INSTITUTE OF INTELLIGENCE PROFESSIONALS 2024

Mihi

It's great to be able to join you today, and thank you for the invitation to speak.

Now, the invitation was actually important, because I'm not sure I would have gotten in the door without it. By which, I mean to say that my intelligence credentials are debatable. On the one hand I lead an intelligence agency, so that gives me something to talk about. On the other hand, I've never actually been an intelligence specialist. I've been a collector and a customer, but I've never had specific training.

I know that sounds disappointing. I did try to clarify my status. I went to that indispensable intelligence tool, Chat GPT, and typed in: "If I lead an intelligence organisation but I've never had training or experience as an intelligence professional, do I belong at a gathering of intelligence professionals?" The answer from Chat GPT said, "It's debatable." A disappointingly ambiguous answer. But perhaps not an unhelpful disclaimer ahead of my chat with you today.

The theme for this conference is Demystifying Intelligence. To demystify is to make clearer, easier to understand, to illustrate, to de-romanticise. To be frank with you, my first thought was: "Do we want to do that?" Our sources, our tools and our methods are extremely valuable. Maintaining a bit of mystery can be very useful. At Pipitea House we have an original German Enigma machine on display. Keeping a shroud of mystery around the decryption of Enigma communications helped the Allies to win the war. Every spy thriller ever has a mystery of some sort. Mystery can be good. I mean, where would our recruiting be without it?

I was already on strike one with Chat GPT, but I decided to give it a second chance. I typed in: "Give me a perspective on demystifying intelligence. In fact, I'm first up at a conference and the crowd is going to be tough. Try to make it humorous." Then as an afterthought (and thinking about the diverse minds that work in intelligence) I added, "Actually, make it poetic as well." After thinking for roughly two seconds, this is what it gave me:

In the world of deception, hidden and sly,
Where secrets are kept, and truth is a lie,
Intelligence seems so mysterious and grand,
So let's demystify, let's understand.

It's not all gadgets, and thrilling chases,
Or ticking bombs in exotic places.
Sometimes it's just a desk and a chair,
And Bob with his coffee, pulling out hair.

Bob sifts through data, in mountains so tall,
While hoping his network won't suddenly stall.
He dreams of explosions, and world-saving tricks,
But it's spreadsheets and data, and computer mouse clicks.

He loves all the movies, the glamorous scenes,
Of fast cars and gadgets, and stealth submarines.
"But real life is quieter," he's often heard to say,
"It's hours' worth of reading a desktop display."

So next time you think that intel's a thrill,
Remember poor Bob, and his big data hill.
Intelligence work, when demystified bare,
Is reading and coffee, year after year.

So another distressing answer from Chat GPT. If this was intelligence demystified, then I really was going to have a recruiting problem if this got out. Chat GPT's lame sense of humour also needs work.

I decided to look at things a different way. Just as we always expect leaders do, I decided to think about myself. How is it that I'm fortunate to lead an organisation that's in the strong position that it is now in 2024 – strong recruiting, talent and relationships, recent investment and growth, demand from customers. Some 12 years ago the GCSB was making the front pages for all the wrong reasons.

The answer in very large part is because of the careful and deliberate development of public trust and confidence – the growth of social license – over the years since then. From the Kitteridge report of 2013 to the Cullen-Reddy review of 2016, from the strengthened role of the Inspector General of Intelligence and Security (IGIS) to the new Intelligence and Security Act of 2017, to an increasing number of public speeches and appearances by successive director generals. Incrementally, the mission of the GCSB has been very deliberately demystified.

This strategy of transparency is ongoing, and even when on the many occasions complete transparency is not possible, the IGIS is there with an all access pass as the public's proxy. It is no longer possible for us to operate in spite of public trust and confidence – we can only truly succeed when we have it. And by succeed I mean secure the funding to be successful, secure the talent, secure the community and industry partnerships – to succeed at our mission. It is a journey, and the headlines are still sometimes inconvenient. But it's about the long game, not the short one.

Of course it's not only us. The NZSIS is taking a similar path of opening up where it's possible to. The Government for its part is now proactively publishing its National Security Intelligence Priorities. In 2023 we had a National Security Strategy published for the first time. Previously in New Zealand this was not a field for great sharing or proactive conversation.

So the need for public trust and confidence is paramount. But there are geostrategic benefits of transparency too. In the lead-up to the Russian invasion of Ukraine and immediately thereafter, highly classified intelligence was being declassified and published in the world's media, every day, at risk to sources it must be said.

Just as importantly, commercial providers added their own product into the open domain for all to see. This was incredibly useful for defeating Russian disinformation. It's impossible to claim on the international stage that Ukraine planted civilian bodies in the street when several different public imagery sources show the same bodies there two days earlier under Russian occupation. Putting Government and commercial intelligence into the public domain has really helped to galvanise a strong international response.

That's not to say the process is easy. Transparency comes with risks. But if we could build on this successful transparent verifiability into the future – for example into the less terrestrial and harder to visualise domains, such as Space and Cyber – it could be a shot in the arm for those in the international community struggling to shore up our rules-based international system. After all, it's the grey zone deniability that has such a corrosive effect on the will to take action.

How might this kind of shared transparency support collective South Pacific security in the future?

I'm getting a little ahead of myself. Bearing in mind Chat GPT's equivocal view of my credentials, let me slip back into the comfortable shoes of the enthusiastic amateur. I'll give you a sense for how I myself have found it useful to demystify intelligence. To oversimplify it to make it more chewable, leadable, maybe even investable.

About 10 years ago I was leading Defence Intelligence at the NZDF when it occurred to me that we were in the oil industry. And today I believe that in the NZIC we are in the oil industry, and you probably are too. Let me explain.

Intelligence is a product, a perishable consumable. It exists to help people make good decisions about things. Intelligence fuels decisions. Intelligence is fuel. Where does that fuel come from? In my line of business, a lot of it comes from offshore, from large oil producers who conduct their own oil exploration. In addition, we conduct a modest amount of drilling ourselves. We receive the offshore oil as well as our own drilled oil and we pass it onto our customers who need it to fuel their decisions.

That's the model, and you'll be aware of it. But here are a few observations. First of all, when you're significantly dependent on offshore oil sources, you have to take special care of the pipeline. When that breaks down, there's no oil. And in our business, that pipeline is kept open by two things: the first is investment in the technology of the pipeline; the second is trust, because without a strong foundation of trust, the pipe fractures and the oil is lost.

And just like the physical infrastructure, trust needs ongoing investment and maintenance too. We can't afford to take it for granted. You can't surge trust when you need it most – it has to be carefully built and maintained over time beforehand. Now, those gathered here come from all over the intelligence world, but I'm sure that nearly everyone will have some kind of pipeline.

My second observation is that, while we receive a lot of oil from offshore, and we drill for some oil ourselves, oil is not the same as fuel. Oil is a raw product, while fuel is a refined and processed product. It's processed fuel that fuels decision making, not unprocessed oil. Generally speaking, when I pass snippets of raw oil to my customers, they'll tolerate it for a while if they have to, especially if it's all we've got and it's needed immediately. But it's not well tolerated for any length of time and we should try not to feed it to them. Raw unprocessed oil makes my customers' decision engines run rough, and it slows them down.

So our oil business needs a good refinery. The place where raw unprocessed data oil is turned into high grade decision fuel. A number of you here today work in this kind of refinery, so you know how important that is.

My third observation is that we should never assume that the oil is free. In the NZIC's world, we are not charged by the barrel for it, but there is a modest expectation that since we are in a partnership, we will provide some reciprocal value in some way. We have some choice in what that looks like. In some cases we are sharing oil back in the opposite direction, which is an in-kind payment, or collaboratively working on shared problems. In other cases, simply using the oil to power good decisions that help to uphold a strong rules-based international system is a good value-add. Good partners are predictable, reliable and add value to each other.

I think I've probably just about exhausted the oil business metaphor. But – before I do move on, let me just make a couple more notes from my own experience – perhaps they'll sound familiar.

Firstly, I've noticed that my customers don't always know what kind of fuel is best for their decision engines to run on. It can be easy to assume the customer knows best, but it's just not always the case. If you agree, then this is really worth thinking about, because there are several transformational projects underway out there in the intelligence world to switch to self-service fuel pumps. Now I think that self-service pumps are actually great, and they definitely need to be part of the solution - but I doubt they can be the full solution.

Secondly, we've got to keep questioning the value of the fuel we are providing. Back when I was with Defence Intelligence, I recall one particular day providing a senior customer with their weekly intelligence fuel, only to be abruptly informed that he had in effect already gassed up with the same fuel earlier in the morning at the more convenient station around the corner – by which I mean that he had already read the same information in the open media that same day.

And so that leads to one final note regarding this whole fuel metaphor. The station around the corner is not our competition. In our business, there's room in the market and it's often mutually beneficial. If we think back to the real world operational examples I mentioned earlier, other commercial players add real value. We should from time to time think afresh about where we are best to focus our own scarce talent and resources – what our specific core business and value-add should be, and what is best done by others.

Right. Enough. Let's move on from the whole fuel thing.

A question: How do we know when we're doing a good job in the intelligence business? What measures should we use? That's not a rhetorical question – it's something I wrestle with all the time, and I'm often looking around to see who out there is leading the way in their thinking on this.

I provide intelligence to my customers so that they make better decisions. So the successful outcome of my intelligence is their informed decision. I could draw parallels with measuring fuel quality by the performance of the engine, but I've promised to move on from that whole thing. The point is it's very hard to try and measure the quality of someone else's decision – that's usually done years later by a historian.

In practise we use a range of measures that nibble around the core outcome: responsiveness, customer satisfaction, post-publication requests. So there's room to improve, and it's an important area to try to demystify. If the outcome can't be well measured, then the budget for the input will never be too little.

The sole measure of customer demand is not particularly great. If customer demand was a good measure, the iPad would never have been invented, because no-one knew they needed it. Conversely, good intelligence can sometimes be delivered to a somewhat Teflon coated customer – where the Teflon is a coating of cultural and environmental assumptions. Customers can be delivered good intelligence but still suffer strategic surprise. In that regard I think of New Zealand's lack of practical preparedness for WWII in comparison with other countries. Same bed time reading, different nightmares.

Which is perhaps a good segue to the strategic environment we find ourselves in today - consistently being described as deteriorating and fast-moving. This environment requires us to regularly reorient ourselves, as our assumptions of yesterday are often being superseded by changing realities the next day.

Assumptions of who supports whom, risk thresholds, the usefulness of international institutions, international legitimacy, timelines for disruptive technologies. A challenge for today's intelligence professional is to wake up each day to look at the data anew with fresh eyes. Perhaps not every day, but enough to stay one step ahead of the news.

As for the customers, in my line of business – national security – it's resilience that they are thinking about a lot. The resilience of our critical national infrastructure, the cyber resilience of New Zealand's information systems – to both the state and non-state actors who target us. Social and physical resilience of our communities. Resilience of our supply chains and economy in the event of conflict. Resilience of our relationships. And they want to know, with the limited funds available, where can they invest for best effect.

In this emerging environment, a push of relevant intelligence, or even a push-pull arrangement is probably not enough. In my view, the more successful – and useful – arrangement is probably going to be one in which there is space for verbal Q & A, for discussion of context, for exploring what-ifs. Perhaps you have this arrangement in place already. For others, perhaps that looks more like a finance business partner type arrangement. The right intelligence relationship with the customer is an assumption that could be useful to unpick.

Looking ahead, resilience is a theme that's going to recur, and not just for our customers. In the intelligence business we need to shore up our relationships and pipelines. Information security is something that requires constant attention. Our sources are often fragile, so that requires attention.

Perhaps most importantly though, we need to ensure our people foundation is strong. Naturally that means sufficient numbers, and I recognise that we're only recently arriving off the back of Covid staff migrations and recent agency restructures. Numbers certainly matter, but no one ever gets the numbers they want.

Just as important is the development of our intelligence professionals. In the NZIC we have fantastic people, and we're often thinking about how best to develop them further. How do we ensure we deliberately grow our future leaders, and what would that look like?

You will all have views on that. From my perspective, it's valuable to have intelligence professionals who have spent some time walking in their customers' shoes, so those kinds of growth or secondment opportunities are useful. For leadership roles, political nous and people skills are also going to be really important, so again that points to the need for some career fluidity and deliberate planning.

I'm particularly struck by the larger number of neuro-diverse people we have in our business, and the value they bring to our work. I'm aware of the risk that if we are not more deliberate about attracting and retaining that kind of talent, we may turn good people away at the door. I've recently had discussions with my overseas counterparts about how to normalise processes to ensure we attract and retain good neuro-diverse talent. This is a whole other topic for a meaty discussion some time.

Suffice to say that resilience in this changing environment is going to be important, and that includes our people.

So, in leaving you with that point, I'd like now to wrap up. How best to summarise my demystified musings this morning? I've already mentioned that I've struck out twice with Chat GPT for this conference. But I do believe in AI as a tool for the intelligence professional, so I thought I'd give it just one more chance. I asked Chat GPT for the most succinct way to summarise a theme like this. Rather surprisingly, one option it recommended was a haiku. So then – here goes:

Public trust is key
We're in the oil industry
Build more resilience

Thanks for listening and good luck with the rest of the conference.

//NCSC

Te Tira Tiaki
Government Communications Security Bureau

Event information & speaking notes

Date:	22/08/2024
Event:	NZ Institute of Intelligence Professionals Conference
Timing:	2pm – 3pm
Location:	Parliament's Grand Hall
Form of engagement	A panel session regarding engaging with the Public
Other participants	Global Risk Consultants Managing Director Chris Kumeroa s9(2)(a) of Te Whatu Ora

Overview:

A representative from the NCSC (Mike Jagusch) has been asked to be part of a panel session at the NZ Institute of Intelligence Professionals annual conference. This year's theme is Demystifying Intelligence - Mā te Mōhio o te Whakakitenga, Ka Mārama.

The panel session is focused on **engaging with the public** which Mike will present in his capacity of Director Mission Enablement. Director-General GCSB, Andrew Clark, is speaking earlier at the conference.

The other panellists for this session are:

- The Global Risk Consultant, Chris Kumeroa
- s9(2)(a) Chief Advisor Intelligence, National Public Health Service, te Whatu Ora
- Robynleigh Cowan-Emery, NZIC Māori Cultural Advisor

Points of contact:

s9(2)(a)	NZIIP Board (New Zealand Institute of Intelligence)	s9(2)(a)

Topics of discussion:

- Intelligence engagement with the public
    - What strategies do you use to communicate complex intelligence findings to the public in an understandable way?
    - Based on your experience, what methods of engagement would you say are the most effective within the public intelligence sector?
    - ***OR*** How would you best define 'effective public intelligence'?

Background information on topic

Public intelligence refers to the collective process of gathering, analysing and sharing information by engaging with the wider community, outside the traditional confines of government agencies. This approach especially ***challenges the notion that intelligence in an exclusive domain for government insiders,*** instead emphasizing that valuable insights can come from a wide range of sources. ***By engaging the public and promoting transparency, we can dispel misconceptions and build trust, making intelligence less about secrecy and more about shared knowledge and collective problem-solving.***

In keeping with the theme of today's conference, public intelligence is central to the idea of demystifying intelligence as it brings traditionally opaque processes of intelligence gathering and analysis into the open. By **involving public and non-governmental entities in the intelligence process**, it breaks down the barriers between official agencies and the broader community, making intelligence more accessible and understandable to the public.

Introduction

- Tēnā koe e te Rangatira (to the panel host) He uri tēnei nō Ngāti Maniapoto. Ko Mike Jagusch tōku ingoa.
- Tēnā koutou katoa (to the crowd). My name is Mike Jagusch and I'm the Director of Mission Enablement at the National Cyber Security Centre.

About the GCSB / NCSC

GCSB background (if needed - noting AC spoke earlier)

- As you will know, the GCSB is Aotearoa New Zealand's lead agency for signals intelligence (SIGINT), meaning we specialise in intelligence derived from electronic communications.
- The GCSB has two principal functions; we provide primarily foreign intelligence, in accordance with the Government's priorities, and secondly, where we come in at the National Cyber Security Centre – is to provide cyber security services to all New Zealanders.
- Our mission is to provide our customers with intelligence advantage and cyber resilience to successfully navigate an unpredictable world.

NCSC & integration

The National Cyber Security Centre (NCSC) is part of the GCSB. I understand you heard from our Director-General, Andrew Clark, earlier today so I'll trust that he has spoken about the mission of the GCSB overall. I will speak on the NCSC specifically, as a Directorate of the GCSB, and our focus and mission.

We strengthen New Zealand's cyber resilience.

Traditionally, we have worked across government and critical infrastructure organisations to ensure the data and online services that New Zealand relies on are protected against hazards and risks.

We also support the Director-General GCSB role as the Government Chief Information Security Officer, providing system stewardship of information security across government.

Some of you may be aware that last year the Government announced their decision to integrate CERT NZ and the NCSC, to create a single lead operational cyber security agency for New Zealand.

Through the integration with CERT NZ, we are now also responsible for providing cyber security advice and education to all New Zealanders and for delivering cyber security uplift in the Pacific. We also offer support to New Zealanders that have been the target of malicious cyber activity

This creates a similar cyber security agency structure to those operated by Australia, the UK and Canada – single agencies with a wide span of responsibilities and customers.

I think this integration decision is a great illustration of this kaupapa we are talking about today. The unique insights we have as an intelligence agency aren't for us – they are so New Zealanders can make the best decisions they can about their cyber-security.

Cyber security is a domain where the "bulk" happens outside of government – it's individuals, it's organisations, it's the cyber security industry.

We can't achieve our cyber security mission without working with others.

Shift in intel agencies being more forthcoming with information / 'public intelligence'

Some of you may have noticed in recent years there has been a shift in the intelligence agencies to be more forthcoming with information that may impact our nation's collective safety and security.

I reflect back when I started in NCSC, we were working 1-to-1 with organisations and often that was under non-disclosure agreements.

Now, we are running annual cyber awareness campaigns with ads/billboards/news interviews. We've come a long way. We also partner with private sector publicly to deliver some of our services.

Something we are continuously working on, particularly in the cyber security realm, is making our intelligence insights more accessible.

We do this most consistently through releasing cyber security vulnerability alerts, advisories with international partners on a range of issues and topics and hosting quarterly security information exchanges with trusted stakeholders.

Even more public, and a first for the NCSC, was our attribution of malicious state cyber activity to the PRC regarding an earlier intrusion into our Parliamentary IT systems. This involved, I'm sure some of you will have seen, a media conference with the Director-General, and our Deputy Director-General Cyber Security.

We are increasingly trying to share information about emerging threats and vulnerabilities as we know how important these insights are for a range of our stakeholders. Cyber security is hard – so people want to know where to focus.

In saying this, there will always be a large secret component to our work. That is important to protect our sources and methods, but there is a lot of information we can get out there and we are constantly challenging ourselves and our mindsets around what might be possible in the public intelligence space.

Q: What strategies do you use to communicate complex intelligence findings to the public in an understandable way?

Firstly, I think it's on us as cyber security professionals to challenge the notion that what we do is "complex". We have a range of audiences that we communicate with ranging from Chief Executives and Boards of nationally significant organisations and Info Sec leaders to everyday New Zealanders.

If we aren't communicating in a way that works, then we aren't doing our jobs.

An anecdote I often share – if I think about my mum, as soon as I talk about cyber security she will say "oh that's too technical". But if I ask her why the All Blacks lost the 2007 rugby world cup quarter final, she will explain to me the complex physics and velocity about what makes a forward pass.

Rugby rules are complex too – but she cares enough, and is interested enough, to dedicate time to learning it.

So, I think a big challenge is how we make cyber security feel interesting and important to New Zealanders and New Zealand organisations – which is getting better!

We always encourage cyber security teams to talk to their decision-makers in a way that aligns with other business processes. Boards understand risk, so talk about cyber security in risk to business and use the same tools/templates as other risk management parts of the organisations so decision-makers are familiar with the frameworks.

Also something about sharing in a way that suits customers

For big, technically capable, audiences we have a service called MFN. MFN is a threat detection and disruption service that provides near real-time threat intelligence reflecting current malicious activity targeting New Zealand organisations. It is designed to strengthen New Zealand's cyber defence capabilities and brings our unique cyber security capabilities to a large number of nationally significant New Zealand organisations.

We identify New Zealand-specific threat information, or indicators, which are then disseminated in a structured and automate way to our partner organisations.

Our partners span the New Zealand telecommunications, managed service provider, and cyber security vendor markets. They then use this threat intelligence to detect and disrupt cyber threats to their respective customers.

This wouldn't work for others – so another important way we share our understanding of the cyber threat landscape with the public is by **publishing our intelligence and advice through products we call alerts and advisories.**

Alerts focus on urgent critical vulnerabilities in people's systems or networks, and advisories are longer form research products that will often contain descriptions of the tools, techniques and procedures being used by malicious cyber actors.

The objective for us in releasing these products to the public is to put as much knowledge about adversary capabilities into the hands of those that can disrupt the operations of those using them.

But these are still technical for every day New Zealanders so we also have social media accounts where we use more "human" communication tools and focus on a smaller set of practical tips. In these cases we are using words like "own your online" and have used other every day New Zealanders stories to give a message that resonates.

Q: Based on your experience, what methods of engagement would you say are the most effective within the public intelligence sector?

To go back to your definition of public intelligence, Emelye, that public intelligence is about "making intelligence more about shared knowledge and collective problem-solving." I think our most effective forms of engagement are when we approach it with that idea at the core.

In the cyber security realm of the NZIC I think we have found that relatively easier to do because at the end of the day, if we want to raise the cyber resilience of the nation and in turn protect our national security, we need New Zealanders on board and trust us and our work in collectively striving for a better outcome for New Zealand's cyber security posture.

SIE's I think these forums are an important way that the NCSC emphasises this idea of shared knowledge and collective problem-solving and most importantly that we're here to help and guide these organisations. Having this two-way communication forums to discuss key issues and topics are hugely valuable.

We have also had positive feedback about our public attribution earlier this year of malicious cyber activity by the PRC on Parliamentary systems. This again reiterates the idea of increasing transparency and building up that trust with the public through shared knowledge. Alongside this attribution, we released fact sheets and guidance alongside international partners to help our InfoSec community mitigate the threat of this actor – promoting the idea of collective problem solving

Q: [If needed] How would you best define 'effective public intelligence'?

I think effective public intelligence is communicating important intelligence insights in a timely way that is understandable and valuable to the receiver of that information.

Central to this however is building and maintaining effective relationships with those who are frequent receivers of information.

It needs to be two-way – we don't know everything, so getting insights about what is happening in reality is crucial for guiding our priorities.

For example, we facilitate 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) that are focused on specific aspects of Aotearoa New Zealand's critical infrastructure. SIEs are invitational trust groups for cyber security professionals in the energy, finance, government, network-provider, tertiary, and transport and logistics sectors.

These are really important forums for us to safely share intelligence insights in a Traffic Light Protocol (TLP) setting with originations that benefit from our information. These are also great forums to discuss any of our recent alerts and advisories and discuss these in more detail.

Reactive messaging (additional proposed questions)

How do public and community opinions influence your intelligence operations and how do you manage this dynamic?

Ultimately, we're a public service department, and our work is directly in service of New Zealand and New Zealanders. We need social licence to do our work, but often because of the nature of our role and operations, we can't be as transparent as we'd like.

We are always looking at how we balance national security considerations around classification with being as transparent as we can.

A recent example of this influence that I'm sure some of you may be aware of is our recent internal review to examine our procedures and practices when we receive reports of malicious cyber activity involving foreign state-sponsored actors targeting identified New Zealand individuals.

The review was prompted by concern at the NCSC's handling of reports of malicious cyber activity targeting IPAC members and identified several improvements to be made.

The review recommended that the NCSC's response to incidents needs to ensure it considers the wider implications of cyber security incidents, and not focus solely on the technical response to such incidents.

It also recommended that the NCSC consider engagement with individuals targeted by foreign state-sponsored actors.

Overall, we heard from stakeholders that some of our settings may not be quite right and from our internal review findings, have changed our settings accordingly.

How might we navigate the way in which the public is informed about intelligence efforts through the media?

I think this is something we will always have to navigate and experienced most recently with our public attribution of malicious cyber activity by the PRC in Parliamentary systems. The dynamics between wanting to be forthcoming and transparent with information whilst protecting our sources and methods will be something that will always be a consideration in terms of public intelligence.

The media conference we held regarding this attribution, although not having the ability to say a significant amount, we found that even being willing to front media and speak to the information we could share was received really well.

Again, going back to your comment Emelye regarding public intelligence building trust - we saw this as a good step towards building that trust with the media and promoting a new-sense of transparency that the media hadn't traditionally seen from the GCSB/NCSC.

What skills and experiences are most valuable for individuals seeking to work in the public intelligence sector and what advice would you give to someone interested in pursuing a career in public intelligence?

I look at this primary from my area of cyber security - My view is that we need to change some of the existing notions about what a cyber-security professional is. I don't see anyone in my office with a hood-up and the matrix screen playing in the background

Yes, some of the important roles are engineers, analysts, forensic responders, cyber security consultants.

But my team is made up of communications advisors, people who work on social media, policy advisors, strategy developers.

Cyber security – and intelligence more broadly – requires a range of skills to be effective, especially as it becomes more integrated with daily life and society.

I really encourage people not to be put off if you aren't a coder - is everyone in Ministry of Health a doctor?

In your opinion, how is emerging technology, such as AI and big data analytics, transforming the public intelligence sector?

The breadth of emerging technologies, their rapid pace of development, their disruptive and unpredictable impacts, as well as the lack of existing rules and norms governing their use, present a range of challenges.

Emerging technologies can be used to enable or commit harmful activity, such as foreign interference and espionage, violent extremism, and transnational organised crime, and may create disruptive social and economic changes that we must adapt to or overcome.

These technologies are likely to increase the problems caused by disinformation, including the emergence of synthetic media such as 'deepfakes' as well as machine learning and artificial intelligence.

From a Cyber Security perspective, we have been working closely with our Five Eye partners to better understand and mitigate the cyber security risks posed by AI systems.

AI systems are at-risk of being exploited by cyber-incidents as they are subject to new security weaknesses alongside traditional cyber security threats. AI can also be used by malicious cyber actors to increase their effectiveness of malicious activity, including using generative AI to craft convincing phishing emails.

Cyber security is an essential pre-condition for the safety of AI systems, and is required to ensure their resilience, privacy, fairness, reliability, and predictability.

We have released a few guidelines and publications alongside our international partners about developing Secure AI Systems. We released the first of their kind to be agreed globally in November last year – available on our website.

How do you envision the future of public intelligence?

For the NCSC, I envision this notion of public intelligence will become increasingly important in our work.

Following the CERT integration, we are needing to not only communicate the threats we are seeing to New Zealand's NSOs but also threats to individuals. This requires us to be collecting and analysing intelligence of a much broader cyber threat landscape and taking these insights to inform government, organisations, businesses and individuals.

As I've mentioned, engagement from our stakeholders and audiences is central to us making a difference and through public intelligence, we can help equip New Zealand and New Zealanders with what they need to protect themselves in an increasingly complex cyberspace.

Additional material

General public engagement/publications

Cyber smart week

Around half of all New Zealanders experience a cybercrime within a six-month period, ranging from scam phone calls and phishing to online shopping scams and extortion.

CERT NZ run an annual public awareness campaign regarding raising cyber security awareness.

This is an important way we engage the public to help raise the importance of cyber security and help New Zealanders to be more secure and resilient online.

This involves a significant amount of engagement and partnership with New Zealand businesses who partner with us to amplify the messaging with their customers and stakeholders.

Quarterly & annual reports

CERT NZ also publish quarterly insights reports that provide a snapshot of the types of cyber security threats and incidents that have been reported each quarter, and an update on our work to protect New Zealanders online.

The NCSC has traditionally in recent years also published an annual Cyber Threat report which reports on the domestic and international cyber threat landscape each financial year. These are an important way we use public intelligence to communicate the key threats and trends we are seeing in an unclassified form.