CYBERSIGHT 360

A legal perspective on cyber security and cyber insurance

2023/24

LANDER & ROGERS

FOREWORD

Welcome to CyberSight 360 - a legal perspective on cyber security and cyber insurance

2023 continued to be a big year for cyber security and cyber insurance globally.

2023 - The year of strategies

As cyber threat actors became more targeted and sophisticated in 2023, so too did governments, organisations and individuals in their response to the rising threat and occurrence of cyber attacks.

It was a year of significant data breaches; proposals for regulatory reforms; significant launches of ambitious cyber security strategies and action plans from two key jurisdictions, the US and Australia; and further development and maturing of international law enforcement cooperation on taking offensive action to disrupt the operations of threat actors, particularly ransomware gangs.

This was so particularly as geopolitical tensions escalated state-sponsored attacks, the vulnerabilities of critical infrastructure became increasingly apparent, and gaps in the current cyber, privacy and data legislative framework became evident.

On the cyber insurance front we continued to see insurers devising forward-thinking solutions for capacity, developing innovative cyber insurance products to better suit different businesses, and investing in cultivating cyber insurance talent to ensure that underwriting keeps up with changes in technology and associated risks.

What is on the horizon?

As we continue to modernise and make way for new and emerging technologies such as 5G and the proliferation of Internet of Things (IoT) devices, the cyber security risks that come with these technologies will define 2024 and beyond.

Existing cyber security threats and risks will also continue to evolve and increase in sophistication and scale. While the risk of ransomware may not be new, changes in method and approach will take us by surprise if we are not sufficiently prepared. Geopolitical conflicts will also continue to shape cyber security threats and risks into the future.

The issue of cyber security is inherently political, and with cyber security at the top of the political agenda in many jurisdictions including Australia, this raises important questions about how governments can design realistic long-term cyber security strategies that build cyber resilience while withstanding political complexities and power dynamics between various actors with competing interests – questions which we set out to answer in this guide.

All of this has a profound impact on the cyber insurance industry, which continues to thrive but also seek out solutions to ensure it remains sustainable. This will mean adapting to the risks brought about by new technologies, rethinking its existing products, and bolstering its capability with new skills and talent to address an increasingly complex set of challenges.

In this guide we explore the cyber trends, legislative reforms and regulatory changes that defined 2023, and the developments we are likely to see in the year ahead. We also examine the coordinated actions being taken around the world to counter cyber threats and data breaches, and identify areas of growing priority – such as the increasingly critical space technology sector.

We hope you find our insights valuable and informative.

Melissa Tan
Partner and Head of Cyber Insurance
Insurance Law & Litigation

Contents

KEY CYBER INCIDENTS GLOBALLY IN 2023

Authors: Melissa Tan and Rebekah Maxton

As they say: "Learn from the past, prepare for the future, live in the present."

Taking time to reflect on the key cyber incidents that occurred in 2023 can help us prepare for the future and assist our present understanding of the cyber threats we face. The following is a representative selection of cyber attacks that were publicly reported in 2023, from which we can gain valuable insights.

In 2023, critical infrastructure, professional services and global software companies were popular targets. As geopolitical conflicts escalated, cyber attacks on governments by state-backed actors also continued to gain pace.

The scale of attacks also increased, with the exploitation of high-risk software vulnerabilities a critical trend observed in 2023. As reported by Qualys Threat Research Unit in December 2023, a total of 26,447 vulnerabilities were disclosed in 2023, surpassing the previous year by over 1,500 common vulnerabilities and exposures (**CVEs**).[1] Within this, about 1% of CVEs posed the highest risk with a weaponised exploit and were actively exploited by ransomware gangs and other threat actors, or actively exploited in the wild.[2]

LockBit, APLHV/BlackCat and CL0P also continued to prevail as the top ransomware-as-a-service groups, claiming many of the high-profile and significant breaches we saw in 2023 as well as weaponising many critical vulnerabilities in carrying out their extensive attacks.[3]

1 https://blog.qualys.com/vulnerabilities-threat-research/2023/12/19/2023-threat-landscape-year-in-review-part-one

2 Ibid

3 https://blog.qualys.com/vulnerabilities-threat-research/2023/12/19/2023-threat-landscape-year-in-review-part-one, "Most Active Malware of 2023"

2023 KEY CYBER INCIDENTS GLOBALLY

January
February
March
April
May
June
July
August
September
October
November
December

12 January 2023

Target
Royal Mail

Country
United Kingdom

Threat actor
LockBit Ransomware

Type of attack
Ransomware and DDoS

Sector
Critical infrastructure - Royal Mail's national postal network is included in the UK government's Critical National Infrastructure framework, as a subsector of the communications sector.[1]

Key details

- US$80 million (£67 million or approx. A$127 million) ransom demanded. All parcels and letters came to a standstill. Royal Mail reverted to manual processes, which left big delays and impacted international parcel volumes.
- Chat transcripts with Royal Mail were released on the dark web by LockBit.
- Royal Mail said it would not pay the ransom and it appears that data of employees at the Royal Mail was leaked online,[2] with a 44GB dump of data leaked on the dark web on 23 February 2023.
- Royal Mail spent £10 million repairing and strengthening its cyber defences. The impact of the January attack was revealed in half-year financials published by Royal Mail's parent company IDS, noting a 6.5% year-on-year revenue decline for the 26 weeks to September 2023 (a half-year loss of £319 million).

30 January 2023

Target
JD Sports

Country
United Kingdom

Threat actor
Unknown

Type of attack
Data breach

Sector
Retail industry

Key details

- The cyber attack impacted several JD Sports brands including JD, Blacks, Millets, MilletSport, size?, and Scotts. It appears the threat actors infiltrated an internal system that contained customer information on online orders from November 2018 to October 2020.
- Personal and financial information of 10 million customers was potentially accessed. This included names, billing and delivery addresses, phone numbers, order details and the last four digits of customers' credit cards.
- JD Sports reacted quickly and commenced notification to affected customers before a full investigation was complete.

30 January 2023

Target
GoAnywhere

Country
Global

Threat actor
Cl0p Ransomware

Type of attack
Data breach, supply chain, zero-day vulnerability exploitation (CVE-2023-0669)

Sector
Software - FORTRA GoAnywhere MFT (Managed file transfer)

Key details

- The threat actor leveraged the then-unknown vulnerability to create unauthorised user accounts in some customer environments. Although suspicious activity was only detected on 30 January 2023, the first signs of exploitation could be traced back to 18 January 2023. This indicates the vulnerability was actively being exploited undetected for approximately two weeks before GoAnywhere discovered the security breach.
- The data breach appears to have affected at least 130 organisations globally including Australian organisations such as the Tasmanian government, Meriton, Crown Resorts and Rio Tinto.
- The extent of the Tasmanian government's breach was discovered in April when personally identifiable information from the Tasmanian Department for Education, Children and Young People was compromised, including school children's personal information.
- Crown Resorts was one of 100 entities to which Cl0p issued ransomware demands in March that stem from the GoAnywhere attack.

1 https://www.parliament.uk/globalassets/documents/commons-committees/Exiting-the-European-Union/17-19/Sectoral-Analyses/27-Post-Report.pdf

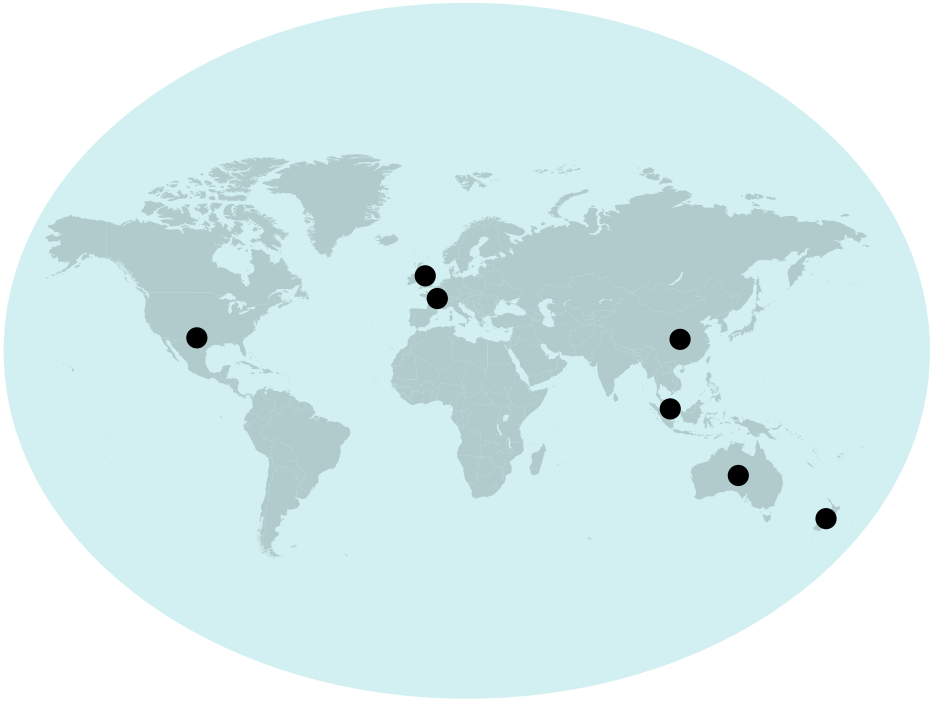
2 https://techmonitor.ai/technology/cybersecurity/royal-mail-lockbit-ransomware

5 https://www.forbes.com/sites/brianbushard/2023/02/28/dish-network-shares-hit-14-year-low-after-cyber-attack-caused-major-outage/?sh=2468d8ad5a0e

KEY GLOBAL CYBER REFORMS AND THE REGULATORY LANDSCAPE IN 2023

Authors: Melissa Tan and Rebekah Maxton

2023 was the year that many countries around the world sought to consolidate or articulate their national cyber security strategy and action plan towards building a cyber resilient future for the country. It was also a year where the momentum for cyber and privacy legal reforms continued to increase in pace, most notably in Australia. Select a country below to view the major initiatives implemented or proposed in 2023 to manage cyber and privacy risks.



Interactive map

CLICK THE POINTS TO BEGIN

THE CYBER TRENDS THAT SHAPED 2023

Authors: Melissa Tan, Jack Boydell and Rebekah Maxton

TRENDS

As the cyber threat landscape continues to evolve, so too have countries, governments, businesses and individuals in their approach to cyber security.

If 2022 was the year Australia awakened to the stark reality of cyber threats and their serious implications following several high-profile data breaches, 2023 was the year Australia and many in the rest of the world strategised, developed further defence mechanisms and adopted offensive strategies to enhance their cyber resilience.

These are the six key cyber trends that shaped and defined 2023.

1 Governments take action on cyber security strategies

2023 was the year that cyber security strategies and action plans were launched or evaluated, particularly for Australia and its allies.

This was largely driven by the geopolitical landscape and global conflicts including the Russia-Ukraine war, China-Taiwan tensions and the Israel-Hamas conflict.

The US launched its National Cybersecurity Strategy Implementation Plan in the first part of 2023. The much-anticipated 2023-2030 Australian Cyber Security Strategy and Action Plan were released in November 2023. The UK published its National Cyber Strategy 2022-23 progress report and Ministry of Justice Cyber Security Strategy: 2023 to 2028. Germany released its first-ever National Security Strategy and New Zealand its National Security Intelligence Priorities, with cyber security as one of the key focus areas. It is evident that the governments of key global and regional powers are proactively setting up frameworks to secure their citizens and businesses from cyber threats, build up national cyber resilience, and establish better coordination and international collaboration amongst allies on the cyber front.

In Australia, a National Cyber Security Coordinator was appointed in July 2023 to lead Australia's strategic response to cyber security threats and enhance cyber resilience across business, critical infrastructure, and the broader community. The Coordinator supports the Minister for Cyber Security and is responsible for:

- national cyber security policy
- responses to major cyber incidents
- whole-of-government cyber incident preparedness efforts
- strengthening Commonwealth cyber security capability.

In 2024 and beyond, we expect to see cyber security strategies put into practice with domestic cyber security legislative reforms formulated, international cyber security law and norms fleshed out, enhanced coordination and collaboration domestically and internationally, and more countries taking on both a defensive and offensive stance towards global cyber threats.

2 Critical infrastructure continues to be a key target

Critical infrastructure assets and networks worldwide continued to be a key target of cyber attacks throughout 2023, causing major and debilitating disruptions for network operators and users dependent on these essential services.

Globally, the energy, health, transport, telecommunications and financial services industries are attractive targets for threat actors as these assets often possess sensitive information, maintain essential services and often have high levels of connectivity with other organisations. These sectors are vulnerable to cyber attacks due to a broad attack surface, remote access points, interconnected systems and reliance on legacy systems.

In Australia in 2023, critical infrastructure networks were regularly subjected to a mix of targeted and opportunistic malicious cyber attacks. The Australian Signals Directorate (**ASD**) indicated in its annual cyber threat report that in the 2022-23 financial year, it responded to 143 incidents reported by entities that self-identified as critical infrastructure, an increase from the 95 incidents reported in 2021–22.[1] The ASD reported that the majority of these incidents were characterised as low-level malicious attacks or isolated compromises. About 57% of cyber incidents reported by critical infrastructure entities involved compromised accounts or credentials; compromised assets, networks or infrastructure; and denial of service attacks.

The DP World Australia cyber attack, which disrupted port operations for several days and severely impacted critical shipping operations nationwide, was a timely reminder of the cyber security risks to essential transportation services and the global supply chain, which can have serious implications for Australia's trade and commerce.

Looking ahead to 2024 and beyond, critical infrastructure will likely remain a target for cyber attacks by threat actors, including state-backed actors. Given its vulnerabilities, it continues to represent a significant cyber risk for countries worldwide due to the potential range of impacts on essential services. Governments and operators of critical infrastructure assets and networks must focus on continuing to enhance cyber security measures for critical infrastructure to ensure resilience against such attacks.

3 The growing trend of law firms being under attack

A growing number of law and professional services firms were the target of cyber attacks in 2023.

As governments and industries wise up to the importance of uplifting their cyber resilience and start taking action, the stakes have become higher for threat actors to secure monetary gain more efficiently and against more high-value targets. This leaves them looking for easier targets — such as law firms, which are lucrative because:

- they hold not only personal information but also high-value confidential commercial information, including intellectual property and clients' trade secrets, and politically sensitive information. The theft of such information can cause serious reputational harm for law firms and their clients, which adds to the pressure to pay any cyber extortion demand
- they occupy a unique position within the supply chain, which means access to a law firm's data can be a gateway to the sensitive information of multiple clients at once, including high-value targets such as critical infrastructure industries and government clients. For threat actors, this presents an efficient way to extort multiple high-value victims with one attack
- they frequently deal with payments and account details through their main mode of communication — email, which provides another avenue for business email compromise or social engineering attacks.

Law firms have also traditionally been playing catch-up with uplifting their cyber security posture, which makes them an easier target. The siege on law firms and professional services in general will likely continue and so, firms and in-house teams should map out their supply chains and take measures to address and mitigate any risks that may leave them exposed to a cyber attack.

1 Fourth ASD Cyber Threat Report 2022-2023 published on 15 November 2023. https://www.asd.gov.au/news-events-speeches/news/2023-11-15-australian-signals-directorate-releases-2023-asd-cyber-threat-report

4 A shift towards the offensive

2023 saw a definite shift by governments and cyber attack victims towards offensive strategies rather than relying on defensive mechanisms.

In Australia, the Hack the Hacker Taskforce was set up to enhance the country's offensive capabilities. This is a permanent operation comprising approximately 100 police and defence personnel from the Australian Federal Police and Australian Signals Directorate to "hack the hackers", with an immediate priority to target ransomware groups. [2]

"This operation will collect intelligence and identify ring-leaders, networks and infrastructure in order to disrupt and stop their operations – regardless of where they are... [The operation will aim to] stop... incidents before they start... [and] where incidents do take place... cyber criminals will be hunted down and their networks disrupted."

– Clare O'Neil MP, Mark Dreyfus A-G and Richard Marles MP[3]

Victims of cyber attacks and data breaches are also now taking proactive action and using the court system to assist preventing or minimising a data leak or publication. Victims have long felt powerless as they work on containing and recovering from an attack and at the mercy of the threat actor in regards to the misuse of their stolen information. However, in 2023, victims in Ireland and Australia increasingly attempted to regain control through legal intervention and by securing injunctions to prevent the sale, publication, possession, or other use of any data that may have been stolen.

While serving an injunction order on a threat actor on the dark web is unlikely to stop them from publishing the stolen information, these court orders do prevent anyone else who has knowledge of the order, including the media, from publishing, making available to the public, or sharing any of the stolen information.

It is heartening that the courts, media and various social media providers have been willing to assist in such situations, and demonstrates that victims of cyber attacks are not entirely powerless. This may signal the beginning of victims' ability to take control of the situation and slowly shift the power balance back to their side.

5 Cyber attacks continue to run parallel with geopolitical conflicts

Ongoing geopolitical tensions, and particularly prevailing tensions between Russia-Ukraine, China-Taiwan and Israel-Hamas, continued to influence cyber threats in 2023.

Notably, the Israel-Hamas conflict coincided with a significant surge in cyber attacks, mirroring the early days of the Russia-Ukraine conflict. Hacktivism has been prominent in the Israel-Hamas conflict, as outside groups with vested interests in the conflict engage in operations using DDoS attacks and defacements targeting popular websites, media outlets and emergency response infrastructure. These tactics have aimed to cause disruption and influence public opinion through disinformation campaigns.

The Russia-Ukraine conflict has led to the continued escalation of state-sponsored cyber attacks and offensive cyber operations. The destructive targeting of Ukrainian critical infrastructure and government agencies has been a major part of the conflict to disrupt systems and destroy supply chains.[4] Despite this, Ukraine has demonstrated its ability to contain and defend against significant cyber activity from Russian and pro-Russian actors, noting that it has also received significant support from the international community.

The cyber front to China's offensive against Taiwan also gained momentum in 2023. Google has reportedly observed a massive increase in Chinese cyber attacks on Taiwan as tension heightens between them.[5] A senior engineering manager in Google's threat analysis unit reported that there are more than 100 groups in China alone trying to access the computers of Taiwan's defence sector and government agencies. [6] This has certainly prompted Taiwan to bolster its cyber resilience and brace for a potential cyber war. [7]

As the Russia-Ukraine conflict persists and the Israel-Hamas conflict unfolds, it is becoming increasingly evident that cyber attacks are shaping the dynamics of modern warfare. These conflicts reinforce the need for robust cyber security measures and international cooperation to address the risks and challenges presented by cyber warfare.

2 https://www.afr.com/politics/federal/australia-to-hack-the-hackers-behind-medibank-attack-o-neil-20221112-p5bxor

3 https://ministers.ag.gov.au/media-centre/joint-standing-operation-against-cyber-criminal-syndicates-12-11-2022

4 https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/

5 https://www.thedefensepost.com/2023/12/01/china-cyberattacks-taiwan-rising/

6 Ibid

7 https://www.thedefensepost.com/2023/10/04/taiwan-bracing-cyberwar-china/

8 https://kpmg.com/kpmg-us/content/dam/kpmg/pdf/2023/

6 AI-generated deepfakes lead to a rise in political disinformation

In our 2022/23 edition of CyberSight 360 we warned that threat actors would increasingly automate and launch AI-powered cyber attacks, including the use of deepfake technology.

The number of deepfake videos available online increased by 900% between 2022 and 2023[8].

AI-generated deepfakes rose in prominence in 2023, particularly in the political arena, and the weaponisation of this cheap and widespread disinformation technology impacts democracies and non-democracies alike. Recent examples of deepfake footage being used to deceive the public about statements and actions purportedly taken by political leaders include the following:

- On 2 March 2022, shortly after Russia's invasion of Ukraine, Ukraine24 released a video of President Volodymyr Zelenskiy taking to the lectern and asking Ukrainians to put down their arms and surrender to Russia. Except, this was not a true statement from President Zelenskiy but a deepfake video.[9] That said, it is unclear how many viewers were fooled by the video due to the discrepancies between the skin tone and pixelation on President Zelenskiy's neck and face, and the odd accent heard in the video.
- Days before Slovakia's October 2023 election, deepfake audio recordings were circulated on Meta social media platforms of Michal Šimečka, leader of the pro-Western Progressive Slovakia party, talking about rigging the election and doubling the price of beer.[10] Šimečka immediately denounced the audio as fake. Because the posts were audio, they were able to exploit a loophole in Meta's manipulated-media policy, which dictates that only fake videos—where a person has been edited to say words they never said—go against its rules.[11] Progressive Slovakia eventually lost the election.
- In March 2023 a deepfake image of Pope Francis in an ankle-length, belted white puffer jacket was circulated.[12] While the stakes of this fabrication were low compared to the potential harms inflicted by other political deepfakes, due to the Pope's status as a religious and political figure it hints at the pervasiveness of AI-generated deepfakes and the potential for disinformation. In recognition of this, the Pope called for a global treaty to regulate AI in a message titled "Artificial Intelligence and Peace".[13]
- Ahead of the 2023 Turkish presidential election, Recep Tayyip Erdoğan promoted a deepfake video that appeared to show his main rival, Kemal Kılıçdaroğlu, being endorsed by the Kurdistan Workers' Party – a designated terrorist group in Turkey. Although Kılıçdaroğlu pointed out the manipulation, the video had already circulated widely, and he ultimately lost the election.[14]
- In June 2023 hackers aired a deepfake video of President Vladimir Putin on a number of Russian television broadcasting networks calling for military mobilisation and declaring martial law, an incident the Kremlin described as a "hack".[15]
- In the US, ahead of the 2024 elections, Republican candidates were already resorting to AI-generated images in their campaign. On 5 June 2023 the DeSantis campaign published AI-generated images of Donald Trump and Anthony Fauci hugging, in a bid to sway public opinion.[16] A pro-Ron DeSantis super PAC also used an AI version of Donald Trump's voice in a television ad (Never Back Down) attacking the former president.[17]

deepfakes-real-threat.pdf

9 https://www.reuters.com/world/europe/deepfake-footage-purports-show-ukrainian-president-capitulating-2022-03-16/

10 https://www.wired.co.uk/article/slovakia-election-deepfakes

11 Ibid

https://transparency.fb.com/en-gb/policies/community-standards/manipulated-media/

12 https://www.bloomberg.com/news/newsletters/2023-04-06/pope-francis-white-puffer-coat-ai-image-sparks-deep-fake-concerns

13 https://www.forbes.com/sites/britneynguyen/2023/12/14/pope-francis-calls-for-global-treaty-to-regulate-ai-after-viral-deepfake-of-him-wearing-a-puffer-jacket/?sh=74ff8545f0fa

14 https://www.reuters.com/world/middle-east/erdogan-rival-accuses-russia-deep-fake-campaign-ahead-presidential-vote-2023-05-12/

https://www.afr.com/technology/deepfakes-will-supercharge-conspiracies-in-biggest-election-year-ever-20240103-p5euvo

15 https://www.nytimes.com/2023/06/05/world/europe/putin-deep-fake-speech-hackers.html

16 https://edition.cnn.com/2023/06/08/politics/desantis-campaign-video-fake-ai-image/index.html

https://www.washingtonpost.com/politics/2023/06/08/desantis-fauci-trump-ai-video/

17 https://www.politico.com/news/2023/07/17/desantis-pac-ai-generated-trump-in-ad-00106695

18 https://factcheck.afp.com/doc.afp.com.33YP34M

- US President Joe Biden has also been a target, including in a February 2023 deepfake video showing him announcing a military draft for Americans to fight in Ukraine,[18] as well as a recent fake robocall urging Democrats not to vote in the New Hampshire primary.[19]

The use of impersonation in political ads is certainly not new. However, AI-generated deepfakes demonstrate considerable potential to impact political campaign advertising, sway public opinion and ultimately dictate political outcomes — particularly in democracies with elections, and when combined with other types of attacks such as DDoS or network shutdowns to prevent correction of the disinformation.

Deepfake technology is advanced, cheap and accessible. If done with the right tools, the discrepancies can be difficult to notice. To address this, Google announced it would impose new labels on deceptive AI-generated political advertisements that could fake a candidate's voice or actions. From November 2023, Google has mandated all political advertisements label the use of artificial intelligence tools and synthetic content in their videos, images and audio.[20] US lawmakers are calling on social media platforms such as X (formerly Twitter), Facebook and Instagram to do the same in a bid to minimise voters' exposure to widespread disinformation.[21]

AI-generated disinformation (including political disinformation) is a cyber security threat because it can be used to fuel cyber attacks on a large scale. It uses deception to produce harm, particularly on widely-used social media platforms. By tapping into the political fervour surrounding elections, political campaigns and war, it can lead an unsuspecting individual to easily fall prey to social engineering attacks linked to AI-generated deepfakes and political disinformation being spread.

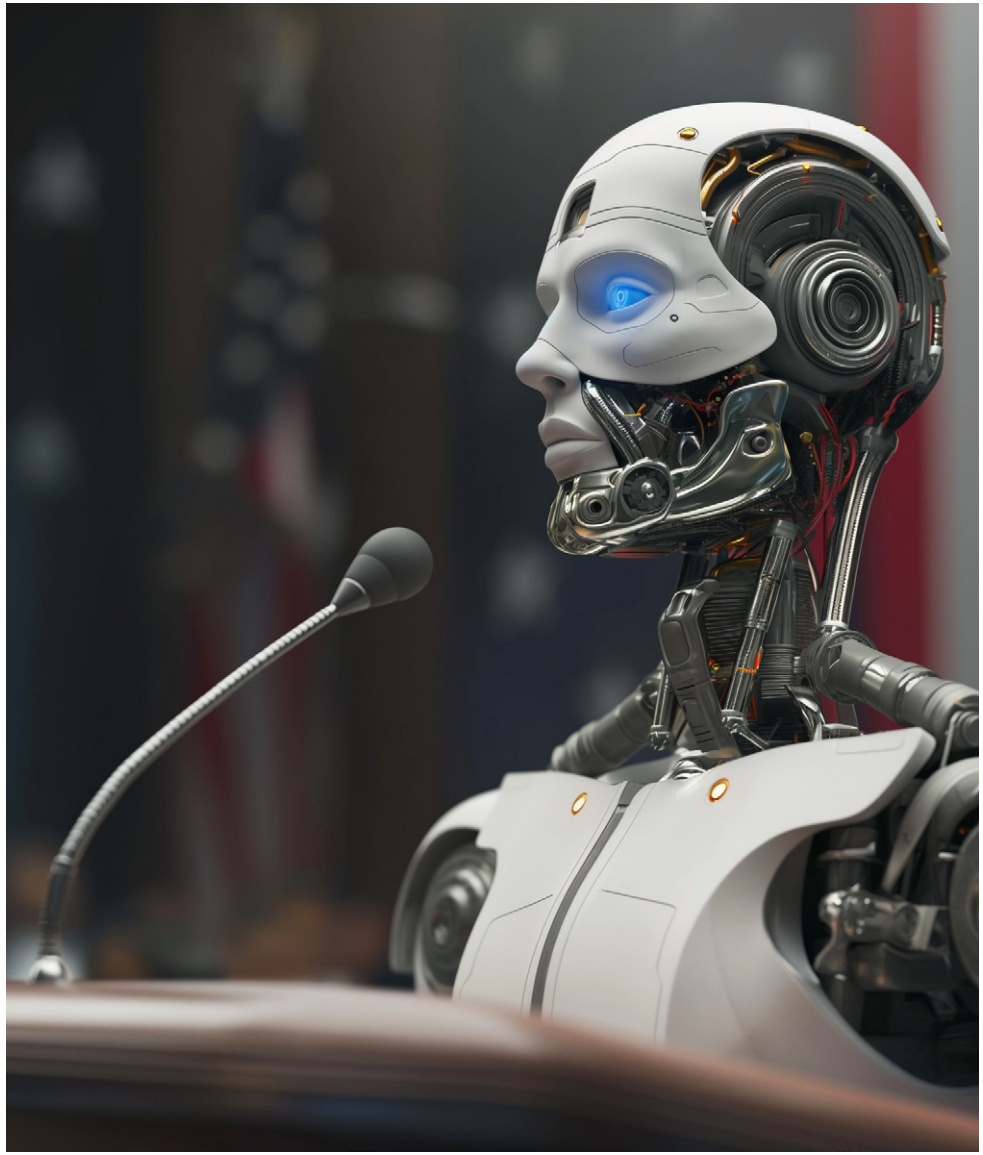
2024 is going to be a big year for elections, with major electoral events taking place in the US, Taiwan, India, Indonesia, Brazil and Russia. It will be interesting to see how deepfake technology will drive and determine the outcome of these elections, and the corresponding cyber security threat that comes with it.

19 https://www.nbcnews.com/politics/congress/fake-biden-robocall-alarms-capitol-hill-unclear-congress-will-act-rcna135248

https://www.wired.com/story/biden-robocall-deepfake-danger/

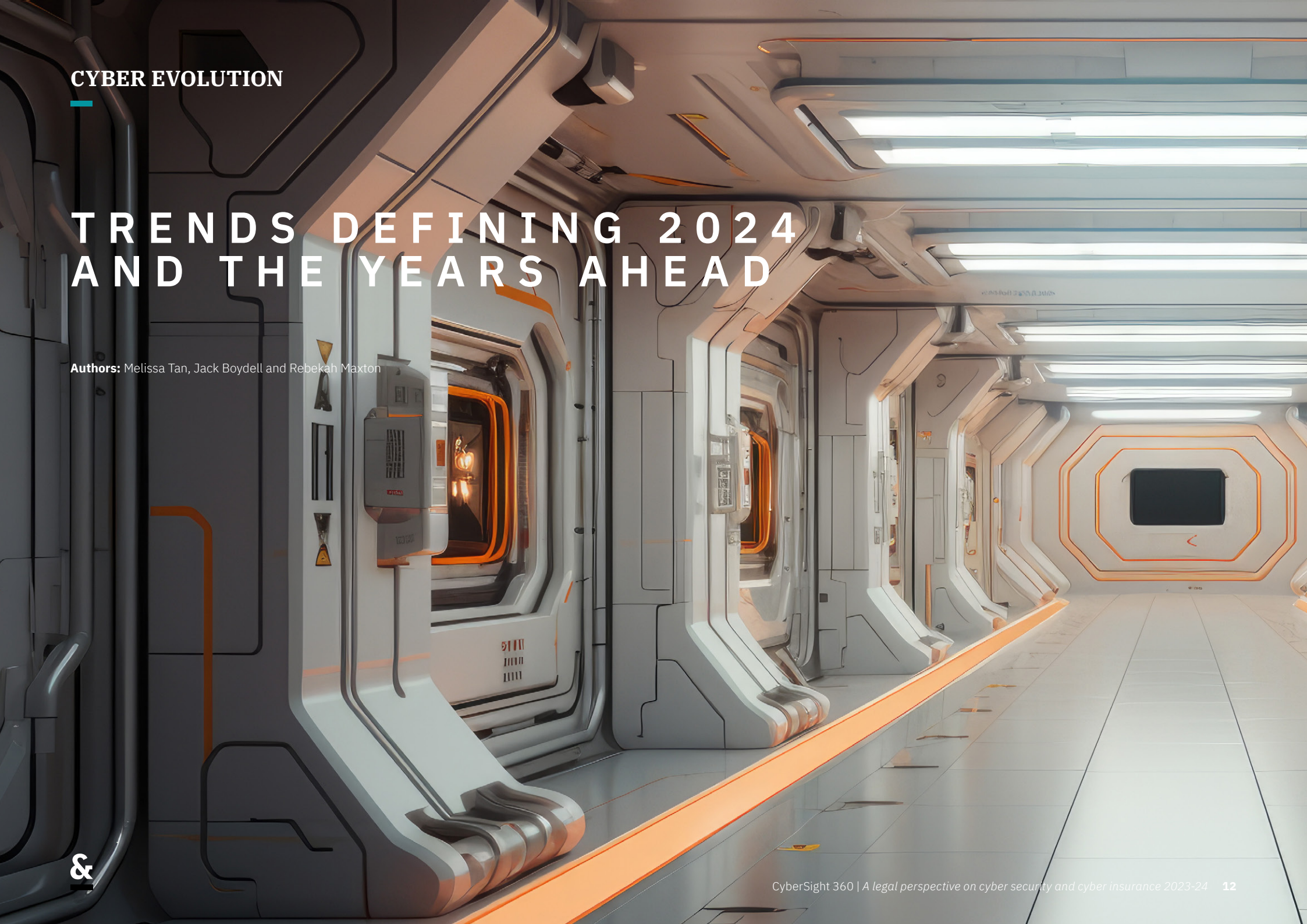
20 https://www.politico.com/news/2023/09/06/google-ai-political-ads-00114266

21 https://www.pbs.org/newshour/politics/u-s-lawmakers-question-meta-and-x-over-ai-generated-political-deepfakes-ahead-of-2024-election



TRENDS DEFINING 2024 AND THE YEARS AHEAD

Authors: Melissa Tan, Jack Boydell and Rebekah Maxton



The cyber risk landscape is not static, and new avenues of attack for cyber criminals continue to emerge.

The cyber threats and cyber trends that will define 2024 and beyond will arise from:

- new and emerging technologies (5G technology and IoT devices)
- new methods (evolving ransomware), and
- the evolving geopolitical landscape (cyber espionage).

1 New and emerging technologies: 5G, IoT devices and cyber security risks

Australia's three mobile network operators – TPG Telecom (Vodafone), Telstra, and Optus – recently announced the closure of their 3G networks to make way for 5G technology. This closure will happen in stages, with the TPG Telecom-owned Vodafone 3G network closing from 15 December 2023; Telstra commencing a gradual switch-off of its 3G network from 30 June 2024, and Optus phasing out its 3G network from September 2024.[1]

The fifth generation (5G) of wireless technology represents a complete transformation of telecommunication networks and will change the digital landscape, providing a catalyst for innovation, new markets, and economic growth.[2] However, the technology will also pose new cyber security risks that businesses need to prepare for. We predict that the cyber security risks of new and emerging technologies such as 5G will define 2024 and beyond as countries become more reliant on this technology.

5G technology is fundamentally different from previous generations and represents greater connectivity and enhanced network capacity. According to GSMA Intelligence, by 2030 5G will overtake 4G to become the globally dominant mobile technology, with 5.3 billion connections.[3] However, 5G networks also boast a wider attack surface due to the increased number of connected devices and the denser network infrastructure. Additionally, its reliance on cloud, virtualisation, and software-defined networking introduces new avenues for exploitation.[4]

Individuals, businesses, and governments should consider the following risks:[5]

- 5G networks will be exposed to various cyber threats, including ransomware, potential data breaches and DDoS attacks. The increased attack surface, higher data speeds and lower latency provide cyber criminals with new opportunities to launch sophisticated attacks.
- Internet of Things (IoT) vulnerabilities also need to be proactively managed. The proliferation of IoT devices on 5G networks creates a security challenge, as many IoT devices often do not have robust security features.
- The enhanced network capability and increased transmission of data will also bring heightened privacy and data risks.
- Finally, supply chain concerns apply equally to 5G networks. With 5G infrastructure being built by multiple vendors across the globe, the supply chain will become more complex and potentially more vulnerable to cyber attacks. A compromised component within the supply chain could lead to widespread vulnerabilities and potentially catastrophic consequences.

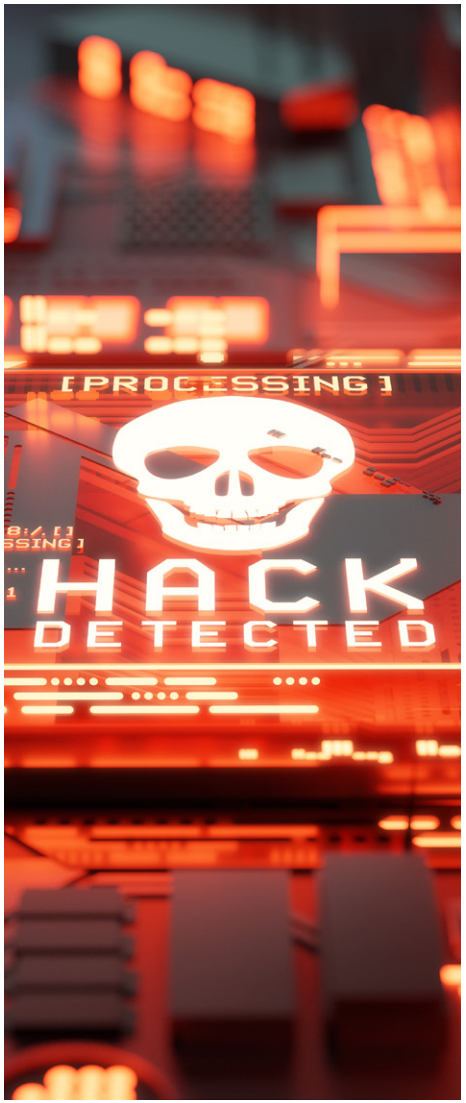
1 https://www.tio.com.au/sites/default/files/2023-12/AMTA_3G%20network%20closure%20release%20Fact%20Sheet.pdf

2 https://www.cisa.gov/topics/risk-management/5g-security-and-resilience

3 https://www.gsma.com/newsroom/article/safeguarding-the-future-managing-5g-security-risks/#:~:text=Cyber%2DAttacks%3A%205G%20networks%20will,potential%20data%20breaches%2C%20and%20ransomware.

4 https://www.gsma.com/newsroom/article/safeguarding-the-future-managing-5g-security-risks

5 Ibid



2 New methods: evolving ransomware

The one certainty about ransomware attacks is that they will continue to evolve to be more mature, sophisticated and targeted.

Ransomware groups have steadily shifted and adapted their techniques in order to remain a threat. In previous years, they would send phishing emails to gain access to an organisation before embedding their malware.[6] Law enforcement, government regulation and user awareness have since forced ransomware groups to adapt.[7]

Although early 2023 saw a slight decline in the number of ransomware attacks, they were more commercialised, advanced and better targeted. This has no doubt contributed to the "stunning success" of ransomware gangs in 2023, which have reportedly stolen more than US$1 billion in 2023 — the largest amount ever recorded, as reported by Chainalysis Inc.[8] This is almost double the US$567 million ransomware gangs made away with in 2022.

In 2023 we also saw ransomware attacks combined with other methods to expand their impact, such as targeting zero-day vulnerabilities in digital supply chains for the attack to penetrate multiple businesses. A report by Akamai Technologies stated that several major ransomware operators were focused on acquiring zero-day vulnerabilities — either through in-house research or procurement from grey-market sources — to use in their attacks.[9] This combined attack method proved to be a more efficient and profitable pathway for cyber criminals as they were able to gain unauthorised access into many organisations through one attack.

The most notable victim of zero-day vulnerability ransomware in 2023 was MOVEit, a file transfer service that was infiltrated using Cl0p ransomware[10]. The vast extent of this hack is still being understood as the breach impacted many companies worldwide including IBM, Shell, British Airways and the BBC. Chainalysis reported that the Cl0p ransomware gang racked up over US$100 million in ransom payments with this breach.[11]

Kapersky's overview of ransomware trends, published in May 2023, identified three key trends that demonstrated the increased sophistication of ransomware.[12]

Firstly, ransomware groups are incorporating self-spreading functionality or imitations into their malware, as seen in recent activity by threat actors Black Basta, LockBit and Play.

Secondly, cyber criminals are exploiting vulnerabilities in antivirus drivers, even targeting industries like gaming. The trend of driver abuse will continue to evolve.

Finally, large ransomware gangs are using leaked or purchased code to strengthen their offensive capabilities. Kapersky recently saw the LockBit group adopt at least 25% of leaked Conti code and issue a new version based entirely on that. Initiatives like these enable affiliates to work with familiar code, while malware operators get an opportunity to boost their offensive capabilities. Collaboration among ransomware gangs has also resulted in more advanced attacks. Groups are working together to develop cutting-edge strategies for circumventing security measures and improving their attacks. The trend has given rise to ransomware businesses that build high-quality hack tools and sell them to other ransomware businesses on the black market.

We predict that as well as ransomware attacks continuing to scale up with increased commercialisation, threat actors' methods will keep evolving to become more impactful, efficient and effective. Threat actors will start using automation as a time and cost-saving technique. Utilising AI techniques to minimise human error, cyber criminals could traffic a high volume of automated ransomware attacks onto one business, making it much harder to defend. Building on the success of cloud-native attacks, hackers could evolve to target the weakest link in the chain, further embedding ransomware until they are able to gain access to a larger company.

Organisations will need to remain vigilant including regularly checking their software and firmware for any vulnerabilities so they can stay a step ahead of the ransomware groups as they continue to adapt and improve their techniques.

6 https://www.akamai.com/blog/security/ransomware-on-the-move-evolving-exploitation-techniques

7 https://www.trendmicro.com/en_vn/ciso/23/b/ransomware-trends-evolutions-2023.html

8 https://www.chainalysis.com/blog/ransomware-2024/

9 https://www.akamai.com/newsroom/press-release/akamai-research-rampant-abuse-of-zero-day-and-one-day-vulnerabilities-leads-to-143-increase-in-victims-of-ransomware

10 https://assets.sophos.com/X24WTUEQ/at/c949g7693gsnjh9rb9gr8/sophos-state-of-ransomware-2023-wp.pdf

11 https://www.chainalysis.com/blog/ransomware-2024/

https://www.insurancejournal.com/news/national/2024/02/07/759806.htm

12 https://www.kaspersky.com/about/press-releases/2023_should-i-stay-or-should-i-go-how-major-gangs-shutdown-affected-ransomware-trends-for-2023

3 The evolving geopolitical landscape and rise of cyber espionage

Cyber espionage, or cyber spying, has been defined as a type of cyber attack in which an unauthorised user attempts to access sensitive or classified data or intellectual property (IP) for economic gain, competitive advantage or political reasons.[13] As geopolitical conflicts and risks continue to evolve and increase in tension, we predict a continued rise in instances of cyber espionage.

Critical infrastructure remains one of the top targets for malicious cyber attacks.[14] Governments and operators of critical infrastructure remain vulnerable due to the sensitive information they possess and their high level of connectivity with other organisations, paving the way for a rise in cyber espionage. In 2023 and the beginning of 2024 in both Australia and the United States, Chinese-led cyber operations have targeted major government infrastructure.[15] In an unprecedented joint statement, on 17 October 2023 intelligence chiefs from the Five Eyes countries — United States, Britain, Canada, Australia and New Zealand — warned against China's cyber attempts to steal various state secrets.[16]

Private sector organisations that possess confidential information have just as much reason to be concerned. Moving into 2024 and beyond, organisations need to be wary of not just the financial risk of harm when undoing a cyber attack, but also the implications of a cyber threat actor targeting sensitive or classified data or intellectual property for non-financial reasons, particularly if a state-backed actor is involved. Several key incidents have demonstrated that threat actors do not need to target government agencies directly for cyber espionage; they can do so through the supply chain, including through legal advisors.

Governments, operators of critical infrastructure and private sector agencies that contain any level of sensitive information or classified data or intellectual property must focus on continuing to enhance cyber security measures to ensure resilience against such attacks.

13 https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/

14 https://www.cyber.gov.au/about-us/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023

15 https://www.reuters.com/technology/us-disrupts-chinese-botnet-targeting-critical-infrastructure-fbi-says-2024-01-31/; https://www.weforum.org/agenda/2023/06/us-china-cyber-espionage-campaign-cybersecurity-news/

https://www.abc.net.au/news/2023-11-15/asd-reports-increase-in-cyber-attacks/103103320

16 https://www.reuters.com/world/five-eyes-intelligence-chiefs-warn-chinas-theft-intellectual-property-2023-10-18/

CYBER INSURANCE TRENDS TO LOOK OUT FOR IN 2024 AND BEYOND

Authors: Melissa Tan, Jack Boydell and Rebekah Maxton

The sustainability of the cyber insurance industry, and particularly concerns over cyber risk accumulation and systemic risks, will continue to be front of mind for the cyber insurance industry for the foreseeable future.

Within this, we have identified the following themes to look out for in the cyber insurance industry in 2024 and beyond.

1 Cyber war exclusions - time to be tested?

Many of the war exclusions we are familiar with, particularly in the property insurance context, date back to conflicts occurring in the 1930s, including the second Italo-Abyssinian War and the Spanish Civil War.[1] An agreement was entered into between the Lloyd's Underwriters Association (LUA) and the Association of British Insurers (ABI) to exclude war and civil war on all policies issued by Lloyd's and London Companies subscribing to the agreement. This led to the introduction of the War and Civil War Exclusion clause NMA 464 1/1/38.

With cyber warfare becoming a common aspect of conflict in recent years, concerns over cyber insurance's exposure to correlated widespread aggregation, as well as uncertainties in the construction of traditional war exclusions as applied to state-sponsored cyber operations, the insurance industry has moved to modernise war exclusions to address cyber warfare risk.

In November 2021 the Lloyd's Market Association (LMA) released four war, cyber war and cyber operation exclusions that were intended to be models for standalone cyber policies. The clauses ranged from a blanket exclusion to gradations of exclusions and exceptions for various losses. In its companion Market Bulletin Y5381, Lloyd's required that all standalone cyber policies have a suitable clause excluding liability for losses arising from any state-backed cyber attack with five minimum requirements,[2] with this requirement taking effect on 31 March 2023. Although the LMA model exclusions themselves were not mandatory, it was said that they would meet all requirements. Insurers were free to use different language, if vetted by counsel and approved by Lloyd's.

On 18 January 2023 eight amended model exclusions were published, differentiated by a Type A and a Type B.[3] Notably, the Type B clauses lack attribution, which means that in order for these clauses to be compliant, carriers will need to articulate to Lloyd's how they expect attribution to be addressed.

The LMA has also conducted a review of a number of sample clauses from various carriers and provided confirmation on compliance with Lloyd's requirements as set out in the bulletin.[4]

Whether they are caught within the Lloyd's requirements or otherwise, insurers will need to modernise their war exclusion for cyber coverage, particularly in relation to how state-sponsored cyber attacks are dealt with. Considering the current geopolitical landscape and ongoing conflicts and tensions around the world, as well as the rise of cyber warfare and state-sponsored cyber operations, the operation and scope of cyber war exclusions will likely be tested in the near future.

1 https://www.insurancejournal.com/news/national/2023/04/04/715079.htm

2 1. Exclude losses arising from a war (whether declared or not), where the policy does not have a separate war exclusion. 2. (Subject to 3) Exclude losses arising from state-backed cyber-attacks that: (a) significantly impair the ability of a state to function; or (b) significantly impair the security capabilities of a state. 3. Be clear as to whether cover excludes computer systems that are located outside any state affected in the manner outlined in 2(a) & (b) above, by the state-backed cyber attack. 4. Set out a robust basis by which the parties agree on how any state-backed cyber attack will be attributed to one or more states. 5. Ensure all key terms are clearly defined.

3 LMA5564A, LMA5564B, LMA5565A, LMA5565B, LMA5566A, LMA5566B, LMA5567A, LMA5567B.

4 https://www.lmalloyds.com/LMA/Underwriting/Non-Marine/Cyber_Clauses/cyber_war_clauses.aspx

2 Active cyber insurance - the next big thing?

Businesses, and particularly small and medium-sized enterprises (SMEs), may increasingly look to active cyber insurance as an alternative insurance product in 2024 and beyond.

In 2023 an active cyber insurer, Coalition, entered the Australian market with a suite of active cyber insurance products.[5] Active cyber insurance differs from traditional insurance coverage in that it focuses on preventing digital risks before a cyber incident occurs. It helps an insured to understand their cyber risk posture and improve their defences to minimise the likelihood of a cyber attack, instead of solely providing financial compensation and incident response support after a cyber incident occurs.

SMEs often lack the resources to invest heavily in uplifting their cyber resilience or tools to detect, assess, and respond to cyber incidents, and only 20% of Australian SMEs currently have cyber insurance.[6] With its unique offering of active security protection and insurance coverage, we may soon see a bigger uptake of active cyber insurance amongst SMEs.

3 Talent shortage issue in underwriting and claims teams

The cyber insurance industry will continue to grapple with attracting and developing talent within its underwriting and claims teams.

Cyber is a class of insurance that is still relatively young and developing, and yet highly technical. The ever-evolving risk landscape and technicalities behind the nature of cyber attacks and claims means specialist knowledge is required to effectively underwrite and manage claims in this area.

Insurers in Australia and internationally have been adding cyber security professionals to their underwriting teams to fill the technical expertise gap. However, there remains a shortage of insurance professionals with specialised cyber security knowledge and expertise, as well as a good understanding of the operations and dynamics of the insurance market.

Investing in internal staff who have an interest in this area and establishing structured development pathways for their progression will likely be a focus for many insurers facing a talent shortage in their cyber line.

4 Developing innovative solutions for capacity

Government backstop and catastrophe bonds

Concerns about systemic cyber risks and cyber catastrophes are not new and continue to be a key item on the agenda for most cyber insurers. In 2023 we saw further development of two alternative solutions to deal with this issue.

In the United States, the first solution being explored by the US Treasury Department is the introduction of a federal insurance backstop for catastrophic cyber events, currently being researched by the Department's Federal Insurance Office in line with the strategic objectives announced in the Biden administration's National Cybersecurity Strategy Implementation Plan.

The US Treasury's "tentative conclusion" regarding the scope of its focus is that because the private market for insurance against attritional cyber risk from losses other than those related to major catastrophes is dynamic and growing, it anticipates that its assessment of a potential federal insurance response will remain sharply focused on catastrophic cyber risk.[7] Further, when assessing the insurance

market for catastrophic cyber risk, it will remain focused on "the policy options for some kind of public-private sector collaboration or other federal response that cabins catastrophic cyber risk alongside the existing and expanding commercial cyber insurance market".[8]

In Australia, the Australian Reinsurance Pool Corporation (ARPC) manages the terrorism pool and cyclone pool. The Australian terrorism pool still excludes cyber terrorism.[9] Although the ARPC may one day include cyber risks (including cyber terrorism) in a cyber pool, we suspect that governments and insurers are waiting to see what emerges from the US Treasury's proposal for a federal insurance backstop for catastrophic cyber events and how that could be replicated or adapted. Work focussed on this proposed solution will continue in 2024 and beyond.

5 Coalition is backed by Allianz Australia Limited.

6 https://insurancecouncil.com.au/issues-in-focus/cyber-risk/

https://www.lifeinsuranceinternational.com/news/coalition-active-cyber-insurance-australia/

7 https://home.treasury.gov/news/press-releases/jy1922

8 Ibid

The second alternative solution is the further development of cyber catastrophe bonds. In January 2023 insurance group Beazley unveiled a US$45 million catastrophe bond, the first insurance-linked securities (ILS) instrument established in the cyber insurance market.

The bond gave Beazley broad cyber reinsurance cover for remote probability catastrophic and systemic events, including tech errors & omissions (E&O) risks, across a one-year term.[10] This was followed by a second cyber catastrophe bond issuance, using the same format of placing it with investors, and adding US$20 million of fresh reinsurance cover from capital markets.[11] A third cyber catastrophe bond issuance provided a further US$16.5 million of reinsurance cover, which means Beazley had US$81.5 million of cyber reinsurance in cyber catastrophe bond form running to the end of 2023, with final maturity on 8 January 2024.[12]

Beazley announced on 2 January 2024 that it had closed its first 144A cyber catastrophe bond providing cover of US$140 million.[13] This inaugural 144A bond builds on its previous US$81.5M million cyber catastrophe bond programme of 2023.

Named PoleStar Re Ltd, the Series 2024-1 Class A notes are designed to cover remote probability catastrophic and systemic events. Structured on an indemnity trigger and per-occurrence basis, the bond runs for a two-year term to the end of 2025.[14]

In November 2023, AXIS Capital Holdings Limited also announced the closing of its first 144A cyber catastrophe bond, a US$75 million Long Walk Reinsurance Ltd transaction that provides the firm's subsidiaries with fully collateralised indemnity reinsurance for systemic cyber events on a per-occurrence basis.[15] We understand that the US$75 million of Series 2024-1 Class A notes are scheduled to mature in January 2026.

These developments suggest that the ILS investor community has confidence in such products and continues to see opportunities in this space. Specialty solutions to address systemic cyber risk and cyber catastrophes will continue to be a key theme for the cyber insurance industry in the years to come.

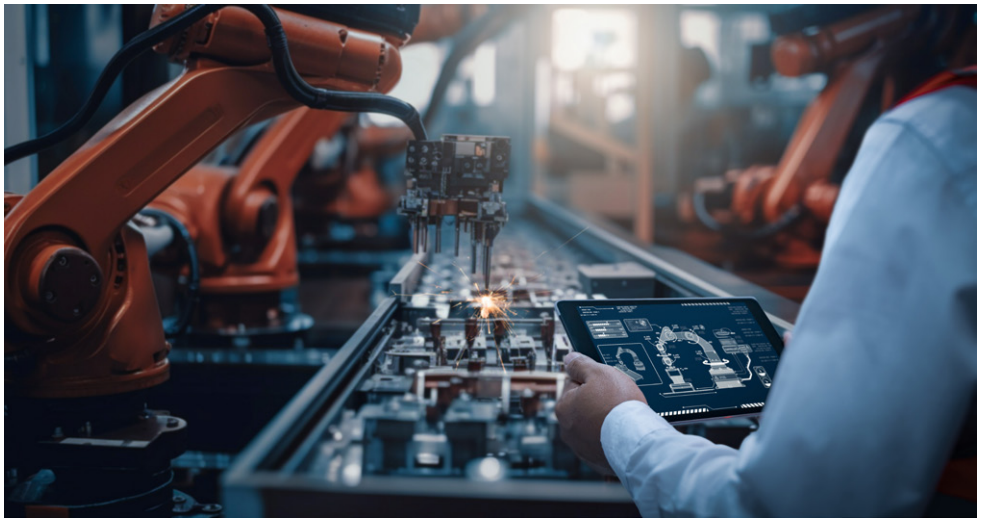
5 Adapting to new risks - OT/IT overlap

To remain sustainable, the cyber insurance industry must be responsive to the risks brought about by emerging technologies and overlapping risks – such as the OT/IT overlap.

Operational technology (OT) remains a critical component of any heavy industry organisation's ability to monitor and control internal systems. Previously, this involved physical servers and machinery that were typically isolated from the digital world. This meant it was more common for information technology (IT) networks to be targeted by hacking groups, as they could be accessed online.

As technology has improved, OT equipment has developed to include aspects of both physical machinery and online networks. An example of this is the recent increase in factories incorporating AI to improve the efficiency of their machinery. As a consequence, OT servers have become more vulnerable to cyber attacks and ransomware and malicious compromise attempts against OT assets have increased significantly.[16]

It is therefore no surprise that the Australian Prudential Regulation Authority (APRA)[17] has issued new standards on operational risk management, Prudential Standard CPS 230 Operational Risk Management, with a focus on operational resilience to maintain continuity of critical financial services, including to combat elevated levels of cyber risk.



The CPS 230 aims to strengthen the management of OT systems and OT risks through new requirements that address weaknesses in existing controls, improve business continuity planning to ensure APRA-regulated entities are positioned to respond to severe disruptions, and enhance third-party risk management by ensuring risks from material service providers are appropriately managed. This prudential standard will commence on 1 July 2025. This will work alongside Prudential Standard CPS 234 Information Security, which seeks to strengthen minimum cyber standards for APRA-regulated entities.

As the cyber insurance industry faces growing challenges posed by overlapping risks, it will need to continue to adapt its products in response.

9 https://arpc.gov.au/resources/mind-the-gap/

10 https://www.artemis.bm/news/beazley-sponsors-third-cyber-catastrophe-bond-16-5m-cairney-iii/

11 The Beazley cyber cat bonds are privately placed Section 4(2) issuances, using as their special purpose insurer (SPI) the Artex Risk Solutions owned and operated segregated account reinsurance transformer platform, named Artex SAC Limited, acting on behalf of a segregated account, or cell. https://www.artemis.bm/news/beazley-tops-up-cyber-cat-bond-cover-with-second-20m-issuance/

12 https://www.artemis.bm/news/beazley-sponsors-third-cyber-catastrophe-bond-16-5m-cairney-iii/

13 https://www.beazley.com/en-us/news-and-events/beazley-closes-$140m-cyber-catastrophe-bond

14 Ibid

15 https://www.reinsurancene.ws/axis-successfully-closes-markets-first-144a-cyber-catastrophe-bond/

16 https://www.cyberinsuranceacademy.com/knowledge-hub/guide/how-is-the-cyber-insurance-industry-dealing-with-operational-technology/#:~:text=These%20measures%20have%20become%20increasingly,event%20consequences%2C%20including%20business%20interruption.

17 https://www.apra.gov.au/operational-risk-management-0

2023-2030 AUSTRALIAN CYBER SECURITY STRATEGY

Factors for success and how we compare

Authors: Melissa Tan, Jack Boydell and Rebekah Maxton

STRATEGY

*On 22 November 2023 the Australian government released the 2023-2030 Australian Cyber Security Strategy (**Strategy**),[1] with the aim of strengthening Australia's cyber defences to enable citizens and businesses to prosper, be resilient to, and recover quickly from cyber attacks.*

The ambitious Strategy sets out a roadmap that will help realise the Australian government's vision of becoming a "world leader" in cyber security by 2030, a mere six years away.

The Strategy explained

The key focus of the Strategy is to implement six "cyber shields" to help defend Australian citizens and businesses from cyber threats, with each "shield" providing an additional layer of defence to make Australia a harder target for cyber attacks. These are:

- Strong businesses and citizens
- Safe technology
- World-class threat sharing and blocking
- Protected critical infrastructure
- Sovereign capabilities
- Resilient region and global leadership.

The Strategy will be delivered across three horizons:

- Horizon 1 2023-25 - strengthening our foundations by addressing critical gaps in the cyber shields, building better protections for our most vulnerable citizens and businesses, and supporting initial cyber maturity uplift across our region. A Horizon 1 Action Plan supplements the Strategy and details the key initiatives that will commence over the next two years. The Action Plan will be reviewed every two years and updated as required.
- Horizon 2 2026-28 - expanding reach by scaling cyber maturity across the whole economy, investing in the broader cyber ecosystem, and continuing to scale up the cyber industry and growing a diverse cyber workforce.
- Horizon 3 2029-30 - advancing the global frontier of cyber security, leading the development of emerging cyber technologies and adapting to new risks and opportunities across the cyber landscape.

The Australian government has committed to working with industry to implement the shields and enhance Australia's national cyber security and resilience in what it is calling a "new era of public-private co-leadership". This includes inviting industry and businesses to "co-design options" for the regulation and legislative changes proposed under the shields.

A consultation paper released in January 2024 outlined two areas of proposed legislative reforms as set out in the Action Plan to urgently address gaps in existing regulatory frameworks and amend the SOCI Act to protect Australia's critical infrastructure.

1. New cyber security legislation:

- Mandating secure-by-design standards for Internet of Things (IoT) devices
- Creating a mandatory no-fault, no-liability ransomware reporting obligation to improve understanding of ransomware incidents across Australia

- Creating a "limited use" obligation for information voluntarily provided to the Australian Signals Directorate and the National Cyber Security Coordinator to encourage industry to continue to collaborate with the government on incident response and consequence management
- Establishing a Cyber Incident Review Board to conduct no-fault incident reviews and share lessons learned to improve our national cyber resilience.

2. SOCI Act amendments:

- Clarifying obligations for critical infrastructure entities to protect data storage systems that store business critical data, where vulnerabilities in these systems could impact the availability, integrity, reliability, or confidentiality of critical infrastructure
- Introducing a last resort consequence management power for the Minister of Home Affairs to authorise directions to a

1 https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf

critical infrastructure entity in relation to the consequences of incidents that may impact the availability, integrity, reliability, or confidentiality of critical infrastructure
- Simplifying information sharing to make it easier for critical infrastructure entities to respond to high-risk, time-sensitive incidents
- Providing a power for the Secretary of Home Affairs or the "relevant Commonwealth regulator" to direct a critical infrastructure entity to address deficiencies in its risk management program
- Consolidating telecommunications security requirements under the SOCI Act.

The Australian government has committed A$586.9 million in funding to the Strategy,[2] on top of a commitment to fund A$2.3 billion of existing related initiatives that will support the Strategy delivered by the Australian Signals Directorate between now and 2030.

Much has been said and written about the Strategy since it was unveiled. Two key issues to consider are how the Strategy will succeed in achieving its ambitious vision; and how it compares against the cyber security strategies of other key jurisdictions.

What will the Strategy's success depend on?

In our view, there are three key determinants for the success of this Strategy.

Firstly, it is important to recognise that as a broad plan to achieve a particular outcome, the Strategy is meant to be ambitious — although it must also be realistic to be successful. Whether or not the Strategy is realistic and successful will largely depend on:

- the Action Plan, which will need to be reviewed every two years as planned to ensure it remains current and relevant through to 2030; and
- active participation in the public-private co-leadership co-design process, which seeks to particularise the specific legislative reforms and non-legislative cyber initiatives and partnerships necessary to give force to the Strategy. Besides submissions to the consultation paper, the Department of Home Affairs has been organising expert roundtables, town halls and deep-dive events which are critical to this co-design process. Active participation by the right cyber security experts with the right expertise is key.

Secondly, the Strategy and Action Plan need to be truly flexible and demonstrate measurable impact that can be reviewed independently. The government has indicated that the Strategy's implementation will be supported by "robust evaluation of all initiatives" and a flexible approach to delivery that adapts to the changing geopolitical landscape, threat environment and trends in the technology market. It is not clear what is planned in concrete terms other than an updated Action Plan every two years, but we suggest that:

- a "robust evaluation of all initiatives" could be undertaken by an independent Strategy Review Committee, with recommendations used to inform the Action Plan and any further legislative and non-legislative reforms; and
- as legislative reforms are often slow to respond to changes to the geopolitical landscape, threat environment and trends in the technology market, non-legislative cyber initiatives and partnerships will be critical for flexibility and faster response times.

Thirdly and most importantly, if Australia is serious about bolstering its cyber defences and resilience and becoming a "world leader" in cyber security by 2030, this Strategy will need to be able to withstand political change and party politics. To achieve a greater good for the country and the region, the Strategy will need the buy-in and commitment of the Australian government for the next six years and beyond, regardless of which political party is in power.

2 This includes: A$290.8 million to support small and medium business, build public awareness, fight cyber crime, break the ransomware business model, and strengthen the security of Australians' identities; A$4.8 million to establish consumer standards for smart devices and software; A$9.4 million to build a threat sharing platform for the health sector; A$143.6 million to strengthen critical infrastructure protections and uplift government cyber security; A$8.6 million to professionalise the cyber workforce and accelerate the cyber industry in Australia; A$129.7 million to strengthen regional cooperation, cyber capacity uplift programs, and leadership in cyber governance forums on the international stage. https://www.globalaustralia.gov.au/news-and-resources/news-items/australias-strategy-become-global-cyber-leader-2030

How do we compare against the US, UK, EU, Singapore and China?

The table on the pages that follow sets out how Australia's 2023-30 Cyber Security Strategy compares with the following international cyber security strategies, particularly where there are similarities or potential overlaps with the six cyber shields:

- The US National Cybersecurity Strategy dated March 2023 and the US National Cybersecurity Strategy Implementation Plan dated July 2023[3]
- The UK National Cyber Strategy 2022[4]
- The EU's Cybersecurity Strategy for the Digital Decade, dated December 2020[5]
- The Singapore Cybersecurity Strategy 2021[6]
- China's National Cyberspace Security Strategy 2016.[7]

We note the following:

- The strategies are each structured around key priorities (shields, pillars, objectives or tasks) that are further broken down into initiatives. The strategies aim for cyber security to be a national effort, with a key focus on building cyber resilience from within.
- Many of the strategies are multi-year plans, with Australia and the US in particular supplementing their strategies with action plans or implementation plans that set out specific goals and timelines. Australia, US and the UK have also implemented ways to measure the success of their initiatives. In contrast, it is not clear how Singapore or China propose to measure and assess the effectiveness of their initiatives.
- There are many similarities in the strategies of Australia and the US, including the proposed establishment of a Cyber Incident Review Board (CIRB) in Australia and the Cyber Safety Review Board (CSRB) in the US.
- Protecting the cyber security of critical infrastructure is specifically highlighted in the strategies of Australia, the US, EU, Singapore and China. Interestingly, there is no specific pillar relevant to critical infrastructure in the UK cyber security strategy, although critical national infrastructure is mentioned under various pillars.
- Improving government threat intelligence capabilities and being on the offensive (besides cyber defensive tactics) are also a common theme across the strategies.
- All strategies recognise the need to attract and retain cyber talent, as well as improve the quality of and expand the cyber security workforce. This is because uplifting cyber resilience requires having the right people with the right cyber security expertise.
- International cooperation and global cyber leadership also feature prominently across all strategies, although this will likely be guided by international politics and allied relationships or partnerships. The US unsurprisingly seeks to take on the global leadership role by expanding its ability to assist allies and partners, while Australia aspires to regional leadership by supporting a cyber resilient region as the partner of choice.

By supplementing the Strategy with concrete actions and proposed priorities as articulated in the consultation paper, co-designing with public-private cooperation, articulating how success will be measured, adopting a flexible approach, and ensuring alignment with the strategies of key allies, we consider there is much potential and promise in the 2023-2030 Australian Cyber Security Strategy as a way forward in strengthening Australia's cyber defences and establishing us as one of the world's leading cyber security nations – as long as this Strategy continues to have the buy-in and commitment of the Australian government for the next six years and beyond, regardless of which political party is in power.

3 https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/13/fact-sheet-biden-harrisadministration-publishes-thenational-cybersecurity-strategyimplementation-plan/

https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf

4 https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022

5 https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

6 https://www.csa.gov.sg/Tips-Resource/publications/2021/singapore-cybersecurity-strategy-2021

7 https://www.cac.gov.cn/2016-12/27/c_1120195926.htm

https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/

HOW AUSTRALIA'S STRATEGY COMPARES WITH OTHER JURISDICTIONS

Australia

(6 cyber shields) - 2023 to 2030

Shield 1

Strong businesses and citizens

- Support SMEs to strengthen their cyber security
- Help Australians defend themselves from cyber threats
- Disrupt and deter threat actors from attacking Australia
- Work with industry to break the ransomware business model
- Provide clear cyber guidance for businesses including sharing lessons learned from cyber incidents by establishing a Cyber Incident Review Board (CIRB)
- Make it easier for Australian businesses to access advice and support after a cyber incident
- Secure our identities and provide better support to victims of identity theft.

US

(5 pillars) - 2023 to FY26

Pillar 1

Defend critical infrastructure

Strategic Objective 1.4: Update federal incident response plans and processes including ensuring that the cyber security community benefits from lessons learned through the Cyber Safety Review Board (CSRB).

Pillar 2

Disrupt and dismantle threat actors

Strategic Objective 2.4: Prevent abuse of US-based infrastructure

Strategic Objective 2.5: Counter cyber crime, defeat ransomware.

Pillar 4

Invest in a resilient future

Strategic Objective 4.5: Support development of a digital identity ecosystem.

UK

(5 pillars) - 2022 to 2025

Pillar 1

UK cyber ecosystem - strengthening the UK's cyber ecosystem

Objective 1: Strengthen the structures, partnerships and networks necessary to support a whole-of-society approach to cyber

Objective 3: Foster the growth of a sustainable, innovative and internationally competitive cyber and information security sector, delivering quality products and services, which meet the needs of government and the wider economy.

Pillar 2

Cyber resilience - building a resilient and prosperous digital UK

Objective 1: Improve the understanding of cyber risk to drive more effective action on cyber security and resilience

Objective 2: Prevent and resist cyber attacks more effectively by improving management of cyber risk within UK organisations, and providing greater protection to citizens

Objective 3: Strengthen resilience at national and organisational level to prepare for, respond to and recover from cyber attacks.

EU

(3 areas of EU action) - 2020 to 2027

Area 1

Resilience, technological sovereignty and leadership

1.2 Building a European cyber shield: Proposal to build a network of Security Operations Centres across the EU, powered by artificial intelligence (AI), which will constitute a real "cyber security shield" for the EU, able to detect signs of a cyber attack early enough and to enable proactive action, before damage occurs

1.6 Greater global internet security

1.7 A reinforced presence on the technology supply chain - dedicated support to small and medium-sized businesses (SMEs), under the Digital Innovation Hubs.

See also **2. Building operational capacity to prevent, deter and respond.**

Singapore

(3 pillars and 2 foundational enablers) - 2021

Strategic pillar 2

Enable a safer cyberspace

- Secure digital infrastructure, devices, and applications that power our digital economy
- Safeguard our cyberspace activities
- Empower our cyber-savvy population for a healthy digital way of life.

Foundational enabler 1

Develop a vibrant cyber security ecosystem

- Develop advanced capabilities for economic growth and national security
- Innovate to build world-class products and services
- Grow cyber security market.

China

(9 strategic tasks) - 2016

Task 4

Strengthening the construction of online culture

Task 6

Perfect network governance systems

Persist in managing and governing the web in a lawful, open and transparent manner, realistically ensure that there are laws to rely on, laws must be relied on, law enforcement must be strict, and violations of the law must be punished.

Task 8

Enhancing cyberspace protection capabilities

Cyberspace is a new territory for national sovereignty. Build cyber security protection forces commensurate with our country's international standing and suited to a strong cyber power, forcefully develop cyber security defence means, timely discover and resist cyber intrusions, and cast a firm backup force to safeguard national cyber security.

HOW AUSTRALIA'S STRATEGY COMPARES WITH OTHER JURISDICTIONS

Australia

(6 cyber shields) - 2023 to 2030

Shield 2

Safe technology

- Ensure Australians can trust their digital products and software
- Protect our most valuable datasets
- Promote the safe use of emerging technology.

US

(5 pillars) - 2023 to FY26

Pillar 3

Shape market forces to drive security and resilience

Strategic Objective 3.1: Hold the stewards of our data accountable

Strategic Objective 3.2: Drive the development of secure IoT devices

Strategic Objective 3.3: Shift liability for insecure software products and services to manufacturers and software publishers

Strategic Objective 3.4: Use federal grants and other incentives to build in security

Strategic Objective 3.5: Leverage federal procurement to improve accountability

Strategic Objective 3.6: Explore a federal cyber insurance backstop.

UK

(5 pillars) - 2022 to 2025

Pillar 3

Technology advantage - taking the lead in the technologies vital to cyber power

Objective 1: Improve our ability to anticipate, assess and act on the science and technology developments most vital to our cyber power

Objective 2: Foster and sustain sovereign and allied advantage in the security of technologies critical to cyberspace

Objective 2a: Preserve a robust and resilient national Crypt-Key enterprise[8] which meets the needs of HMG customers, our partners and allies, and has appropriately mitigated our most significant risks including the threat from our most capable of adversaries

Objective 3: Secure the next generation of connected technologies and infrastructure, mitigating the cyber security risks of dependence on global markets and ensuring UK users have access to trustworthy and diverse supply

Objective 4: Shape global technology standards - work with the multistakeholder community to shape the development of global digital technical standards in the priority areas that matter most for upholding our democratic values, ensuring our cyber security, and advancing UK strategic advantage through science and technology.

EU

(3 areas of EU action) - 2020 to 2027

Area 1

Resilience, technological sovereignty and leadership

1.4 Securing the next generation of broadband mobile networks - EU citizens using advanced and innovative applications enabled by 5G and future generation of networks should benefit from the highest security standard. Under the new Cybersecurity Strategy, Member States, with the support of the Commission and ENISA - the European Cybersecurity Agency, are encouraged to complete the implementation of the EU 5G Toolbox, a comprehensive and objective risk-based approach for the security of 5G and future generations of networks

1.5 An internet of secure things - working to ensure transparent security solutions and certification under the Cybersecurity Act and to incentivise safe products and services without compromising on performance. Possible new horizontal rules to improve the cyber security of all connected products and associated services placed on the Internal Market, which may include a new duty of care for connected device manufacturers to address software vulnerabilities.

Singapore

(3 pillars and 2 foundational enablers) - 2021

Strategic pillar 2

Enable a safer cyberspace

- Secure digital infrastructure, devices, and applications that power our digital economy.

Foundational enabler 1

Develop a vibrant cyber security ecosystem

- Innovate to build world-class products and services.

China

(9 strategic tasks) - 2016

Task 7

Fostering innovation, web safety and talent

Give high regard to software security, and accelerate the dissemination and application of safe and trustworthy products.

8 *"Crypt-Key is the term used to describe the UK's use of cryptography to protect the critical information and services on which the UK government, military and national security community rely, including from attack by our most capable adversaries. It underpins our ability to choose how we deploy our national security and defence capabilities. To be a world-leading Crypt-Key nation we need the right skills and technologies both in government and in the private sector."*

HOW AUSTRALIA'S STRATEGY COMPARES WITH OTHER JURISDICTIONS

Australia

(6 cyber shields) - 2023 to 2030

Shield 3

World-class threat sharing and blocking

- Create a whole-of-economy threat intelligence network
- Scale threat blocking capabilities to stop cyber attacks.

US

(5 pillars) - 2023 to FY26

Pillar 2

Disrupt and dismantle threat actors

Strategic Objective 2.1: Integrate federal disruption activities

Strategic Objective 2.2: Enhance public-private operational collaboration to disrupt adversaries

Strategic Objective 2.3: Increase the speed and scale of intelligence sharing and victim notification

Strategic Objective 2.4: Prevent abuse of US-based infrastructure

Strategic Objective 2.5: Counter cybercrime, defeat ransomware.

UK

(5 pillars) - 2022 to 2025

Pillar 5

Countering threats - detecting, disrupting and deterring our adversaries to enhance UK security in and through cyberspace

Objective 1: Detect, investigate and share information on state, criminal and other malicious cyber actors and activities in order to protect the UK, its interests and its citizens

Objective 2: Deter and disrupt state, criminal and other malicious cyber actors and activities against the UK, its interests, and its citizens

Objective 3: Take action in and through cyberspace to support our national security and the prevention and detection of serious crime.

EU

(3 areas of EU action) - 2020 to 2027

Area 2

Building operational capacity to prevent, deter and respond

2.1 Joint Cyber Unit - the Commission is preparing, through a progressive and inclusive process with the Member States, a new Joint Cyber Unit, to strengthen cooperation between EU bodies and Member State authorities responsible for preventing, deterring and responding to cyber attacks, including civilian, law enforcement, diplomatic and cyber defence communities

2.2 Tackling cyber crime

2.3 EU Cyber Diplomacy Toolbox - the High Representative puts forward proposals to strengthen the EU Cyber Diplomacy Toolbox to prevent, discourage, deter and respond effectively against malicious cyber activities, notably those affecting our critical infrastructure, supply chains, democratic institutions and processes

2.4 Boosting cyber defence capabilities – the EU will also aim to further enhance cyber defence cooperation and develop state-of-the-art cyber defence capabilities, building on the work of the European Defence Agency and encouraging Member States to make full use of the Permanent Structured Cooperation and the European Defence Fund.

China

(9 strategic tasks) - 2016

Task 2

Resolutely safeguard national security

Prevent, curb and lawfully punish any act of using the network to engage in treason, separatism, incite rebellion or subversion, or incite the overthrow of the people's democratic dictatorship regime; prevent, curb and lawfully punish acts of using the network to steal or leak State secrets and other such acts harming national security; prevent, curb and lawfully punish foreign powers using the network to conduct infiltration, destruction, subversion and separatist activities.

Task 5

Attacking cyber terrorism, law-breaking and crime

Strengthen online anti-terrorism, counterespionage and anti-theft capabilities, and strictly attack cyber terrorism and cyber espionage activities.

HOW AUSTRALIA'S STRATEGY COMPARES WITH OTHER JURISDICTIONS

Australia

(6 cyber shields) - 2023 to 2030

Shield 4

Protected critical infrastructure

- Clarify the scope of critical infrastructure regulation
- Strengthen cyber security obligations and compliance for critical infrastructure
- Uplift cyber security of the Commonwealth Government
- Pressure-test our critical infrastructure to identify vulnerabilities.

US

(5 pillars) - 2023 to FY26

Pillar 1

Defend critical infrastructure

Strategic Objective 1.1: Establish cyber security requirements to support national security and public safety by creating new regulations, harmonising and streamlining new and existing regulation and enabling regulated entities to afford security

Strategic Objective 1.2: Scale public-private collaboration

Strategic Objective 1.3: Integrate federal cyber security centres

Strategic Objective 1.4: Update federal incident response plans and processes including ensuring that the cyber security community benefits from lessons learned through the Cyber Safety Review Board (CSRB)

Strategic Objective 1.5: Modernise federal defences.

Singapore

(3 pillars and 2 foundational enablers) - 2021

Strategic pillar 1

Build resilient infrastructure

- Enable a coordinated approach to national cyber security with Critical Information Infrastructures (CIIs) at its core
- Ensure government systems are secure and resilient
- Safeguard important entities and systems beyond CIIs.

EU

(3 areas of EU action) - 2020 to 2027

Area 1

Resilience, technological sovereignty and leadership

1.1 Resilient infrastructure and critical services - proposal to reform the rules on the security of network and information systems, under a Directive on measures for high common level of cyber security across the Union (revised NIS Directive or 'NIS 2'), in order to increase the level of cyber resilience of critical public and private sectors: hospitals, energy grids, railways, but also data centres, public administrations, research labs and manufacturing of critical medical devices and medicines, as well as other critical infrastructure and services, must remain impermeable, in an increasingly fast-moving and complex threat environment.

To respond to the growing threats due to digitalisation and interconnectedness, the proposed Directive on measures for high common level of cyber security across the Union (revised NIS Directive or 'NIS 2') will cover medium and large entities from more sectors based on their criticality for the economy and society. NIS 2 strengthens security requirements imposed on the companies, addresses security of supply chains and supplier relationships, streamlines reporting obligations, introduces more stringent supervisory measures for national authorities, stricter enforcement requirements and aims at harmonising sanctions regimes across Member States. The NIS 2 proposal will help increase information sharing and cooperation on cyber crisis management at national and EU level.

1.3 An ultra-secure communication infrastructure - the EU Governmental Satellite Communications, a component of the Space Programme, will provide secure and cost-efficient space-based communication capabilities to ensure the security- and safety- critical missions and operations managed by the EU and its Member States, including national security actors and EU institutions, bodies and agencies.

2. Building operational capacity to prevent, deter and respond

The proposed Critical Entities Resilience (CER) Directive expands both the scope and depth of the 2008 European Critical Infrastructure directive. Ten sectors are now covered: energy, transport, banking, financial market infrastructures, health, drinking water, waste water, digital infrastructure, public administration and space. Under the proposed directive, Member States would each adopt a national strategy for ensuring the resilience of critical entities and carry out regular risk assessments. These assessments would also help identify a smaller subset of critical entities that would be subject to obligations intended to enhance their resilience in the face of non-cyber risks, including entity-level risk assessments, taking technical and organisational measures, and incident notification. The Commission, in turn, would provide complementary support to Member States and critical entities, for instance by developing a Union-level overview of cross-border and cross-sectoral risks, best practice, methodologies, cross-border training activities and exercises to test the resilience of critical entities.

China

(9 strategic tasks) - 2016

Task 3

Protect critical information infrastructure

National critical information infrastructure refers to information infrastructure that affects national security, the national economy and the people's livelihood, where whenever data is leaked, it is destroyed or loses its functionality, national security and the public interest may be gravely harmed, including but not limited to basic information networks providing public telecommunications, radio and television transmission, and other such services, as well as important information systems in areas and State bodies such as energy, finance, transportation, education, scientific research, hydropower, industry and manufacturing, healthcare and medicine, social security, public undertakings, etc., important internet application systems, etc. Adopt all necessary measures to protect critical information infrastructure and its important data from attack and destruction. Persist in laying equal stress on technology and management, simultaneously developing protection and deterrence, focus on identification, prevention, monitoring, early warning, response, handling and other such segments, in establishing and implementing a critical information infrastructure protection system, expand input in areas such as management, technology, talent and finance, synthesise measures and policies according to the law, and realistically strengthen security protection of critical information infrastructure.

Protecting critical information infrastructure is a common responsibility of government, businesses and the entire society, controlling and operational work units and organisations must, according to the requirements of laws, regulations, rules and standards, adopt the necessary measures to ensure the security of critical information infrastructure, and progressively realise that evaluation happens first, and application afterwards. Strengthen risk assessment of critical information infrastructure. Strengthen security protection in Party and government bodies, as websites in focus areas, grass-roots Party and government bodies' websites must be built, operated and managed according to the intensification model. Establish orderly cyber security information sharing mechanisms for government, sectors and enterprises, and fully give rein to the important role of enterprises in protecting critical information infrastructure.

Persist in opening up to the outside world, and safeguarding cyber security in an open environment. Establish and implement cyber security examination structures, strengthen supply chain security management, launch security inspections for important information technology products and services purchased and used in Party and government bodies, as well as focus sectors, raise the security and controllability of products and services, prevent product and service providers and other organisations from using their superiority in information technology to engage in improper competition or to harm users' interests.

HOW AUSTRALIA'S STRATEGY COMPARES WITH OTHER JURISDICTIONS

Australia

(6 cyber shields) - 2023 to 2030

Shield 5

Sovereign capabilities

- Grow and professionalise our national cyber workforce
- Accelerate our local cyber industry, research and innovation.

US

(5 pillars) - 2023 to FY26

Pillar 4

Invest in a resilient future

Strategic Objective 4.1: Secure the technical foundation of the internet

Strategic Objective 4.2: Reinvigorate federal research and development for cyber security

Strategic Objective 4.3: Prepare for our post-quantum future

Strategic Objective 4.4: Secure our clean energy future

Strategic Objective 4.5: Support development of a digital identity ecosystem

Strategic Objective 4.6: Develop a national strategy to strengthen our cyber workforce.

UK

(5 pillars) - 2022 to 2025

Pillar 1

UK cyber ecosystem - strengthening the UK's cyber ecosystem

Objective 2: Enhance and expand the nation's cyber skills at every level, including through a world-class and diverse cyber profession that inspires and equips future talent.

EU

(3 areas of EU action) - 2020 to 2027

Area 1

Resilience, technological sovereignty and leadership

1.8 A cyber-skilled EU workforce - increased efforts to upskill the workforce, attract and retain the best cyber security talent and invest in research and innovation that is open, competitive and based on excellence.

Singapore

(3 pillars and 2 foundational enablers) - 2021

Foundational enabler 2

Grow a robust cyber talent pipeline

- Support youths, women, and mid-career professionals to pursue a cyber security career
- Create an upskilling culture for a globally competitive workforce
- Foster a dynamic sector with strong professional communities.

Foundational enabler 1

Develop a vibrant cyber security ecosystem

- Grow our cyber security market.

China

(9 strategic tasks) - 2016

Task 1

Resolutely defending sovereignty in cyberspace

Manage online activities within the scope of our country's sovereignty according to the Constitution, laws and regulations, protect the security of our country's information infrastructure and information resources, adopt all measures, including economic, administrative, scientific, technological, legal, diplomatic and military measures, to unwaveringly uphold our country's sovereignty in cyberspace. Resolutely oppose all actions to subvert our country's national regime or destroy our country's sovereignty through the network.

Task 7

Fostering innovation, web safety and talent

Implement the cyber security talent project, and strengthen the establishment of cyber security science majors, forge first-rate cyber security academies and innovation parks, and create an ecology and an environment beneficial to the fostering of talent, innovation and start-ups.develop cyber security defence means, timely discover and resist cyber intrusions, and cast a firm backup force to safeguard national cyber security.

Task 4

Strengthening the construction of online culture

HOW AUSTRALIA'S STRATEGY COMPARES WITH OTHER JURISDICTIONS

Australia

(6 cyber shields) - 2023 to 2030

Shield 6

Resilient region and global leadership

- Support a cyber resilient region as the partner of choice
- Shape, uphold and defend international cyber rules, norms and standards.

US

(5 pillars) - 2023 to FY26

Pillar 5

Forge international partnerships to pursue shared goals

Strategic Objective 5.1: Build coalitions to counter threats to our digital ecosystem

Strategic Objective 5.2: Strengthen international partner capacity

Strategic Objective 5.3: Expand US ability to assist allies and partners

Strategic Objective 5.4: Build coalitions to reinforce global norms of responsible state behaviour

Strategic Objective 5.5: Secure global supply chains for information, communications and operational technology products and services.

UK

(5 pillars) - 2022 to 2025

Pillar 4

Global leadership - advancing UK global leadership and influence for a secure and prosperous international order

Objective 1: Strengthen collective action and mutual cyber resilience - strengthen the cyber security and resilience of international partners and increase collective action to disrupt and deter adversaries

Objective 2: Shape global governance to promote a free, open, peaceful and secure cyberspace

Objective 3: Leverage and export UK cyber capabilities and expertise to boost our strategic advantage and promote our broader foreign policy and prosperity interests.

Singapore

(3 pillars and 2 foundational enablers) - 2021

Strategic pillar 3

Enhance international cyber cooperation

- Advance the development and implementation of voluntary, non-binding norms, which sit alongside international law
- Strengthen the global cyber security posture through capacity-building initiatives and the development of technical and interoperable cyber security standards
- Contribute to international efforts to combat cross-border cyber threats.

EU

(3 areas of EU action) - 2020 to 2027

Area 3

Advancing a global and open cyberspace through increased cooperation

3.1 EU leadership on standards, norms and frameworks in cyberspace - the EU will step up work with international partners to strengthen the rules-based global order, promote international security and stability in cyberspace, and protect human rights and fundamental freedoms online. It will advance international norms and standards that reflect these EU core values, by working with its international partners in the United Nations and other relevant fora

3.2 Cooperation with partners and the multi-stakeholder community - cyber dialogues with third countries, regional and international organisations as well as the multi-stakeholder community will be intensified. The EU will also form an EU Cyber Diplomacy Network around the world to promote its vision of cyberspace

3.3 Strengthening global capacities to increase global resilience - the EU will further strengthen its EU Cyber Diplomacy Toolbox and increase cyber capacity-building efforts to third countries by developing an EU External Cyber Capacity Building Agenda.

China

(9 strategic tasks) - 2016

Task 9

Strengthening international cooperation in cyberspace

On the basis of mutual respect and mutual trust, strengthen international cyberspace dialogue and cooperation, and promote the reform of the global internet governance system. Deepen bilateral and multilateral cyber security dialogues, exchanges and information communications with all countries, effectively manage and control differences, vigorously participate in cyber security cooperation in global and regional organisations, promote the internationalisation of the management of Internet addresses, domain name servers and other such basic resources.

Support the United Nations to play a leading role, promote the formulation of international norms for cyberspace that are universally recognised by all sides, and an international treaty on anti-terrorism in cyberspace, complete judicial assistance mechanisms to attack cyber crime, deepen international cooperation in areas such as policies and laws, technological innovation, standards and norms, emergency response, critical information infrastructure protection, etc.

Strengthen support and assistance to developing countries and backward regions to disseminate internet technology and construct infrastructure, and strive to close the digital divide. Promote the construction of "One Belt, One Road", raise international telecommunications interconnection and interaction levels, and pave a smooth information silk road. Set up the World Internet Conference and other such global internet sharing and common governance platforms, and jointly promote the healthy development of the internet. Through vigorous and effective international cooperation, establish a multi-lateral, democratic and transparent international internet governance system, and jointly build a peaceful, secure, open, cooperative and orderly cyberspace.

IS SPACE THE FORGOTTEN SECTOR IN CRITICAL INFRASTRUCTURE CYBER SECURITY?

Authors: Joann Yap and Melissa Tan

Outer space has become a critical domain for daily life. From essential services and national security applications to the growing role of commercial ventures in space activities, our dependence on space assets, and in particular satellites, cannot be understated.

As cyber operations are enabled by space and space operations are enabled by technology and cyber operations, space security and cyber security are closely interlinked.

While there are no mandatory international cyber security requirements currently in place for space systems, it is critical that space actors put in place adequate cyber security measures.

However, most governments have yet to implement adequate cyber security measures in relation to space assets.

In Australia, space technology was added as one of 11 critical infrastructure sectors covered under the *Security of Critical Infrastructure Act 2018* (Cth) (**SOCI Act**) following reforms in 2021-22. The SOCI Act defines the "space technology sector" as the sector of the Australian economy that involves the commercial provision of space-related services including:

a. position, navigation and timing services in relation to space objects
b. space situational awareness services
c. space weather monitoring and forecasting
d. communications, tracking, telemetry and control in relation to space objects
e. remote sensing earth observations from space, and
f. facilitating access to space.

However, the SOCI Act does not clarify how cyber security reforms implemented in recent years will apply to the space technology sector. For example, the Security of Critical Infrastructure (Application) Rules (LIN 22/026) 2022 (**Application Rules**) which commenced on 8 April 2022 have not "switched on" Part 2 of the SOCI Act (Information Provision Positive Security Obligation (**PSO**)) for the space technology sector. Similarly, with no asset currently prescribed as an asset within the "space technology sector", neither Part 2B of the SOCI Act (Mandatory Cyber Incident Notification PSO) nor the Risk Management Program PSO have been "switched on" for any particular space assets, other than where they may also fall within other deemed critical infrastructure sectors, such as the communications sector.

Even in the US — one of the key space superpowers, which in 2020 issued a comprehensive cyber security policy for space systems (the Space Policy Directive-5 Cybersecurity Principles for Space Systems) — the development and implementation of cyber security standards and measures to protect commercial space systems remains a work in progress. Further, the space sector has not been designated as a critical infrastructure sector, and the debate continues as to whether space should be added as the 17th "critical infrastructure" sector in the US.

This suggests that space continues to be a forgotten (or at the very least, overlooked) sector in critical infrastructure cyber security, which in our view needs to be rectified. As a nation and as a global community, we cannot afford to allow space security to be compromised by cyber security vulnerabilities or malicious cyber threat actors. Cyber security considerations for the space sector should be prioritised for the following reasons.

1 Space systems are essential in daily life

While the reliance of the military on satellites for surveillance and communication is well known, the extent to which space systems are integrated in our daily lives is often underestimated. From powering electrical grids to enabling ride-sharing services, weather monitoring, air traffic control, internet connectivity, cashless payments and stock exchanges, satellite and other space system technology forms the backbone of numerous critical services.[1]

Key to that infrastructure are the Global Navigation Satellite Systems (**GNSS**), a constellation of satellites from several countries, including the Global Positioning System (**GPS**) owned by the United States government. In addition to positioning, GPS allows service providers to measure time with near-perfect precision globally. For example, banks rely on synchronised timing and time stamps to monitor transactions, deal with fraud and ensure payments. When swiping a card at a café, the seamless functioning of this everyday activity requires determining the exact time the transaction occurs in order to prevent the bank account from being overdrawn.[2]

Space systems encompass technologies and infrastructure supporting various applications that have become integral to military, governmental, economic and civilian domains. While these bring a wealth of opportunities, they also present significant challenges, particularly in relation to cyber security. Space systems are a central point of failure for the functioning of critical infrastructure and systems of national significance.[3] While GPS is operated and maintained by the United States Space Force and therefore has many layers of security, other space systems such as those owned by commercial operators are unlikely to have as stringent protections, if any. While commercial space systems will vary in significance and also, therefore, their associated cyber security protections, it is not always clear what is in place, nor what is appropriate (let alone what is or should be best practice). With our heavy dependence on space-based services, any interruption or shutdown could range from being an inconvenience to being disastrous, from both a civilian and humanitarian perspective, in addition to presenting military concerns.

2 Space systems are part of an interconnected threat environment

Cyber attacks on space systems

There are four broad segments of space systems that can be the target of cyber threats:

1. the space segment (including satellites and their payloads)
2. the link segment, being the communications network that connects the other segments
3. the control segment, including launch facilities, ground and control stations, and
4. the user segment, which deals with the application of satellite systems and includes user-facing interfaces and infrastructure for space-based services, such as handheld GPS devices.[5]

The space segment, such as satellites and their payloads, increasingly participates in cyberspace (which can be understood to be the virtual platform and links between computers for communication) in providing internet and other connectivity and is therefore a prime target for cyber threats. Ground-based control segments of space systems are seen as more likely targets, including computer systems on ground infrastructure. This extends risks not only to those actors with assets in space, but also those that are linked to space, for example, through cloud computing, which sends data via satellite.

However, all space system segments can be targeted, which amplifies risks to supply chains and data security.[6] This is particularly concerning given that relatively inexpensive commercial off-the-shelf technology (which may be unpatched or outdated)[7] and open-source software are now more commonly used among satellites and ground control systems,[8] which significantly increases the potential for vulnerabilities to be exploited on a larger scale. The convergence of space systems and cyberspace therefore necessitates an evolution of traditional security measures to address emerging risks.

The collection, transmission and control of data, along with the data itself, are prime targets for cyber attacks, including by interception or illegal transfer. Attacks may aim to deny, disrupt, distort or destroy the functions of space assets, networks and services. Understanding these vulnerabilities is crucial for developing effective cyber security measures.[9]

1 https://cybernews.com/editorial/heres-how-a-hacked-satellite-can-impact-your-life/

2 https://qz.com/1106064/the-entire-global-financial-system-depends-on-gps-and-its-shockingly-vulnerable-to-attack

3 Risk Management in Outer Space Activities: An Australian and New Zealand Perspective - Chapter 6, "Managing the Cyber-Related Risks to Space Activities", Sarah E. O'Connor, page 151

4 https://www.gps.gov/systems/gps/

5 https://www.airforce.gov.au/sites/default/files/2022-09/213304_space_power_emanual_v1.0a%5B1%5D.pdf

6 https://www.cigionline.org/articles/where-outer-space-meets-cyberspace-a-human-centric-look-at-space-security/>

7 Cyber security in New Space: Analysis of threats, key enabling technologies and challenges, International Journal of Information Security, M. Manulis, C. P. Bridges, R. Harrison, V. Sekar & A. Davis

8 Risk Management in Outer Space Activities: An Australian and New Zealand Perspective - Chapter 6 "Managing the Cyber-Related Risks to Space Activities", Sarah E. O'Connor, page 154

9 Ibid, page 156

Escalation risks and uncertainties

Cyber attacks on satellite systems can have cascading consequences, leading to potentially large-scale disruption and catastrophic damage, particularly in times of conflict. While these attacks may seem less escalatory than conventional weapons, they are often difficult to detect, attribute and distinguish from unintentional or natural sources of satellite interference in the space environment, which can pose a real risk in escalating military tension, among other things.

The uncertain dynamics of conflict and escalation in space further complicate the assessment of cyber threats. What one actor perceives as conflict escalation might not be the same in all cases. For example, some governments may view certain cyber attacks on satellites as a trigger for armed conflict, while others may view those as being below that threshold. There is therefore a real danger that efforts to deter or test an adversary by conducting a cyber attack in space could inadvertently lead to military escalation on Earth.[10]

Cyber attacks could be used to harm military and commercial satellites, including by disabling or hijacking the satellite for use as a projectile weapon against other satellites.[11] Such an attack could increase orbital debris hazards in the space environment, which may add to already escalating tensions.

Expanding role of commercial industry

The increasing role of commercial industry in space activities introduces new stakeholders to the design, manufacture, operation and ownership of space system assets and spans a variety of companies and nation states. This amplifies access and other points of vulnerability across software and hardware, including components, services and providers across space system supply chains. Those chains may be involved in the supply, assembly, integration and other access points, further magnified when considering data and other service providers that are linked to space systems.[12]

The more stakeholders involved, the more opportunities for malicious actors to infiltrate space systems through exploits such as malware[13] or data theft, increasing the risks to system and end users. The interconnected nature of space, cyber, and data systems emphasises the need for appropriate cyber security measures, that are likely to require more comprehensive consideration in many cases.

3 Responsible space actors

It is projected that from 2020 to 2030 the satellite and space sector will yield US$1.2 trillion in retail revenues, see over 24,850 satellites launched into space and generate more than 504,000 petabytes in data volume.[14] Although there is no overarching clear and consistent international regime dedicated to managing cyber risks associated with space activities, there is a need for nations and commercial operators to act responsibly and be proactive in their cyber security measures in light of our increasing dependency on space systems.

Proactive cyber security initiatives

A comprehensive approach to cyber security is required across the space system segments. Recognising and addressing vulnerabilities will be key to ensuring the safety and resilience of space systems, minimising the potential harm of this threat to human infrastructure and daily life.

While the SOCI Act recognises space technology as a critical infrastructure sector, the legislation does not yet specify what is captured as a "critical infrastructure asset" within the space technology sector. This regime and its cyber security components have not yet been enacted in respect of space systems (other

than, as noted above, some assets that may be captured under current definitions such as telecommunications assets). Safeguarding space assets as part of critical infrastructure needs to be a priority for government and should not be further delayed.

Proactive cyber security management and learning from best practices

Given the interconnectedness of these systems, the private sector has a crucial role to play in adopting and contributing to collaborative efforts for the cyber defence of space technology. Space actors should take into account known risks, vulnerabilities and dependencies, and proactively manage them through cyber security initiatives. This involves integrating cyber security considerations from the inception of satellite and space project development. Rather than an afterthought, cyber security should be a foundational element in the design and deployment of space systems, irrespective of the operator.

The private sector can leverage existing guides and protocols. For example, on 22 December 2023 NASA released its inaugural Space Security Best Practices Guide[15] to bolster mission cyber security efforts for both public sector and private sector space activities. The guide was designed to benefit international partners, industry, and others working in the expanding fields of space exploration and development and to provide security guidance for missions, programs, or projects of any size.[16]

10 https://www.cigionline.org/articles/where-outer-space-meets-cyberspace-a-human-centric-look-at-space-security/

11 Ibid

12 Ibid

13 Risk Management in Outer Space Activities: An Australian and New Zealand Perspective - Chapter 6 'Managing the Cyber-Related Risks to Space Activities', Sarah E. O'Connor, page 155

14 Northern Sky Research. 2022. Space Cybersecurity: Current State and Future Needs. White Paper. April. www.nsr.com/wp-content/uploads/2022/04/NSR-Space-Cybersecurity-White-Paper-FINAL.pdf

15 https://swehb.nasa.gov/display/SWEHBVD/7.22+-+Space+Security%3A+Best+Practices+Guide

16 https://www.nasa.gov/general/nasa-issues-new-space-security-best-practices-guide/

Space actors can and should consider existing guides and protocols to assist in proactively mitigating cyber security risks to foster responsible behaviour and continuously ensure the peaceful and secure use of outer space. In light of our dependence on space system assets from both a national security and humanitarian perspective, it is crucial to prioritise cyber security to defend this vital sector and its assets. This will require foresight, collaboration, and a commitment to developing best practice norms.

A potential way forward

Given that regulation can take years to formulate, more momentum in the private commercial sector could be the answer to prioritising the cyber security of the space industry.

Regulatory frameworks are rarely able to keep pace with technological innovations, and take time to progress due to the multifaceted needs of multiple stakeholders. Considering the importance and interconnectedness of space and cyber systems, more urgent action is needed.

This presents an opportunity for industry to lead the way, drawing on their best-placed insights into possible threats and the appropriate solutions. At an organisational level, this could involve:

- developing proactive cyber security initiatives
- contributing to the development of guidelines and best practices for products or services
- implementing and updating initiatives with evolving best practices
- embedding responsible behaviours, such as considering the cyber security measures of supply chain participants and uplifting requirements where necessary.

In doing so, organisations will demonstrate and further embed a culture of responsible space behaviour that is a cornerstone of, and generally aligned with and integral to, the values of the space industry.

While these initiatives will involve varying levels of cost and effort, and any initiatives are certainly not a “one size fits all”, we nevertheless consider this would be a worthwhile and crucial endeavour.

By developing responsible cyber-aware industry norms that guide the operation of the space industry, space industry participants will:

- benefit from greater security
- encourage best practice amongst new entrants
- build the trust of customers, domestic and international partners, supply chain participants and the general public, and
- continue to develop and demonstrate the industry’s commitment to the security, safety and sustainability of our critical infrastructure and use of outer space.

Joann Yap is a Senior Associate and Space Lead at Lander & Rogers and Director and Chair of the Space Law Council of Australia and New Zealand. Joann specialises in space law and commercial contracting, and advising on space legal due diligence and strategy.

THE POLITICS OF CYBER SECURITY

Author: Melissa Tan

How can viewing cyber security through a political lens enhance our understanding of the issues at play?

In recent years, cyber security has become one of the top items on the political agenda of many countries, including Australia.

In a show of how seriously Australia's Labor government is taking the issue, the cabinet position of Minister for Cyber Security was created in June 2022. In July 2023 the Australian government also appointed a National Cyber Security Coordinator who supports the Minister for Cyber Security to lead the coordination of national cyber security policy, responses to major cyber incidents, whole-of-government cyber incident preparedness efforts, and strengthening Commonwealth cyber security capability. Reflecting how politically charged the issue of cyber security has become, Minister for Cyber Security Clare O'Neil posted on X (formerly Twitter) last year: *"The previous government left Australia's cyber security in an absolute mess, and the Albanese government is cleaning it up."*[1]

In the US, President Joe Biden has made cyber security a top priority at all levels of government. The Office of the National Cyber Director (**ONCD**) was established by Congress in 2021 as a component of the Executive Office of the President at the White House, and principally advises the President on cyber security policy and strategy. The ONCD also spearheaded the development of President Biden's National Cybersecurity Strategy issued on 2 March 2023, and coordinates the strategy's implementation.

Cyber security is inherently political

Politics is about power and status. We often think of it as a power struggle between competing groups or people to assert their rival interests. But politics is also underpinned by complexity and uncertainty.

The area of cyber security is marked by a complex web of power relationships between multiple competing groups seeking to assert their interests. Against this backdrop, the rapid advancement of technology and tactics and increasing sophistication of threat actors create even more uncertainties in the interplay of power between various actors.

- Consumers feel powerless against organisations who collect their personal information, fearing their data is at risk as they cannot control the organisation's level of cyber security.
- Individuals and organisations feel powerless against faceless threat actors who continue to gain momentum and sophistication and always seem a step ahead.
- Organisations and businesses feel uncertain and worried about the increased regulation and enforcement powers of regulators in relation to privacy and cyber security.
- Governments are constantly trying to keep state-backed actors at bay to protect national security.

- Insureds are constantly worried about whether or not they can obtain affordable cyber insurance, and whether they will have cover for cyberattacks they may suffer.

The list goes on.

1 https://twitter.com/ClareONeilMP/status/1661281005179924480

The power dynamic is not static

However, the power dynamic is not static, and it is not always negative.

Understanding cyber through a political lens and recognising the competing interests at play can enable us to develop and implement actions that benefit cyber security as a whole.

In recent times we have seen the dynamic of these power relationships evolve and shift, and sometimes for the better.

Victim vs threat actor

For example, there has always been an imbalance of power between the victim consumer or organisation, and the threat actor.

The threat actor operates in the shadows and has access to resources and technology that enable them to perpetrate their attacks easily and at an increasingly larger scale. Threat actors have continually come up with new ways to increase pressure on victims and tip the power balance further in their favour.

In November 2023 the ALPHV/BlackCat ransomware group announced that it had breached financial software firm MeridianLink and exfiltrated data without deploying ransomware. Just one week later, the group also posted to its dark web portal a screenshot of an SEC complaint it had made against MeridianLink. In its complaint to the regulator, the ransomware group claimed that MeridianLink had breached new SEC rules requiring companies that experience a data breach deemed to be material to investors to file a Form 8-K reporting the incident within four business days, unless the United States Attorney General determines that an immediate disclosure would be harmful to public safety or to national security. Although the SEC rules did not come into effect until December 2023, this was the first time a ransomware group filed an SEC complaint against a victim, likely

in an attempt to add pressure on the victim organisation to pay the ransom by alerting the SEC to the organisation's failure to abide by the new rules or its regulatory obligations.[2]

In contrast, victim organisations often have limited resources to defend themselves and may not be able to adequately close off all vulnerability gaps. This often leaves a victim in a reactive position to any potential cyber attack, i.e. containing and recovering from the breach, and complying with their privacy obligations through privacy assessments and any relevant notifications. They are held hostage by the actions of the threat actor because they have no control over how the exfiltrated material may be used to cause further harm to the victim organisation and affected persons.

That said, in 2023 we saw victim organisations taking proactive steps to regain control and slowly tip the power balance in their favour. In recent cases including in Australia and Ireland, victim organisations have proactively sought court injunctions to prevent the dissemination and disclosure of leaked data to third parties. While a court order is difficult to enforce against a faceless threat actor, it does allow the victim organisation some control in warning other potential publishers against frustrating the injunctive orders, and in limiting the dissemination of the leaked data to minimise harm to the victim organisation and affected persons.

2 https://www.cpomagazine.com/cyber-security/ransomware-group-trolls-victim-with-sec-complaint-after-data-breach/; https://www.bankinfosecurity.com/alphv-gang-tattles-to-sec-over-victim-disclosing-breach-a-23611

Government / law enforcement vs threat actor

We have also recently seen a shift in the power balance between governments and law enforcement authorities on one hand, and threat actors on the other.

The Australian government supplemented its defensive capabilities with offensive capabilities by setting up the Hack the Hackers Taskforce in November 2022. The permanent operation comprises approximately 100 police and defence personnel to "hack the hackers" with an immediate priority to target ransomware groups and disrupt their operations.

The Australian government also recently named and identified the cyber criminal behind the 2022 Medibank data breach — Russian citizen Aleksandr Ermakov — and imposed cyber sanctions on a threat actor for the first time, including a travel ban and asset restrictions.

The recent takedown of the ALPHV/BlackCat ransomware group[3] and LockBit ransomware group[4] through international operations undertaken jointly by law enforcement agencies such as the Federal Bureau of Investigations (**FBI**), Australian Federal Police (**AFP**) and agencies in Europe and North America has also demonstrated that threat actors may not always have the upper hand or remain untouchable.

Of course, it is no surprise that both ALPHV and LockBit were able to bounce back from the disruptions, with ALPHV unseizing its website and reportedly saying that it was no longer restricting affiliates using its ransomware software from attacking critical infrastructure including hospitals and nuclear power plants,[5] and LockBit re-establishing operations and a new dark-web leak site just days after the global law enforcement effort dismantled the group's infrastructure.[6]

Nevertheless, offensive capabilities have gained momentum and will likely be the catalyst for further actions to disrupt the operations of cyber criminals and eventually tip the power balance in favour of governments and law enforcement authorities.

Regulator vs victim

Following a raft of privacy and cyber security reforms in Australia, including penalties for data breaches rising to A$50 million or more as a result of amendments to the Privacy Act and the more active approach to enforcement taken by regulators such as the OAIC, ASIC and ACMA, it would appear that the power imbalance between the various regulators and victim organisations continues to grow.

However, with a heightened cyber and privacy regulatory environment comes greater awareness amongst victim organisations of their obligations and actions needed to ensure compliance and avoid being the subject of regulatory investigations or enforcement proceedings. In other words, the power dynamic can drive change – understanding the competing interests at play can enable victim organisations to develop and implement actions to uplift their cyber resilience, keeping the power imbalance with regulators in check and bolstering cyber security as a whole.

Insurer vs insured

Insureds often feel powerless against insurers and suspicious of the availability of cover afforded under cyber insurance policies. The adoption of cyber war exclusion wording in cyber insurance policies in recent years has brought to the fore these tensions in the insurer-insured power relationship.

However, this is one power relationship in which the dominance and resources of the cyber insurer, if understood and utilised by the insured, can bring about cyber security gains.

Cyber insurers are motivated to keep claims and losses low, particularly aggregated risks. The cyber insurance industry is well placed and resourced to help lift cyber security practices amongst clients who choose to purchase cyber insurance. For example, cyber insurers increasingly require minimum controls to be in place as minimum underwriting standards before offering to provide cyber insurance. For clients with good or better-than-average controls, they may have access to better cover and/or a lower deductible and/or lower premium, which will in turn continue to encourage better cyber security practices amongst insureds. Many insurers also offer pre-incident services such as assisting in incident response planning or training to assist in uplifting the cyber security practices of their clients.

This is certainly not a zero-sum game relationship and can be beneficial for both parties.

Cyber security should not be used purely for political gains

To ensure a sustainable long-term cyber security strategy that can effectively tackle cyber threats, we need to be careful and strategic in how we approach the uplift of cyber resilience as a nation and globally.

Cyber security should not be the subject of petty politicking domestically or internationally, nor should it be used purely to achieve political gains. The greater good of uplifting the cyber resilience of the nation has to be the key guiding principle.

Ultimately, the politics of cyber security will constantly change, but if the focus remains on developing and implementing actions that bring about cyber security gains despite the power dynamics at play between various actors with competing interests, the broader vision of a cyber resilient nation with strong cyber defences will, and should, be achievable.

3 https://www.afp.gov.au/news-centre/media-release/russian-led-hacking-group-disrupted-australian-businesses-regain-access

4 https://www.afp.gov.au/news-centre/media-release/international-police-operation-takes-down-worlds-most-harmful-2

5 https://www.wired.com/story/alphv-blackcat-ransomware-doj-takedown/; https://www.theverge.com/2023/12/19/24008093/alphv-blackcat-ransomware-gang-site-seized-fbi-doj

6 https://www.cybersecuritydive.com/news/lockbit-revives-operations/708507/

KEY CONTACTS

Insurance Law & Litigation

Melissa Tan
Partner and Head of Cyber Insurance
Insurance Law & Litigation

D +61 2 8020 7889
M +61 438 742 770
E mtan@landers.com.au

Dominica Moar
Special Counsel
Insurance Law & Litigation

D +61 7 3456 5126
E dmoar@landers.com.au

Suzanne Boutsalis
Senior Associate
Insurance Law & Litigation

D +61 2 8020 7896
M +61 418 886 936
E sboutsalis@landers.com.au

Rebekah Maxton
Lawyer
Insurance Law & Litigation

D +61 2 8020 7929
E rmaxton@landers.com.au

Jack Boydell
Lawyer
Insurance Law & Litigation

D +61 2 8020 7724
M +61 439 499 417
E jboydell@landers.com.au

Rose Cavanagh
Lawyer
Insurance Law & Litigation

D +61 2 8020 7741
M +61 439 742 299
E rcavanagh@landers.com.au

Angela Ivanovic
Lawyer
Insurance Law & Litigation

D +61 2 8020 7815
M +61 437 085 753
E aivanovic@landers.com.au

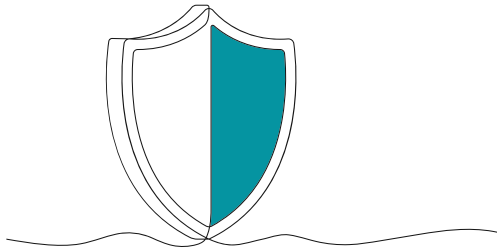
Annie Weng
Paralegal
Insurance Law & Litigation

D +61 2 8020 7665
E aweng@landers.com.au

Space Law

Joann Yap
Senior Associate
Corporate

D +61 2 8020 7719
E jyap@landers.com.au



ABOUT US

Founded in 1946, Lander & Rogers is one of the few remaining truly independent Australian law firms and a leader in legal tech innovation.

With offices across the eastern seaboard of Australia, Lander & Rogers has grown organically resulting in a unified firm with a strong focus on client and staff care.

We believe legal services involve more than just the law – practical, commercial advice and exceptional client experience are equally important to our clients and to us.

Lander & Rogers advises corporate, government, not-for-profit and private clients in insurance law and litigation, family law, workplace relations & safety, real estate, corporate transactions, digital & technology and commercial disputes.

The firm is global in approach, working closely with a network of leading firms to provide advice to clients, both domestically and abroad. Lander & Rogers is also the exclusive Australian member of the largest worldwide network of independent law firms, TerraLex.

Brisbane

Level 11 Waterfront Place
1 Eagle Street
Brisbane QLD 4000

T +61 7 3456 5000
F +61 7 3456 5001

Melbourne

Level 15 Olderfleet
477 Collins Street
Melbourne VIC 3000

T +61 3 9269 9000
F +61 3 9269 9001

Sydney

Level 19 Angel Place
123 Pitt Street
Sydney NSW 2000

T +61 2 8020 7700
F +61 2 8020 7701

landers.com.au