Cyber Threat Report 2021/2022

National Cyber Security Centre

The National Cyber Security Centre is part of the Government Communications Security Bureau

Te Tira Tiaki
Government Communications Security Bureau

Ngā kaupapa

FOREWORD

Whakapuakitanga

The National Cyber Security Centre (NCSC), part of the Government Communications Security Bureau (GCSB), supports nationally significant organisations to improve their cyber security posture and responds to national-level harm. This report provides our insight into cyber threats impacting the domestic and international landscapes, and the incidents to which we responded over the 2021/2022 year.

The NCSC deters, detects, disrupts, and provides advice about the types of malicious cyber activity that could affect Aotearoa New Zealand's wellbeing or prosperity.

In the 2021/2022 year, we recorded 350 cyber security incidents, compared to 404 in 2020/2021. The reduction in recorded incidents is not unique to Aotearoa New Zealand; other countries have also observed a similar trend. The difference may reflect a number of contributing factors, including the NCSC's focus on the potential impact of cyber activity as a consequence of Russia's invasion of Ukraine and our increasing ability to detect malicious cyber activity before actors compromise victim networks.

The NCSC stood up a dedicated effort in response to Russia's February 2022 invasion of Ukraine. We helped Aotearoa New Zealand's nationally significant organisations understand how they could be affected, and we examined the role cyber activity plays in hybrid warfare. We released advisories and threat assessments in order to encourage Aotearoa New Zealand organisations to raise their resilience, and to ease the potential pressure on incident responders around the country.

We have delivered a major uplift in national threat detection and disruption with the launch of Malware Free Networks (MFN). MFN is powered by the NCSC's unique threat insights specific to Aotearoa New Zealand. We work with our MFN partners to detect and disrupt threats before they impact their customers' systems. These partnerships enable us to significantly scale our cyber defence work programme across a large range of Aotearoa New Zealand organisations.

Increasing use of technology to deliver services brings many advantages, including for cyber resilience. It also increases the potential for organisations to experience significant cyber impacts. In 2022, heightened geostrategic tensions have impacted the institutions, rules, and norms that reflect Aotearoa New Zealand's values and key national security interests.

The NCSC has focused on the potential implications for Aotearoa New Zealand networks should malicious cyber actors attempt to leverage their capabilities for strategic advantage. In the coming years, there is a realistic possibility geostrategic tensions will increase. As the global environment shifts, the NCSC continues to deliver timely, relevant guidance and services to support the cyber resilience of Aotearoa New Zealand's nationally significant organisations.

Through our role in supporting the Director-General of the GCSB in the Government Chief Information Security Officer (GCISO) function, we are able to provide a single source of leadership and investment advice about information security risks across the public sector.

We will continue to work closely with our international partners to contribute to global efforts to reinforce the importance of upholding the norms of acceptable behaviour in cyberspace.

While malicious cyber actors continue to find new ways to gain access to systems worldwide, the NCSC is adapting to the rapidly changing environment. Every day, we work to protect Aotearoa New Zealand's nationally significant organisations. I hope our report offers useful insight into the cyber threats facing Aotearoa New Zealand, and encourages organisations to continue to review and elevate their cyber resilience strategies.

Lisa Fong (she/her)
Deputy Director-General,
National Cyber Security Centre

BY THE NUMBERS

Mā ngā tau

350

incidents affecting nationally significant organisations

(COMPARED TO 404 INCIDENTS RECORDED IN 2020/2021)

118

of those, or 34%, indicated links to suspected state-sponsored actors

(COMPARED TO 28% IN 2020/2021)

$317m

Since June 2016, the NCSC has prevented an estimated $317 million worth of harm to Aotearoa New Zealand's nationally significant organisations. $33m worth of harm was prevented in 2021/2022.

81

incidents, or 23%, were likely criminal or financially motivated

(COMPARED TO 27% IN 2020/2021)

122,000

The NCSC disrupted over 122,000 malicious cyber events as part of Malware Free Networks

(30 JUNE 2022)

THE NCSC IN A TYPICAL MONTH*

Detects 7 cyber intrusions affecting one or more nationally significant organisations through the NCSC's cyber defence capabilities

Receives 22 new incident reports or requests for assistance. Of the new incident reports received each month, 14 come from international and domestic partners while 8 come from victim organisations self-reporting.

THE NCSC INCREASED AOTEAROA NEW ZEALAND'S COLLECTIVE CYBER RESILIENCE

Co-chaired **27** sector-based Security Information Exchanges

Published **21** reports and advisories for customers

Delivered **70** incident reports to customers

IN THE 2021/2022 YEAR THE NCSC AND GCSB

Received 179 notifications of network change proposals under the Telecommunications (Interception Capability and Security) Act 2013 (TICSA)

Conducted 19 assessments of regulated space activities under the Outer Space and High-altitude Activities Act 2017 (OSHAA), and 55 assessments of regulated radio spectrum activities under the Radiocommunications Act 1989

Conducted 42 assessments under the Overseas Investment Amendment Act 2021 (OIAA)

* These numbers represent the incidents that meet the threshold for an NCSC response. Our focus is on incidents with a possible national impact, or incidents that may affect Aotearoa New Zealand's nationally significant organisations. For incident reports that do not meet the threshold for an NCSC response, the NCSC will engage with other domestic organisations that can support the victim organisation.

OVERVIEW

Tirohanga whānui

The Cyber Threat Report 2021/2022 provides an overview of the NCSC's work during the year 1 July 2021 to 30 June 2022. This report serves as an annual cyber threat barometer, reflecting changes in both the domestic and international landscapes. It aims to highlight and contextualise observable trends about the nature of cyber security incidents affecting Aotearoa New Zealand's nationally significant organisations. It also offers insight into the pressure points affecting organisations worldwide that may also impact Aotearoa New Zealand networks.

The first section of the report focuses on the Aotearoa New Zealand cyber threat landscape, and offers insight into some of the cyber security incidents that caused the most disruption. In the 2021/2022 year, we recorded 350 incidents – compared to 404 incidents recorded in 2020/2021. This section also describes how we define an incident, and how severity ratings are assigned using an incident categorisation matrix.

Of the 350 incidents recorded, 34% showed links to suspected state-sponsored actors, compared to 28% in the 2020/2021 year. A further 23% indicated links to suspected criminal or financially motivated activity, compared to 27% in the 2020/2021 year.

The remaining 43% of incidents either had insufficient information to make a judgement about attribution, or represented preventative efforts undertaken by the NCSC before the activity could have a significant impact. The earlier a cyber incident is detected, the lower the incident response and recovery effort. Conversely, early detection and disruption means there is less information available about the nature and extent of the activity.

The second section of the report reviews the international cyber threat landscape. The geostrategic environment is becoming increasingly complex. Challenges to sovereignty and territorial integrity are occurring in a number of regions, including the Pacific, with some states undermining the rules-based international order in pursuit of their strategic objectives. Escalations of geostrategic tensions can have significant impacts on the international cyber threat landscape.

Russia's February 2022 invasion of Ukraine transformed the cyber security landscape in a matter of months. Like many organisations, the NCSC has worked through a protracted period of heightened cyber threat, preparing for a range of likely threat scenarios. The NCSC has proactively shared timely and actionable guidance to enable others' preparation.

In February 2022, we advised operators of Aotearoa New Zealand's critical infrastructure to prepare for potential cyber threats amid increasing geopolitical tensions in Europe. In April 2022, in coordination with our Five Eyes partners, we warned about the tactics of Russian state-sponsored and criminal cyber actors, and the threat to critical infrastructure.

The final section of the report explains our mission, vision, objectives, and the services we offer to Aotearoa New Zealand's nationally significant organisations. Improving the resilience of Aotearoa New Zealand against cyber threats is one of the NCSC's key priorities.

Organisations around the world are increasingly dependent on digital technologies, yet are still not managing their cyber risk effectively. A key part of the NCSC's work is to issue advisories and guidance to help organisations better understand risks and threats, and the actions they may need to take to prevent compromise.

We help consenting Aotearoa New Zealand organisations recover from cyber security incidents through prevention work, early detection warnings, and incident response and recovery. We also facilitate the secure provision of telecommunications services, and inform the information security standards for the public sector.

The 2021/2022 year for the NCSC has also been one of new partnerships, increased information sharing, and collaboration with global cloud service providers to develop award-winning baseline security templates.

For more information about NCSC services or guidance, visit our website (**www.ncsc.govt.nz**). For readers unfamiliar with any of the terms used, or how the NCSC defines them, a glossary is provided after the report's conclusion.

AOTEAROA NEW ZEALAND THREAT LANDSCAPE

Te āhuatanga o ngā tuma i Aotearoa

In 2022, Aotearoa New Zealand and the rest of the world faced a more complex geostrategic environment. The NCSC monitored the international threat landscape in an effort to contextualise information for Aotearoa New Zealand organisations. Following Russia's invasion of Ukraine in February 2022, the NCSC did not observe a significant change in the domestic cyber landscape that could be associated with the invasion. This section of the report will explore the key cyber threat trends affecting Aotearoa New Zealand organisations in the 2021/2022 year. This includes the continued blurring of the lines between state- and non-state-sponsored actors, and the potential implications for Aotearoa New Zealand networks.

2021/2022 NCSC incidents

Even with the best cyber defences, cyber security incidents can still occur; malicious cyber actors regularly discover new ways to gain access to systems. Technological innovation compels changes in actors' tactics, which, in turn, drives significant changes in the nature of the malicious cyber activity that victim organisations experience.

This fiscal year, we recorded 350 cyber security incidents. This figure is lower than the previous year's 404 recorded cyber security incidents. The difference may reflect a number of contributing factors, including the potential impact of cyber activity as a consequence of Russia's invasion of Ukraine.

Aotearoa New Zealand's security interests are being challenged by the international rise of strategic competition; states are more readily pursuing their strategic objectives in ways that undermine the rules-based international order. These geostrategic shifts have presented opportunities for both state- and non-state-sponsored cyber actors to take advantage of vulnerable systems and seek persistent, strategic access to networks. It is a realistic possibility that adversaries typically impacting Aotearoa New Zealand organisations have turned their attention elsewhere.

The NCSC has focused on the potential impact of cyber activity as a consequence of Russia's invasion of Ukraine despite no recorded direct cyber impact to Aotearoa New Zealand networks associated with the invasion. While Russian state-sponsored cyber activity associated with the invasion has been focused predominantly on Ukrainian targets, the threat of spill-over effects remains a significant concern for the international community.

Developments in the NCSC's cyber defensive capability have allowed us to scale some services to a significant number of organisations.

How the NCSC defines incidents

An incident can be any malicious threat to a customer's network or information, even where an actor is unsuccessful or there is no confirmed compromise.

Reconnaissance and network scanning, possible attempts to exploit customer vulnerabilities, accidental data leaks, or suspicious events that trigger analysis to determine if they are malicious might all be counted among the NCSC's total incidents.

We categorise incidents by considering the scope, size, and role of the affected victim alongside the possible harm and impact caused by the incident. Incidents range from category 6, being minor or of least concern, to category 1, being critical.

Analysing trends in tactics and techniques

The NCSC uses MITRE ATT&CK as a framework to map cyber security incidents. MITRE ATT&CK is a public knowledge base that provides a common set of terms to describe the tactics and techniques used by actors during various stages of an intrusion. By mapping recorded incidents to MITRE ATT&CK, the NCSC can gain insights into common or emerging trends in actor tactics and techniques. Each malicious incident can include multiple tactics and techniques, depending on the evidence of malicious activity.
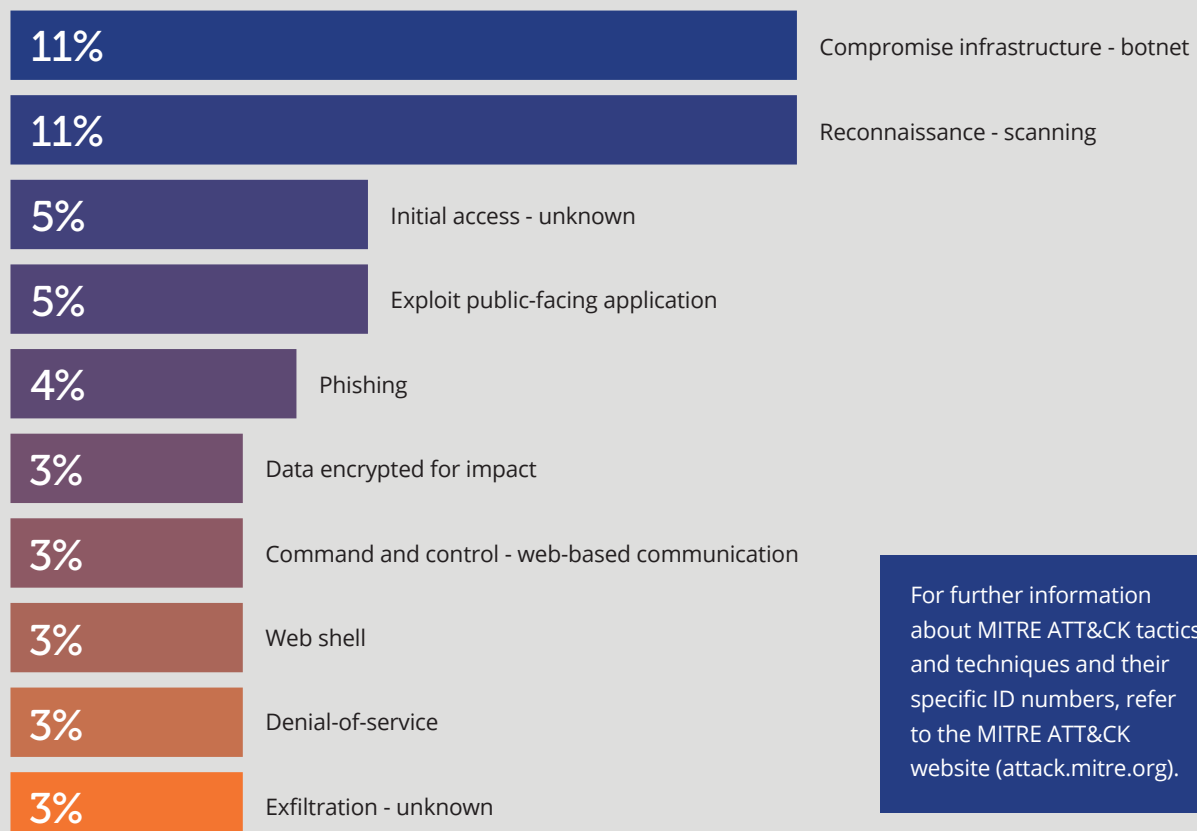
Across malicious incidents from the 2021/2022 year, vulnerability scanning was the second most commonly occurring technique, down from first position in 2020/2021. We also regularly observed infrastructure compromised with botnets. Botnets enable a malicious cyber actor to target thousands of devices all over the world simultaneously. This disproportionately high number is reflected in the graphic below, but does not represent increased targeting of Aotearoa New Zealand organisations.

The most commonly recorded known method of gaining initial access to a network was by exploiting a public-facing application, which mirrors 2020/2021 findings. Yet, there were more incidents where the method of gaining initial access was unknown. Early intervention often means specific detail about malicious cyber activity is unavailable. If a malicious cyber actor pivots through multiple levels of a victim's system, there is more evidence of tactics and techniques – or the 'known knowns'. If the actor is disrupted partway through its activity, there are more 'known unknowns'. If the activity is not detected, or the actor is proactively blocked before it impacts the victim network, there are more 'unknown unknowns'.

Most recorded MITRE ATT&CK tactics and techniques observed by the NCSC in 2021/2022*

11%	Compromise infrastructure - botnet
11%	Reconnaissance - scanning
5%	Initial access - unknown
5%	Exploit public-facing application
4%	Phishing
3%	Data encrypted for impact
3%	Command and control - web-based communication
3%	Web shell
3%	Denial-of-service
3%	Exfiltration - unknown

For further information about MITRE ATT&CK tactics and techniques and their specific ID numbers, refer to the MITRE ATT&CK website (attack.mitre.org).

* This graphic only represents recorded NCSC incidents where MITRE ATT&CK tactics and techniques were observed with a high degree of confidence.
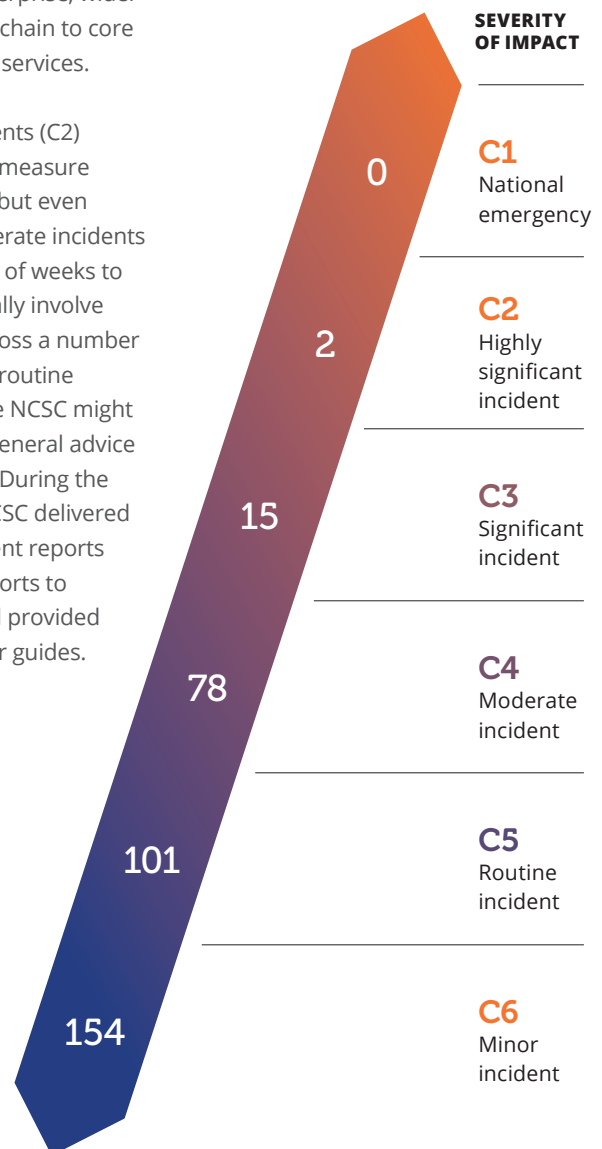
Incidents by category 2021/2022

The annual number of recorded incidents is a useful measure, but it does not reflect changes in the cyber landscape; the context behind each incident is critical to determining the overall impact of malicious cyber activity on the domestic landscape. For example, 20 highly significant incidents in a fiscal year would more radically change the domestic landscape than 400 minor incidents, because the potential impact on critical services, society, and the economy would be greater.

The volume and percentages of how incidents are identified varies over time. Incidents recorded by the NCSC come from a range of sources, including through our cyber detection capabilities, reporting from our international and domestic partners, and direct requests from victim organisations. Over the course of an average month in 2021/2022, the NCSC handled 29 incidents. Of those, about half came from a domestic or international partner alerting us to the possibility of an incident, about a quarter were detected through our own capabilities, and another quarter came from victim organisations self-reporting suspicious activity.

A national cyber emergency (C1) is defined as an incident that causes severe disruption to a core Aotearoa New Zealand service, and/or affects key sensitive data, and/or undermines the economic or democratic stability of Aotearoa New Zealand. At the other end of the scale, a minor incident (C6) is defined as an incident causing a known or likely impact on an individual/individuals, or precursor activity against an individual/individuals, or a small or medium enterprise. In the middle, a significant incident (C3) is defined as an incident causing a known or likely impact on a large commercial enterprise, wider government, or supply chain to core Aotearoa New Zealand services.

Highly significant incidents (C2) consume a substantial measure of time and resources, but even significant (C3) or moderate incidents (C4) can take a number of weeks to resolve, and will generally involve complex responses across a number of teams. For minor or routine incidents (C5 or C6), the NCSC might respond by providing general advice or alerts to customers. During the 2021/2022 year, the NCSC delivered 70 cyber security incident reports or incident analysis reports to specific customers, and provided 21 general advisories or guides.

The year's two most severe incidents were rated C2. These incidents were connected; analysis revealed that after the malicious cyber actor compromised the first organisation, it used its access to target the second victim organisation days later by exploiting the trusted relationship between the two organisations.

SEVERITY OF IMPACT

Value	Category	
0	**C1**	National emergency
2	**C2**	Highly significant incident
15	**C3**	Significant incident
78	**C4**	Moderate incident
101	**C5**	Routine incident
154	**C6**	Minor incident

Support to major events

The GCSB contributes cyber security support to multi-agency efforts on major national events. Planning for major events involves preparing for the possibility a cyber security incident could cause disruption and/or reputational harm.

In 2021/2022, the GCSB, through the NCSC, provided cyber security support to a number of events, including the virtual Asia-Pacific Economic Cooperation (APEC) 2021 forum. The NCSC assisted the agencies involved to ensure the virtual hosting platforms used to facilitate online meetings were secure, and that risk assessment and mitigation processes were in place to protect participants.

The NCSC also supported the Electoral Commission's delivery of a by-election in the Tauranga electorate. This included the provision of cyber resilience advice, and engagement with the Electoral Commission to ensure appropriate incident response processes were in place.

The NCSC will continue to look for opportunities to contribute cyber security support to organisations during major national events such as the forthcoming census and General Election.

Confidentiality

To protect relationships of confidence and trust, the NCSC does not generally comment publicly about whether it is involved in providing investigation or incident response support to victims of malicious cyber activity. Any incidents reported to the NCSC are treated as commercial-in-confidence.

This helps to encourage organisations to engage with us when they have been subject to a cyber security incident. It also helps to protect the integrity of any investigations we are involved in. There are occasionally highly significant incidents where the NCSC and the organisation/s we are assisting may agree that disclosure of our involvement is appropriate.

Links to state-sponsored actors

In the 2021/2022 year, 34% of the NCSC's 350 recorded incidents showed indications of a connection to state-sponsored actors (compared to 28% in the previous year). The 2021/2022 number totals 118 incidents of concern, a similar number to the 113 recorded in 2020/2021. The slight increase in this proportion relative to 2020/2021 likely reflects both the lower total incident count, and the reduction in recorded criminal or financially motivated incidents.

The scale of state-sponsored activity against Aotearoa New Zealand networks makes it challenging to identify, track, respond, and/or attribute the actors involved. State-sponsored actors regularly adapt their tactics in order to escape detection for as long as possible. State-sponsored activity is less likely to disrupt services or cause obvious harm, and less likely to enter the public spotlight, but still has potentially significant economic and reputational impacts for Aotearoa New Zealand. Some states conduct espionage activity to support their economic development; this can involve theft of information and intellectual property.

Case study

The NCSC became aware of a sophisticated actor targeting an Aotearoa New Zealand organisation. After contacting the organisation, we initiated an investigation. Analysis revealed that after compromising the victim organisation, the malicious cyber actor had used its access to target a second victim organisation only days later by exploiting a relationship of trust between the two organisations. We assisted both victims and their service providers to evict the actor and prevent further attempts to compromise their networks. Prompt response efforts and work to identify the full path of the intrusion contained the compromise for both victims, and reduced its impact.

Financially motivated or criminal activity

In the 2021/2022 year, 23% of the NCSC's 350 recorded incidents showed indications of a connection to criminal or financially motivated actors (compared to 27% in the previous year). The 2021/2022 number totals 81 incidents, which is a noticeable reduction from the 110 recorded in 2020/2021. The decrease in this proportion relative to 2020/2021 possibly reflects the increasing opportunities for actors to target systems they identify as valuable following Russia's invasion of Ukraine.

The NCSC observed fewer high-impact ransomware and distributed denial-of-service (DDoS) activities in 2021/2022 than in 2020/2021. It is possible the reduction in ransomware and DDoS activities targeting Aotearoa New Zealand in 2021/2022 is connected to Russia's invasion of Ukraine. The invasion has almost certainly disrupted cyber criminals based in Russia and Ukraine, and likely caused them to reorient their strategic objectives. The observed reduction in ransomware reflects international trends for early 2022, while DDoS

activity has been more turbulent preceding and following Russia's invasion of Ukraine. DDoS activity spiked in some states – including Ukraine, Russia, and a number of states that opposed Russia's invasion of Ukraine – while it decreased elsewhere.

A key trend we are observing year-on-year is the blurring of the lines between state-sponsored and criminal or financially motivated actors. We have increasingly observed non-state-sponsored actors using capabilities that, until recently, were exclusively in the hands of sophisticated state-sponsored actors.

The growth in sophistication among non-state-sponsored actors is particularly concerning because they are increasingly empowered to have significant impacts on critical networks. Some criminal groups also appear to operate without sanction from 'safe havens' in their resident countries. The increasing availability of cyber capabilities reduces technical

barriers to entry, enabling any group with purchasing power to conduct sophisticated cyber operations.

Criminal actors may seek to cause disruption or engage with media in order to pressure victims to pay a ransom, and therefore will focus on targeting victims they consider likely to respond to their demands.

The NCSC anticipates emerging players – both state- and non-state-sponsored – will follow a similar cyber capability development trajectory as traditional adversaries. The increasing diversity of cyber actors using sophisticated, commercially available tools further complicates incident response and attribution efforts. (See 'Calling out malicious cyber activity')

In the 2021/2022 year, 43% of the NCSC's recorded incidents either represented preventative efforts undertaken by the NCSC before the activity could have a significant impact or lacked the information needed to attribute the malicious activity.

Case study

An IT service provider contacted the NCSC after a routine scan identified suspicious software running on one of its customer's servers. The software was a commercial security testing tool often co-opted by malicious state-sponsored and criminal actors – including ransomware operators. We worked alongside the organisation to identify the source, timeline, and extent of the infection. Analysis revealed the network had been compromised for almost four months. The source was traced back to two users who inadvertently downloaded a fake version of a video-conferencing software.

A malicious actor used this counterfeit software to gain an initial foothold on the network and move laterally. Ultimately, 44 servers were impacted. The NCSC was unable to find any forensic evidence of data exfiltration or attempts to deploy ransomware. It remains possible auditing tools did not capture all of the actor's activities, or the actor was interrupted before achieving its ultimate objective.

Russia's invasion of Ukraine

The future trajectory of Russia's invasion of Ukraine is unclear. The NCSC assesses the most significant threat to Aotearoa New Zealand networks from the invasion is indirect malicious cyber activity that affects a critical supply chain. Equally, cyber criminal actors could opportunistically conduct ransomware or similarly disruptive operations against valuable networks, taking advantage of the situation.

Russian cyber activity observed in Aotearoa New Zealand since Russia's February 2022 invasion of Ukraine has reflected international trends. Russia appears to have been careful not to spread its cyber operations wider than its intended targets, which have been based predominantly in Ukraine and neighbouring countries. (See 'International landscape')

In May 2022, the Director-General of the GCSB, Andrew Hampton, noted the NCSC had not observed a significant change in the domestic cyber landscape that could be associated with the invasion. However, he noted the NCSC was alert to the fact the situation could change with no advance warning, as both pro-Russia and pro-Ukraine cyber activity continued to impact systems around the world.

The NCSC has established a dedicated response to the cyber threats arising from Russia's invasion of Ukraine. This has focused on three areas: sharing cyber threat intelligence, using our technical cyber security capabilities to monitor Aotearoa New Zealand networks for malicious activity, and providing advice and guidance to nationally significant organisations to build continued resilience.

In February 2022, we advised operators of Aotearoa New Zealand critical infrastructure to prepare for potential cyber threats – including destructive malicious software (malware), ransomware, DDoS activity, and cyber espionage – amid increasing geostrategic tensions in Europe.

Aotearoa New Zealand publicly condemned Russia's invasion of Ukraine and confirmed its support for Ukraine's sovereignty. The Government imposed sanctions against Russian officials responsible for malicious cyber activity, and subsequently condemned Russia's malicious cyber activity against Ukraine, alongside the European Union and international partners.

"

With the battlefield invasion, has come the cyber offensive, with Russian targeting of Ukrainian digital infrastructure. It may not have been of the scale or had the impact some had anticipated, but it is happening. "

Andrew Hampton, Director-General,
Government Communications Security Bureau
(May 2022 - Speech to the Wairarapa branch of the New Zealand Institute of International Affairs)

Common Vulnerabilities and Exposures

Common Vulnerabilities and Exposures (CVEs) are publicly disclosed information security issues, stored in a database. A CVE number uniquely identifies each vulnerability.

The NCSC continues to observe an increase in the speed and scale of mass exploitation of recently disclosed vulnerabilities. Without effective controls to safeguard data integrity, data will always be vulnerable. This is further challenged by automation, in which massive amounts of data are processed with little to no human involvement. Malicious cyber actors will continue to find ways to exploit organisations that have not adequately protected their data.

Malicious cyber actors quickly take advantage of flaws, scanning for and targeting every device and organisation potentially vulnerable to exploitation in order to secure a foothold. Then, once they have generated enough access vectors, they selectively pick targets for unspecified future cyber operations. This scanning activity is not always concerning or abnormal. Sometimes, reconnaissance activity is merely passive information gathering.

Apache Log4j

Sometimes, however, reconnaissance activity is extremely problematic. The most significant CVE disclosed in the 2021/2022 year was the Apache Log4j vulnerability. In December 2021, a vulnerability was discovered in Apache Log4j, an open-source software library used around the world and found in a vast array of Java-based applications. It left global networks vulnerable to malicious cyber actors remotely accessing systems, stealing information, exfiltrating data, and infecting networks with malware.

The NCSC shared an advisory with its customers which contained information about mitigating the vulnerability and detecting malicious cyber activity. Our MFN capability enabled the NCSC to rapidly disseminate thousands of indicators of Log4j-related activity and proactively block them in near real-time before they could harm Aotearoa New Zealand organisations. In December 2021 alone, our MFN partners disrupted over 20,000 Log4j-related events on their customer networks.

'Calling out' malicious cyber activity

As part of Aotearoa New Zealand's commitment to upholding the rules-based international order and internationally accepted norms of behaviour in cyberspace, the Government may publicly call out actors responsible for malicious cyber activity when it is in the national interest to do so.

The GCSB, through the NCSC, conducts technical attribution of malicious cyber activity and provides this, usually at a classified level, to the Aotearoa New Zealand Government. The Government may draw on the NCSC's technical attribution – as part of an all-of-government process – and use this information to publicly call out a malicious cyber actor.

In July 2021, the Minister Responsible for the GCSB, on behalf of the Aotearoa New Zealand Government, publicly condemned malicious cyber activity by state-sponsored actors from the People's Republic of China. The actors targeted ProxyLogon vulnerabilities in Microsoft Exchange, which enabled them to steal intellectual property and personal information from about 400,000

vulnerable global servers. This attribution was underpinned by a GCSB technical assessment.

In May 2022, the NCSC provided advice to the Ministry of Foreign Affairs and Trade (MFAT) in support of the Minister of Foreign Affairs' statement on behalf of the Aotearoa New Zealand Government, publicly condemning the campaign of destructive cyber activity against Ukraine attributed by our partners to Russia.

The NCSC often becomes aware of malicious cyber activity without knowing the identity of the actor responsible, and it is not always possible to attribute activity to a particular state or malicious cyber actor. Cyberspace enables actors to operate with various degrees of anonymity. The open architecture of the internet enables threat actors – who could be anywhere in the world – to route their activity through third-party infrastructure. The identification of devices used by the actors does not guarantee finding the responsible group, either.

Case study

The NCSC became aware of malicious cyber activity targeting an Aotearoa New Zealand IT service provider, and quickly engaged the organisation to provide notification and offer support. The organisation identified a breach of its identity and access management platform. Investigations determined the organisation had been running an outdated and vulnerable version of software that the actor was able to compromise to gain initial network access. The actor installed tools that allowed it to execute commands, elevate privileges, and maintain remote access to the victim's systems. It was able to exfiltrate usernames and credentials, as well as technical information about system configurations – likely intended for use in gaining further access. Swift detection and containment prevented the actor from establishing persistence on the victim network. The NCSC assisted the organisation to secure its environment, and provided forensic analysis to help inform and guide the organisation's remediation and recovery efforts.

Te āhuatanga i te ao

As the geostrategic environment becomes increasingly complex, there is more potential for Aotearoa New Zealand networks to be targeted by malicious cyber actors attempting to leverage their capabilities for strategic advantage. There is a realistic possibility geostrategic tensions will increase over the coming years. Since Russia invaded Ukraine on 24 February 2022, the international cyber landscape has been impacted.

The invasion roused organisations all over the world to shield their networks and systems. It also fuelled debate about the role cyber activity plays in hybrid warfare. Governments suddenly shifted their intelligence priorities and considered new cyber threat scenarios. Beyond the invasion and other geostrategic tensions, the 2021/2022 international landscape was defined by supply chain vulnerabilities and the increasing sophistication of non-state-sponsored actors. The outlook for the international cyber landscape over the next fiscal year is uncertain.

Russia-Ukraine

Russia's February 2022 invasion of Ukraine was supported by cyber activity. In many instances, Russian cyber operations coincided with kinetic operations. Early indications of cyber activity appeared in the form of DDoS activity and the deployment of destructive wiper malware against a number of Ukrainian targets. In late March 2022, Russian cyber actors disrupted Ukrainian internet service provider Ukrtelecom, which resulted in a widespread internet outage. Less visible, but with significant impact, Russian information operations sowed more chaos into already chaotic circumstances.

Russia's invasion of Ukraine has put networks around the world at a protracted, heightened risk of compromise from both state- and non-state-sponsored cyber actors.

The cyber threat to global networks is not limited to malicious cyber activity emanating from Russia or Ukraine. The volume of unattributed cyber activity associated with the invasion reflects and exacerbates the challenge of attributing activity to a particular actor. It also presents opportunities for states to target victim networks while obfuscating connections to state involvement or tasking.

The heightened awareness and defensive posture of states around the world – including Aotearoa New Zealand – is almost certainly helping them to ward off malicious cyber activity. Incident responders in Ukraine are demonstrating the experience they have earned the hard way, after years of withstanding malicious cyber activity from Russia.

Importantly, though, Russia is only constrained by its decision-makers' desire to be careful to avoid spill-over. This could change at any time.

Pro-Russia cyber actors are not the only participants in cyber activity associated with the invasion. Patriotic and opportunistic cyber actors are taking sides, conducting malicious cyber activity on behalf of either Russia or Ukraine. Pro-Ukraine cyber activity has included various cyber operations conducted by the 'hacktivist' collective Anonymous, and by motivated cyber actors volunteering for the IT Army of Ukraine. Pro-Russia cyber actors engaged in activity related to the invasion has included the groups Killnet, Ghostwriter, and Conti.

The proliferation of cyber vigilantes contributes to the risk of accidental escalation. This has presented challenges around evolving global cyber norms and what responses to threats from adversary states are considered proportionate and reasonable.

Timeline: A selection of pro-Russia and pro-Ukraine cyber operations

13 January 2022
Discovery of WhisperGate destructive wiper malware deployed against Ukrainian targets

14 January 2022
Defacement of Ukrainian government websites

14 February 2022
Successful compromise of Odesa-based critical infrastructure

15 February 2022
DDoS activity disables Ukrainian government, bank, and radio websites for several hours

23 February 2022
HermeticWiper malware impacts Ukrainian finance, IT, and aviation sector organisations

24 February 2022
AcidRain wiper malware targets and disrupts the European Viasat KA-SAT satellite service

24 February 2022
Russia's military invades Ukraine

1 March 2022
Defacement of Anonymous' website

28 March 2022
Cyber operation against Ukrtelecom leads to widespread outages across Europe

8 April 2022
Attempted destructive wiper cyber operation against a Ukrainian energy provider

8 April 2022
DDoS activity targets Finland government websites while the Ukrainian president speaks to the Finnish parliament

22 April 2022
Ukraine's national postal service targeted with DDoS activity

9 May 2022
Russian TV programme breached to screen an anti-war message

2 June 2022
Ukrainian government organisations targeted with Cobalt Strike beacons

17 June 2022
DDoS activity delays the Russian president's speech at the St. Petersburg International Economic Forum

International partnerships

International cooperation across the cyber landscape has surged in the 2021/2022 year. This highlights the importance of states and organisations working in coalition to mitigate threats. There has been a sustained multilateral effort to provide guidance and advisories about what vulnerable organisations should do if targeted.

Aotearoa New Zealand is a member of the Five Eyes multilateral intelligence sharing arrangement, along with Australia, Canada, the United Kingdom, and the United States. Being part of a wider international network with shared interests and values is fundamental to Aotearoa New Zealand's resilience as a small nation. Through the Five Eyes arrangement, which facilitates cooperation on issues including cyber, artificial intelligence (AI), quantum technology, and space, the GCSB and the NCSC can draw on greater support, technology, and intelligence than would otherwise be available to Aotearoa New Zealand.

The international community has responded to Russia's invasion of Ukraine with unprecedented solidarity, speed, and strength, and has sustained momentum as the situation has evolved. Aotearoa New Zealand's Five Eyes partners quickly declassified intelligence and made it public. This helped to unify and inform groups worldwide working to support Ukraine, frustrated the goals of pro-Russia cyber actors by challenging their ability to promote false narratives, and enabled the Five Eyes partnership to more quickly attribute Russian cyber activity.

"

While there is a battle on the land, in the air, and on the ocean raging in Ukraine, there is also a battle raging in the cyber and information domains. **"**

Andrew Hampton, Director-General, Government Communications Security Bureau (May 2022 - Speech to the Wairarapa branch of the New Zealand Institute of International Affairs)

International norms

The NCSC works closely with its like-minded partners to promote norms of responsible behaviour in cyberspace. International cyber norms are an attempt to gain consensus on acceptable behaviour in cyberspace, and more generally to shape the cyber environment. Clarifying states' rights and responsibilities in cyberspace forms a critical part of managing threats to Aotearoa New Zealand networks.

In the current geostrategic environment, in which states are targeting other states with both cyber and kinetic operations, Aotearoa New Zealand organisations must remain alert to potential cyber threats to their networks.

Russia's invasion of Ukraine – and the persistence of both pro-Russia and pro-Ukraine cyber activity – will continue to challenge the international community's efforts to uphold cyber norms. If the international community does not maintain a consistent approach to state-on-state cyber activity, cyber norms may be inadvertently undermined.

Technology plays a key role in global competition. Adversary states will shape their cyber calculus based on how the international community responds to Russia's invasion of Ukraine, and how willing the community is to impose costs on states that conduct malicious cyber activity against others. As technological innovation continues to drive changes in actor sophistication, and global competition more broadly, cyber norms may be further undermined.

Hybrid threats

A key theme in the 2021/2022 landscape has been the threat of hybrid warfare – and, specifically, how Russia might use its hybrid warfare toolkit against Ukraine. Hybrid threats are a mix of military, non-military, covert and overt activities by state- and non-state-sponsored actors that occur below the line of conventional warfare. Cyber as a component of hybrid warfare could appeal to aggressor states because the potential attack surface is constantly increasing.

The adoption of AI, internet-of-things (IoT), telecommunications systems, machine learning, and quantum computing promises technological innovation, but simultaneously threatens all internet-connected systems. Additionally, hybrid warfare instils anxiety and undermines public confidence in state security because targets are pursued from multiple angles. Cyber security best practice and improved information sharing are needed to help counter the evolving and adaptive nature of hybrid threats.

Russia has strategically used cyber operations alongside traditional kinetic operations in pursuit of its goals in Ukraine. The malicious cyber activity observed so far has challenged, and will continue to challenge, assumptions about the role cyber activity plays in hybrid warfare. One thing is clear: the use of cyber operations in warfare exacerbates the ever-present threat to internet-connected devices and the services they support globally.

Malicious cyber activity is unconstrained by state borders, and cyber activity can indiscriminately spill over to target systems all over the world. This increases the risk of collateral damage and accidental escalation caused by misattribution or unintentional disruption of critical infrastructure. Notably, North Atlantic Treaty Organisation (NATO) Secretary General Jens Stoltenberg said in February 2022 that malicious cyber activity could trigger Article 5, the Treaty's principle of collective defence.

"Technology is accelerating the pace and intensity of world events, not vice versa; and cyber security is a lead indicator for world events. What we see unfolding in cyberspace is then evidenced in the real world."

Lisa Fong, Deputy Director-General, National Cyber Security Centre (May 2022 – Speech at CYBERUK, the United Kingdom Government's flagship cyber security event)

International standards

International standards reflect best practice and offer a core and evolving reference from which organisations internationally can build their security practices.

We engage with international standards bodies and keep up-to-date with new approaches and challenges, which we take into account when updating the New Zealand Information Security Manual (NZISM).

Internationally, organisations face a range of new security issues from emerging technology. Notable challenges include the large-scale migration of applications to cloud-hosting services, quantum computing, and increasingly dispersed and interdependent infrastructure.

We are working with our partners to better understand the threats emerging technology presents to the cyber threat landscape, and the security measures required to manage these new risks and threats.

Supply chain

Cyber security weaknesses, conflict, climate change, and COVID-19 have all had major impacts on global supply chains. In today's world, it is no longer sufficient for organisations to ensure the cyber security resilience of their own networks – they must also consider the security of the entire supply chain. The rapid global uptake of IoT devices and connected systems means all organisations are dependent on services that extend beyond what they can oversee and control. The outsourcing of technology services can increase productivity and security, but it can also expose organisations to more risk by increasing the potential attack surface.

A SUPPLY CHAIN COMPROMISE targets software, hardware, or an IT service provider with the ultimate aim to exploit downstream customers.

The interconnectedness of the online environment, together with the comprehensive nature of global supply chains and interoperability of technology, leaves networks worldwide increasingly exposed to a range of potential cyber-related impacts. A recent development in supply chain compromise involves the exploitation of software updates as a means of establishing a presence in customer systems.

An example of this is the December 2020 SolarWinds Orion supply chain compromise, which had widespread international impact. Malicious cyber actors strategically compromised a legitimate software update prior to its distribution by the software provider. Aotearoa New Zealand attributed the activity, along with its international partners, to Russian state-sponsored actors in April 2021.

Malicious cyber actors are shifting to establish more strategic access through the compromise of critical supply chains. State-sponsored actors are likely pre-positioning on networks beyond their strategic objectives by gaining access to multiple networks globally to enable future exploitation. It takes a significant amount of time and resource to develop mechanisms to gain access, and maintain long-term, persistent access, to multiple networks.

"

We are committed to the international rules-based order, which, amongst other things, stipulates global conventions about accepted behaviour in cyberspace. There are a number of nation states that routinely operate outside of those norms. Their activity, and that of sophisticated cyber criminals, drives an ever-evolving threatscape we engage with our partners to defend against. "

Lisa Fong, Deputy Director-General, National Cyber Security Centre
(April 2022 – Speech, delivering the Royal United Services Institute's (RUSI) annual Gallipoli Memorial Lecture)

The NCSC assesses both state- and non-state-sponsored groups will likely continue to seek ways to exploit the digital transformation of organisations, and to infiltrate supply chains via weak access points. As organisations strengthen their own cyber security, their exposure to cyber threats in the supply chain increasingly becomes their weakest point. Adversaries will compromise suppliers to get past the security controls of the target organisation. This could occur via vulnerability scanning, the use of privileged access controls held by the supplier, the compromise of legitimate software updates, or DDoS activity.

Supply chain security can be strengthened with zero trust architecture. The zero trust model leverages the 'principle of least privilege', in which every user or device is only given the bare minimum access permissions needed to perform its intended function. Zero trust is an 'assume breach' posture, which protects systems from a number of levels of compromise. This is especially important for online supply chains, where the shift to cloud-based platforms will increasingly expose weak identity authentication processes. The large-scale migration of applications to cloud-hosting services, combined with a global workforce gravitating towards hybrid work, presents a number of risks to cyber security. In a world of increasingly sophisticated cyber threats, the NCSC's advice and standards are based on a zero trust approach.

Supply chain risk
Read our guidance online at
www.ncsc.govt.nz/resources/

The guiding principles of ZERO TRUST are

1
never trust, always verify

2
employ a least privilege access strategy

3
assume breach

Disinformation

While disinformation does not fall into the scope of the NCSC's work, it poses challenges to analysis of the cyber threat landscape. Malicious cyber actors often spread disinformation to create confusion and exploit divisions among target audiences.

Preceding and following the Russian invasion of Ukraine, Russian leadership spread disinformation and misinformation worldwide about Ukraine and its allies in an attempt to promote their preferred narrative.

The unprecedented declassification of intelligence from our Five Eyes partners in response to Russia's invasion of Ukraine has been critical in efforts to counter Russian disinformation.

While the NCSC has a limited role when it comes to disinformation, we are responsive to reporting from our security partners and the public regarding disinformation campaigns.

Disinformation
The deliberate, intentional spread of false and misleading information designed to achieve a strategic purpose.

Misinformation
Incorrect or misleading information that is not produced and distributed with an underlying purpose.

"
The war itself is challenging our notions of conflict and demonstrating how multifaceted warfare now is, with cyber attacks and prolific disinformation now accompanying the more traditional forms of combat. "

Rt Hon Jacinda Ardern,
Aotearoa New Zealand Prime Minister
(July 2022 - Speech at the Lowy Institute in Sydney, Australia)

ABOUT OUR WORK

Mō ā mātou mahi

Our people work at the heart of Aotearoa New Zealand's cyber defence. We protect our country's wellbeing and prosperity as we work towards our vision of a safer and more resilient digital world for Aotearoa New Zealand. The NCSC supports nationally significant organisations to improve their cyber security, and we respond to national-level harm and advanced threats.

Our strategic objectives

Defend National Security

New Zealand's information security culture is globally respected and trusted; New Zealand's values and way of life are protected.

Raise Cyber Resilience

New Zealand's digital environment is able to withstand adversity, and organisations play an active role in protecting themselves.

Facilitate Digital Transformation

New Zealand organisations embrace technology responsibly and securely.

What the NCSC does

The NCSC is Aotearoa New Zealand's lead organisation for responding to cyber threats that could have an impact on national security and economic wellbeing. Every day, we work to protect Aotearoa New Zealand and its interests. Our mission is to protect Aotearoa New Zealand's wellbeing and prosperity through trusted cyber security services.

When potentially high-impact cyber security incidents happen, we take action to reduce the impact and prevent future harm. We uplift cyber resilience throughout Aotearoa New Zealand, which, in turn, deters Aotearoa New Zealand's adversaries by raising the costs of targeting Aotearoa New Zealand systems. We focus on meeting our strategic

objectives by streamlining our work into four multi-layered areas: detect, disrupt, advise, and deter.

Detect

The NCSC's cyber security technologies find and share indications of malicious activity or vulnerabilities by detecting anomalies and signs of compromise on consenting customer networks.

Cyber defence

The NCSC works with Aotearoa New Zealand's nationally significant public and private sector organisations to deploy defensive capabilities, including those developed through

the CORTEX initiative and MFN service. We use our capabilities to protect organisations from malicious cyber activities including ransomware, DDoS, intellectual property theft, customer data loss, and the destruction or dissemination of private communications. We only deploy our capabilities with consenting organisations, and do not disclose the identities of individual organisations receiving our protection.

The NCSC's capabilities supplement commercial service offerings because they are tailored to the specific threats Aotearoa New Zealand is facing. MFN is powered by the NCSC's unique threat insights.

We work with our MFN partners to detect and disrupt threats before they impact their customers' systems.

These partnerships enable us to significantly scale our cyber defence effort across a large range of Aotearoa New Zealand organisations. We continue to form partnerships with private sector organisations in order to facilitate information sharing and better contribute to cyber resilience uplift across the board.

The NCSC's cyber defence pursues a future in which Aotearoa New Zealand's information security culture is globally respected and trusted, and its values and ways of life are protected.
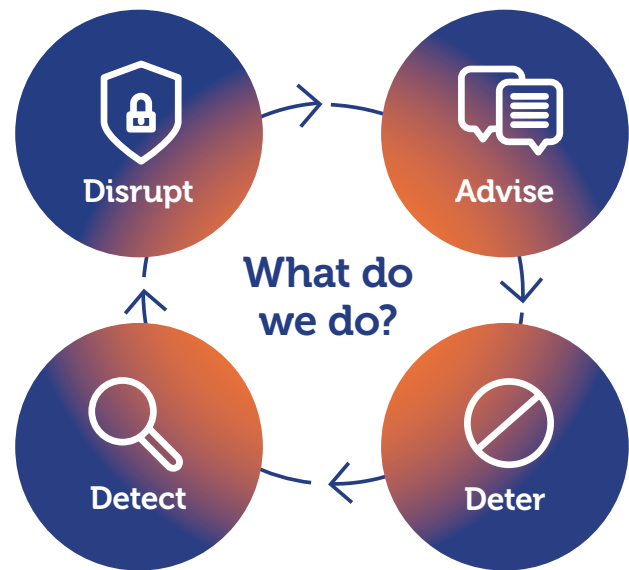
Disrupt

The NCSC disrupts malicious cyber activity from harming its customers' environments by blocking harmful activities through its active disruption capabilities. When required, our incident responders support customers to evict malicious cyber actors from their networks, and support the organisation/s through service restoration and recovery. This can involve on-site deployment.

Malware Free Networks
In November 2021, the NCSC launched its MFN capability. This cyber defence tool provides a cyber threat intelligence feed that contains indicators of malicious activity, generated from a range of sources. MFN is a malware detection and disruption service that enables us to significantly scale our cyber defence effort across a large range of Aotearoa New Zealand organisations.

We deliver MFN in partnership with internet service providers, managed service providers and cyber security service providers. MFN partners use our automated threat feed to detect and disrupt threats before they impact their customers' systems. They provide telemetry back to us, so we can understand the effectiveness of the MFN threat intelligence and gain greater understanding of the domestic cyber threat environment.

MFN now has 11 private sector partners who have live services utilising the MFN threat intelligence; a range of other organisations have enquired about becoming a partner.

As of 30 June 2022, MFN has now disrupted more than 120,000 threats. This figure reflects disruptions of potentially malicious activity with the potential to cause significant harm to Aotearoa New Zealand organisations.

Incident response services
Despite the cyber resilience-raising activity undertaken by the NCSC to prevent Aotearoa New Zealand

organisations being compromised, malicious cyber actors continue to find new ways to gain access to systems. Speed of response is critical to limiting damage to a victim's network and supporting its recovery. We provide a 24/7 incident coordination and response function to assist organisations respond to and recover from potentially high-impact cyber security incidents.

In the event of an incident, we will triage the incident, engage with the victim in order to understand the extent of the activity, and then support the victim throughout the incident's lifecycle. Our support – which supplements inputs from commercial providers – can include on-site incident response, forensic analysis, threat intelligence, and communications advice and guidance. For significant incidents, we work within the National Security System to ensure a coordinated, all-of-government approach to supporting the incident response.
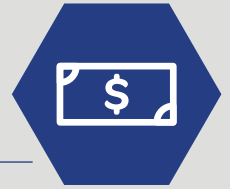
What's the harm?

In 2021/2022, detection and disruption activities undertaken by the NCSC prevented an estimated NZ$33 million of harm to Aotearoa New Zealand's nationally significant organisations. This figure reflects incidents where NCSC engagements protected nationally significant networks from imminent threats, or where our response prevented or reduced the harm caused by targeted attempts to compromise customer organisations.

The potential factors affecting the difference from 2020/2021's NZ$119 million dollar harm reduction calculation are myriad. The decrease may reflect our focus on the potential impact of cyber activity as a consequence of Russia's invasion of Ukraine despite no recorded direct cyber impact to Aotearoa New Zealand networks associated with the invasion. Equally, we recorded a decrease in cyber security incidents classified as highly significant, significant, and routine incidents compared with last year. Another potential contributing factor is the difference in victim organisations, and the varying criticality of their roles and services.

In 2016, the NCSC commissioned independent research to devise a model that could measure the benefits provided by our interventions. The model was reviewed and updated in 2020 to ensure it better reflects international studies about the average cost of cyber security incidents to specific sectors. The pre-emptive and preventive nature of our MFN capability means the impact of MFN generally occurs at a point before its value is able to be reflected in this calculation. However, there were several instances in the 2021/2022 year where activity detected by the MFN capability was significant enough to become an incident. Those incidents are reflected in this calculation.

The model factors in important impacts such as losses caused by intellectual property theft, including copyright and patent infringement. While assigning a dollar value to harm prevention can provide a useful benchmark, many of the impacts of cyber harm are intangible. Loss of public confidence and trust, reduced health and wellbeing, and hesitance to adopt new technologies can all eventuate when cyber resilience is low.

Advise

As trusted, independent advisors, the NCSC reduces the costs of cyber security issues and improves Aotearoa New Zealand's information security maturity by equipping our customers with actionable advice. We assess the cyber threat environment and drive evidence-based decisions by providing cyber threat advice that guides our customers to protect their valuable information, prepare for suspicious activity, and manage risks. We also work to help inform the information security standards for the public sector, and to ensure guidance and advice drives changes in the public sector.

Advisories and alerts
The NCSC supports Aotearoa New Zealand organisations to respond to changes in the cyber and technology threat landscapes by publishing a range of security advisories and alerts about potential or current threats.

Security advisories for our customers share information about specific vulnerabilities or types of malicious cyber activity seen targeting Aotearoa New Zealand networks. They may incorporate technical indicators of compromise and mitigation advice security teams can use to strengthen their defences. In the 2021/2022 year, we disseminated 16 NCSC security advisories and seven international partner security advisories.

We also contributed to, and co-badged, the publication of five security advisories with our international partners. The advisories provided guidance about: Russian state-sponsored and criminal cyber threats to critical infrastructure; top routinely exploited vulnerabilities; protecting against cyber threats to managed service providers; weak security controls and practices routinely exploited for initial access; and PowerShell security measures.

We have a formal process for assessing and triaging CVEs based on their perceived impact to Aotearoa New Zealand. Where a vulnerability may impact Aotearoa New Zealand, we take a number of actions, one of which is to alert nationally significant organisations. In the 2021/2022 year, we disseminated seven critical vulnerability alerts to our customers, highlighting nine critical CVEs. Although NCSC alerts are not a replacement for organisations' internal vulnerability monitoring, they reinforce existing decisions and support out-of-cycle patching and changes where the vulnerability may have a business impact.

The Government Chief Information Security Officer
The Director-General of the GCSB holds the role of the Government Chief Information Security Officer (GCISO), and is responsible for providing a single source of leadership and investment advice about information security risks across the public sector. The GCISO is able to draw on the unique insights and observations from the GCSB, particularly the NCSC, to help inform the public sector about risks associated with emerging technology.

Recent Cabinet papers now support a mandate that includes visibility of public sector investments in cyber security alongside the data and digital system leads. Working with the other system leads, advice can be provided both to agencies and the Treasury to ensure cyber security risks are addressed.

To support the GCISO, a Deputy Government Chief Information Security Officer (Deputy GCISO) role has been established to carry out day-to-day activities and to help direct strategies and objectives. The key focus of the Deputy GCISO is to engage across the public sector on information security matters, and to ensure guidance and advice drives changes in the public sector.

The GCISO leverages the technical capabilities of the NCSC, identifies efficient solutions to common security challenges, ensures effective policy settings are in place across the public sector, supports national incident response efforts, and provides system-level information, security policy, strategic advice and support across government organisations.

The GCISO's efforts are focused on supporting the secure digital transformation of the public service. In addition, it is responsible for identifying systemic risks and vulnerabilities; for co-ordinating the Government's approach to information security; and for establishing minimum information security standards and expectations.

This includes establishing the Aotearoa New Zealand Government information security standards and guidance, as set out in the New Zealand Information Security Manual (NZISM). The GCISO utilises the specialised knowledge of international best practice and Aotearoa New Zealand's threat landscape to help inform the information security standards for the public sector in a manner that is appropriate, responsive, and relevant.

The team responsible for the delivery of the NZISM has developed two major versions for release this year. Version 3.5 provided updated guidance for agencies using cloud services, and added zero trust concepts and terminology. Version 3.6 builds on the secure use of public cloud for government organisations (released in September 2022). This ties security standards back to the system-level work the GCISO carries out to support the secure digital transformation of the public service.

Baseline templates
The primary objective of the templates is to increase cyber resilience across Aotearoa New Zealand by helping public and private sector organisations better assess the compliance of their cloud environments against the NZISM controls. The templates make it easier for organisations to ensure the security of their cloud deployments.

The NZISM Baseline Security Templates provide a powerful demonstration of how the NCSC can leverage its information security expertise and knowledge of the domestic cyber landscape to work with global cloud service providers to improve the value of the services they offer to Aotearoa New Zealand public sector organisations. The collaboration with providers has enabled the GCSB to develop templates which are easy to deploy and cost-effective for organisations to implement and manage.

Success has been measured by the deployment of templates; so far, more than 415 templates have been deployed. As a tool, the templates are tangible and useful, helping government organisations address the hardest part of security by translating the 'what' into the 'how'. The templates provide government organisations with a solution for continuous assurance, and, ultimately, increase Aotearoa New Zealand's cyber security maturity. The templates will be regularly updated as the NZISM changes, offering up-to-date recommendations.

In November 2021, the GCSB won the award for the **best security project** at the annual iSANZ (information security) awards. The award recognised the GCSB's work developing the NZISM Baseline Security Templates in collaboration with Amazon Web Services (AWS) and Microsoft Azure cloud services. This latest award follows the GCSB's iSANZ win in 2018, when its CORTEX capability was named the 'best security project or initiative'.

Security Information Exchanges and cyber security exercises

Threat information and best practice guidance is also generated by public and private sector organisations, and the information security industry. The NCSC facilitates information sharing among organisations facing similar threats and challenges, especially where sharing requires a high level of trust. This primarily takes place through Security Information Exchanges (SIEs) focused on critical infrastructure. In the 2021/2022 year, we co-chaired 27 SIEs across the following six sectors: critical infrastructure, finance, government, network-provider, university, and transport and logistics.

The NCSC also facilitated the National Cyber Security Exercise. The focus of the national exercise was testing Aotearoa New Zealand's Cyber Security Emergency Response Plan (CSERP), and verifying it is fit for purpose. While the NCSC led the national exercise, it included an interagency steering group and participants from various government organisations. The NCSC also supported GridEx, an industry-led exercise. This provided lessons for the National Cyber Security Exercise, as well as an opportunity for industry to engage directly with government and gain a clearer understanding of government response processes.

Cyber Security Emergency Response Plan (CSERP)

CSERP sets the framework for the Government's response to a cyber security emergency, and prescribes the NCSC as the lead agency in Aotearoa New Zealand for incidents categorised as cyber emergencies.

Have I Been Pwned

In early 2022, the NCSC announced its partnership with Have I Been Pwned (HIBP). HIBP is an online resource that compiles open-source information about data breaches into a searchable database. The service is being used to understand potential vulnerabilities within public sector organisations and to enable better protection against incidents that leverage credential-based targeting.

A pilot has been successfully delivered to 15 organisations and has provided insights into their existing cyber security practices through data analytics, trend reporting, and tailored guidance. Insights from HIBP data analysis and organisations' engagement is also being used to improve the NCSC's approach to public sector resilience uplift, policy and guidance.

By proactively engaging with organisations and helping to identify potential vulnerabilities, we aim to collectively uplift the cyber security resilience of Aotearoa New Zealand.

Deter

The NCSC raises the cost of targeting Aotearoa New Zealand networks and deters adversaries by providing world-leading information security services to customers. This, in turn, makes it more difficult for malicious cyber actors to target our customers. This includes work such as: securing our customers' sensitive information; public attribution; supporting robust technology investment across Aotearoa New Zealand's critical systems; and supporting the secure provision of telecommunications services.

Regulatory functions

Aotearoa New Zealand's telecommunications networks are a core part of Aotearoa New Zealand's critical national infrastructure. Organisations and individuals rely on network providers for safe and secure access to digital capabilities, and the secure provision of telecommunications services.

The purpose of the Telecommunications (Interception Capability and Security) Act 2013 (TICSA) in relation to network security is to prevent, mitigate, or remove security risks arising from the design, build, and operation of public telecommunications networks, or from the interconnection of public telecommunications networks to networks in Aotearoa New Zealand or overseas. Part 3 of TICSA establishes a framework under which telecommunications network operators are required to engage with the GCSB, via the NCSC, about network changes or developments that intersect with national security. Many of these changes are currently driven by cloud adoption, increased demand for remote working, the rollout and expanded capacity of fibre optic cabling, and the transition to 5G services.

In the 2021/2022 year, the GCSB received 179 notifications for assessment of network changes. A significant number of these related to the continued rollout of 5G, the diversification of market offerings, international capacity increases, and hardware lifecycle upgrades.

The GCSB's other regulatory mandates are derived from the Outer Space and High-altitude Activities Act 2017 (OSHAA), the Overseas Investment Amendment Act 2021 (OIAA), and the Radiocommunications Act 1989, which is administered by the Radio Spectrum Management (RSM) team at the Ministry of Business, Innovation and Employment (MBIE). Under both OSHAA and RSM, the NCSC and GCSB assist NZSIS and other organisations in assessing space activities, high-altitude activities, and radio communications for national security risks. In the 2021/2022 year, the GCSB conducted 19 assessments of regulated space activities and 55 assessments of regulated radio spectrum activities.

The GCSB's growing regulatory role also includes supporting the NZSIS to provide advice to the Overseas Investment Office about national security risks associated with proposed overseas investment. In 2021/2022, the NCSC conducted 42 assessments under the national security and public order notifications regime of the OIAA.

Technical counter surveillance

The NCSC's Technical Counter-Surveillance Unit (TCU) helps ensure the Government's most sensitive communications are not intercepted or compromised.

The TCU provides a number of services to government, including technical surveillance counter-measure inspections, emanations testing and inspections, and advice about the standards required for sensitive compartmented information (SCI) site and system accreditation. The TCU provides recommendations to the Director-General of the GCSB about the accreditation of SCI sites and systems. The Director-General of the GCSB is the Government's accreditation authority for highly classified information systems and sites.

The GCSB provides technical inspection services and advice, and seeks to ensure these facilities are free from vulnerabilities that would allow unauthorised access to information.

Who the NCSC works with

We work with a number of partner organisations to build a cohesive line of cyber defence.

Our primary international relationships are with the cyber security components of the Australian Signals Directorate (ASD), the Canadian Security Establishment (CSE), the United Kingdom's Government Communications Headquarters (GCHQ), and the National Security Agency (NSA) and the Department of Homeland Security (DHS) in the United States. Respectively, their cyber security components include the Australian Cyber Security Centre (ACSC), the Canadian Centre for Cyber Security (CCCS), the United Kingdom's National Cyber Security Centre (UK NCSC), and NSA Cybersecurity and the Cybersecurity and Infrastructure Security Agency (CISA).

Domestically, we work with CERT NZ, which provides general support to businesses, organisations, and individuals affected by cyber security incidents; government organisations involved in CSERP; and with New Zealand Police, which is responsible for investigating crimes that happen online. We also work closely with regulators and government advisors, including the MBIE, the Overseas Investment Office, the Department of International Affairs (DIA), and the National Cyber Policy Office (NCPO).

We also collaborate with the private sector, including suppliers to victim organisations to support service restoration. We work with global cloud service providers to enable them to build our cyber security standards into their cloud service products, making it easier for those standards to be applied. Through our MFN service, we partner with cyber security providers to make cyber threat intelligence available to help those providers defend their customer networks. (See 'Malware Free Networks')

Our work supports the Aotearoa New Zealand Government's wider digital and data goals. Our work contributes to some key strategies: the Digital Strategy for Aotearoa, the Strategy for a Digital Public Service, the Data Investment Plan and the National Cyber Security Strategy, led by colleagues in the DIA, MBIE, Statistics New Zealand, and the NCPO.

Privacy Act 2020

On 1 December 2020, Aotearoa New Zealand's Privacy Act 2020 came into force. Organisations that carry out business in Aotearoa New Zealand are bound by the Act regardless of where they are based. The law requires organisations that suffer a significant breach that either has caused or is likely to cause anyone serious harm to report that incident to the Privacy Commissioner.

When high-impact incidents prompt the NCSC's assistance, incident responders can provide the forensic support and expertise required to identify whether personal information has been leaked or stolen, and to what extent. In 2021/2022, five cyber security incidents prompted our assistance because they possibly involved a breach of privacy.

Personal information is information about an identifiable individual. The purpose of the Privacy Act 2020 is to promote and protect individual privacy.

CONCLUSION

Whakakapi

In the context of increasing geostrategic competition, the domestic and international cyber threat landscapes are entering a new era.

Against the backdrop of pressures from Russia's invasion of Ukraine, COVID-19, and rising inflation, networks around the world are increasingly vulnerable to malicious cyber activity. With mounting global reliance on complex shared systems for the delivery of services, malicious cyber actors will continue to find new ways to infiltrate weak supply chain access points.

Looking ahead to 2023 and beyond, Aotearoa New Zealand organisations must focus on education to better identify and appropriately respond to malicious cyber activity. Cyber security is a continuous improvement process, rather than an end goal. Good cyber security is not only about having the right technology; it is also about having the right processes in place to continuously improve network resilience, and to conduct regular training for staff. All the cyber security protections in the world will not prevent incidents caused by human error. Implementing zero trust architecture reduces risk across systems by eliminating implicit trust and requiring validation at every access point.

International cooperation is also more important than ever, as there is a realistic possibility geostrategic tensions will increase.

The NCSC is focused on building relationships in order to achieve greater national resilience. Of the 29 incidents the NCSC records each month on average, almost half are sourced from international and domestic partner reporting. This highlights the criticality of information sharing processes to our defence of domestic networks.

Aotearoa New Zealand organisations must remain alert to potential cyber threats in this geostrategic environment where states are increasingly targeting other states with cyber and kinetic operations. We will continue to work closely with our partners to contribute to international efforts to reinforce the importance of upholding the norms of acceptable behaviour in cyberspace.

Malicious cyber actors are becoming more persistent, more proficient at identifying vulnerabilities, and more capable of causing severe impact to service delivery and information security. In this ever-changing cyber landscape, we will continue to defend Aotearoa New Zealand's nationally significant organisations against malicious cyber threats in pursuit of our vision of a safer and more resilient digital world.

Getting in touch

If you have any questions about this report, please contact the communications team at the GCSB.

The resources and guides mentioned in this report can be found on the NCSC's website: **www.ncsc.govt.nz**

To report suspicious activity: If your organisation requires assistance, please complete the Cyber Security Incident 'Request for Assistance Form' (www.ncsc.govt.nz/incidents) You can speak with us directly, by calling (04) 498-7654. You can also contact us via email at incidents@ncsc.govt.nz.

For general enquiries, or to subscribe to NCSC vulnerability alerts: Please email info@ncsc.govt.nz.

GLOSSARY

Rarangi kupu

This glossary of terms is included to assist readers' understanding. It should not be interpreted as a comprehensive list of terms used by the NCSC to describe the cyber threat environment.

TERM / KUPU	DEFINITION / WHAKAMĀRAMATANGA
Advanced persistent threat (APT) / Tuma pakepake arā atu anō	A well-resourced, highly skilled cyber actor or group that has the time, resources, and operational capability for long-term intrusion campaigns. Their goal is typically to covertly compromise a target, and they will persist until they are successful. They are very capable of compromising secured networks using both publicly disclosed, as well as self-discovered vulnerabilities.
Cloud service / Ratonga kapua	Provides ubiquitous, convenient, on-demand access to shared pools of computing resources (such as servers, storage, or online applications).
Common vulnerabilities and exposures (CVE) / Whakaraeraetanga	A vulnerability is a weakness in software, hardware, or a network that can be exploited by an actor. The Common Vulnerabilities and Exposures (CVE) database is a publicly available register of known vulnerabilities, each assigned a unique identifier in the format of CVE-xxxx-yyyy.
Credentials / Whakatūturu pārongo	A user's authentication information used to verify identity – typically a password, token or certificate.
Cyberspace / Āteatāurungi	The global network of interdependent information technology infrastructures, telecommunication networks, and computer processing systems in which online communication takes place.
Cyber security / Whakahaumaru ā ipurangi	Measures to protect systems, data, and devices from unauthorised access, and ensuring the confidentiality, integrity, and availability of information.
Data breach / Raraunga wāwāhi	The intentional or unintentional release of sensitive or private information into an unsecure environment.
Denial of service (DoS) / Whakakore ratonga	An attempt to make an online service unavailable by overwhelming the service with more traffic than it can handle.
Disinformation / Ngā kōrero horihori	The deliberate, intentional spread of false and misleading information designed to achieve a strategic purpose.
Exfiltration / Tāhae	Where an actor has unauthorised access to private organisational data (for example, legitimate credentials or intellectual property), and copies it from a system.
Hybrid threat / Tuma momorua	A mix of military, non-military, covert and overt activities by state- and non-state-sponsored actors that occur below the line of conventional warfare.

TERM / KUPU	DEFINITION / WHAKAMĀRAMATANGA
Incident / Maiki	An occurrence or activity that appears to have degraded the confidentiality, integrity, or availability of a data system or network.
Malicious cyber actor / Nanakia tūkino mōhiohio	An individual or group of people who seek to exploit computer systems to steal, destroy, or degrade an organisation's information. Actors may be individual computer hackers, part of an organised criminal group, or state-sponsored.
Malware / Pūmanawa kino	Malicious software or code intended to have an adverse impact on organisations or individuals' data, such as viruses, Trojans, or worms.
Mitigation / Ārai mōrea	Steps that organisations and individuals can take to minimise and address cyber security risks.
Nationally significant organisation / Whakahaere hira ā-Motu	Organisations such as government agencies, key economic generators, niche exporters, research institutions and operators of critical national infrastructure. If these organisations were affected by a cyber security incident, the impact could lead to national-level harm.
Personal information / Ngā mōhiohio whaiaro	Information about an individual, including name, date of birth, biometric records, medical, educational, financial, and employment information.
Phishing / Hītinihanga	The use of fake, deceptive, or alluring messages to solicit a behaviour from the recipient – such as clicking a link or divulging personal information or credentials.
Public attribution / Whakahuatia whānuitia nō hea	A tool used by governments and private sector organisations to deliberately release information about the source of a cyber intrusion, primarily to uphold norms about what constitutes acceptable state behaviour in cyberspace.
Ransomware / Pūmanawa utu uruhi	A type of malware designed to disrupt the use of computer systems and files until a ransom is paid.
Supply chain compromise / Poke ara ratonga	A form of attack that targets software, hardware, or an IT service provider, where the ultimate aim is exploit downstream customers.
Virtual private server (VPS) / Tūmau tūmataiti mariko	A portion of a large physical server divided into virtual spaces available for temporary use.