The cybersecurity implications of the Russian invasion of Ukraine

Speech to the Wairarapa Branch of the New Zealand Institute of International Affairs – 19 May 2022

Tēnā koutou, good evening, and thank you for the opportunity to address the Wairarapa Branch of the New Zealand Institute of International Affairs.

I am Andrew Hampton – the Director-General of the Government Communications Security Bureau.

When I accepted this speaking opportunity I intended to talk to you more broadly about cyber security in Aotearoa New Zealand.

But in the intervening weeks there has been a seismic shift on the world stage that cannot be overlooked when speaking to an international affairs institute. Therefore, I intend to provide some reflections on the Russian invasion of Ukraine with a particular focus on the implications for global and domestic cyber security.

I will then sketch out the current cyber landscape more broadly as we see it, notwithstanding the added reverberations of the invasion we are currently witnessing in Europe. I will touch briefly at the end on how the Bureau's technical capabilities and its workforce are constantly evolving in response to ever-changing technology and the threatscape we face.

But first I will briefly describe the Bureau's role and function.

The Government Communications Security Bureau

By way of context, the GCSB is a signals intelligence agency and operates in accordance with the Intelligence and Security Act 2017 to "protect New Zealand as a free, open and democratic society".

The GCSB, along with the NZSIS and the National Security Group within the DPMC make up the New Zealand Intelligence Community (NZIC). The NZIC works alongside other agencies, such as New Zealand Defence Force, New Zealand Police, New Zealand Customs Service, Ministry of Foreign Affairs and Trade and Immigration New Zealand to contribute to New Zealand's national security and the wellbeing of New Zealanders.

The GCSB has two principal roles:

- gathering primarily foreign signals intelligence in accordance with Government priorities;
- and, through the National Cyber Security Centre (NCSC), provision of cyber security services to New Zealand organisations of national significance.

Russian invasion of Ukraine

On 18 February the GCSB issued an advisory to New Zealand's nationally significant organisations. Its headline, "Ready your cyber defences against the possibility of an increase in malicious activity".

At the time, grainy satellite images published across online news sites throughout the world displayed columns of Russian military units massing on the eastern Ukraine border. President Putin was telling the world this was a routine military exercise. Partner intelligence, much of which was being put in the public arena to an unprecedented extent, was saying something quite different; that a Russian invasion was a foregone conclusion.

About the same time the Foreign Affairs Ministry's consular division advised Kiwis in Ukraine to leave immediately and for other Kiwis to keep clear. The New Zealand government does not issue advisories like these lightly and would only do so with information that confidently supported it.

Six days later Russia commenced a military invasion upon its European neighbour, the scale of which had not been seen in the region in the 77 years since the conclusion of World War II.

Russia's approach to the invasion and the geopolitical implications

We are now 84 days on from the invasion and most observers would agree that Russia has failed to achieve its initial objectives - something that became evident in the opening days and weeks of the invasion. Moscow probably thought it could effect a regime change in Kyiv and degrade Ukrainian military capability with relative ease.

But it miscalculated.

It miscalculated the resolve of the Ukrainian people who have mobilised against the Russian military. It miscalculated Ukraine's military capability, and it underestimated the speed and cohesion of the global response, including tough sanctions and the supply of military as well as humanitarian support to Ukraine.

The global reaction has been swift and strong. Russia's economy including key commercial sectors and individuals and organisations associated with the regime have been subject to significant sanctions including from Aotearoa New Zealand. These sanctions will continue to bite as the Russian war chest is drained.

The United Nations and other multilateral bodies are standing together with a majority of the international community condemning the invasion, and many choosing to isolate Moscow – even if it comes at an economic cost for some states, for example the reduction or termination of Russian fossil fuel imports.

NATO is on the ascendance with Finland and Sweden now looking to join the 30-member military alliance, something that was unimaginable several months ago.

And other nations will be watching carefully at the fallout Russia is suffering. This conflict, and the reaction to it, has undoubtedly recalibrated long-term global foreign policies for a range of states.

The broader global economic implications are also beginning to be realised. Global food prices are rising and supply chains are disrupted. Russia and Ukraine are major exporters of grain to key markets in the Middle East and Africa, and the resulting food shortages could lead to regional instabilities.

While Europe is preparing to draw down the flow of Russian energy, the switch to green energy will not be an instant one and more Western fossil fuel energy infrastructure investment is likely in the shorter-term.

Information war and intelligence being made public

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. As Director-General of the GCSB it is in these domains where I am best placed to provide some insights.

There is a saying that the first casualty when war comes is truth – and for the people of Russia this is sadly the case. Moscow has attempted to fabricate stories about attacks on ethnic Russians in the Donbas, and more recently – for example – Western bio labs on Ukrainian territory. More generally, it has used disinformation to vigorously promote its rationale for its illegal and unprovoked invasion and its distorted view of how the conflict is progressing.

The Kremlin's use of disinformation appears to have, at least for now, convinced its primary audience – the people of Russia, who remain considerably pro-invasion. In the last few months we have seen a crackdown on independent Russian journalism and social media as the Kremlin firms up its control of the domestic information environment.

The GCSB, as a conduit of partner intelligence, continues to provide thousands of intelligence reports on the Russia-Ukraine crisis to New Zealand government customers through our Intelligence Customer Centre.

In the lead-up to, and the early stages of, the Russian invasion I would frequently walk across to the Beehive to brief Ministers and officials on the latest insights from intelligence. Within hours this intelligence would be declassified by partners and made public – something I have not seen before. As we all know the intelligence community is traditionally secretive. But these are extraordinary times.

As Director Bill Burns of the CIA, a key partner in the global intelligence community, said this month, the U.S. government has shared accurate and precise insights and information with its allies from the start. And the credibility of that shared intelligence has helped cement the solidarity of the global effort in support of Ukraine.

At President Biden's direction, the U.S. government has taken unprecedented steps to declassify intelligence and use it publicly to pre-empt the false narratives and false flag operations that Russia has used so often in the past.

And in Director Burns' words: "by being open with some of our secrets, we made it harder for Putin to obscure the truth of his unprovoked and vicious aggression. Those decisions can never be taken lightly, given the importance of protecting sources and methods, but in this case they have made a crucial contribution to a successful, whole-of-government strategy. They reflect the need for new thinking and new tactics, in this new and demanding era for intelligence."

I have no doubt the unprecedented public release of intelligence in this conflict, including its use as a diplomatic tool, will have significant and ongoing implications for the sharing and declassification of intelligence in other contexts.

So what have we seen on the cyber front?

In February we told operators of New Zealand critical infrastructure to prepare for potential cyber threats – including destructive malware, ransomware, distributed denial-of-service (DDoS) attacks and cyber espionage – amidst increasing geopolitical tensions in Europe.

Following the invasion some international media commentators expressed surprise that there hadn't been more noticeably disruptive Russian cyber activity. They suggested this may be because of disjointed Russian military planning or the fact that battleground warfare takes precedence over malicious cyber activity during wartime. It has also been suggested that the Ukrainians, with support from its partners, have been able to sustain a credible cyber defence.

The New Zealand government has publicly attributed a range of malicious cyber activity to the Russian state prior to the 24 February invasion, and indeed again in a release issued by Foreign Minister Nanaia Mahuta last week. Russia has form and capability in malicious cyber-attacks against other states. I will talk more about attribution shortly.

The GCSB has stood up a dedicated effort in response to the cyber threats arising from the Russian invasion, which is focussed on three areas: Sharing cyber threat intelligence with New Zealand organisations, using our technical cyber security capabilities to monitor New Zealand networks for malicious activity, and providing advice and guidance to our most important organisations to build continued resilience.

Let me touch on my three key observations in the cyber context spanning from this invasion.

- Firstly, 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.
- Secondly, the Russian cyber offensive's impact on the global cyber threatscape to date has also been of a lesser scale than some expected. It could be assumed Russia is being mindful not to miscalculate and escalate on the global cyber-front beyond

Ukraine, the same as it is on the battlefield. In equal measure the heightened cyber defensive posture of other nations is almost certainly successfully warding off attacks.

- And thirdly, on our domestic front we have not seen a significant change in the cyber landscape that can be associated with the conflict. We remain alert and there always remains the possibility things may change.

In saying that, of equal concern to a direct state-sponsored Russian cyber-attack on Aotearoa New Zealand is an indirect attack that affects a critical supply chain, or an opportunistic cyberattack by a criminal group, such as a ransomware attack. These actors may be either sympathetic to Russia or simply motivated by financial gain and are taking advantage of the global disruption.

What is Russia's cyber capability and what have they done?

Recently the GCSB along with our Five Eyes partners issued a joint advisory warning Russia's invasion of Ukraine could expose organisations both within and beyond the region to increased malicious cyber activity.

This activity – we warned – may occur as a response to the unprecedented economic costs imposed on Russia through sanctions as well as material support provided by other states.

Evolving intelligence indicates Russia is exploring options for cyberattacks. Recent state-sponsored cyber operations have included DDoS attacks, while previously Russian operations have included malware attacks against Ukrainian government critical infrastructure organisations.

Additionally, some cyber-crime groups have recently publicly pledged support for the Russian government. These groups have threatened to conduct retaliation attacks for perceived cyber offensives against the Russian government. Some have also threatened cyber operations against countries and organisations providing material support to Ukraine, while others have attacked Ukrainian websites, likely in support of the Russian military offensive.

Broadly speaking, the Five Eyes advisory warns Russian state-sponsored cyber actors have demonstrated capabilities to compromise IT networks; develop mechanisms to maintain long-term, persistent access to IT networks; exfiltrate sensitive data from IT and operational technology networks; and disrupt critical industrial control systems by deploying destructive malware.

And we don't just work with our international intelligence partners.

Several weeks ago Microsoft reported the cyber component of Russia's assault on Ukraine had been "destructive and relentless", and included at least six Russian advanced persistent threat actors carrying out attacks and espionage operations while Russian military forces attacked Ukraine by land, sea and air.

Microsoft also reported that groups aligned to Russian military intelligence (GRU) have unleashed cyber attacks on Ukrainian networks at a rate of two to three incidents a week,

which have permanently destroyed files in hundreds of systems since the eve of the invasion.

But there are widespread reports of a Ukrainian cyber response. For example, you may have seen media reporting saying pro-Ukraine cyber actors are collectively gathering behind a state-led "IT Army of Ukraine", which has claimed to have hit the websites of Russian banks, the Russian electricity grid and rail system, and multiple DDoS attacks.

As I have already noted, a greater Russian cyber offensive campaign may have been expected by some pundits and observers, but what we do know for sure is Russia is unpredictable. Things may change and we will need to remain alert to the potential of a spike in malicious Russian cyber activity affecting Aotearoa New Zealand, at any time.

Cyber security

I'm now going to move away from the Russian invasion of Ukraine and talk more generally about the Bureau's cyber security mission and outline the security environment we operate in.

In November the NCSC released its annual cyber threat report that showed there were 404 incidents affecting nationally significant organisations in the 2020/21 year. This represents a 15% increase on the previous year. This included high profile incidents impacting the Reserve Bank, Waikato DHB and NZX, all of which involved the NCSC providing incident response services.

All three of these incidents were rated as highly significant, and all attracted well-warranted public concern. The organisations themselves, or Ministers, spoke publicly about our involvement, but generally, to protect relationships of confidence and trust, the NCSC does not comment publicly on incidents, or victims of, malicious cyber activity.

Of the 404 incidents recorded last year, 28% showed links to suspected state-sponsored actors, while a similar proportion, 27%, were likely criminal and financially motivated.

The increasing sophistication of tools used by criminal actors means it is becoming much more difficult to distinguish between state and criminal actors, particularly in cases where we are able to intervene early. This situation is sometimes exacerbated with some states offering safe harbour to criminal organisations.

State-sponsored activity

While the past year has seen increasingly sophisticated and impactful incidents by criminal groups, malicious activity by state actors was a significant concern even prior to the Russian invasion.

For example, in the 2020/2021 year the New Zealand Government publicly attributed two malicious state-sponsored cyber campaigns, one Russian (compromise of the SolarWinds Orion platform) and the other to Chinese state actors (exploitation of a Microsoft Exchange vulnerability), based on technical assessments by GCSB and our international partners. I will return to these shortly.

In the last few years we have called out foreign states, including Russia, China and North Korea, on eight occasions for their malicious cyber activity. We are aware of other countries involved in state-sponsored cyber activity both internationally and on New Zealand networks. The examples I have referenced have gone through New Zealand's public attribution process.

Recently the Bureau has also provided classified briefings to the Government about state actors targeting several key governmental organisations and the role of the NCSC in identifying and evicting the attackers, and helping the victim agencies restore their systems.

A point I would make is state-sponsored activity is less likely to disrupt services and, indeed, sophisticated actors will go to great lengths to hide their activity from detection, while attempting to extract valuable data that may help in gaining a geostrategic or political advantage.

Criminal actors on the other hand seek to cause disruption and media coverage in order to pressure victims to pay a ransom.

The fact that we are also an intelligence agency is important in the context of cyber defence. It gives us access to technical capabilities, legal authorities and international cyber threat intelligence not available to other cyber security service providers.

Current cyber threat vectors

Three particular features of the current cyber threatscape that I want to highlight are the rise of ransomware, the mass exploitation of recently disclosed vulnerabilities, and supply chain compromises.

In recent years, sophisticated criminal actors have been shifting their ransomware targeting strategy towards higher-profile organisations that are more vulnerable to extortion. Malicious actors are putting considerable effort into researching the sensitivity of the data, operating environments, and financial information of their victims. Organisations holding particularly sensitive personal or commercial information are especially at risk.

This strategy is sometimes called "big game hunting".

One of the drivers of the growth in ransomware attacks is the relative ease that technically savvy cyber criminals - with access to the necessary funds, most likely in a crypto currency – can purchase ransomware-as-a-service tools off the Dark Web. Ransomware as a service enables a cyber-criminal or other malicious actor to purchase a ransomware kit and tools to manage it, with some even offering a service desk function, much like an organisations' own IT support.

Another driver of ransomware is availability of anonymous payment systems such as Bitcoin and the range of other crypto currencies. They make it extremely difficult even for international law enforcement agencies to "follow the money" to track down the people behind these attacks. In situations where ransoms are demanded, the GCSB advises against making payments – paying the ransom does not guarantee that data will not be exploited in the future, in fact it could just encourage them to come back again.

We are also seeing an increase in the speed and scale of scanning and mass exploitation of IT system vulnerabilities. Malicious actors, both state sponsored and criminal, are quickly taking advantage of newly discovered vulnerability by targeting every device and organisation that is potentially vulnerable to exploitation. They do this to establish a foothold into networks, and then selectively pick their targets for further compromise. A recent example of this was the targeting of Microsoft Exchange vulnerabilities which was publically attributed by the New Zealand Government and international partners to the Chinese state.

These days it is not sufficient to just ensure the cyber security resilience of your own organisation, you also need to consider how secure your supply chain is. A recent development in supply chain attacks has been compromising software updates as a means of establishing a presence in customer systems. The SolarWinds Orion platform exploitation, which Aotearoa New Zealand attributed to Russian state actors last year, is an example of this.

Outsourcing of technology services has been an increasing trend in recent years. When implemented effectively it can increase efficiencies and enable greater security, but it can also expose you to increased risk. Organisations need to keep in mind that while you can outsource the service, you are not outsourcing the risk. In fact you may just be increasing your potential attack surface by providing another vector for malicious actors to compromise an aspect of your operation.

What we are doing about it – cybersecurity

The GCSB, primarily through the NCSC, provides a broad range of services to New Zealand organisations of national significance, including malware detection and disruption, onsite incident response and communications support, and sharing of guidance and threat information to build cyber resilience.

We are also the security regulator for the telecommunications sector, we provide technology services to the 15 government agencies that operate at the Top Secret classification level, and I provide leadership and set standards for the broader public service as the Government Chief Information Security Officer.

Our analysis based on an independently devised model indicates the NCSC's cyber defence capabilities prevented an estimated $284 million in harm to New Zealand's nationally significant organisations since June 2016.

In December, the NCSC formally launched Malware Free Networks (or MFN) – a scaling up of cyber defence capabilities, which makes our cyber threat intelligence available to commercial cyber security providers to help defend their customers' networks. It has already disrupted hundreds of thousands of threats to New Zealand networks.

However, it has to be stressed that no single cyber security capability is a silver bullet. Nor are we the country's one-stop cyber security firewall.

We still need organisations to ensure they have effective cyber security governance, understand their critical systems and risks – particularly across their supply chain – and to have a plan for how they would respond to a cyber-security incident.

Working in partnership with organisations to help build their cyber resilience is therefore one of our key priorities. Cybersecurity has to be a team effort.

For example, we have recently worked with Microsoft and Amazon Web Services to deploy our government information security standards into cloud services baseline security templates. This means that organisations who use the templates automatically have the government's security controls built into their cloud infrastructure.

Signals intelligence mission

Let me now return to our other mission – the collection, assessment and reporting of intelligence. In the past year the GCSB provided signals intelligence to 19 government customer agencies, and their Ministers, on topics ranging from COVID-19 to climate change. While much of what we do in this area we tend to not talk about publicly, I can provide a high-level overview to give some idea of our work.

The GCSB's activities always need to be undertaken in accordance with the Government's National Security Intelligence Priorities, legislation, and New Zealand's human rights laws. We are also subject to robust oversight, including from the Inspector-General of Intelligence and Security and the Parliament's Intelligence and Security Committee.

A core part of our signals intelligence role centres on informing the Government of growing geostrategic pressures, including in our region, and the implications for Aotearoa New Zealand. Our intelligence on the ever-changing geostrategic landscape has helped shape national policy decisions across government and will continue to do so.

We work closely with our international partners, particularly the Five Eyes in this area.

As well as briefing government customers on intelligence regarding the Russia Ukraine conflict, we also provide intelligence support to New Zealand Defence Force operations, including last year's evacuations in Afghanistan.

The GCSB makes a unique and highly valued contribution to global counter-terrorism efforts, including contributing to the disruption of attack planning. As well as UN-designated terrorist entities, this work has focussed on identity motivated extremists.

And last year we saw one of the largest and most significant law enforcement disruptions in international organised crime – Operation VAN – which was in-part enabled through an FBI-developed encrypted communication app used by criminal networks throughout the world. The GCSB provided support to New Zealand Police during the course of Operation VAN.

Technology and evolving capability

A significant moment for the GCSB last year was the decision to retire the two satellite interception domes and dishes at Waihopai.

The two dishes were no longer operationally important, contributing less than 0.5% of our overall intelligence reporting by the time we decided to retire them. But it was significant from a public perspective as they were the most visible part of the New Zealand intelligence apparatus.

There have been huge technological advancements in the 33 years since the first dome was installed at Waihopai. The world is cabled up, there is ubiquitous encryption and we have seen the advent of this thing called the internet, which has changed almost every aspect of how everyone in society goes about their lives, within half a generation.

Technological acceleration represents a constant challenge, and as new communications technologies emerge, our intelligence community must be able to evolve capability quickly and seamlessly.

The Bureau's legislation enables us to intercept high frequency radio communications, seek assistance from telecommunications network operators and service providers, and of course receive intelligence from our international partners. Our legislation also allows us to access information infrastructures, which is more than just interception; "accessing information infrastructures" also allows us to retrieve digital information directly from where it is stored or processed. This type of activity is sometimes referred to as computer network exploitation, or CNE, but we prefer to use the term "accessing information infrastructures" in line with the wording in our legislation.

With perhaps the exception of our high-frequency radio interception at Tangimoana, our capabilities have well and truly moved on and today we do things a lot differently than what we did in when the first dish went up in 1989 – the age of landlines, VHS cassette players and fax machines.

Budget 2022

We are of course a public agency and our capability relies on the allocation of the public purse. Today was Budget Day and GCSB and NZSIS received a combined $72 million extra funding over the next four years on top of our baseline funding. This funding allocation will boost public sector cybersecurity, work on dealing with increased geostrategic competition in our region, and with NZSIS, our counter terrorism effort. NZSIS also received for their work on countering foreign interference in New Zealand.

Today's budget allocation continues investment by successive Governments since 2016 into the GCSB's capabilities. As I said earlier we are a technology-based organisation and successive investment has enabled new technology – most of our technical capabilities, or at least the details of them, need to be classified to be effective – but one I can tell you about is the recent upgrade of our cryptographic capability – a $440m Cryptographic Products Management Infrastructure project, which broadly speaking, encrypts Aotearoa New Zealand's most sensitive information.

Investment helps us equip and evolve our capabilities in the face of accelerating technology and growing geostrategic pressures, including in our region.

The people of the GCSB

Lastly I would like to touch upon the most important part of GCSB – our people.

The success of our missions doesn't just depend on our technical capability, the relationships we have with our international partners and the private sector, or the legislation and the social licence we operate within. It depends most on the expertise, professionalism and dedication of hard working staff at the Bureau.

A strong focus for me and for the organisation as a whole is ensuring we have a diverse workforce that reflects the community we serve, and a workplace that is inclusive, and which truly values the different perspectives that comes with this diversity.

This is fundamental to not only ensuring we bring to bear the broad range of perspectives on the problems we are seeking to solve, but that we can attract the best people from all parts of society to come and work for us.

It is also vital to public trust and confidence by providing assurance that, while we operate in secret, our people reflect the values and perspectives of contemporary Aotearoa New Zealand.

As we grow as an organisation, we are becoming more diverse and inclusive.

Over half our senior leaders are women. We have eliminated gender pay gaps for like-for-like roles and reduced the overall gender pay gap by over half in five years. We have also doubled in this period the proportion of our staff from ethnically diverse backgrounds.

And, along with the NZSIS we were the proud winners of the New Zealand Supreme Rainbow Excellence Award.

And that brings me to the end of my speech, thank you for listening, I am now very happy to take questions.