SECURITYSERVICE MI5

Joint address by MI5 and FBI Heads

MI5 Director General Ken McCallum and FBI Director Chris Wray have warned of the growing threat posed by the Chinese Communist Party to UK and US interests.

The two spoke to an audience of business and academic leaders at an unprecedented joint address at Thames House today.

The Director General said:

Welcome

Good afternoon everyone. Thank you for coming. It's a pleasure to welcome you all. I'm Ken McCallum, Director General of MI5; this is my friend and colleague Chris Wray, Director of the FBI.

Our two organisations, born within a year of each other more than a century ago, have long been closely partnered. The FBI office in London opened in 1942 and our teams work tirelessly together every day to keep our two nations, and our allies, safe. But today is the first time the Heads of the FBI and MI5 have shared a public platform.

We're doing so to send the clearest signal we can on a massive shared challenge: China.

We'll describe the challenge.

We'll talk about the whole-of-system response that we need: partnership not just between us, but with all of you, if we're to protect our economies, our institutions, our democratic values.

And we'll say what you can do, starting today, to protect yourselves.

I'll lead off; then hand over to Director Wray; then after a brief pause, we'll take questions together.

Introduction

In 2022, MI5 is having to stretch itself as never before – in multiple different directions. Front and centre of our minds is of course Ukraine where the human costs are horrifying. The long-term implications of Putin's actions are a subject for another day. But while our countries strain every sinew to support Ukraine in resisting appalling overt aggression, we're also working to safeguard our homelands from covert threats from the Kremlin.

Meanwhile, MI5's counter-terrorist work remains intense. Syria, Somalia and Afghanistan continue to generate threats. Our most immediate UK challenge is lone terrorists – Islamist extremist and right-wing extremist – radicalised online, acting at pace, in unpredictable ways.

Our subject for today lies right at the opposite end of the spectrum. Rather than lone actors, a coordinated campaign on a grand scale. Rather than lightning pace, a strategic contest across decades. Rather than the actions of volatile individuals, we see planned, professional activity:

The most game-changing challenge we face comes from the Chinese Communist Party. It's covertly applying pressure across the globe. This might feel abstract. But it's real and it's pressing. We need to talk about it. We need to act.

I want to be really clear up front on a couple of points:

- First, the aim here is not to cut off from China – one fifth of humanity, with immense talent. China is central to global issues: economic growth, public health, climate change. Having, for example, almost 150,000 Chinese students in the UK's universities is, in almost all cases, good for them and good for us. The UK wants to engage with China wherever it's consistent with our national security and our values. There are situations where the risks are sharper – and you'd expect the head of MI5 to focus on those. But even then, our aim is to make conscious choices on issues that are rarely binary. We want a UK which is both connected and resilient.
- My second point is we're talking today about the activities of the Chinese Communist Party and certain parts of the Chinese State [I'll mostly use the shorthand 'CCP']. We're not talking about Chinese people – in whom there is so much to admire. We wholeheartedly welcome the Chinese diaspora's hugely positive contribution to UK life. Responding confidently to specific covert activities is just us doing our job. If my remarks today elicit accusations of Sinophobia, from an authoritarian CCP, I trust you'll see the irony.

My main messages to you today are:

I. By volume, most of what is at risk from Chinese Communist Party aggression is not, so to speak, my stuff. It's yours. The world-leading expertise, technology, research and commercial advantage developed and held by people in this room, and others like you.

II. There is plenty you can do to protect yourself. Proportionately. Without making your organisation, your start-up or your university a fortress; while still engaging with the world, including China.

III. We're stronger together. The CCP adopts a whole-of-state approach in which businesses and individuals are forced by law to co-operate with the Party. In our free societies, we can do better. By building trusted partnerships – across our national systems, and, as symbolised today, internationally.

Risks To Your Business, Your Research, Your Future

Acquiring Advantage

Early in his time as leader, President Xi said that in areas of core technology where it would otherwise be impossible for China to catch up with the West by 2050, they "must research asymmetrical steps to catch up and overtake". The scale of ambition is huge. And it's not really a secret. Any number of public strategic plans, such as Made in China 2025, show the intent plainly.

This means standing on your shoulders to get ahead of you. It means that if you are involved in cutting-edge tech, AI, advanced research or product development, the chances are your know-how is of material interest to the CCP. And if you have, or are trying for, a presence in the Chinese market, you'll be subject to more attention than you might think. It's been described as "the biggest wealth transfer in human history". MI5 teams see the CCP working to extract UK advantage in multiple ways. To list a few:

- Covert Theft. Late last year Chinese intelligence officer SHU Yenjoon was convicted in a US court on charges of economic espionage and theft of trade secrets from the US aviation sector. SHU was active in Europe too: he'd been part of a prolific Ministry of State Security network targeting the aerospace sector. MI5 worked with those being targeted in the UK to mitigate the risks until the FBI action could solve the problem for both of us.

- Then there is Tech Transfer. Clandestine espionage methodology isn't always necessary. Take the tale of Smith's Harlow, a UK-based precision engineering firm. In 2017 Smith's Harlow entered into a deal with a Chinese firm, Futures Aerospace. The first of three agreed technology transfers saw Futures pay £3m for quality control procedures and training courses.

You know how this ends: after further sharing of valuable IP, Futures abandoned the deal. Smith's Harlow went into administration in 2020. As their Chairman put it: "They've taken what they wanted and now they've got it, they didn't need the shell of Smith's".

- Next, Exploiting Research. Both our countries have had to take action to stem CCP acquisition of cutting-edge national security advantage. In 2020 the US stopped issuing new visas in certain fields to researchers from People's Liberation Army universities. In the UK we've reformed the Academic Technology Approval Scheme to harden our defences, and we've seen over 50 PLA-linked students leave.

- Information Advantage. The CCP doesn't just use intelligence officers posing as diplomats in the classic fashion. Privileged information is gathered on multiple channels, in what is sometimes referred to as the 'thousand grains of sand' strategy.

In Germany a retired political scientist and his wife who together ran a foreign policy think tank passed information to the Chinese intelligence services for almost ten years.

In Estonia a NATO maritime scientist was convicted for passing information to his Chinese handlers, who claimed to be working for a think tank.

We issued a UK espionage alert on an individual working in think tanks and academia who was in regular contact with Chinese intelligence officers.

- Cultivating New Contacts. The deceptive use of professional networking sites is well known. Seemingly flattering approaches turn into something more insidious – and damaging.

In one example a British aviation expert received an approach online, ostensibly went through a recruitment process, and was offered an attractive employment opportunity. He travelled twice to China where he was wined and dined. He was then asked – and paid – for detailed technical information on military aircraft. The 'company' was actually run by Chinese intelligence officers. That's where we stepped in.

- And then there's Cyber. A wide range of government and commercial targets were attacked by the three so-called 'Advanced Persistent Threat' groups which the UK government has attributed to China's Ministry of State Security.

Over the last year the UK has shared intelligence with 37 countries to help defend against such espionage. In May we disrupted a sophisticated threat targeting critical aerospace companies.

I'll leave Chris to say more on cyber; his teams have led the way in taking the fight to those behind the keyboards.

These examples, from a far larger set, show some of how the CCP uses UK expertise to boost its success – at your cost. Security messages probably do seem repetitive, but we aren't crying wolf. We are seeing, cumulatively, the damage we had feared. And much of it is preventable damage.

Interference

Running alongside all this acquisition of advantage are sophisticated interference efforts. Normalising mass theft as "the cost of doing business these days". Seeking to bend our

economy, our society, our attitudes to suit the Chinese Communist Party's interests. To set standards and norms that would enable it to dominate the international order. This should make us sit up and notice.

The widespread Western assumption that growing prosperity within China and increasing connectivity with the West would automatically lead to greater political freedom has, I'm afraid, been shown to be plain wrong. But the Chinese Communist Party is interested in our democratic, media and legal systems. Not to emulate them, sadly, but to use them for its gain.

Obviously, much influencing activity is wholly legitimate: every country, every organisation, every business, wants to put its best face forward. The overt diplomatic activities of the Chinese Ministry of Foreign Affairs and attempts to grow China's 'soft power' are not where MI5 is focused.

Where we come in is unearthing, and seeking to neutralise, what we call interference activity – influencing that is clandestine, coercive or corruptive. Where the Chinese intelligence services, or bodies within the CCP itself – such as its United Front Work Department (UFWD) – are mounting patient, well-funded, deceptive campaigns to buy and exert influence.

Some of you will recall the Interference Alert issued earlier this year by MI5 to Parliament. This highlighted the risk posed by an individual connected to the UFWD, who had developed extensive links within Parliament. Through networks of this sort, the UFWD – described by Mao as one of the CCP's "magic weapons" – aims to amplify pro-CCP voices – and silence those that question the CCP's legitimacy or authority. This has very real consequences in communities here in the UK. It needs to be challenged.

We and our partners see growing indicators of the threat. In Australia, Senator Sam Dastyari resigned his position following allegations that he had taken money from a Chinese benefactor connected to the UFWD in return for advocating positions favourable to the CCP. Other 5EYES partners and European colleagues share concern about such interference. This requires a concerted response.

To quote some MI5 protective security advice:

"The motive behind Chinese intelligence service cultivation of Westerners is primarily to make "friends": once a "friendship" is formed [they] will use the

relationship to obtain information which is not legally or commercially available to China and to promote China's interest.

Cultivation of a contact of interest is likely to develop slowly: [they] are very patient. … The aim of these tactics is to create a debt of obligation on the part of the target, who will eventually find it difficult to refuse inevitable requests for favours in return."

That advice was produced in 1990. Three decades on, the internet allows for much greater scale – but the tactics are identical. One consequence of this subtle, patient approach is that many of those considered by the CCP to be helpful agents of influence in the West, are Westerners who may have no idea that that is how they are viewed.

The UK is a free country and people are free to hold whatever opinions they choose. But if their advocacy of CCP positions is a consequence of hidden manipulation, I would prefer for them – and us – to be conscious of that. And I would urge them to hold in mind that their reputations and advocacy are used by the CCP to whitewash its more egregious activities. A CCP repressing Uyghur Muslims in Xinjiang and pro-democracy protesters in Hong Kong. A CCP which recently declared a "friendship without limits" with Putin's Kremlin. And, as Director Wray will describe, a CCP that seeks to stifle criticism by coercing and repatriating Chinese nationals under what is known as Operation Foxhunt.

Building Our National Resilience, Together

One element is a stepped-up operational response from the security and intelligence Agencies, backed by government investment. MI5 has already more than doubled our previously-constrained effort against Chinese activity of concern. Today we're running seven times as many investigations as we were in 2018. We plan to grow as much again, while also maintaining significant effort against Russian and Iranian covert threats.

And it's not just about scale, it's about reach. Working hand-in-glove with international partners, sharing data in new ways and mounting joint operations make us much more than the sum of our parts. China is top of the 5EYES Heads' agenda, and our teams are working together closely on our shared priorities. We're doing likewise with our close European partners. These alliances will remain at the heart of our response.
But countering State Threats, whether from the CCP, Putin's Russia or Iran, also needs a profound whole-of-system response. Bringing together not just the national security community but counterparts in economic and social policy, in industry, in academia. Just

as we learned at pace how to join up across domains to contend with mass-casualty terrorist tactics, we're now progressively stepping up against State Threats:

- Since January the National Security & Investment Act has enhanced the government's powers to scrutinise investments and acquisitions, drawing on US experience across many years.

We're already seeing a steady flow of cases where critical national interests are engaged – whether that's technologies with military applications; advanced materials; or data and AI.

These require nuanced judgements that rely on expertise held in different places. It's not about choosing either prosperity or security, but instead focusing collectively on how they combine.

- The National Security Bill currently before Parliament will if passed be a long-needed and essential shift in powers to combat State threats. Threats not just to national secrets but to your intellectual property, your commercial edge, your unique research. It's right that Parliament draws new lines for the 21st century.

As well as updating the core espionage offences, the Bill seeks to tackle covert influencing in our democracy, and other forms of hidden interference. We and our policing colleagues badly need a full set of tools to protect the UK effectively against these very real threats. The Bill provides those tools.

But the right model can't be to scale the operational agencies to somehow take on all of this activity. As well as being unaffordable, that would be wildly disproportionate in a country where – unlike the CCP – we're here to protect democratic values and freedoms. In our view the most crucial improvement is to make the UK a harder target. We need to play the long game too.

What You Can Do To Protect Yourself

Since its earliest days, alongside MI5's secret responsibilities has sat a parallel responsibility for helping the UK reduce its vulnerability to attack – whether from sabotage in naval dockyards during World War I, or from hostile Foreign Direct Investment today. That protective responsibility sits with the Centre for the Protection of National Infrastructure, CPNI, accountable to me as Director General. Working in close partnership with the National Cyber Security Centre.

Over the last two decades, CPNI has played a central role as the UK has learned to protect itself from new forms of terrorism – responding resolutely, but not over-responding in ways which would do the terrorists' work for them.

Those same principles apply to the still-broader teamwork we now need to build resilience to State Threats. As today's session hopefully makes clear, critical national infrastructure is only one part of the picture: the contest now is much broader.

And so is our protective security response. Examples of CPNI campaigns, such as Trusted Research, Secure Innovation, and Protected Procurement are available here today and online. In May we released the Think Before You Link app – to help protect against the widespread deceptive exploitation of professional networking platforms. User reports from the app have already generated more than 100 new intelligence leads; a good example of the feedback loops we need.

Please take advantage of the advice that's available. No set of guidance can cater with precision for each and every situation: I'm afraid I can't make this simple for you. The answers have to lie in combining our unique knowledge of the threats, with your unique knowledge of your business.

So reach out to our advisers – through established channels if you have them, or through LinkedIn or the CPNI website. The teams are there to give you expert insights into the risks you face, and to work with you to make your organisation a hard nut to crack.

If you are worried about something that's happened, report it. Anything you tell us will be handled with discretion. Even better, of course, is to engage before you have a problem – mend the roof when the sun is shining, not when it's raining hard.

There's much more to do. CPNI's ambition is to reach ten times more organisations. As it grows its reach, it'll probably need a new name. More on that another day. But I want you to think about MI5 in 2022 as an organisation focussed as much on countering State Threats as on our still-vital role in countering terrorism. And an MI5 that's not just about running intelligence operations, but is working with you to help strengthen UK resilience in an increasingly contested world.

We see many examples of good practice. But as I wrap up, I'll leave you with some questions that I think deserve careful thought in every company; research institution; or

venture:

- Do you have a strategic approach to managing the risks I've described, and discuss those risks round your Board table? Or is it the subject you never quite get to?

- Do you have a thoughtful security culture at all levels in your organisation? Or does everyone leave it to a Security Department that's off to one side, only to be contacted in an emergency?

- Does your organisation know what its crown jewels are, which if stolen would compromise your future?

- Have you put in place the right controls to assess the risks attached to your funding sources and partnerships, and to protect your supply chain?

We know how hard you work to generate financial and intellectual capital. We want to help you to protect it, and to seize – safely – the many opportunities that are opening up. To be both connected and resilient.

I said that today was about sending the clearest signal yet about the risks posed by Chinese State action. Hostile activity is happening on UK soil right now. We don't need to build walls to shut ourselves off from the rest of the world. We do need to build our awareness - and make conscious choices to grow our resilience.

You - the UK's innovators and technologists, our researchers and scientists, our businesspeople - are one of the UK's greatest strengths. That's why you're being targeted. Let's not let your success be China's competitive advantage. Let's take on this challenge together. Thank you.

06 July 2022