National Cyber Security Centre | Te Tira Tiaki Government Communications Security Bureau

Cyber Summit Korea 2026: "Connected World, Security Together"

Navigating the Cyber Threat Landscape – the New Zealand Experience

(U) Tēnā koutou katoa.

(U) Good afternoon, and greetings to you all. Thank you for the opportunity to be here today at Cyber Summit Korea 2026.

(U) For those I have not met, my name is Catriona Robinson.

(U) I am the Deputy Director-General for Cyber Security and head of New Zealand's National Cyber Security Centre, commonly known as the NCSC.

(U) It is a privilege to join such a distinguished international audience of cyber security professionals, business leaders, policymakers, and technology experts.

(U) I would like to thank the National Intelligence Service and National Security Research Institute for hosting the Cyber Summit and acknowledge the dignitaries attending here today.

(U) It is a mixed blessing to have the opportunity to provide the final address to this conference: many of the clever things I prepared to say have already been said by the many clever people attending this conference! I note too – my Australian and British colleagues have been urging me to drop lyrics from the conference theme song into my address. I don't have the lyrics, or I would. But I think you will find that themes of security, AI and "better together" come up a lot.

(U) What I intend is to give you an outline of the cybersecurity world as it looks from the New Zealand perspective. As I draw my remarks together at the end, that will also serve as something of a summary of the conversations that we've been having throughout this event.

(U) [Compliments to the Koreans on the quality of the AI transliteration/translation tool; Alexa and Siri not nearly as good at understanding the New Zealand accent; Tesla example: voice activated command to "deploy wipers".]

(U) So: where to begin? Although we come from different countries and sectors, the cyber-defence community is united by common challenges and risks. The operation of our economies, governments, businesses, and communities is reliant on digital infrastructure, and that infrastructure is threatened by malicious cyber actors on a daily and hourly basis.

(U) Digital technology has created tremendous opportunity, but it also means cyber security has become one of the defining resilience challenges of our time.

(U) The theme of this conference is “Connected World, Security Together”. That theme resonates strongly with me. I’ve travelled here from Wellington, New Zealand, via Washington DC – that’s a lot of time in aeroplanes over the last week, and many thousands of miles covered. But despite the geographical distance that separates us, the conversations that I have in New Zealand, in north America and in Asia are the same.

(U) Cyber threats do not respect national borders. A vulnerability discovered in one country can be exploited globally within hours, an event on one side of the world can generate cyber activity that affects organisations thousands of kilometres away – whether deliberately or not.

(U) For that reason, cyber resilience is no longer simply a technical issue. It is an economic issue, a security issue; it’s a leadership issue.

(U) Today I would like to share New Zealand's perspective on the evolving cyber threat landscape, how the New Zealand system is working to build a more resilient environment, the trends we are seeing, and how we are thinking about the impact of artificial intelligence as it reshapes both the threats and opportunities before us.

New Zealand's Cyber Security System

(U) To understand New Zealand's approach, it is useful to briefly explain our national system.

(U) I am the head of New Zealand's National Cyber Security Centre, which is our lead operational cyber security agency. The NCSC is responsible for helping organisations understand cyber threats, build resilience, respond to incidents, and strengthen New Zealand's overall cyber security posture.

(U) The NCSC is a business group within New Zealand's Government Communications Security Bureau, which is a cryptologic agency and part of the New Zealand intelligence community.

(U) In 2024 New Zealand’s Computer Emergency Response Team – or CERT NZ – which focused on cyber security for small and medium sized businesses and individuals was integrated into the NCSC.

(U) The integrated agency now supports cyber resilience across the entire New Zealand economy, from individual citizens and small businesses through to government agencies and critical infrastructure.

(U) The NCSC also perform regulatory functions related to government information security and telecommunications security and provides intelligence that helps organisations make informed risk decisions.

(U) I think about my responsibility as New Zealand's head of operational cybersecurity in four ways:

- (U) Make sure that our organisations, large and small, understand cyber threats through intelligence, analysis, warnings, and guidance; and
- (U) support prevention and preparedness by promoting practical security measures and resilience initiatives.
- (U) Manage an organisation that's ready to respond to significant cyber incidents, providing technical assistance and coordinating with partners across government and industry. And do the capability uplift that's needed to get our organisation ready for the next phase of the 21st century: which includes maximising the impact that we can get from AI tools.
- (U) And playing our role in the international cyber community, working closely with domestic and international partners to strengthen collective cyber security and figuring out where New Zealand can and should have an impactful voice.

The New Zealand Cyber-Security Ecosystem

(U) The NCSC is at the heart of New Zealand's cyber security ecosystem.

(U) We are not the sole defender. We are not the only source of expertise. But we play an important role in bringing together information, partnerships, operational capabilities, and national coordination.

(U) But no government can secure cyberspace alone. As you know, resilience depends on cooperation between governments, industry, academia, technology providers, and citizens.

(U) In my six months in this role, I have quickly learned as so often in national security that cyber security is ultimately about people. Technology matters enormously, but resilience is determined by leadership decisions, organisational culture, and the partnerships of trust that we build with one another.

(U) That is why international conferences like this are so important, and why I am so delighted to have had the opportunity to attend. By meeting one another and learning from each other we strengthen our capability and our determination to disrupt and protect against the malicious actors we know are seeking to do us harm.

Geo-political shift

(U) In the physical world, distance matters. In geographical terms New Zealand is isolated. Our closest neighbour is Australia, a mostly benign nation some 1500 kilometres to our west. We are a trading nation, with a big distance to have to move our goods. Our reliance on our digital infrastructure is high relative to our size; finance, logistics, agriculture sectors all depend on it. But our geographic isolation amplifies our reliance on extra-territorial service providers. Our limited domestic size means a smaller talent pool, fewer large cybersecurity firms, and constrained fiscal headroom, BUT we enjoy good levels of societal and institutional trust; great partnerships in a small community where everyone knows everyone; and a pragmatic regulatory posture, all of which are useful for a cybersecurity agency.

(U) Three 'big shifts' in the international order are fundamentally changing the way that New Zealand thinks about the world we're in.

(U) First, a shift from rules to power. We're moving towards a multi-polar world where rules are more contested and the relativity of power between states assumes a greater role in shaping international affairs.

(U) Second, a shift from economics to security. Economic relationships are reassessed in light of increased military competition in a more securitised and less stable world.

(U) Third, a shift from efficiency to resilience. We're seeing changes in the drivers of economic behaviour, where building greater resilience and addressing pressing social and sustainability issues become more prominent.

In this context, we can't do everything but we must do something. We have to focus on what matters the most.

(U) The foundation for our thinking is New Zealand's **Cyber Security Strategy 2026-2030,** released in February this year.

(U) The strategy recognises that cyber security is not something governments can deliver alone. It requires a whole-of-society approach.

(U) The Strategy identifies four objectives:

- **(U) Understand:** we are well aware of cyber risks and know how to protect ourselves.
- **(U) Prevent and prepare:** we manage cyber risks to prevent harm and are well-prepared when incidents occur.
- **(U) Respond:** We react effectively and decisively to adverse cyber incidents; and
- **(U) Partner:** Our resilience to cyber threats is bolstered by strategic and targeted cooperation.

Some of the practical things we have underway are:

- (U) Establishing a single point for cyber incident reporting which covers breaches, cybercrime and scams and extortion, to improve quality of data and make it easier to access advice, guidance and help in response and recovery from cyber incidents. That should be operational early next year. It means that those reporting an incident no longer need to worry about which govt agency they should be talking to. The system will direct their report to where it needs to go; and they will receive AI-generated advice tailored to their situation about immediate steps they can take to ameliorate their particular incident.
- (U) Ensuring higher and more consistent security standards are embedded in digital procurement and design across government, this includes supporting the government's Digital Action Plan to reduce duplication among government agencies. This is a great opportunity for us to ensure that security is built in from the beginning.
- (U) Ensuring that New Zealand is ready with quantum-resistant cryptographic material to ensure our most sensitive information is protected against evolving cyber threats.
- (U) Together with our Ministry of Foreign Affairs and Trade, bolstering cyber resilience in the Pacific and strategically engage on regional digital and technology issues, including in the wider Indo-Pacific region where it makes sense to do so.

(U) Several challenges stand out.

(U) One challenge is uneven cyber maturity.

(U) As in every country, I worry that in New Zealand, there are organisations demonstrating world-class cyber security practices, others continue to struggle with basic controls.

(U) Another challenge is the growing interconnectedness of digital ecosystems.

(U) Most organisations no longer operate in isolation. They rely on cloud services, software providers, managed service providers, and extensive digital supply chains.

(U) As dependency grows, so does systemic risk.

(U) Finally, there remains a persistent challenge that I'm sure this audience will recognise. We still see too many incidents that could have been prevented through consistent implementation of well-understood security fundamentals.

Themes and Trends from the Last Year

(U) Over the last year we recorded approximately 4,700 cyber security incidents. Those are just the ones people told us about, and definitely represent the tip of the iceberg. Of

those, just under 10% were assessed as nationally significant and required specialist technical support, equivalent to roughly one nationally significant incident every day.

(U) Analysis of these incidents reinforces some judgements about the nature of the cyber threat landscape in New Zealand.

(U) First, as we know, AI is rapidly changing the cyber landscape, and frontier AI will supercharge the risks and opportunities. I'll speak more about AI in a little while.

(U) Second, state-sponsored cyber activity remains a persistent threat to New Zealand organisations and businesses. In New Zealand the primary focus of state activity directed against us has been espionage, but internationally we see state actors using cyber tools to undertake intimidation, intellectual property theft, disruption of networks and critical services, and in some cases, sabotage.

(U) We are also seeing a concerning trend by state actors toward more aggressive and assertive activity in cyberspace, a trend that is eroding norms of behaviour in cyber activity.

(U) Third, cybercrime and especially extortion are escalating in severity. We are seeing two main trends in this area:

(U) Firstly, cybercriminals are becoming more capable both technically and operationally. Some cybercriminals are using sophisticated tools to plan and orchestrate attacks, thereby reducing the effort expended on individual exploits. They are also becoming more considered and capable in their efforts to evade detection. AI will only amplify this trend.

(U) Secondly, cybercriminals have become more aggressive in their pursuit of monetary payment, via ransoms or extortion. The tactics include:

- (U) Targeting individuals
- (U) Increased harassment of potential victims
- (U) Increased focus on theft and exposure of highly sensitive information (such as health, legal or insurance records)
- (U) Greater focus on victims with a low tolerance for disruption, such as infrastructure or health service providers.

(U) New Zealand was one of the first countries in the world to prohibit government agencies from paying ransoms to cybercriminals, and we continue to urge our colleagues in the private sector not to pay – in order to damage this business model and disrupt their criminal enterprise.

(U) Fourth, our reliance on digital supply chains continues to be a major risk for New Zealand business.

(U) Digital supply chain compromises have been responsible for several major incidents in New Zealand in the last year, potentially resulting in loss of personal information and identity data for hundreds of thousands of users.

(U) Organisations in the health sector in particular have been targeted on multiple occasions, especially by cyber criminals aiming to access and steal highly sensitive personal information held on third party applications for the purpose of extortion.

(U) The starting point of many supply chain attacks has been the exploitation of credentials, either stolen or extracted using social engineering techniques.

(U) In other words, applying basic cyber-security controls such as Multi-factor authentication, access limitations and data encryption would go a long way to reducing the impact of supply-chain breaches.

(U) That brings me to social engineering, the manipulation of individuals to access networks and systems, which also remains a persistent threat to organisations and individuals

(U) Social engineering techniques are sometimes associated with scams and simple fraud, but the reality is the targets often include multi-national businesses, government agencies and third-party suppliers.

(U) The techniques and tactics used to undertake social engineering attacks are evolving rapidly with the use of generative AI providing cybercriminals and other malicious actors with new tools to persuade, manipulate and deceive individuals.

(U) I can definitely envisage a world in the near future where AI is building stronger cyber defences at the software layer, which makes humans the weakest link. Social engineering will become a more important vector for criminals and other malicious actors to obtain credentials and breach cyber security. In other words, the manipulation of human factors may become more important, not less, as the AI revolution continues.

(U) The most depressing fact of all: many successful attacks still rely on common weaknesses:

- Poor patching practices
- Weak credentials and access control
- Targeting legacy systems
- Over permissioned access.

(U) The uncomfortable truth is that attackers continue to exploit these weaknesses because they continue to work. And while that remains the case, they won't need the high end expensive AI tools to penetrate our systems.

The Challenges and Opportunities Presented by AI

(U) To finish, let's go back to the challenges and opportunities presented by AI.

(U) No issue has generated more discussion in cyber security over the last year than artificial intelligence.

(U) Existing AI models were already changing the threat landscape. Malicious actors are using publicly available models to automate aspects of cyber operations, increasing the speed and scale of cyber attacks and lowering the expertise required to conduct more sophisticated exploits.

(U) I started this role at about the same time as Anthropic's "Mythos moment", so my whole time as the head of cybersecurity in New Zealand has been dominated by the topic of frontier AI.

(U) As this audience knows, frontier AI models put reasoning and analytical capabilities previously accessible only to advanced nation states and the largest organisations, into the hands of individuals and groups.

(U) These advanced models are demonstrating capabilities that include vulnerability discovery, software analysis, and the autonomous identification of security weaknesses.

(U) As these capabilities mature, they have the potential to significantly accelerate the pace at which vulnerabilities are discovered and exploited. And they will keep getting better. The tools we have today are probably the worst they are ever going to be.

(U) This presents a clear challenge for defenders.

- (U) The time between a vulnerability being identified and being weaponised will continue to shrink.
- (U) Organisations definitely need to respond faster than they do today.

(U) Recognising the scale of this challenge, in June I joined my counterparts from the cyber security agencies of Australia, Canada, Great Britain and the United States in issuing a **Call to Action** on frontier AI and cyber security.

(U) Our Call warned that frontier AI is accelerating the speed, scale, and sophistication of cyber threats and that traditional approaches to cyber risk management are no longer sufficient. We stressed that a step change in cyber defence is required and urged organisations to begin preparing now rather than waiting for these capabilities to become mainstream.

(U) The message was straightforward: **AI is not a future consideration. It is already here.**

(U) We deliberately did this as a group to have an impact. I was and remain concerned that while leaders in New Zealand may recognise the shift that frontier AI will have at an intellectual level, they're still not feeling the urgency and not doing enough right not to take action.

(U) There will be increasing numbers of vulnerabilities, incidents, and operational disruption as frontier AI capabilities continue to mature. Organisations *need* to think about what being ready for this looks like for them.

(U) However it is also clear that frontier AI also creates unprecedented opportunities for defenders.

(U) The same technologies that help identify vulnerabilities can be used to secure software before deployment.

(U) The same automation that benefits attackers can support tools to monitor activity, detect intrusions, provide fast response and analysis, and speed recovery.

(U) In many respects, cyber security is entering a new era where success will depend not on who has the most advanced tools, but rather on who is using them most effectively.

(U) In the New Zealand context we are actively engaging with frontier AI developers, international partners, and cyber security practitioners to better understand both the risks and opportunities these technologies create.

(U) At a technical level my agency is involved in the testing of the latest frontier AI models, including but not limited to Mythos, to understand their capabilities and to use our learning to strengthen cyber defences for the New Zealand government, businesses, and organisations. Our work includes testing New Zealand government-owned code to improve its security, as well as gauging how best to apply the right tools to the right tasks to maximise outcomes. Simply burning through tokens is not, to my mind, a sign of success!

(U) I know other agencies and partners are doing similar investigation and evaluation work. In the coming year I can see our agencies using these insights to provide a significant volume of advice, guidance and direct assistance to our clients to help them adapt to the new environment and sharing best practice with each other.

(U) But while understanding the risks and opportunities from frontier AI is important, it does not change the importance of cyber security fundamentals. It increases it.

(U) I know everyone in this audience understands the message, but it bears repeating.

(U) Organisations should focus on reducing unnecessary exposure, improving patching processes, strengthening identity controls, addressing legacy technology, and preparing for incidents before they occur.

(U) These actions are not new, but they must now be executed more consistently and more quickly.

(U) Those measures were effective before AI. They remain effective today. And they will become even more important t in the future.

Conclusion

(U) Like many leaders in this profession, I believe that cyber security is ultimately about people. Technology matters enormously, but resilience is determined by leadership decisions, organisational culture, and the partnerships we build with one another.

(U) And in an interconnected world where cyber threats are increasingly global, collaboration is no longer optional. It is essential.

(U) That is why New Zealand is an active and engaged partner with many countries around the world in building cyber defence capabilities, and it is why I am here at Cyber Summit Korea to share our experiences, and to learn from yours. As we close this very successful summit, we can all reflect on the benefits of opportunities like this to bring our nations together.

(U) The cyber threats we face may come from sophisticated states, organised criminal groups, hacktivists, supply chain compromises, or emerging AI-enabled actors. They may be deliberately aimed at us, or we may be the unwitting victims of a thoughtlessly crafted attack aimed elsewhere.

(U) The technologies and tactics will change, and the threat landscape will continue to develop.

(U) Faced with these challenges we need to keep sharing information, to keep collaborating and to build partnerships between industry and government that strengthen our shared interests.

(U) And as leaders our job is not to react to change but to anticipate it.

(U) To build organisations capable of adapting.

(U) To create systems that are resilient even when they are tested. To keep building relationships of collaboration and trust with international partners.

(U) And to ensure that the trust placed in our agencies to keep our nations safe is maintained.

(U) Thank you again for the opportunity to speak to you; and congratulations to our hosts for a very successful summit.

Tēnā koutou, tēnā koutou, tēnā tatou katoa.

ENDS