Professor Danielle George CBE delivers RUSI's Prince Philip Lecture 2026 - full address

The as-delivered address as the Chief Scientific Adviser for National Security explores 'Science at the Heart of Society' to an audience of technology experts and RUSI members.

Delivered at RUSI, 61 Whitehall on Monday 20th July at 17:30 BST

'Science at the Heart of Security' - The 2026 Prince Philip Lecture

Lord Evans, my Lords, Excellencies, ladies and gentlemen — thank you. It is both a privilege and, I confess, a slightly surreal experience to be standing here at the oldest defence and security think tank in the world as someone who, not so very long ago, was turning the Shell Centre Building on the South Bank into a giant game of Tetris in order to convince a 10 year old how cool engineering is.

I hope you'll forgive me for starting there, but that 10-year-old and the thousands like her across the country embody the curiosity, the ambition and potential, that inspire me as a scientist and drives my work in this role.

Today, I would like to talk about three things: what it means to serve as Chief Scientific Adviser for National Security; why scientific advice on issues of national importance has never mattered more; and the critical role that our universities play in educating the scientists and engineers who will confront the security challenges and opportunities of the decades ahead.

So let me begin with the job.

A Chief Scientific Adviser provides scientific and technical advice to support their department's operations, strategy, and capability development, and as a member of the Government Chief Scientific Adviser's wider team, it carries responsibility for providing strategic scientific counsel on science and technology across the government more broadly.

So that's a slightly vanilla version of what a CSA does, Now take that role, multiply its complexity by a thousand, drape it in a cloak of secrecy and global geopolitical tension...and welcome to the demanding and exhilarating world of the Chief Scientific Adviser for National Security which provides science and technology advice to the UK Intelligence Community (UKIC), which consists of GCHQ, MI5 and MI6.

Now the scope is simply breathtaking. And thankfully! a National Security CSA isn't expected to be an expert in all fields of critical or emerging technology; here's the best part:

A CSA is only effective if they're surrounded by brilliant scientists. Their expertise, their curiosity and their way of seeing the world.

Scientific advice in national security isn't about telling decision-makers what to do; it's about ensuring that major decisions are informed by rigorous scientific and technical understanding. The role is to bridge technical possibility, and policy reality, bringing clarity, challenge and evidence to complex problems.

This is increasingly important because today's security threats are deeply technical. Advances in AI, quantum technologies, biotechnology, cyber capabilities, satellites, drones, advanced manufacturing - they are all reshaping both risks and opportunities. In this environment, decision-makers need access to the best available scientific advice, unfiltered, accurate and free from wishful thinking.

That requires intellectual rigour and honesty: recognising uncertainty where it exists, distinguishing evidence from assumption, and providing technically sound advice even when it challenges operational preferences. Maintaining that integrity is essential to effective decision-making in national security.

There were many differences as I made the move from academia to UKIC. I'm a Professor of Radio Frequency Engineering with a background in astrophysics. I've spent 26 years in academia doing research, teaching and leadership in the higher

education sector. Now, on the surface, these two worlds look like different planets. One is full of conferences, citations, theoretical debates. The other involves fast decisions, high stakes, and quite a lot of things you can't talk about over dinner. But once I found that you look closer, you realise they're not actually opposites—they're more like cousins who grew up in different households.

Both worlds are built on **curiosity** and **critical thinking**. Whether you're writing a journal article or a briefing for senior leaders, you're trying to understand a complicated problem and explain it clearly. Both rely on **expertise**. The deep knowledge you build in academia translates incredibly well into national security work.

And both value **collaboration**. In academia, it's co-authors and lab mates; in national security, it's analysts, policy folks, and subject-matter experts working on a shared mission. Either way, nobody succeeds alone.

The existence of a CSA for National Security reflects an important institutional commitment, it's a recognition that science is a core function for national security. And that the quality of scientific engagement with the intelligence community must be structured, accountable, and expert. And to do that well, as CSA I need one thing more than anything else: Scientists. Curious scientists.

We should all value scientists more than ever before, because the problems we face now are scientific at their core.

Without scientific insight, we misjudge risks. Without scientific creativity, we miss opportunities. Without scientific integrity, we make fragile decisions. Without scientific foresight, we get surprised by predictable futures.

The future of national security is scientific, technical, interdisciplinary, and deeply analytical. That's exactly where scientists thrive.

Scientists live in the messy middle where systems interact, variables change, and outcomes aren't always predictable.

National security needs people who can separate the signal from the noise, build models from imperfect information, make reasoned judgments under uncertainty.

Now, this isn't new, the intelligence services have always put science and technology at the forefront of their capability, just look at the work of the women and men at Bletchley Park who changed the arc of technological history and who altered the course of history with it. And in the past year I've seen first-hand how National Security values scientific perspectives, the mechanisms of thinking, their discipline, their creativity, and their courage to question assumptions.

So let me turn to the broader question — not the mechanics of the role itself, but the stakes.

We are living through a period of technological acceleration that has no historical precedent in its speed or its breadth. The industrial revolution transformed economies over generations. The digital revolution transformed them over decades. The changes we are now experiencing — in AI, biotechnology, quantum computing, quantum sensing, autonomous systems — they are unfolding over years and sometimes even months. And the national security implications are profound.

Take AI. UKIC has access to cutting edge models on our Top Secret systems. The integration of AI into defence and intelligence workflows is moving rapidly across every major state actor and there's a narrowing window for the UK and our allies to stay ahead.

Tech companies are releasing AI-driven innovations at a remarkable pace, with untold consequences, as algorithms are weaponised often just below that threshold of traditional warfare.

And we need to reimagine cyber security in the AI world. In the past few months, GCHQ has developed the blueprint for a new national cyber defence capability that will hardwire cutting-edge AI into machine speed cyber defence. The objective of the Government's Cyber Shield is to build a national-scale, collaborative approach to agentic cyber defence, using frontier AI to identify, reduce and resolve our national security cyber risks.

And as we draw upon decades of expertise in machine learning to reimagine cyber security, we're also embedding frontier AI deeper into our operations – responsibly and ethically – to enhance algorithms, translate foreign languages and find needles in haystacks faster than ever before. And all of this means the deployment of AI in national security requires people who understand how these systems work, where they break, and what the failure modes look like. It requires rigorous evaluation frameworks. It requires the confidence to challenge capability claims that are commercially motivated. That's scientific advice.

Or take biological threats. The scientific advisory infrastructure that governments need to respond to a crisis such as a pandemic has to be assembled, to a certain degree, on the fly. During the Covid-19 pandemic, SAGE did remarkable work under exceptionally difficult conditions. The pandemic also revealed what happened when scientific advice remains structurally peripheral to decision-making rather than embedded within it; when evidence is heard selectively, uncertainty is communicated poorly, and the gap between scientific understanding and public perception widens.

Now, consider that same challenge applied to a deliberately engineered biological agent, deployed by a hostile state or non-state actor, in a context where the very nature of the threat may be obscured. The demands on scientific advice — on its quality, its speed, its integration into operational response — would be orders of magnitude greater than anything we've experienced during the pandemic. And the margin for error would be correspondingly smaller.

And take quantum. In National Security, we're focused on harnessing all of this game-changing technology to drive rapid innovation alongside the exciting growth opportunity for quantum technology hardware companies in the UK.

Quantum sensing is here - our cutting-edge work with academia and industry is identifying the fingerprints of stealth. And once they're operational, quantum computers will be able to complete, in a matter of seconds, tasks that currently take years. That includes defeating the codes and the encryption that keeps our secrets safe today. So our scientists are working to protect critical systems from future quantum attacks, and sharing guidance with businesses to act now.

I raise these examples not to be alarmist, though the threats are real, but to make a specific point about what scientific advice enables. It enables proportionality. Without rigorous scientific understanding, we tend toward one of two failure modes: we either underestimate emerging threats because we don't understand them, or we overreact to them because we don't know their limits. Scientific advice is what allows decision-makers to be more accurate, to calibrate response to the actual nature and scale of the threat, rather than to hopes or fears.

But scientific advice isn't just about understanding threats; it's about building capability. The UK's security has long depended on scientific and engineering innovation. So, the real question is: what capabilities are **we all** investing in today that will deliver a sovereign advantage tomorrow, and are we doing enough to develop the people who will create them?

Which brings me to my third point.

I have spent most of my career at the University of Manchester, helping students grow into engineers and scientists who will sustain the UK's future technical strength. More than research breakthroughs or rankings, this, to me, is the most important contribution universities make.

Yet the link between education and national security is often overlooked. Developing a Radio Frequency engineer, cryptographer or specialist biologist takes many years. The expertise needed to address future security challenges can't be created at short notice.

The decisions we make about science and engineering education today will determine the UK's technical and national security implications in the 2030s and beyond. I'm not convinced we always make those decisions with that long-term perspective in view.

So let me be specific about what I think universities need to do — and what I think we need to do to support them.

Two things matter. First, universities must have the breadth alongside the technical depth. AI, quantum, biology and cyber challenges don't fit neatly within disciplinary boundaries, and specialists who lack exposure to operational, policy, ethical or security contexts may struggle to translate their expertise into that real-world impact. Universities should combine deep technical education with a broader understanding of how capability is applied, through deliberate curriculum design and strong partnerships with employers in the security community.

Second, engagement with national security should begin as early as possible. The National Cyber Security Centre's certified degrees in cyber security and closely related fields is a great example of sector-level engagement. But for many talented students, particularly those from underrepresented backgrounds, security careers can feel distant or inaccessible. Universities and the intelligence community should provide sustained, meaningful exposure to the people, the problems and purpose of national security work, helping a wider range of students see themselves as contributing to this mission.

When I was growing up nobody in my immediate world was a scientist. I was given a telescope when I was eight years old, and I became fascinated — I'd get up in the middle of the night to observe Saturn's rings or lunar eclipses. I was fortunate. I had a family who would get up with me and watch those eclipses and never say "I don't know "to my constant 'why questions', they'd say "let's find out together".

Not everyone has those nudges at the right moments. Part of the work of our education system, including our amazing universities is to create those moments more deliberately — to make the path visible to students who might not otherwise see it. And part of the work of the intelligence community is to make itself legible to those students — to show what careers in national security actually look like.

The relationship between university research and national security is essential but it does require careful balance. Universities must remain places of open inquiry, academic freedom, international collaboration and challenge, because these are the foundations of long-term scientific and technical strength. But, in research areas such as AI, quantum technologies, advanced materials and synthetic biology they also raise important questions about dual-use risk, governance and how discoveries relate to national capability.

Addressing these issues requires sustained collaboration between universities, government, industry and the intelligence community. Where engagement is weak, research can become disconnected from policy needs, capability gaps remain unaddressed, and valuable discoveries fail to translate into operational impact. A key priority for me in this role is strengthening the connections between academia and national security building the trust, relationships and shared understanding needed to ensure both sectors benefit from each other's expertise and insight.

The last thing I want to say about universities is about diversity. The threats we face are global, complex, and multifaceted. The intelligence community needs people who think differently — who have different cultural frameworks, different intellectual traditions, different ways of approaching problems. For UKIC, diversity is mission critical. We're working hard to address this because if our technical community is drawn from a narrow demographic, we will have systematic blind spots. We will ask the wrong questions. We'll miss things.

Universities are a major funnel through which the future security workforce passes. If universities are not themselves genuinely diverse — in the students they recruit, in the staff they hire, in the curricula they design — then that restriction will propagate into the national security community. And we will be poorer for it.

I was the 6th woman in 189 years to give the Royal Institution Christmas Lectures. The 2nd woman in 150 years to be the President of the Institute of Engineering and Technology. The first woman CSA for NS. We have the first female chiefs of GCHQ and MI6. We've come a long way but not far enough. And in national security, as in engineering more broadly, the representation gap is still significant.

Let me bring these threads together.

We're living through a period of profound technological change, where the security landscape is evolving faster than many of our institutions were designed to respond. In this environment, scientific and technological understanding is a strategic necessity.

That's why scientific advice must be at the heart of government decision-making. When it is embedded, independent and connected to the best expertise across the country, it improves policy, reduces risk and helps identify opportunities that might otherwise be missed. When it is ignored, marginalised or filtered, the consequences may be significant.

My role is to help ensure that science informs national security decisions in the right way. And that depends on a thriving scientific ecosystem: our universities, researchers, engineers and innovators, and a diverse pipeline of talent ready to meet the increasingly complex challenges and opportunities of the future.

That pipeline doesn't build itself. It requires investment: in STEM education from primary school through to postgraduate research. It requires deliberate engagement between government, the intelligence community, universities, and industry. It requires cultural change in who we invite to be engineers and scientists, and in how we make that invitation heard. And it requires a long-term view — an understanding that the capability decisions we make today will determine the security outcomes of the 2040s.

I said at the start of this talk that this role feels connected to a 10-year-old turning the Shell Centre Building on the South Bank into a giant game of Tetris who might, one day, choose engineering because someone showed them it was possible, and exciting, and theirs to claim. I mean that, not as sentiment, but as a strategy.

The national security challenges of the next 30 years will be solved by people who are, right now, in school classrooms and university lecture theatres and apprenticeship programmes and research labs. Our job — **the job of everyone in this room** — is to make sure that those people are equipped for what awaits them. That they're diverse enough to see the problems we might miss. That they're expert enough to understand the threats we've not yet imagined. That they're connected enough to the institutions of national security to know that their skills are needed, valued, and consequential.

I am deeply proud — to be a scientist working in national security.

Because every day, I see the difference scientific thinking makes.
Every day, I see how much stronger, smarter, and more resilient our agencies become when they listen to science.
And every day, I see the extraordinary scientists who step forward to serve — with intellect, with integrity, with imagination.

If we don't bring scientists into the room we are preparing for the wrong century.

So here's my 3 science take-homes:

Science gives us the knowledge to understand the world as it is and imagine the world as it could be.

Science creates understanding. Understanding drives innovation. And innovation changes the world.

Science is a deterrent to conflict, because knowledge, understanding and innovation are the foundations of security, resilience and peace.

Thank you.

PUBLISHED

20 July 2026