22,2024]

[18] *Security of Critical Infrastructure (Australian National University) Rules (LIN 22/041)*. [Online] Available: https://www.legislation.gov.au/F2022L00315 [Accessed: May 22,2024]

[19] European Parliament, 2022. *Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (CER Directive)*. [Online] Available: https://eur-lex.europa.eu/eli/dir/2022/2557/oj [Accessed: Jun. 3,2024]

[20] European Parliament, 2022. *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)*. [Online] Available: https://eur-lex.europa.eu/eli/dir/2022/2555/oj [Accessed: Jun. 3,2024]

[21] European Parliament, 2022. *Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. [Online] Available: https://eur-

lex.europa.eu/eli/reg/2022/2554/oj [Accessed: Jun. 3,2024]
[22] European Agency for Cybersecurity (ENISA), *Cybersecurity Certification Framework*. [Online] Available: https://www.enisa.europa.eu/topics/certification/cybersecurity-certification-framework [Accessed: Jun. 3,2024].
[23] Khurshid, A., Alsaaidi, R., Aslam, M., & Raza, S.,(2022), "EU Cybersecurity Act and IoT Certification: Landscape, Perspective and a Proposed Template Scheme," *IEEE access,* vol. 10, pp. 129932-129948, doi:10.1109/ACCESS.2022.3225973.
[24] United States. *Homeland Security Act,* 107th Congress Public Law No. 107-296, 2002.
[25] United States. The White House. (2013). *Presedential Policy Directive/PDP-21 Critical Infrastructure and Security Resilience*. [Online] Available: https://www.cisa.gov/sites/default/files/2023-01/ppd-21-critical-infrastructure-and-resilience-508_0.pdf [Accessed: May 13,2024]
[26] United States Department of Homeland Security. (2013). *National Infrastructure Protection Plan*. [Online] Available: https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf [Accessed: May 14,2024]
[27] United States. *Energy Policy Act,* 109th Congress Public Law No. 109-58, 2005.
[28] United States. *Federal Power Act,* 66th Congress Public Law No. 117-58, 2021.
[29] Congressional Research Services, "The Legal Framework of the Federal Power Act," 2020. [Online]. Available: https://crsreports.congress.gov/product/pdf/IF/IF11411 [Accessed: May 14,2024]
[30] United States. Department of Energy, Federal Energy Regulatory Commission, *Reliability Primer,* n.d. [Online]. Available: https://www.ferc.gov/sites/default/files/2020-04/reliability-primer_1.pdf [Accessed: May 14,2024]
[31] Rosinger, C. & Uslar, M.), "Smart Grid Security: IEC 62351 and Other Relevant Standards," (Power Systems. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 129-146.
[32] United States. The White House. (2013). *Executive Order 13636 - Improving Critical Infrastructure Cybersecurity*. [Online] Available: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity [Accessed: May 18,2024]
[33] United States. The White House. (2024). *National Security Memorandum 22 on Critical Infrastructure Security and Resilience.* [Online] Available: https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/ [Accessed: May 18,2024]
[34] Oxford English Dictionary,(2009), *"security, n."*, 3rd ed. Oxford University Press (in English)
[35] Oxford English Dictionary,(2009), *"resilience, n.".* 3rd ed. Oxford University Press (in English)
[36] Škanata, D.,(2020), "Improving Cyber Security with Resilience," *Annals of Disaster Risk Sciences*, doi:10.51381/ADRS.V3I1.43.
[37] Hausken, K.,(2020), "Cyber resilience in firms, organizations and societies," *Internet of things (Amsterdam. Online),* vol. 11, p. 100204, doi:10.1016/j.iot.2020.100204.
[38] Kott, A. & Linkov, I.,(2019), *Cyber Resilience of Systems and Networks*, 1st 2019. ed. (Risk, Systems and Decisions). Cham: Springer International Publishing, ISBN: 3-319-77492-1
[39] National Academies, *Disaster resilience : a national imperative*, 1st ed. Washington, District of Columbia, United States: National Academies Press, 2012.
[40] Connelly, E. B., Allen, C. R., Hatfield, K., Palma-Oliveira, J. M., Woods, D. D., & Linkov, I.,(2017/03/01 2017), "Features of resilience," *Environment Systems and Decisions,* vol. 37, no. 1, pp. 46-50, doi:10.1007/s10669-017-9634-9.
[41] Panteli, M. & Mancarella, P.,(2015), "The Grid: Stronger, Bigger, Smarter?: Presenting a Conceptual Framework of Power System Resilience," *IEEE power & energy magazine,* vol. 13, no. 3, pp. 58-66, doi:10.1109/MPE.2015.2397334.
[42] Center for Chemical Process Safety,(2018), *Bow Ties in Risk Management: A Concept Book for Process Safety* (Process safety guidelines and concept books). Newark: American Institute of Chemical Engineers, ISBN: 1119490391
[43] Hatch, D. & Geddes, A., "CHASE - Visualising cyber security vulnerabilities and risk," presented at the Hazards Australasia 2019, 2019, HA1910.
[44] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity (NIST CSF)*: U.S. Department of Commerce, 2018.
[45] National Institute of Standards and Technology, *The NIST Cybersecurity Framework (CSF) 2.0*: U.S. Department of Commerce, 2024.
[46] Buzdugan, A. & Căpățână, G., "The Trends in Cybersecurity Maturity Models," Singapore, 2023, vol. 321: Springer Nature Singapore, pp. 217-228, doi:10.1007/978-981-19-6755-9_18
[47] United States. Department of Energy. "Cybersecurity Capability Maturity Model." https://c2m2.doe.gov/about [Accessed: Jun. 4,2024]
[48] Australian Energy Market Operator, "Australian Energy Sector Cyber Security Framework, AESCSF Version 2 - Summary of Chnages." [Online]. Available: https://aemo.com.au/-/media/files/initiatives/cyber-security/aescsf/2023/aescsf-v2-summary-of-changes.pdf?la=en [Accessed; Jun. 5,2024]
[49] *Information security, cybersecurity and privacy protection - Information security management systems - Requirements (ISO/IEC 27001:2023)*, International Organisation for Standardisation, 2023. [Online]. Available: https://www.saiglobal.com [Accessed; Jun. 5,2024]
[50] Malatji, M., Marnewick, A. L., & Von Solms, S.,(2022), "Cybersecurity capabilities for critical infrastructure resilience," *Information and*

computer security, vol. 30, no. 2, pp. 255-279, doi:10.1108/ICS-06-2021-0091.

[51] Pagnacco, A., "Critical Information Infrastructure Protection: Between Cybersecurity and Policymaking," in *Italian Conference on Cybersecurity*. [Online]. Available: https://api.semanticscholar.org/CorpusID:245331222 [Accessed: May 28,2024]

[52] Australia. Foreign Investment Review Board, *Guidance Note 8 - National Security*. 2022. [Online] Available: https://foreigninvestment.gov.au/sites/firb.gov.au/files/guidance-notes/GN08_NationalSecurity_1.pdf [Accessed: Jun. 5,2024]

[53] Australia. Foreign Investment Review Board, *Submission to the Senate Economics Reference Committee on the Foreign Investment Review Framework*. 2016. [Online] Available: https://www.aph.gov.au/DocumentStore.ashx?id=73e10e1d-5eb4-4aaa-9efd-a411a692fb73&subId=407762 [Accessed: Jun. 5,2024]

[54] United States. Department of Defence, National Security Agency, *Joint Cybersecurity Advisory - People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection.* 2024. [Online] Available: https://media.defense.gov/2023/May/24/2003229517/-1/-1/0/CSA_PRC_State_Sponsored_Cyber_Living_off_the_Land_v1.1.PDF [Accessed: Jun. 5,2024]

[55] United Nations. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security.* 2021. [Online]. Available: https://digitallibrary.un.org/record/3934214/files/A_76_135-EN.pdf?ln=en [Accessed: Jun.6,2024]

[56] Kouloufakos, T.,(2023), "Untangling the cyber norm to protect critical infrastructures," *The computer law and security report,* vol. 49, p. 105809, doi:10.1016/j.clsr.2023.105809.

[57] Weiss, M. & Biermann, F.,(2023), "Cyberspace and the protection of critical national infrastructure," *Journal of economic policy reform,* vol. 26, no. 3, pp. 250-267, doi:10.1080/17487870.2021.1905530.

[58] European Parliament. *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (the "NIS Directive")*. [Online] Available: http://data.europa.eu/eli/dir/2016/1148/oj [Accessed: May 30,2024]

[59] Krzykowski, M.,(2021), "Legal aspects of cybersecurity in the energy sector—current state and latest proposals of legislative changes by the eu," *Energies (Basel),* vol. 14, no. 23, p. 7836, doi:10.3390/en14237836.

[60] Ferguson, D. D. S.,(2023), "The outcome efficacy of the entity risk management requirements of the NIS 2 Directive," *International cybersecurity law review,* vol. 4, no. 4, pp. 371-386, doi:10.1365/s43439-023-00097-8.

[61] Pursiainen, C. & Kytömaa, E.,(2023), "From European critical infrastructure protection to the resilience of European critical entities: what does it mean?," *Sustainable and resilient infrastructure,* vol. 8, no. sup1, pp. 85-101, doi:10.1080/23789689.2022.2128562.

[62] Chandler, M. "Ausgrid response to the 2023-30 Australian Cyber Security Strategy: Legislative Reform Consultation Paper " Ausgrid. https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-legislative-reforms/Ausgrid-submission.pdf (accessed.

[63] Australia. Department of Home Affairs. *2023-2030 Australian Cyber Security Strategy*. 2023. [Online] Available: https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf [Accessed: Jun. 6,2024]

[64] Australia. Department of Home Affairs. *Critical Infrastructure Resilience Strategy*. 2023. [Online] Available: https://www.cisc.gov.au/resources-subsite/Documents/critical-infrastructure-resilience-strategy-2023.pdf [Accessed: Jun. 6,2024]