SPEECH

Director GCHQ's speech on global security amid war in Ukraine

Director GCHQ Sir Jeremy Fleming's full speech from the Australian National University (Thursday 31st March 2022)

Good morning and thank you Rory for the introduction.

And thanks to the National Security College for hosting this event in this fabulous building. I can't tell you how good it is to be back in Australia and especially, to see friends and colleagues here in Canberra.

Now, it's stating the obvious to point out that the World has changed since my last visit: the pandemic, the profile and dominance of technology and cyber, the role of China, the end of the Afghan campaign and now Putin's invasion of Ukraine.

Any one of these could be viewed as a historic shift. Taken together, they add up to a period of generational upheaval. The economic, societal and geo-political consequences are still playing out – and will do for decades to come.

And that's obviously the case in the world of National Security too. Here, the threats we face and our approaches to their mitigation are changing rapidly.

There's much talk of the need to design a new global security architecture. My contention is that it is already happening. It is already different.

And I know that you feel that here. This week's announcement of major increases in defence and intelligence spending shows that Australia gets this new reality.

So, I'm in Canberra to talk about these themes and to understand how you're thinking about the challenges we face.

But I'm also here because tomorrow marks the 75th anniversary of ASD. Their history is long and illustrious – they've played a major role in keeping Australia safe. I congratulate the generations who have delivered this critical mission.

I thank them for their partnership. For at times like this, it is more obvious than ever that we stay together. We owe the people of ASD a debt for their service and we are humbled in GCHQ to be able to count on their friendship.

I'm keen to leave plenty of time to chat with Rory and take your questions, so I'm going to press on with a few of the themes and have a stab at a some implications for our sovereign and allied response.

Firstly, the pandemic. Of course, we have a way to go until we declare it's over. The human costs are horrendous. But the amazing work of the scientists and medics leave us in a much better place. And the experience has helped us to learn some painful – and I believe useful - lessons about national security.

Perhaps most importantly, we now have a much better understanding of national resilience.

Before 2020, who here would have realised that the global supply chain for face masks would be such a critical dependency? Or that a grounding of a containership in the Suez would cause such chaos…? Or even, that semi-conductor availability would be so fragile it would affect everything from smart phone to washing machine availability…?

The pandemic has made clear that we are interconnected and dependent in ways we hadn't fully understood. We've had to wake up to the reality of what that means for our economies and our security.

And we've seen how vital technology is to stay connected, to keep our economies going and to change the way that we work…even in the national security community.

Yet it's also shown how vulnerable our nations are to cyber threats and how quickly our adversaries adapt to take advantage.

The lesson, for me, that our cyber security isn't good enough and we need to invest in making it better.

The second area I want to talk about is Russia's invasion of Ukraine.

Believe it or not, it's only 36 days since Vladimir Putin launched an unprovoked and premeditated attack on Ukraine. It's been shocking in every sense of the word. But it wasn't surprising. We've seen this strategy before. We saw the intelligence picture building. And we're now seeing Putin trying to follow through on his plan. But it is failing. And his Plan B has been more barbarity against civilians and cities.

Clearly, he plays by different moral and legal rules. Far too many Ukrainians and Russians have already lost their lives. And beyond this toll, many, many more have had their lives shattered. The UN estimate that in just over a month, more than ten million people have already fled their homes. It's a humanitarian crisis that need never have happened. And it's not over yet.

That said, it increasingly looks like Putin has massively misjudged the situation. It's clear he misjudged the resistance of the Ukrainian people. He underestimated the strength of the coalition his actions would galvanise. He under-played the economic consequences of the sanctions regime. He over-estimated the abilities of his military to secure a rapid victory. We've seen Russian soldiers – short of weapons and morale - refusing to carry out orders, sabotaging their own equipment and even accidentally shooting down their own aircraft.

And even though we believe Putin's advisers are afraid to tell him the truth, what's going on and the extent of these misjudgements must be crystal clear to the regime.

This week, the Russian MOD stated publicly that they will drastically reduce combat operations around Kyiv and a city in the North. It looked like they have been forced to make a significant change.. But then they proceeded to launch attacks in both of those places. Mixed messages or deliberate misinformation – we'll have to see how it unfolds.

It all adds up to the strategic miscalculation that our leaders warned Putin it would be. It's become his personal war, with the cost being paid by innocent people in

Ukraine and increasingly, by ordinary Russians too.

The great irony is, of course, that through his actions, Putin has brought upon himself exactly what he was trying to avoid – a Ukraine with a renewed sense of nationhood, a NATO that is more united than ever, and a global coalition of nations that condemn his actions.

Just over a month in, it is far too early to confidently draw out all the implications of this crisis. But I'm going to outline a few aspects that really stand out to me.

I'll start with the prominence of the information front.

Russia wrote the hybrid warfare book. State media, on-line media and agents of influence are all used to obfuscate motivations and justify military actions. We've seen them use this playbook in Syria and many other theatres. Their aim is to promulgate disinformation. To sow mistrust in the evidence and to amplify false narratives. It's also to make sure that the real picture of what's going on doesn't get exposed inside Russia.

And that's where the most dangerous disinformation war is being waged. We know Putin's campaign is beset by problems – low morale, logistical failures and high Russian casualty numbers. Their command and control is in chaos. We've seen Putin lie to his own people in an attempt to hide military incompetence.

And all of that means, he seeks brutal control of the media and access to the internet, he seeks the closing down of opposition voices, and he's making heavy investment in their propaganda and covert agencies.

But here again, it's clear that Putin has miscalculated. President Zelensky's information operation has shown itself to be extremely effective. It's agile, multi-platform, multi-media and extremely well-tailored to different audiences. One only has to look at the way Ukraine's flag - a field of sunflowers under a sky of blue – to see it flying everywhere, including outside GCHQ, to see how well the message has landed.

And it's a message supported by information campaigns all over the World. In the UK, it's focused in a new Government Information Cell which identifies and

counters Kremlin disinformation targeted at UK and international audiences. It brings together expertise from across government to challenge false narratives. It deals in facts, not falsehoods; making sure that the truth is told well.

And increasingly, many of those 'truths' come from intelligence. It is already a remarkable feature of this conflict just how much intelligence has been so quickly declassified to get ahead of Putin's actions.

From the warnings of the war. To the intelligence on false flag operations designed to provide a fake premise to the invasion. And more recently, to the Russian plans to falsely claim Ukrainian use of banned chemical weapons.

On this and many other subjects, deeply secret intelligence is being released to make sure the truth is heard. At this pace and scale, it really is unprecedented.

In my view, intelligence is only worth collecting if we use it, so I unreservedly welcome this development.

Of course, other aspects of this confrontation play out in cyber space.

There has been commentary expressing surprise that we haven't seen the Russians deploy a major cyber-attack as part of their campaign.

I think a lot of this misses the point. Whilst some people look for cyber 'Pearl Harbours', it was never our understanding that a catastrophic cyber-attack was central to Russian's use of offensive cyber or to their military doctrine. To think otherwise, misjudges how cyber has an effect in military campaigns.

That's not to say that we haven't seen cyber in this conflict. We have – and lots of it.

Through the National Cyber Security Centre, a part of GCHQ, we've seen sustained intent from Russia to disrupt Ukrainian government and military systems. We've seen what looks like some spill over of activity affecting surrounding countries. And we've certainly seen indications which suggests Russia's cyber actors are looking for targets in the countries that oppose their actions.

So just as we pay tribute to the Ukrainian military's brave actions, we should pay tribute to Ukrainian cyber security too. We and other allies will continue to support them in shoring up their defences. And at home, we are doing all we can to ensure sure that businesses and Government urgently follow through on plans to improve basic levels of cyber resilience. I know your ACSC is doing the same here in Australia.

Now my third observation of this conflict is the extent to which non-state actors are involved and have a say in its outcome.

Some of this is on the battlefields in Ukraine. It's clear Russia is using mercenaries and foreign fighters to augment its forces. This includes the Wagner group which has been active in Ukraine since Russia's illegal annexation of Crimea in 2014.

The group works as a shadow branch of the Russian military, providing implausible deniability for riskier operations.

Recently, we have seen that Wagner is looking to move up a gear. We understand that the group is now prepared to send large numbers of personnel into Ukraine to fight alongside Russians.

They are looking at relocating forces from other conflicts and recruiting new fighters to bolster numbers. These soldiers are likely to be used as cannon fodder to try to limit Russian military losses.

But it's not just in the military sphere that we see the influence and potential of other actors. We've seen cyber hacking and ransomware groups pledging allegiance to both sides. We've seen businesses all over the world distance themselves from the Russian economy. We've seen technology providers step up to make sure that Ukraine can stay connected, or to address disinformation.

It's all making the space very complicated, and in some ways, way beyond the control of Governments. It's another reminder of the interconnectedness of the World today. And as no single entity holds the whole solution, it highlights a need for global institutions effectively working in coalition.

Putin's aggression has certainly galvanised NATO. The war has triggered an unprecedented international response - 141 countries condemned it at the UN General Assembly. All over Europe countries are overturning decades long approaches to their defence policy; investing more too. And further afield, including in this region, countries like Australia and Japan are leaning in. It's also showing, in stark relief, those countries that choose to either support Putin or abstain from making a choice.

And those choices will affect the global order and our national securities for decades to come.

And of course, here in this region, the most concerning issues relate to the choices China makes as it thinks about its interests in the longer term.

Now, Russia's position on this is clear. It has made a strategic choice to align with China as China has become more powerful and in direct opposition to the United States. In the current crisis, Russia sees China as a supplier of weapons, as a provider of technology, a market for it's hydro-carbons and as a means to circumvent sanctions.

We know both Presidents Xi and Putin place great value on their personal relationships. But Xi's calculus is more nuanced. He's not publicly condemned the invasion, presumably calculating that it helps him oppose the US. And, with an eye on re-taking Taiwan, China doesn't want to do anything which may constrain its ability to move in the future.

It's also the case that China believes Russia will provide additional impetus and support to its digital markets and it's technology plans. We can see China is seizing the opportunity to purchase cheap hydro-carbons from Russia at the moment, to meet its needs too.

But there are risks to them both (and arguably more for China) in being too closely aligned. Russia understands that long term, China will become increasingly strong militarily and economically. Some of their interests conflict; Russia could be squeezed out of the equation.

And it is equally clear that a China that wants to set the rules of the road - the norms for a new global governance – is not well served by close alliance with a regime that wilfully and illegally ignores them all.

Now this comes into particularly sharp focus when we think about the future of technology eco-systems and the norms and governance that guide their use.

And for me, this as much about values as it is about technology. And both are vital to the competitive edge of a country.

That's why it's also increasingly the focus for geopolitical competition.

Historically, technology development was largely driven and owned by the West. Shared values amongst involved nations meant industry standards for emerging technologies tended to be global. Investment in technology brought status, wealth and security.

Today, we are in a different era. We can see that significant technology leadership is moving East. It's causing a conflict of interests. Of values. Where prosperity and security are at stake.

Now obviously, China is a sophisticated player in cyberspace. It has increasing ambition to project its influence beyond its borders and a proven interest in our commercial secrets.

It also has a competing vision for the future of cyberspace and it's increasingly influential in the debate around international rules and standards. China's bringing all elements of state power to control, influence design and dominate technology, if you like, the cyber and the fibre.

As I've said previously, without action it is increasingly apparent that the key technologies on which we all rely on for prosperity and security won't be shaped and controlled by the West in the future.

If we don't act – with our allies, with our partners and with the private sector – we will see undemocratic values as the default for vast swathes of future tech and

the standards that govern it. There is no doubt that democratic nations are facing a moment of reckoning.

Now these are all pretty big themes. And they have big stakes.

Whether we're building on the lessons from the pandemic, understanding the implications of Russia's invasion, or grappling with the implications of China's rise, it's clear that we must step up.

There are many ways for us to do that, but it seems to me that two things are very important.

The first is that we have to find new ways to collaborate and cooperate with partners. For those of us in National Security, that's about ensuring the health of existing relationships. It's about securing our alliances, like the Five Eyes, NATO and in this region, ASEAN. And it's about working with businesses in new and truly collaborative ways. And to do this we need to make sure that our counteroffer – to states who haven't yet decided which way they should jump – is persuasive and coherent. Too often it's not.

And the second is that in whatever we do, we must make sure that we stay true to our values, those that have made our systems and democracies so successful and will do so in the future too.

I spoke at the beginning about how against a backdrop of historic shifts, a new global security architecture was emerging. And all of this change will take decades to resolve. But what I can be clear on now is that how we approach these challenges will be as important as what our response is.

And all of us in this room today must play our part in following that through.

Thank you

PUBLISHED

31 March 2022

DATE OF SPEECH

31 March 2022

LOCATION

Australian National University