Securitization of Cyber Threats: A Foucauldian Discourse Analysis of Cyber News Articles in 'The Australian' between 2023 and 2024

Elzinga, Ayla

Universiteit Leiden

Securitization of Cyber Threats: A Foucauldian Discourse Analysis of Cyber News Articles in '*The Australian*' between 2023 and 2024

MA Thesis International Relations: Global Conflict in the Modern Era

Faculty of Humanities, Leiden University

Ayla Elzinga

Supervisor: Dr. A. J. Gawthorpe

Second Reader: Dr. V. K. L. Chang

January 31, 2025

Word Count: 14908.

APA 7th ed.

Abstract

There is a growing prominence of the cyber dimension in global conflict in today's modern era. A useful way to study the security agenda around cyber threats is through *securitization theory*. This thesis paper expands the current, dominant scholarly body by focusing on securitization of cyber issues beyond elite speech acts in the United States, with a Foucauldian discourse analysis of cyber feature and opinion articles in *the Australian* newspaper between December 2023 and December 2024. The findings demonstrate that securitization is enforced through speech acts that mobilize meaning through discourse that legitimizes, reifies and dissimulates. The scholarly debate behind cyber operations' cost and effectiveness is dissimulated to legitimize the likelihood of cyber sabotage attacks on critical infrastructure. Furthermore, while traditionally securitization is best known for middle level referent objects like 'the state' or 'national security', a wide range of referent objects are utilized to securitize various cyber threats through linguistic devices. Military synonyms combined with national heritage were employed to reify the more intangible threat of cyber issues. Finally, desecuritizating speech acts were demonstrated to be present at the same time as securitizating speech acts, illustrating a complex interplay in making sense of cyber issues and their future trajectory.

Table of Contents

Abstract 2

Introduction 5

Literature Review 6

Introduction 6

Securitization Theory 6

Securitization Theory and the Copenhagen School 7

Cyber Threats as Securitized? Scholarly Debate 7

Desecuritization 9

Setting the Scene: Australia and Cyber 9

Cyber Threat Perception in Australia 10

Cyber Threat Perception beyond Australia 13

(Traditional) Elite Perceptions: Government and Policy Papers 13

Media Cyber Threat Depictions 14

Methodology 17

Method 17

Sampling and Data Collection 20

Operationalization 20

Validity, Reliability and Limitations 20

Analysis 21

Presupposition of Cyber Operations' Low-cost and Effectiveness 21

The analogy of territoriality in cyberspace 22

Borders and 'the Securable Cyberspace'. 22

Sovereignty as Referent Object and Measure. 24

Critical Infrastructure in Relation to the Nation. 25

Referent Objects: From Middle Level to Individual and System Level 26

Middle Level: National Security. 26

System-level: Democracy, International Rules-based Order and Alliances. 27

Individual Level: Australians and Children. 28

Military Associations 30

Kinetic Weapon Synonyms. 30
Nuclear Synonyms. 31
The Sydney Harbour Bridge: National Heritage 31
Desecuritization 32
Discussion 34
Conclusion 35
Notes 37
References 37
Appendices 46
Appendix A: News Article Sample 46
Appendix B: Coding Overview 49

Introduction

As the cyber dimension of global conflict has become increasingly prominent over recent years, so too has the need for research in this domain. Interestingly though, the catastrophic capacity of cyberattacks has remained disputed for the lack of real-world incidents that demonstrate such a reality. A so-called 'Cyber Pearl Harbor' or "combined attacks [on critical infrastructure] that result in human death and physical destruction and that paralyzes an entire nation" (former United States Secretary of Defense, Mr. Leon Panetta, as cited in Lilja et al., 2024) has yet to take place. In fact, cyber incidents have so far not caused any human casualties and have caused limited, lasting physical destruction (Gomez & Whyte, 2021). Therefore, cyber catastrophe scenarios arguably "still belong for the most part to the domain of our imagination" (Boer & Lodder, 2012, p. 1).

Lewis (2018, p. 5) argues that a tendency to overemphasize cyberattacks against critical infrastructures does not "accurately reflect how cyber operations are used by our opponents, whose primary efforts have concentrated on espionage and crime and whose most damaging actions have manipulated information online to achieve harmful political effect" in the U.S.. Indeed, we are noticing an increase in espionage operations and decline in destructive operations worldwide coming from nation-state and state-affiliated threat actors, posing a more long-term threat (Microsoft, 2023, p. 48). Additionally, out of the 124 worldwide suspected state-sponsored cyber operations recorded by CFR, 101 operations were acts of espionage (81%) in 2024, compared to an already high share of 71% in espionage operations in 2022 (CFR, 2024). Despite this trend and historical evidence, a 'cyber doom' scenario causing physical damage has remained popular (Brito & Watkins, 2011; Lawson, 2013).

This points to a potentially problematic contradiction: a disproportionate focus on an Oppenheimer-like cyber scenario risks overshadowing a multitude of more mundane cyber threats that have demonstrated their frequent – though less exciting – occurrence time and time again (Rader and Wash, 2015). Such 'selective securitization' of one particular type of cyber threat risks a disparity in resource distribution (Brito & Watkins, 2011). This phenomenon presents an opportunity for useful research into gaining a better understanding of threat constructions through the process of 'cyber securitization'. Such research has already been conducted, but has mainly focused on elite cyber threat perceptions and consequent securitization in the U.S..

This research will therefore discuss threat perceptions in an under-researched field;

namely by combining a discourse analysis of cyber securitization by a non-elite actor – the media – in Australia. The main research question will therefore be: '*How are cyber threats securitized in cyber news media coverage in* the Australian *between 2023 and 2024?*'

Literature Review

Introduction

Before continuing with the analysis, it is relevant to sketch the current scholarly debate and how it relates to the main research question of this paper. Firstly, securitization theory will be explained and related to its main scholars, after which its relation to cyber threats is uncovered as it currently stands. Afterwards, a transition into the Australian case will be made, sketching current research on cyber threat perceptions in Australia, as relating most closely to securitization studies which are limited in the case of Australia. Continuing this, a connection will be drawn to cyber threat perceptions beyond Australia, with its current most important insights as relating to securitization theory.

Securitization Theory

Securitization Theory falls under the discipline of security studies, which is a sub-field of international relations. Securitization theory challenges more traditional views of security within International Relations, in that it does not assume that issues *are* threatening and therefore does not view national security policy as a "natural given, but carefully designated by politicians and decision-makers" (Eroukhmanoff, 2018, p. 1). In this way, securitization theory goes against the realist and neorealist assumption that language simply describes a certain reality, in that it acknowledges that this language is *constitutive* to that reality (Balzacq, 2009). Therefore, securitization theory is more aligned with the international relations theory of social constructivism, and is even argued to take "the constructivist insights to their most elaborate form" (Vuori, 2016, p. 64) by socially constructing threats "to gain legitimacy for unpalatable policies that broke the rules of everyday politics" (Vuori, 2016, p. 65).

Securitization Theory and the Copenhagen School

Securitization theory originates from the Copenhagen School consisting of notable scholars like Barry Buzan, Ole Waever and Jaap de Wilde (Stritzel, 2014). Essentially, the concept of security here deals with national security discourse and aims to go beyond a state centric and military emphasis. In this way, securitization theory surpasses the state centrism within traditional security studies, by providing room to adequately address modern anxieties that are a result of a globalized world (Otukoya, 2024). Securitization theory is therefore argued to be useful to study (the construction of) threats posed by non-state actors and by transnational challenges like cyberattacks (Otukoya, 2024).

Studying securitization then, deals with how something is constructed as a threat or as an enemy. In other words: "the exact *definition* and *criteria* of securitization is constituted by the intersubjective establishment of an existential threat with a saliency sufficient to have substantial political effects" (Buzan et al., 1998, p. 25). This notion of an 'existential threat' is key within securitization theory, as a threat is constructed to be existential to the survival of not exclusively the state, but also to a population, an identity or a social order for example (Buzan et al., 1998).

Securitization goes one step beyond *politicization* in that the securitized issue supersedes political debate on its gravity with a discussion whether and what policy and resources from the government are required, and is now being handled with more urgency and speed potentially inflicting normal legal and social violations (Hansen and Nissenbaum, 2009). The securitized issue has now become an existential threat and is accepted as such by the public, as a result of which extraordinary measures are justified in order to tackle the threat (Eroukhmanoff, 2018). An often cited example of this is the increased surveillance since the War on Terror after 9/11 and consequent debates on privacy violations after the Snowden revelations. Securitization of cyber threats can result in similar patterns, where heightened surveillance and personal data collection are justified, consequently challenging legal rights to privacy and freedom of expression (Garhwal & Pareek, 2024).

Cyber Threats as Securitized? Scholarly Debate

As the applicability of securitization theory to a range of new challenges in this globalized world has been disputed, unsurprisingly, its relevance to cyberspace has also been called into question.

Fouad (2019) has engaged with the 'existential threat' dimension of securitization theory and has applied it to the case of cybersecurity. She recognizes that existentiality as such is disputed in the case of cybersecurity, as "the majority of cyber attacks that are seen as the most serious in history were neither objectively existential from a technical viewpoint, nor portrayed as such by the concerned actors" (Fouad, 2019, p. 636). Nevertheless, her empirical multi-actor analysis of cyber threat constructions demonstrates that existentiality is not a precondition for disruptive consequences to be seen as "immanent, urgent, and as serious threats to national security" (p. 636).

Dunn Cavelty (2008, p. 137) argues that the securitization of cybersecurity matters has failed, as she argues there is an absence of "exceptional measures" and acceptance by the audience, by referring to Buzan et al.'s (1998) framework. Nevertheless, Eriksson (2001) argues that the use of extraordinary measures like secrecy and the use of violence as part of securitization is rooted in a "traditional military-bureaucratic realm of security policy" (p. 212) which contradicts its applicability to non-military threats. From Eriksson's point of view then, exceptional measures in this sense are not necessarily a prerequisite for issues to be securitized. This idea is shared in some of the broader securitization literature, as arguably "an action or observable change of behaviour connected to the securitizing move" is what is important (Floyd, 2015, p. 684). It might therefore be arguably more fruitful to look at these as *measures* that indicate a *clear shift* from the status quo.

On a different note, threats like the ones coming from cyberspace have become so intuitively correlated with 'security' (as indicated by the now, widely accepted term of cybersecurity) that the applicability of securitization theory can be disputed according to Ole Waever (2014). From this perspective, viewing the issue as something that was previously not considered to be a security issue like religion or immigration, is less applicable. The notion that cyberspace arguably poses inherent risks and requires security measures is almost natural, in a similar way as nuclear power was quickly discovered to be exploitable for its destructive capacity and has therefore intuitively become a security risk. Following this reasoning, securitization theory has still been argued to be useful if applied to cyber issues. As Waever (2014, 10:53-11:03) states "we can then study how different securitizing actors want to make different referent objects the centre of attention, focus on different threats, different extraordinary measures". This would mean that "the variation – the struggle going on within something that is generally accepted as a security issue – is still a powerful tool to understand" (Waever, 2014, 11:04-11:12). In other words, beyond analyzing speech acts that highlight cyber as a security issue, assessing speech acts for their differing foci on specific

cyber issues (1), what referent object it is that they threaten (2), and what extraordinary measures it is that they emphasize (3) can provide relevant insights. This is exactly what will be done in this research, through identifying these three dimensions and more specifically: *how* these dimensions are legitimized through speech acts and discursive methods.

Desecuritization

Apart from a process of securitization, Waever (1995) also recognized the possibility of *de*securitization, which means a security issue is being moved back into the domain of 'normal' politics. As a result, it de-escalates the heightened threat perception of an issue. As for cybersecurity, the risk is that society itself becomes securitized through fostering fear and mistrust among citizens as well as the tightening of the grip of government and its agencies through increased surveillance and control (Burton & Lain, 2020). Previous literature hardly discusses the exact practices that mark a process of desecuritization. However, from a logical reasoning it can be deducted that desecuritization avoids fostering fear among citizens by precisely empowering them with the tools to combat cyber threats. Furthermore, mistrust can be avoided by promoting collaboration and open conversation among different stakeholders.

When talking about a cyber threat, it is arguably easy to speak of all the ways that make the issue threatening. What is a lot harder to do is to provide tangible solutions to a threat that go beyond abstract, traditionally state-led measures like collecting intelligence and resorting to diplomacy or even force. In order to de-securitize, is therefore important to bring cybersecurity issues out of this restrictive framework and empower citizens and other stakeholders in providing them with more clear-cut advice.

Often times, desecuritization is viewed as something that happens only after securitization. Nevertheless, it is important to note that these two processes can happen at the same time as has been empirically proven before (Austin & Beaulieu-Brossard, 2017).

Setting the Scene: Australia and Cyber

The cyber threat in Australia began to take a serious form as a national security issue in 2008. Then Prime Minister Kevin Rudd stated in his inaugural 2008 National Security Statement to Parliament that cyber threats are now one of Australia's first-rate national security priorities (Rudd, 2008). This was quickly succeeded by the first Australian Defence White Paper to mention the term 'cybersecurity' in 2009 (Delavere, 2019). This was also

when the Cyber Security Operations Centre (CSOC) was created, which consisted of members from the ADF, DSD and DTSO and was established to achieve national security aims (Department of Defence, 2009, as cited in Delavere, 2019). Globally, the Australian government has been a strong supporter of cyber diplomacy, promoting values associated with a free, open, secure and internationally stable cyberspace while safeguarding national security (Feakin & Weaver, 2020). Nevertheless, Australia has been critiqued to use inconsistent cyber terminology and be inconsistent in its cyber policy development (Ladewig, 2018). Furthermore, Ladewig (2018) shows that there are parts of cyber policies and strategic documents that do not comply with current Australian strategies and endorsements of national resilience by the UN. This shows that there is still some ground to gain in terms of adequate cybersecurity awareness and policy development.

Cyber Threat Perception in Australia

(Traditional) Elite Perceptions: Government and Policy Papers.

Since literature on securitization of the cyber threat in Australia is limited, the scope has been broadened to include scholarship that discusses the cyber threat perception in Australia more generally.

Delavere (2019) discursively analyzed the changing perceptions of cybersecurity in Australia and found that between 2000 and 2019 discourses around cybersecurity have significantly changed in the Australian Federal Government's cyber security policies. This shift was marked by a turn from a policing framework towards a national security framework, with popular terms shifting from 'technology enabled crime' to 'cyber warfare' (p. 67) and from 'national intelligence infrastructure' to 'critical infrastructure' (p. 25). Another interesting finding is that state sponsored cyber attacks were not mentioned as an issue in any defense documents up until the 2013 Defence White Paper, which specifically mentions China as a concern (Delavere, 2019).

The study by Delavere is nicely succeeded by Brodtmann et al. (2023), who researched the views of the 46th Australian parliament (2019-2022) on cybersecurity and critical technology issues. They found that state-sponsored cyberattacks on critical infrastructure were seen as the most concerning cyber threat for Australia by its parliamentarians. In this study, state-backed cyber espionage came in second, and state-backed cyber-enabled foreign interference third. One of the parliamentarians explained that

they ranked state-backed activity higher because they thought organized crime is mostly focused on money whereas state actors focus more on collecting intelligence and have the power "to cause massive disruption to their political enemies" (Brodtmann et al., 2023, p. 10).

This heightened threat perception amongst parliamentarians could be explained by a state-backed actor targeting the Australian government and institutions with ongoing hacks as announced in 2020 (BBC News, 2020), after the political parties and parliament's computer network were already targeted with an attempted cyberattack in 2019 (BBC News, 2019). Despite the aversion of a 'catastrophe' so far, it has been shown "that the single most important determination of threat perception is the penetration of a network of computers to which the elite is directly connected" (Lewis, 2014, p. 566) which also explains the Australian case.

Influence of the Media on Cyber Threat Perceptions.

Studying how news media depict the cyber threat is valuable since research shows that "news sentiment has a strong correlation with cyber risk perception" among the public (Xu et al., 2021, p. 1) reaffirming previous findings on risk perception (Liu et al., 1998). The strength of this correlation is more nuanced in other studies, highlighting the importance of other elements like psychographic aspects and cultural values (Kapuściński & Richards, 2016; Ng & Tan, 2022; Mazur, A. 2006). Therefore, news media' influence on individual threat perceptions is difficult to support, yet it can be said that they influence the wider perceptual environment in shaping how individuals view the dominant opinion around them in their community and how much importance the community attaches to it (Mutz & Soss, 1997). Furthermore, *national* perceptions of the cyber threat can be constructed through global media coverage (Lewis, 2014). As an example, Lewis points to great media attention by outlets like the BBC focused on the 'Anonymous' hacker group. Anonymous is a "loosely affiliated group of hackers engaged in 'anti-establishment' dissent and pranks", thereby falling under the category of 'hacktivism' (Lewis, 2014, p. 571). As a result, many governments realized a new type of threat could come from this type of activity. Yet Anonymous' actual success has later been called into question and their activities have been regarded as "a minor irritation" where their "greatest skill seems to lie in writing press releases" (p. 571).

Media Cyber Threat Depictions.

Only one study has researched Australian newspaper cyber threat constructions, which has been reflected on by the original authors on the separate occasions in their 2015 and 2016 papers, respectively (Jarvis et al., 2015 & Jarvis et al., 2016). Their sample consisted of 535 news items, across 7 countries and focused specifically on threat constructions of *cyberterrorism*[1]. This sample included 6 Australian newspapers: The Australian, Australian Telegraph, Australian Financial Review, The Sydney Morning Herald, The West Australian, and The Sun Herald. One of their most important findings in 2015 was that a large part of the analyzed media coverage "expresses real concern over the current or future threat posed by [cyberterrorism]" (Jarvis et al., 2015, p. 73). They point to a discrepancy between this threat construction and actual reality, as whether the capabilities and motives of potential cyberterrorists to involve themselves in this activity are present has often been questioned by other academics (Conway, 2014; Denning, 2012; Giacomello, 2004; Lewis, 2002). This would mean that "news coverage has a constitutive rather than corresponding relationship to the 'reality' of cyberterrorism" meaning that "it is actively involved in the production of this potential security threat" (Jarvis et al., 2015, p. 73).

The same authors reflect more extensively on their findings in their 2016 paper, where they pointed to a surprisingly heterogeneous news media coverage of cyberterrorism instead of a unitary, exaggerated discourse on an imminent threat. The heterogeneity of coverage consisted of differing levels of anxiety; varying ideas on what potential cyberterrorists would look like; differing contexts and varying threatened or referent objects. Another interesting observation by the scholars is a tendency in media threat constructions to use larger referent/threatened objects such as 'the West' and 'the globe' which are inclined to result in greater anxiety (Jarvis et al., 2016, p. 85). This suggests a moving away from more traditional threat constructions around 'the state' and 'national security' as being threatened, and instead indicates "a broader anxiety toward threats against interconnected and potentially vulnerable systems" (Jarvis et al., 2016, p. 85).

While Jarvis et al. (2015 & 2016) provide a great starting point on studying Australian news coverage on the cyber threat, their scope is limited to conceptions of 'cyberterrorism' specifically. As a highly contested concept, news coverage is likely to contain more conventional and accepted terms like 'cyberattacks' and 'cyber crime' which would yield more representative results of the current debate around cyber threats. Furthermore, while their combined approach of news articles from the UK, Australia and U.S. definitely poses a

strength, in the end their research analyzes the big heap of these news articles from 'the West' and does not distinguish between each nation. By zooming in on Australia specifically, clearer patterns might emerge which might tell us more about how the cyber threat is constructed from a more discursive, qualitative perspective.

Audience Perceptions.

Manwaring and Holloway (2021) conducted a survey among 1504 Australian citizens and a focus group with 62 Australian citizens on their threat perceptions of cyber-enabled foreign interference in Australia. They specifically highlight their focus group finding that a substantial amount of Australian citizens' threat perceptions of cyber operations are influenced by media reporting on comparable cyberattacks in other states instead of coverage on Australia. As the authors state "Australian media may well be insufficiently reporting on Australia's challenges relative to, for instance, the "spectacle" of foreign interference in US Presidential elections" (p. 350). The scholars then proceed to translate this finding into a potential indicator for poor knowledge among Australians on actual cyber risks in Australia, where they come from, with which goals and with which capabilities. Potentially another indication follows from this: if multiple studies point to U.S. media' securitization of the cyber threat, there could be a spillover effect to not only Australian media, but also to Australian citizen perceptions.

As research on the Australian case is scarce, the next section will continue to draw parallels with the wider, global context of cyber securitization.

Cyber Threat Perception beyond Australia

(Traditional) Elite Perceptions: Government and Policy Papers

Despite the acknowledged influence of alternative securitizing actors beyond the state within securitization theory, the scholarly body on cyber securitization beyond Australia has still largely focused on official government and political discourse. A majority of academics have analyzed the U.S., but there are also scholars which have analyzed Israel (Cristiano, 2020) for its unique and striking degree of cyber securitization and militarization and Estonia (van Ooijen, 2020) for its cybersecurity leadership after the 2007 cyberattacks targeting its state. Other instances of research include those studying securitization in Russia, the EU,

China and Switzerland (Gorr & Schünemann, 2013; Claessen, 2020; Güven, 2021; Dunn Cavelty & Egloff, 2021). The focus however in this part of the literature review will be on the more elaborate scholarship analyzing American cyber securitization, due to the close alliance and security ties between the U.S. and Australia, including ties concerning cyber security (Kelton & Rogers, 2020). Drawing from both American and Australian scholarship will therefore be useful to see whether similarities or patterns arise in the analysis part of this thesis.

Hjalmarsson (2013) used a qualitative and quantitative content analysis to study the presence of securitizing speech acts on cybersecurity under the Obama Administration in official press releases and speeches by the DoS and the DoD. In the qualitative section he found that securitization is made possible through talking about cyberspace as a "series of connected referent objects, bound together by a network" that is under a continuous threat from a range of adversaries (Hjalmarsson, 2013, p. 20). Furthermore, he found that by referring to known catastrophes like Pearl Harbor and 9/11, the securitizing actors reinforce an existential threat narrative with ripple effects to a range of cyber-connected objects. In this way, "urgent and decisive action to combat the threat posed to the sovereignty of the nation" is justified by Obama and former Secretary of Defense Leon Panetta (p. 20).

Cruz Lobato and Kenkel (2015) draw a comparison between Brazil and the U.S. in their cyber securitization discourse. While analyzing media texts in addition to policy documents, the emphasis lies largely on policy documents. Nevertheless, the authors still arrive at relevant findings. They note that in the case of Brazil, securitization discourse is part of a "slow and restricted process" of securitization (p. 37) by pointing to a discourse on cybersecurity that is broader than defense with limited audience recognition. On the contrary, for the U.S. they found that the securitization process is much more consolidated, evident from a discourse that relies much more strongly on references to the military sector. This points to an evolving of securitization in the U.S. to a process of militarization of cyberspace, which is in line with previous research highlighting a trend among American policy-makers "to frame cyber security as a strategic-military issue and to focus on countermeasures such as cyber offence and defence, or cyber deterrence" (Dunn Cavelty, 2012, p. 104).

Media Cyber Threat Depictions

Despite a scholarly tendency to analyze elite speech acts, securitization theory does acknowledge alternative securitizing actors beyond the state and its elite actors (Waever,

2014). For example, some scholars have veered into a more interdisciplinary domain by focusing on media discourses through employing both a securitization and media framing angle. In his study on securitization processes around terrorism and migration in the U.S., Qadri (2020, p. 2) found that "press framing appears to have influenced public attitudes, above and beyond political elite signals, suggesting that the media can act as an independent and strategic actor". Considering the (sometimes neglected) crucial aspect of audience acceptance within securitization theory, this makes the abovementioned finding of the importance of media within securitization processes all the more relevant (Buzan et al., 1998; Côté, 2016). Not only can media influence public perception on a security issue, media narratives can also be instrumentalized by political actors in drawing attention to an issue as one that ought to be viewed as a threat to security (Tagliapietra, 2021).

Among the few scholars that have combined securitization theory with cybersecurity and a (content and discursive) media analysis is Hart (2012). She applied a quantitative content analysis to news articles on cybersecurity from prominent American newspapers published between 1990 and 2010. In the second part, Hart employed a qualitative framing analysis and applied it to the year of 1990 and 2010 to see how the cybersecurity discourse and framing developed over time. Hart found that in 1990 there was still a strong emphasis on anti-regulatory (cybersecurity regulations should not go at the expense of the economy) and civil liberties (no government monitoring) frames in relation to cybersecurity. By 2010 however, the scales had started to tip as most articles had a strong national security emphasis pointing into the direction of cybersecurity as an accepted threat to national security. Furthermore, by 2010, "increased control and surveillance of cyberspace were portrayed not as a threat to civil liberties, but rather as a necessary measure in order to secure freedom" (Hart, 2012, p. 132), indicating potential successful securitization. What is even more noteworthy is that the media in this case did not only reflect securitization, but were also *used* to securitize. As Hart (2012, p. 132) states: "by understanding that the media is an audience itself, security professionals were able to use journalistic conventions to manipulate the framing of this event so as to change the terms of the cybersecurity debate".

The idea that official security actors are aware of the media's tendency to pick up on their official statements as a 'legitimate primary source' according to journalistic conventions reflects Tagliapietra's (2021) notion that elite actors instrumentalize the media to highlight security issues. While previous research has shown that the majority of sources used in European news media when talking about migration issues are political actors (Berry et al., 2016), within cybersecurity news it is possible that the majority of sources constitutes both

political actors and cybersecurity professionals. This is because commercial threat reports "constitute the largest, and often the only, source of data on cyber operations" which can then consequently influence how policy-makers, academics and media report on threats (Maschmeyer et al., 2021). Private sector reporting on cyber operations has found to be prone to bias on use of unique TTPs, high-profile targeted victims and high-profile threat actors – a bias which can then replicate itself in government and media reporting (Maschmeyer et al., 2021). The reason for such a private sector bias might be commercial (Maschmeyer et al., 2021), but could also be the result of a 'visibility bias' where clandestine cyber operations take a long time to be discovered and as such are underreported despite having a very real influence within the cyber operations landscape (Oppenheimer, 2024).

The replication of this private sector bias or 'double bias' by the media regarding cyber operations was studied by Makridis et al. (2024), who found that more news stories focus on zero-day exploits and provide more coverage on disruptive and destructive cyber operations than on espionage operations (84% to 100% more, Makridis et al., 2024, p. 74). Furthermore, the scholars found that most new stories focus on healthcare and energy sectors, and less stories cover military, finance, government and media sectors.

Fouad (2019) provides another, excellent discourse analysis of the construction of cyber threats by media and other actors in the U.S. from 2003 to 2016. She points out that current scholarship on cyber securitization mostly focuses on official and government discourses which does not accurately reflect reality where cybersecurity narratives are co-produced. Fouad differentiates between *threat* and *attack* attribution, and notes that the government and certain think tanks are inclined to participate in threat attribution (of cyberattacks that have not occurred yet) whereas the private sector focuses more on attack attribution (of cyberattacks that *have* occurred). She argues that it is precisely the *threat* attribution that contributes to securitization, as cyberattacks are attributed to conventional enemies "as a facilitating condition for securitization" (p. 635). This connects to the findings from Boholm's (2021) research, who does not touch on securitization theory but does analyze cyber threats in Swedish news coverage. He found that although newspapers do cover actual events, they mostly demonstrate "amplification without the event" (p. 1), meaning that threats are not connected to actual events which goes against common news conventions.

Given the empirical evidence outside of Australia that points to a reinforcement of cyber securitization by news media using specific cyber threat narratives, this research will be relevant in demonstrating whether similar securitizing patterns can be observed for the Australian case.

Methodology

Australia was chosen as a case study for its unique geographic location, being a western power in close proximity to China, potentially indicating a heightened threat perception. Furthermore, the recently approved revolutionary under-16 social media ban in Australia could indicate a strong presence of heightened threat perception in relation to cyberspace (Ritchie, 2024). The analysis will focus on Australian news media, looking at cyber editorial and opinion pieces in '*The Australian'* between December 1 2023 and December 1 2024. The specific time span was selected to allow for an analysis of the most recent news coverage, with a limit of one year to allow for a qualitative over quantitative analysis. Following Fouad's (2019) reasoning, editorial and opinion pieces were selected instead of general news articles, as these are "presumably more explicit on policies and threat perceptions on the subject matter than news reporting" (p. 634). *The Australian* newspaper was selected for its popularity and for its sufficient amount of opinion pieces on cyber issues. The news articles were obtained through NexisUni, an online archive for news sources.

Method

The method employed is a qualitative discourse analysis, as this method is a good fit for studying securitization discourse, as studying securitization inherently deals with analyzing speech acts. Analyzing what specific cyber threat perceptions are constructed and securitized through Australian news media speech acts can help to gain a better understanding of the process of cyber securitization and can help uncover potential priorities and biases. Discourse analysis looks at language 'above the sentence'. Within this process, the aim is to identify patterns which can go beyond one sentence (Cameron & Panović, 2014). With a qualitative discourse analysis, the goal is not to approach *how many* speech acts occur in a certain category which is reserved for a quantitative approach. Rather, the qualitative approach is more useful to help "illustrate *how* (…) textual and social processes are intrinsically connected and to describe, in specific contexts, the implications of this connection for the way we think and act in the contemporary world" (George, 1994, as cited in Milliken, 1999, p. 225). Therefore, it is useful to study how Australian news articles depict cybersecurity, as a discourse analyses exposes how these textual processes explain how securitization is constructed through speech acts.

The specific type of discourse analysis used is a Foucauldian discourse analysis

(FDA). FDA takes the context of broader structures of meaning, history and society into account. From the Foucauldian view on discourse analysis, individual speech acts only become meaningful from their "interconnection with other texts, the different discourses on which they draw, and the nature of their production, dissemination, and consumption" (Phillips & Hardy, 2002, 3-4). As securitization is something that is socio-politically constructed, it is helpful to look at the context within which a speech act occurs which Foucauldian discourse analysis facilitates. This will be done by taking into account the social and historical contexts that give meaning to a certain speech act. Furthermore, applying securitization theory facilitates further reflection above the sentence level, by identifying patterns in the referent objects (1), main cybersecurity issue (2) and the securitizing actor(s) (3). This reflection will be included for each speech act where meaningful patterns can be observed. From Phillips & Hardy's (2002) conceptualization then, the focus in this analysis will be on connections with other speech acts and texts and the various discourses that are used to trigger certain frames. Furthermore, the three identified categories within securitization theory zoom in mainly on the nature of the *production* of speech acts and their consequent securitization.

A useful framework to help us identify certain meaningful speech acts is provided by Chilton (1987). This author talks of 'critical discourse moments' (CDMs) which are associated with ideological practices. He notes that "the aim is to "mobilise meaning" by (1) legitimising (2) reifying (3) dissimulating" (Chilton, 1987, p. 17) all of which can be uncovered in "the linguistic fine detail of discourse" (Chilton, 1987, p. 12). In this way, "legitimation and reification are accomplished by means of claiming common ground; reification and dissimulation can be accomplished by verbal avoidance tact" (Chilton, 1987, p. 12). At the time, Chilton mentioned this framework would be suitable to study militarization in nuclear discourse, yet he also acknowledged it would be fit for studying other forms of discourse.

This framework is also particularly helpful to look at securitization in cyber discourse. For example, legitimation within cyber securitization can be achieved by emphasizing a particular referent object that is threatened like (conventionally) the state or national security. Reification is also particularly relevant, as arguably it is likely that the intangibility of cyber would go hand in hand with discourse including the use of metaphors that attempt to make cyber issues more tangible in order to increase threat perception. Furthermore, identifying dissimulation can be helpful to lay bare that what is not being said – or deliberately being left out of the picture – in order to achieve a more successful securitization of cyber issues.

Chilton (1987) speaks of metaphors and euphemisms as the two key categories of ideological discourse.

Metaphors

According to Chilton (1987, p. 17), metaphors "trigger frames" and "map frames onto other frames", where the function can be to legitimize, reify or dissimulate. Within metaphors, linguistically speaking the discourse can either be lexical or a grammatical metaphor. Lexical means attributing a certain characteristic to the subject, like saying 'cyberattacks are a pandemic'. A grammatical metaphor can be subdivided into pronouns (a), modal ambiguity (b) and nominalisations (c). Pronouns like 'we' and 'our' can be used to infer shared responsibility and legitimize securitization. Modal ambiguity refers to imposing an uncontested opinion of something or controlling an action that has been decided already by the actor. For example, 'cybersecurity must be the number one priority to protect the nation'. Here, a practical urgency frame is imposed on the referent object that is 'the nation', which serves to legitimize the securitizing action. Nominalisation is the process of transforming a verb into a more abstract noun. This can be used to dissimulate the agent and the one affected, like transforming 'deter' into 'deterrence', which eliminates the need for naming the one who deters and the one who is deterred.

Euphemisms

Euphemisms are used to create a softer impression of something that would otherwise be considered unpleasant or harsh. Euphemisms can again be either lexical or grammatical.

A lexical euphemism refers to replacing one word (group) with another word (group), such as 'kill' with 'neutralize' (Chilton, 1987, p. 17).

Grammatical euphemisms can be subdivided into nominalisations (a), passive constructions (b) and presuppositions (c). A nominalization serves to dissimulate the agent and/or the one affected, for example by saying "nuclear release" (Chilton, 1987, p. 17) which dissimulates the actor and/or the one affected. A passive construction is for example seen in a phrase like 'Cybersecurity training must be installed' which dissimulates by whom and creates distance. A presupposition can be found in a phrase like 'why we must defend against our enemies in cyberspace', which presupposes 'we have enemies in cyberspace' and that 'we must defend'.

Sampling and Data Collection

The final sample was obtained through the online news archive of NexisUni (see Appendix A). Articles were filtered by the time span December 1, 2023 to December 1, 2024 in *The Australian*. The search terms 'Commentary Cyber', 'Cybercrime' and 'Cybersecurity' were used to select relevant news articles fitting in the category of cybersecurity news. For each category, articles were filtered to include only editorial and opinion pieces. Additionally, only articles were selected that placed sufficient focus on cyber issues (at least one paragraph) as opposed to news articles mentioning cyber only once in a listing of a variety of issues for example. This search resulted in a total of 43 articles. For a qualitative approach, this sample size allows for sufficient opportunity for patterns to emerge and to zoom in on specific instances in the analysis. A bigger sample size would require a bigger research scope and is arguably better suited for a quantitative analysis, which is outside of the scope of this specific research. Furthermore, the fact that patterns were reinforced by similar speech acts that kept arising towards the end of the analysis indicates a sufficient level of research saturation.

Operationalization

The final analysis took place by coding all speech acts through categorization (see Appendix B). Each article was numbered in sequence of analysis, to allow for easy reference. Based on the literature review and securitization theory, the categories of 'central cyber issue', 'securitizing actor', 'referent object' and 'emergency measures' were created beforehand. An iterative approach was also utilized here to allow for new categories to emerge throughout the analysis. The coding was executed through indexing the data by "making marginal notes about significant remarks or observations" (Bryman, 2016, p. 581) which later helped to spot patterns and highlight meaningful findings when writing the analysis.

Validity, Reliability and Limitations

The internal validity of this research was affirmed by data developed out of the discourse analysis that was in line with the developed theoretical ideas. The external validity of this research is reinforced by the fact that some of the findings align with previous empirical findings from other case studies in different settings and could therefore be applicable (to a certain extent) to the grand social setting of the process of securitization

(Bryman, 2016). The research's rigor is strengthened by using an iterative process which allows for a critical reflection throughout the analysis.

The external reliability can be a bit tricky to ensure in qualitative research. Nevertheless, the findings should be replicable to the extent that one looks at the similar body of literature in cyber securitization and observes comparable patterns in the news articles (Bryman, 2016). Since only one observer conducted the research, internal reliability is not applicable in this case.

A limitation of this research is that it cannot fully account for the role of the audience within securitization processes. However, news media have been theorized before as both securitizing actors and audience (Hart, 2012). This analysis therefore provides at least some insights into how securitizing moves are picked up on by the media as an audience. However, to gain a more comprehensive understanding of the role of the audience additional research through for surveys, interviews and focus groups is recommended.

Analysis

Presupposition of Cyber Operations' Low-cost and Effectiveness

1) "The **most immediate, low-cost and potentially high-impact vector for sabotage is cyber**." (Uhlmann, 2024, para. 4) *central cyber threat:* cyber sabotage of critical infrastructure // *securitizing actor*: ASIO (Australian Security Intelligence Organization) director-general Mike Burgess
2) "Yet today, saboteurs targeting our infrastructure are **more likely to come with USB sticks than sticks of dynamite**." (Rogers, 2024, para. 3) *central cyber threat:* state-sponsored cyber sabotage of critical infrastructure // *securitizing actor*: Retired Admiral Mike Rogers, former head of US NSA

Quote number 1 is stated as a fact: this is a the grammatical euphemism of a presupposition and 'dissimulates' (Chilton, 1987, p. 17) the entire debate on the unknown cost of a cyberweapon (Smeets, 2016) and the critical discussion on the one-use only nature of zero-day cyberattacks which calls into question the efficiency of certain cyberweapons (Hall & Rowe, 2018). Quote number 1 also does not acknowledge that high risk OT systems such as those operating in nuclear power plants and secretive defense systems use air-gapped systems. This does not mean that they are safe from cyberattacks altogether, but it does imply

that a higher degree of sophistication is required in order to penetrate the system. While a 100% air-gapped system cannot be penetrated purely from the outside, malware can be installed through physical insertion of an infected USB-drive or through manipulating an insider into installing a malicious file. Quote number 2 does acknowledge a USB stick is required, yet fails to reflect on it as a technique that would require a high degree of sophistication. Furthermore, the insertion of a USB stick still requires a physical presence at the site, which eliminates the higher chance of remaining anonymous usually provided through cyber operations. This quote number 2 therefore dissimulates a convincing reason *why* saboteurs are more likely to come with USB sticks than dynamite. These examples show what is *not being said* within the speech acts of number 1 and 2. By factually stating cyber used for sabotage as 'low cost' and as 'more likely to be used than dynamite', therefore implying a higher degree of efficiency, the actual scholarly debate on these ideas very much contesting their factuality is swept under the rug. The dissimulation of this debate therefore serves to legitimize the likelihood of cyber sabotage attacks on critical infrastructure.

The analogy of territoriality in cyberspace

Even though a key agreed upon feature of cyberspace is its transnational and borderless nature, a pattern was identified in speech acts that pointed to cyberspace as something that could be nationally construed. This became clear from references to borders, but also to sovereignty and critical infrastructure in relation to the nation.

Borders and 'the Securable Cyberspace'.

3) "The landmines for a future war have likely already been laid **inside our borders**." (Uhlmann, 2024, para. 1) (A5) *central cyber threat:* cyber sabotage of critical infrastructure // *securitizing actor:* journalist
4) "… the enemy is already **inside the castle walls**." (Uhlmann, 2024, para. 6) (A5) *central cyber threat:* cyber sabotage of critical infrastructure // *securitizing actors*: ASIO, FBI, journalist
5) "… virtual bombs are planted **on home soil** …" (Uhlmann, 2024, para. 16) (A5) *central cyber threat:* cyber sabotage of critical infrastructure // *securitizing actor:* journalist
6) "**Clearly the digital world is the new frontier in crime**." ("Cyber attacks now", 2024, para. 4) (A6) *central cyber threat:* cyberattacks against hospitals and courts of law // *securitizing actor:* journalist

7) “**Our fight against cyber crime is being fought on many fronts** but evolving quickly.” (Owen, 2024, para. 1) (A43) *central cyber threat:* cybercrime // *securitizing actor*: Deloitte Australia

Quote number 2 refers to warnings issued by ASIO (Australian Security Intelligence Organization) and the FBI about China having infiltrated critical infrastructure systems. In this case, using the lexical metaphor of castle walls for borders triggers the frame of a castle that needs to be protected and defended. In this way, reification is used to make the sense that borders require protection more tangible.

This reiteration of borders is also visible in quote number 4 (‘new frontier’) and quote number 5 (‘on many fronts’). By referring to ‘the digital world’ and ‘cybercrime’ as something that can be defended from behind a front or border, it discursively constructs an artificial sense of control. Interestingly enough, this discursive movement of looking at cyberspace as a territory divided by borders has been recognized priorly. Balzacq and Cavelty (2016, p. 196) state that “this type of politics is about the establishment of territoriality and borders in the virtual realm, about nationally owned space and a nationally definable space, based on physical infrastructures”. This creates the idea of a “closured, safe cocoon of a delimited and thus defendable and securable place newly reordered by the state as the sole real guarantor of security” (Balzacq and Cavelty, 2016, p. 196). Only in this case are multiple securitizing actors at play, beyond the state: journalists, intelligence and security agencies and private consulting firm Deloitte. Mainly the latter three actors share an interest in legitimizing their ability to defend from cyber threats that can seemingly appear from any direction. Journalists actively contribute to reinforce this idea through similar reporting in feature articles and opinion pieces. The tendency to legitimize the ability to defend through constructing territoriality fits into a ‘Westphalian process’. Coined by Demchak and Dombrowski (2011, p. 36), this Westphalian process is part of “a new cybered conflict age in which states need to define territorial spaces of safety to reassure their citizens’ safety and economic well-being”. In this way, the Westphalian ideology is instrumentalized by the different securitizing actors to create a sense of control and legitimize their role.

Sovereignty as Referent Object and Measure.

Another striking pattern that was derived from the discourse analysis is a focus on (IT) sovereignty.

8) “Microsoft and Crowdstrike did not issue statements about the outage until about four hours after it left businesses paralysed. This has exposed a gaping flaw in **Australia's IT sovereignty**.” (Lynch, 2024a, para. 15) (A31) central cyber threat: foreign IT dependency, Crowdstrike incident // securitizing actor: journalist
9) “we need to attract all the local tech talent we can if we are **to build our IT sovereign capability**.” (Lynch, 2024b, para. 12) (A39). central cyber threat: foreign IT dependency, Crowdstrike incident // securitizing actor: journalist
10) "downplaying the threat of foreign interference only serves to embolden the CCP and undermines Australia's ability **to protect its sovereignty**".” (Naparstek, 2024, para. 37) (A27) central cyber threat: CCP data collection through Tiktok // securitizing actor: security professional/risk advisor
11) “The US bipartisan consensus gives the Albanese government political cover **to protect our sovereignty** by following the US approach …” (Naparstek, 2024, para. 41) (A27) central cyber threat: CCP data collection through Tiktok // securitizing actor: security professional/growth consultant

What is noteworthy here is that, in the case of quote number 8 and number 9, sovereignty is connected to the Crowdstrike incident. This is interesting, because at the time Crowdstrike had already disclosed that it was *not* a (state) hacker’s doing that caused the system outage. Usually, sovereignty is used as a device of international law to fall back on when another state is threatening to interfere in a state’s (domestic) affairs. It can therefore be called into question to what degree sovereignty is useful to emphasize as a referent object in the case of the Crowstrike incident. If international law can only be breached by states, and in the case of Crowdstrike there was not even an attack but an incident at play, the usefulness of sovereignty as a referent object is strongly debatable.

Arguably then, in the case of quote number 10 and 11 the case made for sovereignty as a referent object is more convincing. Data collection by the CCP through Tiktok that is discussed around these quotes is exercised below the level of the use of force. Sovereignty then, becomes a useful concept to instrumentalize for securitization of this data collection cyber threat (Jančárková, 2023).

Another way to view the use of sovereignty within this discourse is to see it as a measure argued for within the securitization of cyber threats. This is most apparent in quote number 9 "*to build* our IT sovereign capability" and indirectly through quote number 8 "a gaping flaw in Australia's IT sovereignty", implying it requires fixing. Furthermore, in the latter case, the grammatical euphemism of a presupposition assumes that Australia *already* possesses IT sovereignty or otherwise *should strive* for IT sovereignty. This is not surprising, considering the general popularity of wider discourses on technology sovereignty during times of turbulence (Edler et al., 2023). In this way, where international trade based on globalism is otherwise the norm, arguing for IT sovereignty can be seen as a measure justified through the securitization of foreign dependency on IT. This is because at the core of IT sovereignty lies the aim to exercise control over the development of IT technologies and processes (Edler et al., 2023).

Critical Infrastructure in Relation to the Nation.

12) "A smart enemy will do everything … **to break any internal systems keeping the nation on its feet**." (Bergin & Jennings, 2024, para. 7) (A7) central cyber threat: global supply chain warfare (with China) // securitizing actor: Strategic Analysis Australia (think tank)
13) "**Hardening the nation's cyber defences**, **especially those protecting infrastructure and essential services**, must be an increasingly important priority." ("Threats to infrastructure", 2024, para. 4) (A41) central cyber threat: hacking of critical infrastucture // securitizing actor: journalist
14) "… ASD director-general Rachel Noble has been warning about the threat posed by state-based hackers **to critical infrastructure** for years." (Uhlmann, 2024, para. 9) (A5) central cyber threat: hacking of critical infrastructure // securitizing actor: ASD (Australian Signals Directorate), journalist
15) "But the **more worrying danger** is if, or more likely when, a major government agency or **piece of national critical infrastructure is affected**." (Thompson, 2024, para. 9) (A29) central cyber threat: reliance on foreign (cyber) technology // securitizing actor: cybersecurity professional
16) "… so if we get more people entering the profession with diverse backgrounds professionally and personally, **we will be better able to protect critical infrastructure**." ("Driving diversity for", 2024, para. 23) (A33) central cyber threat: cyberattacks on critical infrastructure // securitizing actor: cybersecurity professional

As previously suspected and demonstrated in the literature review, the referent object of critical infrastructure was indeed a reoccurring pattern. Here it is useful to analyze how cyber threats are discursively securitized by means of critical infrastructure as a referent object. In the case of quotes number 1 and 2, (critical) infrastructure is linked to "keeping the nation on its feet" and to requiring special protection from the "nation's cyber defenses". By using the reification of "keeping the nation on its feet" for critical infrastructure, the threat of an attack on that very infrastructure is made more tangible. It implies that it is the very foundation of the nation upon which it rests, and swiping that away would be the literal downfall of the nation. "Hardening the nation's cyber defenses" functions as a measure arguing for an increase in cyber defense resources which is then justified through the referent object of critical infrastructure as threatened by hacking.

That a particularly high focus is placed on critical infrastructure as the referent object of cyber threats, is nicely illustrated by quotes number 4 and 5. In quote 4 cyberattacks on national critical infrastructure and major government agencies are stated to be "the more worrying danger" as opposed to a data breach of club patrons in New South Wales. "*Are* the more worrying" serves as a modal ambiguity for strengthening the threat of a cyberattack on critical infrastructure while at the same time dissimulating why this is the case. In quote number 5, more cybersecurity professionals are stated as the measure needed to combat the referent object of critical infrastructure threatened by cyberattacks. What is interesting here is that critical infrastructure is the *only* referent object named without it being the main topic of the news article. This dissimulates the range of other cyber issues that could benefit from more cybersecurity workers and legitimizes the securitization of cyberattacks on critical infrastructure specifically.

Referent Objects: From Middle Level to Individual and System Level

While traditionally securitization is best known for middle level referent objects like 'the state' or 'national security', from the analysis it became clear that in the case of cyber threats in Australia a wide range of referent objects are utilized to securitize cyber threats. This is done .

Middle Level: National Security.

17) "The outage was **not just** a matter of inconvenience that stopped people from paying for groceries at check-outs or complete online banking, **but a matter of national**

security." (Lynch, 2024a, para. 5) (A31) central cyber threat: Crowdstrike incident // securitizing actor: journalist

18) "As the attacks demonstrate, it is also **a weak link in our national security**." ("Cyber attacks now", 2024, para. 4) (A6) central cyber threat: cyberattacks against hospitals and courts of law // securitizing actor: journalist

In quote number 17, the importance of national security as the referent object threatened by the Crowdstrike incident is reinforced by placing it above 'a mere inconvenience'. In quote number 18, Australian national security as a referent object is reinforced by referring to its weakness and to the cyberattacks against Victoria's court system and the St Vincent Health Australia. It is noteworthy that in both cases this amplification goes hand in hand with an actual cyber event, which is in line with news conventions.

System-level: Democracy, International Rules-based Order and Alliances.

On the system-level, various referent objects were identified that were utilized in different contexts.

19) "It [Beijing] runs a relentless information war aimed at **undermining our democracy and our alliances**." (Uhlmann, 2024, para. 20) (A5) central cyber threat: cyber-enabled influence operations (by CCP) // securitizing actor: journalist

20) "To voice no objection no matter what it decides to do **in the world, our region** or our nation." (Uhlmann, 2024, para. 25) (A5) central cyber threat: cyber-enabled influence operations (by CCP) // securitizing actor: journalist

21) "A smart enemy will do everything to isolate Australia from **its allies** …" (Bergin & Jennings, 2024, para. 7) (A7) central cyber threat: global supply chain warfare (with China) // securitizing actor: Strategic Analysis Australia (think tank)

22) "Under Xi's rule, Australia and Indo-Pacific allies have been subjected to aggression ranging from … state-sanctioned cyber attacks targeting critical infrastructure, foreign interference campaigns undermining **democratic institutions** …" (Chambers, 2024a, para. 7) (A18) central cyber threats: [stated above] // securitizing actor: journalist

23) "… to ensure that we uphold the **international rules-based order** …" (Lam and Lynch, 2024, para. 15) (A22) central cyber threats: cyberattack by Russian hacker against Medibank // securitizing actor: Australian minister of foreign affairs

What is immediately noteworthy here is that all of these cyber threats are linked to either China or Russia, which seems to trigger to need for using a referent object at the system-level. This tendency in media threat constructions to use larger referent objects aligns with prior research (Jarvis et al., 2016), yet has not been linked to nation-affiliated cyber threats before. This greater anxiety invoked by using system-level referent objects can be utilized to heighten threat perception of cyber threats coming from other nations or nation-sponsored groups. It can also be logically explained by viewing the cyber threat as stemming from a state that has a different ideology, resulting in a macro-level referent object (Buzan & Waever, 2009). In this way, the level of the state is transcended, by referring to higher, interconnected systems like "the international rules-based order" in quote number 23 or "our region" in quote number 20.

Surprisingly, alliances as a referent object were also underscored in some news articles. This is apparent in quote number 19 "our alliances" and quote number 21 "its [Australia's] allies". 'Undermining' of these alliances and 'isolation' from these allies are used to legitimize the cyber threats of cyber-enabled influence operations and global supply chain warfare. This legitimization also stems from the importance of alliances to Australia's security in the Asia-Pacific, particularly its alliance with the US (ANZUS) (Beeson, 2015).

What is noteworthy here though, is that there is a tension at play here in the referent object of alliances. Australians place greater value on the US alliance during Obama's and Biden's presidencies than during Bush's and Trump's (Lowy Institute, 2024). The news articles from quote number 19 and 21 were published under Biden's presidency. This would mean that the use of 'alliances' and 'allies' as referent objects of cyber threats was likely more effective for cyber securitization at the time than today and in the foreseeable future under Trump's presidency.

Individual Level: Australians and Children.

24) "… we need to make sure our cyber security workforce is equipped with the right skills to protect **us all** against fast-moving cyber threats." (Owen, 2024, para. 15) (A43) *central cyber threat:* cybercrime // *securitizing actor*: journalist

25) "It is time for the Albanese government to get serious … following the US TikTok crackdown, updating electronic surveillance laws, … joining global pressure campaigns targeting tech giants and legislating powers giving security agencies tools and resources they need to protect **families, children** and our economic interests." (Chambers, 2024b, para. 13) (A17) central cyber threats: Chinese and Russian foreign-

interference (through Tiktok) and state-sponsored cyber attacks targeting critical infrastructure // securitizing actor: journalist

26) "There is **no doubt our children are paying the price**." (Miller, 2024, para. 5) (A40) central cyber threat: tech monopolies // securitizing actor: chairman news corporation Australia
27) "It's time for a digital environment that protects vulnerable people rather than preys on them. It's time to protect **our children, our parents** and our national identity." (Miller, 2024, para. 25) (A40) central cyber threat: tech monopolies // securitizing actor: chairman news corporation Australia

In the case of quote number 24, the lexical pronoun of 'us' is used as a metaphor. The frame of "all of us" is then triggered to infer shared victimization and legitimize the securitization of cybercrime by promoting the measure of a 'well-equiped cyber security workforce'.

However what is most striking here is the use of children and families/parents as referent objects in quote number 25, 26 and 27. In the case of quote number 25, "giving security agencies tools and resources they need" are named as an extraordinary measure to protect children and families from Chinese and Russian foreign interference through Tiktok. In quote number 28 children and parents are not only constructed as a referent object through emphasizing the protection they need as "vulnerable people", but also through a reification of the alternative. The alternative is that they would be 'preyed on' by tech monopolies, which serves to make the threat more tangible. Even though tech monopolies are no human threat, use of 'preyed on' does share similarities with an animalistic dehumanization which has been shown throughout history can be very effective in heightening threat perception. More importantly perhaps, attributing animalistic characteristics legitimizes taking consequent (extraordinary) measures against the threat. By linking the article from quote 26 and 27 to the article of 25, we can place this in a bigger debate. These articles share the same cyber threat, namely tech monopolies and specifically foreign interference by China through TikTok. Advocating for extraordinary measures like "updating electronic surveillance laws" and "giving security agencies tools and resources they need" then become justified.

Military Associations

Kinetic Weapon Synonyms.

28) "**The landmines for a future war** have likely already been laid inside our borders." (Uhlmann, 2024, para. 1) (A5) *central cyber threat:* cyber sabotage of critical infrastructure // *securitizing actor:* journalist
29) "**The bombs may never be detonated** but the intention is clear, and hostile." (Uhlmann, 2024, para. 2) (A5) *central cyber threat:* cyber sabotage of critical infrastructure // *securitizing actor:* journalist
30) "… **virtual bombs** are planted on home soil …" (Uhlmann, 2024, para. 16) (A5) *central cyber threat:* cyber sabotage of critical infrastructure // *securitizing actor:* journalist
31) "… scammers are **sharpening** their **digital weapons** …" (Keane, 2024, para. 1) (A12) *central cyber threat:* online scammers // *securitizing actor:* journalist

What is noteworthy here, is that in all four cases lexical metaphors are used to reify cyber threats. Quote numbers 28, 29 and 30 refer to the same article, where different metaphors were used in various ways. By referring to 'landmines' and '(virtual) bombs' that can be 'detonated', the journalist makes the threat of cyber sabotage of critical infrastructure more tangible. By using these lexical metaphors, a frame of conventional, kinetic weapons is triggered in order to securitize the threat. Combined with the earlier identified use of "borders" and "home soil" as analogies for territoriality, together these frames reify and legitimize the cyber threat.

In quote number 31 a similar process can be observed, as a lexical metaphor of a 'weapon' that can be 'sharpened' is used. This serves to reify the tactics used by online scammers, to make it more tangible and securitize online scams.

These observations align with the intangibility of cyber which creates the need to use metaphors that attempt to make cyber issues more tangible in order to increase threat perception. It is noteworthy that in each of the cases characteristics or synonyms from kinetic weapons are used, which people are likely more familiar with and which can trigger many frames from earlier (mediatized) experiences.

Nuclear Synonyms.

In line with the previous observation, but more specific and worth separating is the use of nuclear synonyms.

32) "Global IT **meltdown** shows faults spread like lightning." (Fortson, 2024, title) (A10) *central cyber threat:* CrowdStrike incident // *securitizing actor:* journalist
33) "… last year's network **meltdown** …" (Lynch, 2024c, para. 6) (A21) *central cyber threat:* 2023 Optus outage // *securitizing actor:* journalist
34) "… world's biggest tech outage, which is arguably a thousand times worse than Optus's **meltdown** last year." (Lynch, 2024b, para. 1) (A39) *central cyber threat:* CrowdStrike incident // *securitizing actor:* journalist

Using the lexical metaphor of a 'meltdown' by applying it to an IT outage triggers the frame of a nuclear disaster. This serves to reify the threat and securitize it. In the case of quote number 32 "spread like lightning" is another lexical metaphor used to emphasize the uncontrollable speed with which the outage spread across systems running on CrowdStrike software. This reifies its uncontrollable nature and further legitimizes the securitization of the threat.

The Sydney Harbour Bridge: National Heritage

Deserving its own category are the speech acts involving reference to bridges, or more specifically: the Sydney Harbour Bridge.

35) "Another insider labelled the -attempts to control critical infrastructure as the "electronic equivalent" of Chinese commando groups **putting bombs underneath bridges** or on high-voltage pylons for the purposes of blowing them up during a war." (Uhlmann & Lewis, 2024, para. 6) (A20) *central cyber threat:* Volt Typhoon critical infrastructure infiltration // *securitizing actor:* government inside source, journalists
36) "This is something that should be shouted from the rooftops because it is **no different to planting a bomb on the Sydney Harbour Bridge**." (Uhlmann, 2024, para. 14) (A5) *central cyber threat:* Volt Typhoon critical infrastructure infiltration // *securitizing actor:* government inside source, journalists

The significance of using the Sydney Harbour Bridge as a lexical metaphor for cyber sabotage cannot be underestimated. The Sydney Harbour Bridge is considered national

heritage and is the main pipeline between the North and South of Sydney. This bridge is not only symbolic to the city, but also to the country. Its sight is iconic for its background during the firework displays every new year's eve, with Australia being the first country in the world to transition into every new year. Architect Francis Greenway wrote in his letters to *The Australian* in 1825 that the bridge would "give an idea of strength and magnificence that would reflect credit and glory on the colony and the Mother Country" (The Australian, 1825, as cited in Museums of History, n.d., para. 2). Since then, it has become "a symbol of Australian progress, modernity and ingenuity" (National Museum Australia, n.d., para. 3).

To use the metaphor of a bomb planted on the Sydney Harbour Bridge for cyber sabotage by China triggers a frame that the average Australian will hold very dearly and could not imagine its country without. It is almost as though a bomb were to be planted at the heart of the nation, of progress and stability, which would consequently be destructed upon its explosion.

Desecuritization

Perhaps the most revealing finding of all, was that also multiple patterns of desecuritization could be identified. This confirms previous empirical findings within securitization studies that securitization is less black and white then it is sometimes made out to be (Austin & Beaulieu-Brossard, 2017). The same can now also be said for cyber issues specifically, which are not only securitized through various means, but also at the same time *de*securitized.

37) "Millions of dollars already have been lost by Australians in online shopping scams this year, but **there are ways to protect yourself**." (Keane, 2024, para. 2) (A12) *central cyber threat:* online scammers // *desecuritizing actor:* journalist

38) "Our AustraliaNOW data shows that timely, accurate and transparent information - with clarity about the **steps customers can take to protect themselves** - rebuilds brand trust, repeat purchase and advocacy." (Randell, 2023, para. 11) (A13) *central cyber threat:* cyber breaches // *desecuritizing actor:* CEO market research

Quotes number 12 and 13 emphasize that citizens can take steps to protect themselves. The difference is that for quote number 13, the article does not aim to provide these steps and is therefore only hinting at desecuritization. Quote number 12 however, is followed by actual

steps the reader can take to avoid online scams, which effectively works to desecuritize the issue by empowering the reader.

39) "This **includes regular stress tests** and **updates to security protocols**. This also ensures any compromised infrastructure can be rapidly recovered." (Rajkovic, 2024, para. 13) (A14) *central cyber threat:* cyberattacks on the Olympics // *desecuritizing actor:* managing director cybersecurity company
40) "Comprehensive campaigns should **teach attendees** how to spot phishing attempts, avoid scams, and report suspicious behaviour." (Rajkovic, 2024, para. 14) (A14) *central cyber threat:* cyberattacks on the Olympics // *desecuritizing actor:* managing director cybersecurity company
41) "**Employee education** is crucial in the fight against cyberthreats." (Sreedhar, 2024, para. 12) (A26) *central cyber threat:* cyberbreach of personally identifiable information // *desecuritizing actor:* IT management company

In each of these three quotes, pointing to actual steps that can be taken to tackle the cyber threat helps to desecuritize the cyber threat. What is important here is that the solution does not simply lie with the state, but that citizens are discursively framed as playing a role in tackling the threat in a way that is tangible and non-abstract. In this way, excessive fear and mistrust that can normally result out of securitization are averted by empowering citizens through speech acts of desecuritization here.

There is also a careful first attempt at broadening the debate beyond high-profile, state-sponsored malicious attacks that was featured in one of the news articles.

42) "But **there's lots of scenarios that are non-malicious. We genuinely need organisations not to just think about** the Russians and Chinese or North Korean hackers, but also about an all-hazards approach." (O'Dowd, 2024, para. 18) (A37) *central cyber threat:* state-sponsored hacks // *desecuritizing actor:* University Professor

The idea of non-malicious (insider) cyber issues is widely recognized in cybersecurity education, but deviates from what is usually reported in news media as all of the other quotes that have been discussed in this analysis also demonstrate. This shows that this tension is starting to show in current news articles as well, where actors try to desecuritize the

disproportionate focus on malicious, nation-state sponsored cyberattacks over a range of other cyber issues. Pointing to "a need" to think about other types of cyber threats demonstrates that a broader cyber agenda needs to be installed in order to deal with the cyber issues of today and tomorrow. Combining this with the empowering of citizens in quotes number 37 to 41 means that not only the *types* of cyber issues that are put on the agenda are contested, but also the *measures* that ought to be taken to adequately address the issues. The scope is expanded beyond state-centered measures that focus on control, to empowering citizens with hands-on steps they can take. This results in the sense that cyber issues are not necessary *disastrous* requiring strong, state-led measures, but are manageable through the right, societal efforts. It will be relevant to see whether these tendencies of desecuritization will take even stronger forms in future news discourse as cyber becomes less novel.

Discussion

The analysis demonstrated that cyber threats are securitized in cyber news media coverage in *the Australian* between 2023 and 2024 by a range of discursive methods. It was found that securitization is enforced through speech acts that give meaning through discourse that legitimizes, reifies and dissimulates. The current scholarly debate on cyber operations' cost and effectiveness is dissimulated in order to legitimize the likelihood of cyber sabotage attacks on critical infrastructure. Although the amount of speech acts was not the goal of this research, it does explain in part why in previous research it was found that Australia's parliamentarians experience heightened threat perceptions of cyber sabotage attacks on critical infrastructure specifically (Brodtmann et al., 2023). When more nuanced, perhaps more technically complex, characteristics behind cyber operations are left out of securitizing news media speech acts, it is perhaps not surprising that threat perceptions heighten. We fear what we do not comprehend, yet it is precisely a more technical and strategic background that is required to nuance our understandings of cyber issues and the challenges they present.

In previous research, newspapers were shown to mostly amplificated "without the [cyber] event" (Boholm, 2021, p. 1) sticking to threats instead of actual attacks that took place, going against common news conventions. The findings of this paper indeed demonstrated a range of securitized cyber *threats* that were not necessarily connected to actual events. However, in the case of an actual event – the CrowdStrike outage – more 'traditional' securitizing conventions were used that were based on sovereignty and national security. This is quite interesting, considering the CrowdStrike incident was caused by a human, non-malicious error. Yet, the mere dependency on international technologies that

could be subject to these insider mistakes, was enough to securitize the issue reverting to advocacy for more sovereignty as national security was discursively employed as the referent object. When looking at this securitizing move up close then, its effectiveness can be disputed. This is because insider, non-malicious errors can happen anywhere, both on domestic and international territory and advocating for more sovereignty by using more domestic technologies would not erase this risk. Although measuring effectiveness (through audience acceptance) of the securitizing move was outside of the scope of this research, it would be interesting for future research to investigate the success of such acts further.

The finding that military synonyms and national heritage were used as synonyms to legitimize cyber securitization, is quite surprising. This is because previous literature has not shed much light on this phenomenon, arguably because the phenomenon is quite new compared to other political issues that have been around for longer. It does confirm the intuitive idea that cyber is rather intangible and would therefore benefit from reification acts that trigger more conventional frames. As the analysis shows, this has indeed been done by using kinetic weapons and nuclear weapons specifically, as synonyms. Furthermore, the reification of the Sydney Harbor Bridge is potentially quite powerful considering the national and cultural significance it beholds. Securitizing cyber sabotage of critical infrastructure by these means then becomes more tangible and potentially, more threatening to audiences.

Perhaps most noteworthy is the finding that there are patterns of *desecuritization* visible which operate in tension with the other, securitizing moves. This is in line with some previous empirical findings in securitization cases studies more generally (Austin & Beaulieu-Brossard, 2017). Nevertheless, this finding is still considerably meaningful as the idea that securitization and desecuritization moves can happen alongside one another instead of chronologically is not widely recognized in securitization literature yet. For this finding to emerge in relation to a (relatively new) securitization topic – of cyber threats – that have not been connected before serves as a meaningful contribution to the scholarly body.

Conclusion

This thesis has answered the research question '*How are cyber threats securitized in cyber news media coverage in the Australian between 2023 and 2024?*'. A Foucauldian discourse analysis of cyber feature and opinion articles in *the Australian* newspaper between December 2023 and December 2024 was utilized to study securitization and expand on existing research focusing on elite actors and the United States. It was shown that cyber threats are securitized through speech acts using legitimization, reification and dissimulation,

which mobilize meaning through the use of synonyms and euphemisms, as well as the use of referent objects on the individual, middle and system levels. The scholarly debate behind cyber operations' cost and effectiveness is dissimulated to legitimize the likelihood of cyber sabotage attacks on critical infrastructure. Furthermore, while traditionally securitization is best known for middle level referent objects like 'the state' or 'national security', a wide range of referent objects are utilized to securitize various cyber threats through linguistic devices. Military synonyms combined with national heritage were employed to reify the more intangible threat of cyber issues. Finally, desecuritization speech acts were demonstrated to be present at the same time as securitization speech acts, illustrating a complex interplay in making sense of cyber issues and their future trajectory.

Future research is advised to further investigate the demonstrated tension between securitization and desecuritization, as an under-accepted phenomenon. Additionally, future studies can contribute much to the cyber securitization body by researching audience perceptions and their role in the acceptance and success of securitization, which was unfortunately beyond the scope of this thesis research. As a relatively new research domain, general studies on the securitization of cyber issues in particular can provide additional new insights.

This thesis paper adds relevant insights to the scholarly body, by confirming and expanding on previous findings from both securitization research and cyber threat perceptions' studies. It has demonstrated that the cyber issues are not only securitized along various dimensions in news articles, but also challenged by speech acts aligning with *desecuritization*. Understanding how this securitization comes about has been effectively achieved by laying bare the discursive processes that constitute it. This also provides considerable impetus for future, valuable research.

Notes

1. While the exact definition of cyberterrorism remains disputed and problematic, scholars largely agree that it involves the use of digital means to inflict harm or destruction (Jarvis and Macdonald, 2015).

References

Austin, J.,, & Beaulieu-Brossard, P. (2017). (De)securitisation dilemmas: Theorising the simultaneous enaction of securitisation and desecuritisation. *Review of International Studies*, *44*, 1-23. 10.1017/S0260210517000511.

Balzacq, T. (2009). Constructivism and security studies. In M. Dunn Cavelty & V. Mauer (Eds.), *The Routledge Handbook of Security Studies* (1st ed., pp. 56-72). Routledge.

Balzacq, T., & Dunn Cavelty, M. (2016). A Theory of Actor-Network for Cybersecurity. *European Journal of International Security*, *1*(2), 176-198.

BBC News. (2019, February 8). Australia parliament hit by cyber-hack attempt. https://www.bbc.co.uk/news/world-australia-47166590

BBC News. (2020, June 19). *Australia cyber attacks: PM Morrison warns of "sophisticated" state hack*. https://www.bbc.com/news/world-australia-46096768

Beeson, M. (2015). Invasion by invitation: the role of alliances in the Asia-Pacific. *Australian Journal of International Affairs*, *69*(3), 305–320. https://doi.org/10.1080/10357718.2014.988207

Bergin, A., & Jennings, P. (2024, September 26). Defence torpor leaves us exposed to the China threat. *The Australian*.

Berry, M., Garcia-Blanco, I. and Moore, K. (2016), Press Coverage of the Refugee and Migrant Crisis in the EU: A Content Analysis of Five European Countries, Geneva, United Nations High Commissioner for Refugees, 2016, http://www.unhcr.org/56bb369c9.html.

Boer, L. J. M., & Lodder, A. R. (2012). Cyberwar: What Law to Apply? And to Whom? In W. R. Leukfeldt & W. Stol (Eds.), *Cyber Safety: An Introduction*. The Hague: Eleven international publishing.

Boholm, M. (2021). Twenty-five years of cyber threats in the news: a study of Swedish newspaper coverage (1995–2019), *Journal of Cybersecurity*, *7*(1), 1-23. https://doi.org/10.1093/cybsec/tyab016

Brodtmann, G., Caples, A., Cave, D. & Keast, J. (2023). What do Australia's parliamentarians think about cybersecurity and critical technology? *Australian Strategic Policy Institute*. https://www.aspi.org.au/report/what-do-australias-parliamentarians-think-about-cybersecurity-and-critical-technology

Brito, J., & Watkins, T. (2011). Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy. *Harvard National Security Journal*, *39*. https://ssrn.com/abstract=1830625

Burton, J., & Lain, C. (2020). Desecuritising cybersecurity: towards a societal approach. *Journal of Cyber Policy*, *5*(3), 449–470. https://doi.org/10.1080/23738871.2020.1856903

Buzan, B., Wæver, O. and de Wilde, J. (1998). *Security: A New Framework for Analysis*. Boulder: Lynne Rienner.

Buzan, B., & Waever, O. (2009). Macrosecuritisation and security constellations: reconsidering scale in securitisation theory. *Review of International Studies*, *35*(2), 253–276. doi:10.1017/S0260210509008511

Cameron, D., & Panović, I. (2014). *Working with written discourse*. SAGE Publications, Ltd, https://doi.org/10.4135/9781473921917

CFR (2024). Tracking State-Sponsored Cyberattacks Around the World. Council On Foreign Relations. https://www.cfr.org/cyber-operations/

Chambers, G. (2024a, January 17). PM must stand up to Beijing and its veiled warnings. The Australian.

Chambers, G. (2024b, April 24). PM must log on to our clear and present dangers. The Australian.

Chilton, P. (1987). Metaphor, Euphemism and the Militarization of Language. *Current Research on Peace and Violence*, *10*(1), 7–19. http://www.jstor.org/stable/40725053

Claessen, E. (2020). Reshaping the internet – the impact of the securitisation of internet infrastructure on approaches to internet governance: the case of Russia and the EU. *Journal of Cyber Policy*, *5*(1), 140–157. https://doi.org/10.1080/23738871.2020.1728356

Conway, M. (2014). Reality check: assessing the (un)likelihood of cyberterrorism'. In T. Chen, L. Jarvis, & S. Macdonald (Eds.), *Cyberterrorism: Understanding, Assessment and Response*. New York, NY: Springer.

Côté, A. (2016). Agents without agency: Assessing the role of the audience in securitization theory. *Security Dialogue*, *47*(6), 541–558. https://www.jstor.org/stable/26293812

Cristiano, F. (2020). Israel: cyber defense and security as national trademarks of international legitimacy. In S. Romaniuk & M. Manjikian (Eds.), *Routledge Companion to Global Cyber-Security Strategy*. https://scholarlypublications.universiteitleiden.nl/handle/1887/138587

Cruz Lobato, L. & Kenkel, K. M. (2015). Discourses of cyberspace securitization in Brazil and the United States. *Revista Brasileira de Política Internacional*, *58*(2), 23-43. https://www.scielo.br/j/rbpi/a/zDC3D9BWxQvBxk56CmLdckJ/?format=pdf&lang=en

Cyber attacks now a direct threat (2024, January 2). *The Australian*.

Delavere, S. (2020). Cybercrime to cyberwar: changing strategic perceptions of cyber security in Australia (Version 1). Macquarie University. https://doi.org/10.25949/19434404.v1

Demchak, C. C., & Dombrowski, P. (2011). Rise of a Cybered Westphalian Age. *Strategic Studies Quarterly*, *5*(1), 32–61. http://www.jstor.org/stable/26270509

Denning, D. (2012). Stuxnet: What Has Changed? *Future Internet*, *4*(3), 672-687. DOI:10.3390/fi4030672

Driving diversity for a secure cyber future (2024, May 19). *The Australian*.

Dunn Cavelty, M. (2008). *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. Routledge. https://www.researchgate.net/publication/277714726_Cyber-Security_and_Threat_Politics_US_Efforts_to_Secure_the_Information_Age

Dunn Cavelty, M. (2012). The Militarisation of Cyber Security as a Source of Global Tension. In D. Möckli & A. Wenger (Eds.), *Strategic Trends 2012: Key Developments in Global Affairs* (pp. 103-124). Center for Security Studies, ETH Zurich. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Strategic-Trends-2012.pdf

Dunn Cavelty, M., & Egloff, F. J. (2021). Hyper-Securitization, Everyday Security Practice and Technification: Cyber-Security Logics in Switzerland. *Swiss Political Science Review*, *27*(1), 139–149. https://doi.org/10.1111/spsr.12433

Edler, J., Blind, K., Kroll, H., & Schubert, T. (2023). Technology sovereignty as an emerging frame for innovation policy: Defining rationales, ends and means. *Research Policy*, *52*(6), 1-13. https://doi.org/10.1016/j.respol.2023.104765.

Eriksson, J. (2001). Cyberplagues, IT, and Security: Threat Politics in the Information Age. *Journal of Contingencies and Crisis Management*, *9*(4), 200–210. https://doi.org/10.1111/1468-5973.00171

Eroukhmanoff, C. (2018). Securitization Theory: An Introduction. E-International Relations Theory, E-IR Foundations Beginner's Book (pp. 1-4). E-IR Foundations Beginner's Book.

Feakin, T., & Weaver, J. (2020). Cyber diplomacy. In E. Tikk & M. Kerttunen (Eds.), *Routledge Handbook of International Cybersecurity* (pp. 277–285). https://doi.org/10.4324/9781351038904-29

Floyd, R. (2015). Extraordinary or ordinary emergency measures: what, and who, defines the 'success' of securitization? *Cambridge Review of International Affairs*, *29*(2), 677–694. https://doi.org/10.1080/09557571.2015.1077651

Fouad, N. (2019). The Peculiarities of Securitising Cyberspace: A Multi-Actor Analysis of the Construction of Cyber Threats in the US (2003-2016). *Conference: The 18th European Conference on Cyber Warfare and Security (ECCWS 2019).*

Fortson, D. (2024, July 21). Global IT meltdown shows faults spread like lightning. *The Australian*.

Garhwal, S. K. & Pareek, K. S. (2024). Securitization of cyber threats: implications for privacy and digital rights. *The Indian Journal of Political Science*, *85*. 741-751. https://www.researchgate.net/publication/385134412_SECURITIZATION_OF_CYBER_THREATS_IMPLICATIONS_FOR_PRIVACY_AND_DIGITAL_RIGHTS

Giacomello, G. (2004). Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism. *Studies in Conflict and Terrorism*, *27*(5), 387–388.

Gomez, M. A. & Whyte, C. (2021). Breaking the Myth of Cyber Doom: Securitization and Normalization of Novel Threats. *International Studies Quarterly*, 65(4), 1137–1150. https://doi.org/10.1093/isq/sqab034

Gorr, D. & Schünemann, W. J. (2013). Creating a Secure Cyberspace – Securitization in Internet Governance Discourses and Dispositives in Germany and Russia. *The*

International Review of Information Ethics, *20*, 37-51. https://doi.org/10.29173/irie159.

Güven, D. (2021). Securitization of Cyberspace Governance and the Right to Privacy: Cases of the US, China, and Iceland (Order No. 29044878). https://www.proquest.com/docview/2652556182?pq-origsite=gscholar&fromopenview=true&sourcetype=Dissertations%20&%20Theses

Hall, C. G. & Rowe, N. C. (2018). Options for Persistence of Cyberweapons. *Proceedings of the 23rd International Command and Control Research & Technology Symposium*. https://faculty.nps.edu/ncrowe/oldstudents/iccrts18_cghall.htm

Hansen, L. & Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, *53*, 1155-1175.

Hart, C. E. (2012). *Securing Freedom: A media framing analysis of cybersecuritization*. [M.A. Thesis, Simon Fraser University]. SFU Summit Research Repository. https://summit.sfu.ca/item/12560

Hjalmarsson, O. (2013). The Securitization of Cyberspace: How the web has won. *Lund University*. https://www.lunduniversity.lu.se/lup/publication/3357990

Jarvis, L., & Macdonald, S. (2014). What Is Cyberterrorism? Findings From a Survey of Researchers. *Terrorism and Political Violence*, *27*(4), 657–678. https://doi.org/10.1080/09546553.2013.847827

Jarvis, L., Macdonald, S., & Whiting, A. (2015). Constructing Cyberterrorism as a Security Threat: a Study of International News Media Coverage. *Perspectives on Terrorism*, *9*(1), 60–75. http://www.jstor.org/stable/26297327

Jarvis, L., Macdonald, S., & Whiting, A. (2016). Unpacking cyberterrorism discourse: Specificity, status, and scale in news media constructions of threat. *European Journal of International Security*, *2*(1), 64-87. doi:10.1017/eis.2016.14

Kapuściński, G. & Richards, B. (2016). News framing effects on destination risk perception. Tourism Management, 57, 234-244. https://doi.org/10.1016/j.tourman.2016.06.017

Keane, A. (2024, November 20). How to outsmart scammers when pre-Christmas shopping. *The Australian*.

Kelton, M., & Rogers, Z. (2020). The United States and Australia: Deepening ties and securitising cyberspace. In O. Turner, & I. Parmar (Eds.), *The United States in the*

Indo-Pacific: Obama's legacy and the Trump transition (pp. 94-111). Manchester University Press. https://doi.org/10.7765/9781526135025.00013

Ladewig, J. C. (2018). Australia's readiness for a complex cyber-catastrophe. *Australian Army Journal*, *14*(2), 57–78. https://search.informit.org/doi/10.3316/informit.344436178524413

Lam, J., & Lynch, J. (2024, January 22). What the government's sanctions on Russian hacker mean. *The Australian*.

Lawson, S. (2013). Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats. *Journal of Information Technology & Politics*, *10*(1), 86–103. https://doi.org/10.1080/19331681.2012.759059

Lewis, J. A. (2002). Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. *Center for Strategic and International Studies*. http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf

Lewis, J. A. (2014). National Perceptions of Cyber Threats. *Strategic Analysis*, *38*(4), 566-576, DOI: 10.1080/09700161.2014.918445

Lewis, J. A. (2018). Rethinking cybersecurity: Strategy, mass effect, and states. *Center for Strategic and International Studies*. https://www.csis.org/analysis/rethinking-cybersecurity

Lilja, J., Eishayea, E., & Huskaj, G. (2024). Defining the "Cyber-Pearl Harbor" - Validation of the DSLP-framework in "Offensive Cyberspace Operations Targeting Ukraine: A Cyber Pearl-Harbor". *Proceedings of The 19th International Conference on Cyber Warfare and Security*, *19*(1), 527-534.

Liu, S., Huang, J. C., & Brown, G. L. (1998). Information and risk perception: A dynamic adjustment process. Risk Analysis, 18(6), 689–699.

Lowy Institute (2024). *Poll 2024 Relations in the Indo-Pacific: US alliance: importance to Australia's security*. https://poll.lowyinstitute.org/charts/importance-of-the-us-alliance/

Lynch, J. (2024a, January 22). CrowdStrike tech failure a matter of national security. *The Australian*.

Lynch, J. (2024b, July 23). Labor double standard at play in CrowdStrike outage. *The Australian*.

Lynch. J. (2024c, May 20). What Optus's poaching of NBN boss really reveals. *The Australian*.

Makridis, C., Maschmeyer, L., & Smeets, M. (2024). If it bleeps it leads? Media coverage on cyber conflict and misperception. Journal of Peace Research, 61(1), 72-86. https://doi.org/10.1177/00223433231220264

Manwaring, R., & Holloway, J. (2022). Resilience to cyber-enabled foreign interference: citizen understanding and threat perceptions. *Defence Studies*, *23*(2), 334–357. https://doi.org/10.1080/14702436.2022.2138349

Maschmeyer, L., Deibert, R. J., & Lindsay, J. R. (2020). A tale of two cybers - how threat reporting by cybersecurity firms systematically underrepresents threats to civil society. *Journal of Information Technology & Politics*, *18*(1), 1–20. https://doi.org/10.1080/19331681.2020.1776658

Mazur, A. (2006). Risk Perception and News Coverage Across Nations. *Risk Management*, *8*, 149–174. https://doi.org/10.1057/palgrave.rm.8250011

Miller, M. (2024, June 6). Tech monopolies trade in misery: time for Australian rules. *The Australian*.

Milliken, J. (1999). The study of discourse in international relations: A critique of research and methods. *European Journal of International Relations*, *5*(2), 225-254. https://doi.org/10.1177/1354066199005002003

Museums of History New South Wales (MHNSW) (n.d.) Sydney Harbour Bridge guide. https://mhnsw.au/guides/sydney-harbour-bridge-guide/

Mutz, D. C., & Soss, J. (1997). Reading Public Opinion: The Influence of News Coverage on Perceptions of Public Sentiment. *The Public Opinion Quarterly*, *61*(3), 431–451. http://www.jstor.org/stable/2749580

Naparstek, B. (2024, April 27). Biden's TikTok message to China. *The Australian*.

National Museum Australia (n.d.). *Defining Symbols of Australia: Sydney Harbour Bridge*. https://www.nma.gov.au/exhibitions/defining-symbols-australia/sydney-harbour-bridge

Ng, R. & Tan, Y. W. (2022). Media attention toward COVID-19 across 18 countries: The influence of cultural values and pandemic severity. PLoS One, 17(12), 1-12. doi: 10.1371/journal.pone.0271961

O'Dowd, C. (2024, May 18). How safe is your super? Google fail raises concerns. *The Australian*.

Oppenheimer, H. (2024). How the process of discovering cyberattacks biases our understanding of cybersecurity. *Journal of Peace Research*, *61*(1), 28-43. https://doi.org/10.1177/00223433231217687

Otukoya, T. A. (2024). The securitization theory. *International Journal of Science and Research Archive*, *11*(01), 1747-1755. https://doi.org/10.30574/ijsra.2024.11.1.0225

Owen, D. (2024, March 19). We need to work smarter, not harder, to fight cyber threats. *The Australian*.

Phillips, N., & Hardy, C. (2002). *Discourse Analysis: Investigating Processes of Social Construction*. Thousand Oaks, CA: Sage.

Qadri, S. N. (2020). *Framing terrorism and migration in the USA: the role of the media in securitization processes.* PhD thesis, University of Glasgow. https://theses.gla.ac.uk/77872/

Rader, E. & Wash, R. (2015). Identifying patterns in informal sources of security information, *Journal of Cybersecurity*, *1*(1), 121–144. https://doi.org/10.1093/cybsec/tyv008

Rajkovic, D. (2024, September 2). Lessons from Paris can prevent cyber havoc at Brisbane Games. *The Australian*.

Randell, I. (2023, December 3). In the wake of a cyber attack, don't forget the customer. *The Australian*.

Ritchie, H. (2024, November 29). Australia approves social media ban on under-16s. *BBC News*. https://www.bbc.com/news/articles/c89vjj0lxx9o

Rogers, M. (2024, March 25). Why state-sponsored cyber sabotage is on the rise. *The Australian*.

Rudd, K. (2008, December 4). Transcript 16289 | PM Transcripts. https://pmtranscripts.pmc.gov.au/release/transcript-16289

Smeets, M. (2016, November 21). How Much Does a Cyber Weapon Cost? Nobody Knows. *Council on Foreign Relations*. https://www.cfr.org/blog/how-much-does-cyber-weapon-cost-nobody-knows

Sreedhar, V. (2024, February 3). Be proactive on cybersecurity. *The Australian*.

Stritzel, H. (2014). Security in translation: Securitization theory and the localization of threat. Palgrave Macmillan UK eBooks. https://doi.org/10.1057/9781137307576

Tagliapietra, A. (2021). *Media and Securitisation: The Influence on Perception*. Istituto Affari Internazionali IAI.

Thompson, M. (2024, May 7). Breach shows we rely too heavily on foreign tech. *The Australian*.

Threats to infrastructure via hacking must be faced (2024, April 27). *The Australian*.

Uhlmann, C. (2024, April 26). China's cyber traps already inside the castle wall. *The Australian*.

Uhlmann, C., & Lewis, R. (2024, April 26). Volt Typhoon: China's invisible cyber invasion. *The Australian*.

Van Ooijen, M. (2020). Cyber securitization or cyberization of conflict? The militarization of Cyber Security in Estonia. https://studenttheses.uu.nl/handle/20.500.12932/37990

Vuori, J. A. (2016). Constructivism and Securitization Studies. In M. Dunn Cavelty & T. Balzacq (Eds.), *Routledge Handbook of Security Studies* (2nd Ed., pp. 64-74). Routledge.

Waever, O. [OpenLearn from the Open University]. 2014, October 3. *Securitisation theory – International Relations (3/7)* [Video]. YouTube. https://www.youtube.com/watch?v=wQ07tWOzE_c

Xu, W., Murphy, F., Xu, X. & Xing, W. (2021). Dynamic communication and perception of cyber risk: Evidence from big data in media. Computers in Human Behavior, 122, 1-14. https://doi.org/10.1016/j.chb.2021.106851

Zeffiro. A., Niessen, G., Oberst, C., McEwan, S., Cochrane, A.-C., & Durand, J. (2022). Discourses on cybersecurity: The politics of the data breach as a security crisis. *Rivista di Digital Politics, 3*, 369-398. doi: 10.53227/106451

Appendices

Appendix A: News Article Sample

Article number	Search term NexixUni	Reference
A1	'Commentary Cyber'	Lord, J. (2018, February 21). Asia is outpacing the West in a new kind of industrial revolution. *The Australian.*
A2	'Cybercrime'	Lynch, J. (2024, January 18). 'Rapidly evolves': AI to spark new wave of cyber attacks. *The Australian.*
A3	'Cybercrime'	Southern, K. (2024, January 7). 'Stolen voices' key to virtual kidnapping. *The Australian.*
A4	'Cybercrime'	Kirby, J. (2024, May 22). Believe it or not, financial scam losses are shrinking. *The Australian.*
A5	'Cybercrime'	Uhlmann, C. (2024, April 26). China's cyber traps already inside the castle wall. *The Australian.*
A6	'Cybercrime'	Cyber attacks now a direct threat (2024, January 2). *The Australian.*
A7	'Cybercrime'	Bergin, A., & Jennings, P. (2024, September 26). Defence torpor leaves us exposed to the China threat. *The Australian.*
A8	'Cybercrime'	Fixing the 'blue screen of death' (2024, July 21). *The Australian.*
A9	'Cybercrime'	Fleeced by criminals via big tech (2024, August 19). *The Australian.*
A10	'Cybercrime'	Fortson, D. (2024, July 21). Global IT meltdown shows faults spread like lightning. *The Australian.*
A11	'Cybercrime'	Lynch, J. (2024, July 19). How did one company cripple the world? *The Australian.*
A12	'Cybercrime'	Keane, A. (2024, November 20). How to outsmart scammers when pre-Christmas shopping. *The Australian.*
A13	'Cybercrime'	Randell, I. (2023, December 3). In the wake of a cyber attack, don't forget the customer. *The Australian.*
A14	'Cybercrime'	Rajkovic, D. (2024, September 2). Lessons from Paris can prevent cyber havoc at Brisbane Games. *The Australian.*
A15	'Cybercrime'	Gerrard, J. (2024, June 7). Online scams rife as tech giants put profit ahead of policy. *The Australian.*

A16	'Cybercrime'	Keane, A. (2024, June 12). Online shopping traps: how to avoid getting stung. *The Australian.*
A17	'Cybercrime'	Chambers, G. (2024, April 24). PM must log on to our clear and present dangers. *The Australian.*
A18	'Cybercrime'	Chambers, G. (2024, January 17). PM must stand up to Beijing and its veiled warnings. *The Australian.*
A19	'Cybercrime'	Dupont, A. (2024, June 4). Ramp up defences against Beijing's takeover by stealth. *The Australian.*
A20	'Cybercrime'	Uhlmann, C., & Lewis, R. (2024, April 26). Volt Typhoon: China's invisible cyber invasion. *The Australian.*
A21	'Cybercrime'	Lynch. J. (2024, May 20). What Optus's poaching of NBN boss really reveals. *The Australian.*
A22	'Cybercrime'	Lam, J., & Lynch, J. (2024, January 22). What the government's sanctions on Russian hacker mean. *The Australian.*
A23	'Cybercrime'	Lam, J. (2024, May 30). What you need to know about alleged Ticketmaster breach. *The Australian.*
A24	'Cybercrime'	Rogers, M. (2024, March 25). Why state-sponsored cyber sabotage is on the rise. *The Australian.*
A25	'Cybersecurity'	Nicks, D. (2023, December 26). Affordability challenge. *The Australian.*
A26	'Cybersecurity'	Sreedhar, V. (2024, February 3). Be proactive on cybersecurity. *The Australian.*
A27	'Cybersecurity'	Naparstek, B. (2024, April 27). Biden's TikTok message to China. *The Australian.*
A28	'Cybersecurity'	Blue sky thinking (2024, October 18). *The Australian.*
A29	'Cybersecurity'	Thompson, M. (2024, May 7). Breach shows we rely too heavily on foreign tech. *The Australian.*
A30	'Cybersecurity'	China's cyber criminals exposed (2024, July 10). *The Australian.*

A31	'Cybersecurity'	Lynch, J. (2024, January 22). CrowdStrike tech failure a matter of national security. *The Australian.*
A32	'Cybersecurity'	Camp, G. (2024, October 31). De-risking of the procurement process must become a priority. *The Australian.*
A33	'Cybersecurity'	Driving diversity for a secure cyber future (2024, May 19). *The Australian.*
A34	'Cybersecurity'	White, R. (2024, January 6). Education reforms needed to prepare future tech workers. *The Australian.*
A35	'Cybersecurity'	Gutting Home Affairs a risk for national security (2024, July 26). *The Australian.*
A36	'Cybersecurity'	Lam, J. (2024, July 25). Hero response saved PCs from 'blue screen of death'. *The Australian.*
A37	'Cybersecurity'	O'Dowd, C. (2024, May 18). How safe is your super? Google fail raises concerns. *The Australian.*
A38	'Cybersecurity'	James, C. (2024, July 16). How to be scam proof. *The Australian.*
A39	'Cybersecurity'	Lynch, J. (2024, July 23). Labor double standard at play in CrowdStrike outage. *The Australian.*
A40	'Cybersecurity'	Miller, M. (2024, June 6). Tech monopolies trade in misery: time for Australian rules. *The Australian.*
A41	'Cybersecurity'	Threats to infrastructure via hacking must be faced (2024, April 27). *The Australian.*
A42	'Cybersecurity'	Time's up on TikTok and national security threat (2024, March 15). *The Australian.*
A43	'Cybersecurity'	Owen, D. (2024, March 19). We need to work smarter, not harder, to fight cyber threats. *The Australian.*

Appendix B: Coding Overview

Speech acts	Corporate suicide (A1), vital issue (A1), unsubstantiated one-brush anti-China sentiments (A1), the next industrial revolution is upon us (A1), There are more Huaweis to come; this is the new norm (A1) // harness the power (of AI) (A2); most Australian companies won't know they have even infiltrated their systems (A2); an AI arms race (A2); cyber-crime has been escalating (A2); attacks lobbed (A2); hacks were unleashed (A2); (generative AI) changed the game (when it comes to cybersec) (A2); rapidly evolves (A2); single biggest external threat (A2); top issue that keeps them awake at night (A2); nearly every attack (A2); lacks long-term threats (A2); market failure (A2); fight AI (A2); the stakes are high (A2); huge technical process problem (A2); Of nearly all the big attacks we've seen, the root cause that led to the incident was already known to the organisation and that's very concerning for boards of course because that had regulatory and legal impacts (A2) // terrifying new developments (A3); a threat it believes is increasing (A3); a loved one's voice (A3); Even a cybersecurity expert can fall victim (A3); makes us all potentially at risk (A3); (advances in AI) blurred the boundaries between fantasy and reality (A3); Professor van der Linden … stop them capturing your voice (A3) // appear to be swamping (A4); dramatic (A4) // landmines for a future war (A5); hunting for weaknesses (A5); the first sign may be when the lights go out and the dams empty (A5); most immediate, low-cost and potentially high-impact vector for sabotage is cyber (A5); the enemy is already inside the castle walls (A5); interconnected zombie batallion (as synonym for botnet) (A5); computational muscle (as synonym for botnet) (A5); 'living off the land' (definition) (A5); parasite (A5); "This is something … blatant act of aggression." (A5, para. 14); "Our security agencies … a government desperate to remarry an unrepentant, abusive partner… hiding the bruises." (A5, para. 15) // worrying escalation (A6, para. 1); demonstration of just how unprepared we are as a society to deal with it (A6, para. 1); threat goes well beyond scraping credit card details from unprepared businesses (A6, para. 1); ramifications could be deadly (A6, para. 2); Clearly the digital world is the new frontier in crime (A6, para. 4); The power unleashed by new systems of artificial intelligence significantly increases the risk (A6, para. 4); more than a menace (A6, para. 7) // They pretend instead to have "stabilised" relations with Beijing. (A7, para. 11); China could hit kill switches on industrial control systems (A7, para. 17); an earlier, less threatening era (A7, para. 18) // "blue screen of death" (A8, para. 2); results could have been deadly in the extreme (A8, para. 5); In a globalised economy, real solutions rest with technical companies, their expert staff and national security agencies (A8, para. 6) // scam and fraud epidemic (A9, para. 1); inflict pain (A9, para. 2) // (faults) spread like lightning (A10; title); global IT failure (A10, para. 2); (may go down as the) worst in history (A10, para. 2); cloud computing had become "as indispensable as electricity" (A10, para. 10); immense vulnerability (A10, para. 11); can immediately propagate across the whole Azure universe (A10, para. 11); Kurtz *was* (A10, para. 12); a single bit of code can bring the globe to a standstill. (A10, para. 24) // cripple the world (A11, title); upended the world (A11, para. 1); knocked out big banks, hospitals, media companies (A11, para. 1); chaos (A11, para. 2); Australians - and millions of others across the globe (A11, para. 3); blue

	screen of death (A11, para. 3); paralysed (A11, para. 15); activating a "doomsday command" or "kill switch" (A11, para. 23); IT has become as essential as running water (A11, para. 27); It has become the bedrock of our economy and when it sneezes, everyone catches a cold. (A11, para. 27); fresh cause of insomnia for the nation's top execs (A11, para. 28) // but there are ways to protect yourself (A12, para. 2) // cyber havoc (A14, title) // horrifying pace (A17, para. 2); the myriad of risks and threats (A17, para. 2) // cyber assaults (A22, para. 2) // Why state-sponsored cyber sabotage is on the rise (A24, title) // ever-evolving cyber critical risk (A25, para. 28); The risk is always there (A25, para. 28) // Cyberthreats are on the rise (A26, para. 17) // aggressive data collection practices (A27, para. 13); what John Garnaut has described as "the canary in the coalmine of Chinese Communist Party interference" (A27, para. 36); espionage and foreign interference as more prevalent than ever, having "surpassed terrorism as Australia's principal security concern â€¦ if we had a threat level for espionage and foreign interference, it would be at â€¦ the highest level on the scale". (A27, para. 38 – ASIO Mike Burgess); appetite for information seemed limitless (A27, para. 39 – reference to Beijing); to stare down the kids (A27, para. 41) // cyber security has never been more critical (A28, para. 15) // this risk is omnipresent across all industries and everything we do digitally, and it goes far beyond the more obvious threat of a data breach (A29, para. 5); it's easy to imagine a more detrimental data breach taking place (A29, para. 10) // its insidious presence (A30, para. 3 – of Volt Typhoon); poised for a strike (A30, para. 3) // global chaos (A31, para. 1 – Crowdstrike); crippled key services (A31, para. 2); not just a matter of inconvenience .. but a matter of national security. (A31, para. 5) // This is not just a matter of efficiency; it's a matter of national security (A32, para. 5); The future of our national security depends on getting this right (A32, para. 11) // Every person and every industry is affected by cyber security (A33, para. 23) // increasingly important aspect of national security (A35, para. 5) // “blue screen of death” (A36, para. 2) // The touch of a button is all it takes to wipe your data (A37, para. 1); crippled (A37, para. 1); serious vulnerability (A37, para. 1) // world's biggest tech outage, which is arguably a thousand times worse than Optus's meltdown last year. (A39, para 1) // before the algorithms turned us into addicts (A40, para. 3); leading people down dangerous algorithmic rabbit holes (A40, para. 7); this is the tip of a very large iceberg (A40, para. 8); In the words of a British father who lost his child to suicide: "They monetise misery." (A40, para, 11); a digital environment that protects vulnerable people rather than preys on them (A40, para. 25) // national security implications (A42, para. 2); must be treated as a special case (A42, para. 2 – Tiktok)

Military speech acts	Landmines for a future war (A5); cyber batallions (A5); bombs … detonated (A5); conflict with China (A5); the enemy is already inside the castle walls (A5); virtual bombs (A5, para. 16); relentless information war (A5, para. 20) // global supply chain warfare (A7, para. 1); Modern war is so unthinkable, governments choose not to think about it. (A7, para. 10); Could China copy Mossad by supplying and exploding the communications devices of ADF commanders? Never say never. (A7, para. 18); In a war, China would set out to cause havoc at a national level through cyber and malware disruptions. (A7, para. 19); As always, the vibe from Canberra is torpor. Is that a pager we hear beeping? (A7, para. 25) // global IT meltdown (A10 -title); I felt like I was defusing a bomb (A10, para. 17); Australia's IT sovereignty (A11, para. 15); sharpening their digital weapons (A11, para. 1) // fallout of a cyber incident (A13, para. 14) // China's legion of hackers (A19, para. 11); China's state-sponsored army of hackers (A19, para. 13) // China's invisible cyber invasion (A20, title); "electronic equivalent" of Chinese commando groups putting bombs underneath bridges or on high-voltage pylons for the purposes of blowing them up during a war. (A20, para. 6) // network meltdown (A21, para 6); outage fallout (A21, para. 15) // Yet today, saboteurs targeting our infrastructure are more likely to come with USB sticks than sticks of dynamite (A23, para. 3) // detonate digital bombs (A24, para. 4); digital bombs are easier to plant, harder to detect but potentially just as devastating (A24, para. 14); ticking technology time bombs (A24, para. 14) // anxieties about Beijing weaponising TikTok to shape US public opinion through misinformation (A27, para. 4); TikTok may have lost its battle already (A27, para. 28); Chinese aggression (A27, para. 39); hostile adversary (A27, para. 40) // Behind the facade of panda diplomacy lurk hostility and aggression (A30, para. 1); Chinese hostility towards Australia (A30, para. 2) // the meltdown (A31, para. 11) // meltdown (A39, para. 1) // cyber battalions (A41, para. 2 – of PRC); Australia's deteriorating strategic situation (A41, para. 3) // Our fight against cyber crime is being fought on many fronts (A43, para. 1); wicked problem (A43, para. 7 -cybercrime)
Cybercriminal speech acts	The bad guys (A2), threat actors (A2), criminal groups (A2); links to state based actors (A2) // scammers (A4) // cyber batallions (A5); one nation-state (A5); Volt Typhoon (A5) // online criminals (A6, para. 1) // a hostile power (A7, para. 5) // hardened criminals (A9, para. 2) // hostile nation states (A11, para. 10) // Cybersecurity Minister Clare O'Neil branding hackers "cowards" and "scumbags" who "hide behind technology" (A22, para. 2) // Online criminals (A31, para. 7) // attackers (A43, para. 3)
Central cyber issue	Issues of cybersecurity (A1) // AI enhanced cyber attacks (A2) // cyber-kidnapping (powered by AI) (A3) // financial scams (A4) // cyber sabotage of critical infrastructure (A5) // cyberattacks against hospitals and courts of law (A6) // global supply chain warfare (A7, para. 1) // Crowdstrike outage (A8, para. 1) // online scams and fraud (A9) // Chinese and Russian foreign-interference and state-sponsored cyber attacks targeting critical infrastructure (A17, para. 9) // state-sanctioned cyber attacks targeting critical infrastructure, foreign interference campaign (A18; para. 7) // cyberattacks on energy grids (A25) // cyber

	security breaches and foreign interference (A30, para. 1 – by China) // cybercrime (A43)
Securitizing actor	John Lord – chairman Huawei Australia (A1) // Global law firm & risk practice Ashurst (A2); Australia's corporate leaders (A2) // the FBI (A3) // ASIO director-general Mike Burgess (A5); Australian Signals Directorate (A5) // FBI Director Christopher Wray (A5); CrowdStrike (A11) // US Director of National Intelligence (A24, para. 4) // former head of US National Security Agency Retired Admiral Mike Rodgers (A24, para. 9) // Damien Nicks, chief executive AGL Energy (A25) // ASIO director-general Mike Burgess (A27, para. 38) // Marcus Thompson adviser/director companies & former head of information warfare ADF (A29, para. 16) // Geoff Camp, defense lead JLL Australia (A32) // cyber professional (A33) // Deloitte Australia (A43)
Referent object (that is threatened)	Business growth (A2); (harm) individuals (A2); key digital assets & crown jewels (A2) // (banking) customers, especially elderly Australians (A4, para. 6) // 'inside our borders' (A5); critical infrastructure (A5); And the risk that poses to every American requires our attention now (A5); American citizens and communities (A5); home soil (A5, para. 16); our nation (A5, para. 19); inside our borders (A5, para. 19); undermining our democracy and our alliances (A5, para. 20); the world, our region, or our nation (A5, para. 25) // a weak link in our national security (A6, para. 4); It has become a direct threat to the community at large. (A6, para. 7) // even household technology (A7, para. 5); isolate Australia from its allies (A7, para. 7); break any internal systems keeping the nation on its feet (A7, para. 7) // national security threat (A11, para. 9) // families, children and our economic interests. (A17, para. 13) // democratic institutions (A18, para. 7) // our own democracy (A19, para. 23) // international rules-based order (A22, para. 15); Australians (A22, para. 26) // underestimating the existential threat faced (by TikTok's foreign interference) (A27, para. 10); sovereignty (A27, para. 37); a national threat (A27, para. 40); our sovereignty (A27, para. 41) // major government agency or piece of national critical infrastructure (A29, para. 9); data sovereignty (A29, para. 16) // if we get more people entering the profession … we will be better able to protect critical infrastructure (A33, para. 23) // There is no doubt our children are paying the price (A40, para. 5); And our economy is also (A40, para. 6) // It's time to protect our children, our parents and our national identity (A40, para. 25) // (especially) infrastructure and essential services (A41, para. 4) // us all (A43, para. 15)
Emergency measures (acts/agreements)	vowing to launch widespread reforms to govern the technology's use (A2); strengthening existing laws than creating new ones (A2) // Dealing with cyber crime must be a national priority. (A6, para. 4) // . As such, the federal government's Mandatory Scams Code Framework cannot come soon enough (A15, para. 22) // national security and online safety laws are outdated and not fit-for-purpose. (A17, para. 1); If our security agencies don't have contemporary, world-leading powers and resources to fight terrorists, spies, criminals, pedophiles and extremists, their hands are

	effectively tied behind their backs. (A17, para. 5); legislating powers giving security agencies tools and resources they need to protect families, children and our economic interests. (A17, para. 13) // procurement of contractors and supplies (A32, para. 3) // banning the payment of ransoms … and the use of crypto currency (A34, para. 19) //
Promoted practices	Open discussions (with China) (A1) // Whatever the benefits of collaboration, it is up to Meta to protect customers by taking down scam ads, investigating those that are suspicious and acting to thwart criminals (A9, para. 3) // we need to attract all the local tech talent we can if we are to build our IT sovereign capability (A39, para. 12) // Hardening the nation's cyber defences (A41, para. 4) // modern intelligence gathering measures and recruiting the right people, capable of using that intelligence to make the right choices (A43, para. 17)
Desecuritization	but there are ways to protect yourself (A12, para. 2) // "Pleasingly, the Australian government's new Cyber Security Strategy … put our customers at the heart of decision-making" (A13, para. 5); Our AustraliaNOW data shows that timely, accurate and transparent information - with clarity about the steps customers can take to protect themselves - rebuilds brand trust, repeat purchase and advocacy (A13, para. 11); Cyber incidents and system outages are awful events and are likely here to stay, but they don't have to be catastrophic for brand reputation (A13, para. 15) // This includes regular stress tests and updates to security protocols. This also ensures any compromised infrastructure can be rapidly recovered (A14; para. 13); . Visitors to the Games and Brisbane's locals must be educated on staying alert and identifying suspicious activity. Comprehensive campaigns should teach attendees how to spot phishing attempts, avoid scams, and report suspicious behaviour. (A14, para. 14); Beyond collaboration with the event's immediate stakeholders, intelligence sharing around potential threats and adversarial tactics must extend to international agencies and private security firms to enhance preparedness and response capabilities. (A14, para. 17) // A16 // A23 // Employee education is crucial in the fight against cyberthreats. (A26, para. 12) // But there's lots of scenarios that are non-malicious. We genuinely need organisations not to just think about the Russians and Chinese or North Korean hackers, but also about an all-hazards approach (A37, para. 18 – Monash uni prof Nigel Phair) // A38