

Draft strawman for discussion: New Zealand is secure and confident in the digital world

New Zealand is increasingly dependent on information communication technology and an open, trusted Internet. Our potential vulnerability grows in proportion to our dependence. Internet connectivity is an integral part of New Zealand’s economic growth and international competitiveness, and our responses to risks to this connectivity needs to be commensurate with our dependence. But this technology provides opportunities for those with criminal or hostile intentions.

This Strategy signals the government’s commitment to ensuring New Zealand is secure and confident in a digital world. New Zealand’s scale and relatively simple telecommunications and network structure enables the public and private sector to work closely together to embed a cyber security culture, and to respond nimbly to evolving cyber risks. New Zealand is a modern, progressive, safe and internationally collaborative country. Our cyber security system is maturing. New institutions have been established, and are building significant connections in the wider system both domestically and internationally. Now we need to move to ensure we are making the best use of our strengths while opening and using more channels for collaboration and collective action both domestically and internationally.

Our values	Six priorities for cyber security (2019 - 2023)						
<p>Partnerships are essential The government has a role to play in cyber security – but not on its own. Close partnerships with the private sector, non-government organisations and the international cyber community are required. Businesses drive the New Zealand economy and depend on the Internet and networked technology. They must protect the information that is critical to their commercial success. The private sector and technical community also have considerable cyber security expertise, and our overseas partners have the scale capability we need to be embedded in to tackle cybercrime domestically.</p>	<p>1 Cyber security aware and active citizens</p> <p>We have a culture in which people are secure online, and know what to do if something goes wrong.</p>	<p>2 Strong and capable cyber security workforce</p> <p>Businesses, community organisations, and public sector agencies rely on a strong cyber security workforce capable of preventing, adapting to, and responding to threats.</p>	<p>3 Resilient and responsive NZ</p> <p>New Zealand can resist cyber threats, and we have the tools and know-how to protect ourselves</p>	<p>4 Internationally active</p> <p>New Zealand’s cyber interests are advanced and protected through our international activity.</p>	<p>5 Proactively tackle cybercrime</p> <p>New Zealand is secure because we proactively and collaboratively prevent, investigate, deter, and respond to cybercrime.</p>	<p>6 Adapt and challenge</p> <p>New Zealand has a strong foundation for well-informed action, and innovation.</p>	What we want to achieve
<p>People are secure online The openness of the Internet is part of its unique value – allowing for unrestricted participation and the free flow of information. Cyberspace should be a trusted medium, where users have confidence in the integrity of information and the protection of their private and financial details. They should be able to engage online without suffering harm or unlawful interference, and be able to pursue criminal and consumer redress when things go wrong. Human rights apply online as they do offline. This includes the right to freedom of expression, and the protection of privacy, as set out in New Zealand law and existing international law.</p>	<p>Our planning and work will focus on:</p> <ul style="list-style-type: none"> practical, targeted, and regular awareness campaigns including simple and actionable prevention messages making it easier to report cybercrime increasing availability of educative tools so people can be secure online sharing research so people can understand the threat and vulnerability landscape for New Zealand 	<p>Our planning and work will focus on:</p> <ul style="list-style-type: none"> incentivising the growth of the cyber security industry in New Zealand incentivising and increasing the supply of skilled cyber security workers supporting the expansion of roles and opportunities for cyber security workers supporting industry and professional organisations to promote responsible management of cyber security across their organisations and workplaces 	<p>Our planning and work will focus on:</p> <ul style="list-style-type: none"> vigorously protecting New Zealand’s most important information infrastructures supporting businesses, NGOs, and community organisations to be protected and ready to respond responding to major incidents using cyber tools and partnerships to further New Zealand’s interests including national security and law enforcement activities ensuring critical national infrastructure organisations take responsibility for the cyber security of their systems improving the information security capabilities and resilience of the public sector 	<p>Our planning and work will focus on:</p> <ul style="list-style-type: none"> prioritising and building international partnerships and cooperation at both policy and operational levels influencing to support the rules-based international order preventing, deterring, and responding to malicious behaviour strengthening regional capacity-building, confidence, and operational cooperation including for law enforcement activities enabling New Zealand’s economic prosperity. 	<p>Our planning and work will focus on:</p> <ul style="list-style-type: none"> encouraging reporting of cybercrime and improve sharing of information about cybercrimes making the law fit for purpose investing more to act internationally to increase access to information, and contribute to global deterrence of cybercrime especially organised cybercrime increasing support for victims of cybercrime investing more in skilled people and resources to combat cybercrime 	<p>Our planning and work will focus on:</p> <ul style="list-style-type: none"> building and implementing a collaborative model for working together across all sectors investing in research to better understand the threat and vulnerability landscape for New Zealand supporting and incentivising researchers to produce high quality cyber security research incentivising the cyber security industry to realise research findings understanding, exploring, and responding to cyber security opportunities and risks arising from emergent technology actively building cooperation between government, private sector, NGOs, and community organisations to achieve better cyber security outcomes 	What we will focus on
<p>Economic growth is enabled Strong cyber security practices result in businesses remaining productive, profitable and transparent to customers and shareholders. New Zealand will be recognised as a desirable place to do business, store data, innovate and invest. ICT and enhanced connectivity will continue to boost economic growth, and minimise costs of cyber insecurity.</p>	▶ [to come]	▶ [to come]	▶ [to come]	▶ [to come]	▶ <i>Example: accede to the Budapest Convention and get an operating agreement to work with Europol to get better access to information to support our investigations, and contribute to the global effort.</i>	▶ [to come]	First up
<p>National security is upheld Cyber threats to New Zealand – particularly state-sponsored espionage, cyber terrorism, theft of intellectual property from government and critical infrastructures – are national security risks. Upholding New Zealand’s national security in the face of this threat is a fundamental part to a successful Strategy.</p>	<p>We will work together across the public, private, education, research, and community sectors in a way that:</p> <ul style="list-style-type: none"> builds and maintains trust is people-centric, respectful, and inclusive balances risk with being agile and adaptive uses our collective strengths to deliver better results and outcomes is open and accountable enhances cyber security and New Zealand’s reputation. 						How we will do it

