Innovation, Sovereignty and Collaboration:

Lessons for the Allied Defence Industrial Base

Delivered by Robin Ashby at a Manchester Metropolitan University Security & Technology Conference, 16 May 2026

Â

1. Introduction: Why This Matters — Now

You have gathered here to discuss emerging technologies, cybersecurity, AI and the future of security innovation.

I hope to offer something useful from the practitioner's side of that conversation — the messy, urgent, often frustrating reality of turning technological promise into deployed military capability.

The Roman military writer Vegetius wrote: 'Si vis pacem, para bellum' — if you want peace, prepare for war. He wrote that in the fourth century AD. Rarely has it been more relevant than today.

And there is a companion warning from the philosopher George Santayana, adopted by Churchill and many since: 'He who forgets history is doomed to repeat it.' This morning I intend to hold both of those thoughts together.

In 1941, Churchill told Roosevelt: 'Give us the tools and we will finish the job.' It is to industry — and to the innovation ecosystems that surround and supply it — that nations must now turn.

But the whole environment in which that industry operates is beset with structural problems that require urgent resolution.

My purpose today is to identify the most critical of them, illustrate them with historical and contemporary examples, and suggest what students, researchers, and institutions like yours have to contribute.

A former UK Foreign Secretary wrote recently of the conflicts in Ukraine and the Middle East that the science of war is progressing so rapidly — integrating data, AI and signals intelligence with drones and missiles to such devastating effect — that any major country needs to keep up.

Countries such as the UK, planning a slow build-up of defence, must act with more speed and innovation if they are to defend themselves against any future attack.

That is not hyperbole. It is a measured assessment from someone with full access to the intelligence picture.

The EU's Defence Commissioner Kubilius has been equally direct: by 2027, reconstituted Russian forces will be supported by a war-footing economy.

The Allied nations must have adapted their defence industrial base, acquisition models, and cooperation frameworks within that timeframe.

Last week, Sweden's Defence Chief, Michael Claesson, was asked when Russia might be able to test NATO's resolve with a sneak attack.

His answer was a single word: 'Now.'

I want to give that word some geography.

I wrote recently about the possibility of a Russian seizure of Svalbard — the Norwegian archipelago in the High Arctic.

It may sound like a cold land far away with a tiny population. Diplomatically it is complex — Russia has treaty rights there.

But Svalbard controls a narrow channel that keeps Russia's Northern Fleet from the North Atlantic in times of crisis.

Strategically, it is rather like the Straits of Hormuz. Seize it, and you change the naval balance at a stroke.

If that seizure were met with inaction — because it is distant, complicated, and involves few people — NATO's credibility would be destroyed. Perhaps fatally.

That is what 'Now' means in practice. Not an abstract threat. A concrete geography, a specific vulnerability, a decision that would have to be made in hours. And there are others, such as the Baltic.

The window for meaningful reform is not years away. It is now.

I will focus on three interlocking themes: the gap between innovation and deployment; public-private collaboration and the role of government as a monopoly customer; and the delicate but urgent challenge of intellectual property, sovereignty and Allied collaboration.

I will use UK examples — not because we are especially good, we are not — but because I know them best.

And I will try to draw out, at the end, what this means for the researchers and students in this room.

2. The Innovation Gap: From Idea to Battlefield

The pace problem

We are living through an era of exponential technological development — artificial intelligence, machine learning, quantum computing, hypersonics, autonomy, directed energy.

Our adversaries are embracing these technologies through calculated military-commercial alliances. They prototype and manufacture flexibly, adapting in months or weeks. And so does Ukraine, from whom we have a lot to learn.

By the time our traditional acquisition systems have completed their technical reviews, compliance processes and legacy approvals, the battlefield may have moved on entirely.

This is not a new problem. It is an old problem made newly lethal by the pace of change.

History is instructive — and I make no apology for reaching back to illustrate it, because those who forget history are indeed doomed to repeat it.

The Spitfire lesson

Consider the Spitfire. In 1938, only about 30 were operational. By Dunkirk, it was in squadron service. By the Battle of Britain, 2,000 had been built. Over the course of the war, more than 20,000 were produced.

Not only by Supermarine, but by subcontractors at Castle Bromwich and at 'shadow' sites where engineering firms pivoted from peacetime manufacturing to wartime production.

Twenty-four marks of Spitfire were introduced in six years, improving every element of capabilities. That is iterative development, rapid prototyping, and surge manufacturing — carried out under existential pressure, without a single PowerPoint slide or procurement framework document.

And then there is the Mosquito — my favourite example of institutional stupidity redeemed by individual and commercial courage.

The Air Ministry initially rejected development of the de Havilland Mosquito entirely.

Only after de Havilland built one in secret and demonstrated it in November 1940 did the Air Ministry draft a specification and place an order.

It was exactly what the country needed: metal and metal workers were in short supply. They were made largely of wood, built by furniture manufacturers and joiners who had never built an aircraft.

It entered production in mid-1941 and served until 1963. 7,783 were built across Britain, Canada and Australia. It was an exemplary fast precision bomber and night fighter.

The lesson is not just that innovation matters — it is that institutional resistance to innovation is a recurring feature of military procurement, and overcoming it requires both courage and bloody-mindedness.

There is a human story here too. The Air Transport Auxiliaries ferried aircraft to operational bases — including the ATA girls, women who had taught themselves to fly but were barred from the RAF.

They would collect an aircraft with only a few typed pages of notes covering single, twin and four-engine types, take off, and rely on their charm to beg lifts on motorbikes or in sports cars to the nearest railway station to get back to the factory. The flew up to 4 trips each day.

I met several of these formidable women in later years. They embodied exactly the agility, adaptability and improvisation that we need to recover today.

They did not wait for a framework. They just got on with it.

Ukraine: the lesson being written now

Fast-forward to today. The former Ukrainian Foreign Minister Dmytro Kuleba put it with striking clarity:

'Ukraine has compensated for its manpower shortage with innovation — robots on the ground and drones in the sky that now kill five Russian soldiers for every Ukrainian.'

That is not a boast. That is a documented asymmetry achieved through relentless, decentralised, rapid innovation — often by small teams, often with commercial components, always under fire.

Ukraine has demonstrated that cheap commercial drones, adapted at speed, can reshape the

battlefield within weeks.

Electronic warfare, AI-enabled target acquisition, and data integration are not future capabilities. They are present ones, being deployed and iterated right now, on both sides. Though note we have ethical issues.

The side that iterates faster wins. We need to be on the right side of that equation.

DragonFire: proof that our side can move fast too

DragonFire is a Royal Navy directed-energy weapon designed primarily for drone defence.

The marginal cost of its laser shot is around ten to fifteen euros — compare that to the cost of the missiles currently used to intercept cheap commercial drones.

Originally scheduled for deployment in 2032, DragonFire is now expected to reach initial operational capability by 2027, possibly sooner.

How? Procurement reform — a minimum deployable capability delivered rapidly, then developed further in service. Live testing at Porton Down and the Hebrides. Industry collaboration between MBDA, Leonardo and QinetiQ. And bridged funding: £100 million since 2017, £350 million through to 2027.

The original Type 45 single-warship fit has grown to plans for four destroyers by 2027. In my opinion we need many more.

DragonFire demonstrates that when procurement reform, industry collaboration, live testing and committed funding come together, the timeline from demonstration to frontline capability can be compressed dramatically.

That is replicable. The question is whether we have the will to replicate it — and the institutional courage to do so before the threat materialises, not after.

3. Public-Private Collaboration: Government as Monopoly Customer

Innovation is only half the battle. Rapidly producing those innovations at scale is just as critical.

Capabilities must be not only technically advanced but available in sufficient quantities to matter — and that requires a functioning relationship between government and industry that is currently broken in most Allied nations.

Consider Babcock's Type 31 frigate programme. The first ship was expected in service in 2023.

It could now be as late as 2030. Partly because the build programme forgot some of the hard-won lessons of sequencing a ship build — lessons that had been learned before and then lost as the workforce aged and institutional memory faded.

That is not a technical failure. It is a management and continuity failure. It is what skills fade looks like in practice.

Defence governments are not ordinary customers. They are monopoly customers. In most countries there is one buyer for a tank, one buyer for a warship, one buyer for a military communications system.

That creates an asymmetry of power that government consistently fails to use wisely.

Instead of leveraging that power to drive innovation, set clear requirements, provide predictable

funding and hold industry to account for delivery, governments too often oscillate between micro-management and neglect — producing the worst of both worlds.

There is a persistent 'black hole' in defence spending: extra funds, when they arrive, tend to be absorbed by overrunning legacy programmes rather than directed towards new capabilities.

Overruns in time and budget are the norm rather than the exception. Politicians who mouth the words 'the market will decide' in a sector where there is no functioning market are either ignorant or dishonest — and in either case, dangerous.

There is good news: budgets are rising. Germany is substantially boosting defence investment. France is accelerating modernisation. The UK has committed to raising defence spending to 2.6% of GDP within two years. Some Eastern European nations already exceed the NATO target, for obvious reasons.

But increased budgets without acquisition reform simply means more money disappearing into the same black hole.

Responsible monopoly customer behaviour means setting clear strategic requirements with unambiguous timelines. It means predictable, sustained funding that industry can plan against. It means streamlining acquisition to balance oversight with agility.

It means taking calculated risks in early-stage funding. It means coordinating multinational procurement to maximise economies of scale. And it means holding industry accountable for delivery while enabling flexibility in execution.

I should also note the role of government as instigator of collaboration between industry and academia.

The most effective innovation ecosystems in defence today are networks: large platform

companies, specialist SMEs, university research groups, and national laboratories, connected by shared data standards, open Application Programming Interfaces and genuine intellectual exchange.

Government can convene and fund those networks. It rarely does so with sufficient commitment or consistency.

And there is a supply chain communication problem that is both simpler and more embarrassing than any of the above.

When I was promoting a bidder for the missile programme that became the Anglo-French Storm Shadow, I spoke to subcontractors who did not even know that their components had defence applications.

The prime contractor had simply failed to tell them. They had no idea what they were contributing to, or why it mattered.

If you cannot tell your own supply chain what they are part of, you cannot expect them to prioritise, to surge, or to innovate in the right direction.

That is a failure of communication so basic it should embarrass everyone involved. And yet it is not unusual.

4. Intellectual Property, Sovereignty and Allied Collaboration

This brings me to what I consider the most structurally complex challenge: how do Allied nations protect the intellectual property that underpins their sovereign industrial capability, while enabling the cross-border collaboration that the threat environment now demands?

Sovereignty over key industrial capabilities is a legitimate concern.

Robust IP protection is not a legal formality — it is essential to maintaining industrial competitiveness and to incentivising the long-term innovation that national defence depends on.

No rational company will invest in breakthrough capability if it believes that capability will simply be appropriated by a foreign partner or a procurement process that lacks proper IP safeguards.

And yet overly rigid IP regimes, siloed development and nationalistic procurement models are self-defeating.

The Eurodrone programme is an instructive — and frankly painful — cautionary tale.

A French general described it as 'yesterday's technology delivered tomorrow.'

Germany insisted on two engines, in case a single-engine failure caused the aircraft to drop debris on an urban area.

A reasonable concern, perhaps, in peacetime. A crippling constraint when you need to move fast and at scale.

The result is a programme delayed in part by disagreements over national IP claims, industrial workshare, and design-by-committee compromises. The politics of 'who owns what' has repeatedly trumped the operational imperative of 'when do we need it.'

Conversely, AUKUS Pillar II on undersea autonomous systems demonstrated that with pre-agreed IP handling protocols and common security standards, real progress can be achieved quickly, even in highly sensitive domains.

I note that recent political developments have introduced new uncertainties into that programme. But the model remains valid. The lesson is not that all IP should be shared — it is that the rules of engagement for IP need to be agreed before programmes begin, not litigated during them.

What is needed is a new model that safeguards core sovereign technologies while enabling trusted collaboration across borders. It requires four things.

First, mutual recognition of classified research and IP protections across Allied nations, allowing trusted partners to engage in co-development without compromising national security.

Second, escrowed IP and controlled-access licensing models, giving coalition partners the ability to integrate systems without requiring full ownership or exposing sensitive source material.

Third, agreed frameworks for joint IP ownership and benefit-sharing, particularly for technologies developed through publicly funded multinational programmes.

And fourth, a harmonised Allied IP enforcement regime backed by genuine political commitment — one that rewards transparency and penalises exploitation.

Sovereignty and collaboration are not mutually exclusive. They are complementary pillars of strategic resilience.

The nations that understand this earliest will move fastest — and in the current environment, speed is a strategic asset in its own right.

5. The Role of Universities and Researchers

I want to speak directly to students and researchers in this room — because your role in this ecosystem is both underestimated and underutilised.

The innovation ecosystems that will determine strategic advantage in the next decade are not being built solely in the laboratories of prime defence contractors.

They are being built at the intersection of academia, startups, and government — and universities are a critical node in that network.

The dual-use technologies reshaping the battlespace — AI, autonomy, quantum sensing, advanced materials, cybersecurity tools — were in many cases developed first in university research groups, often without any defence application in mind.

But it is not enough to wait for serendipity.

Skills fade in critical areas. I mentioned the Type 31 programme. Nuclear submarine engineering is another example — craftsmen have retired and a generation of trainees was simply not recruited.

That is partly a consequence of universities and industry failing to maintain a conscious, strategic relationship.

Scholarships, sponsored research programmes, defence-relevant apprenticeships, embedded industrial PhD schemes: these are the pipeline through which the next generation of strategic thinkers, developers and production engineers will flow.

Or not flow, if we fail to build or enlarge such pipelines.

University researchers can also make a specific contribution to the problems I have described today.

The fragmentation of Allied standards is partly a technical problem amenable to research.

The challenge of IP frameworks that balance sovereignty with collaboration is a legal and policy research question.

Supply chain resilience — mapping sub-tier supplier networks, identifying single points of failure, building digital twins of critical supply chains — is a data science and systems engineering problem.

These are not abstract academic questions. They are live operational challenges for which practitioners desperately need better tools and frameworks.

The most effective thing this conference could do is to strengthen the relationships between the researchers here and the practitioners who need what they produce.

Governments and industry need to articulate their research needs in terms academics can engage with.

And universities need to engage with the defence and security domain without the institutional ambivalence that has sometimes characterised that relationship.

The stakes are too high for ambivalence now.

6. Conclusion: Carpe Diem

Our adversaries exploit speed, leverage asymmetric tactics, and press our seams.

But we possess a defining advantage: the collaborative resolve of the world's wealthiest, most innovative nations — with deep university sectors, sophisticated private technology ecosystems, and democratic institutions capable of genuine accountability.

That advantage is not automatic. It requires active stewardship.

The Mosquito was built in secret because the Air Ministry lacked the imagination to commission it.

DragonFire was accelerated because a small number of people decided to do things differently and were given the political cover to do so.

The ATA girls flew because someone decided the need was greater than the regulation.

In each case, progress came from individuals who refused to accept the institutional default.

Ukraine's drone battalions were not created by a procurement committee. They were created by engineers, coders and soldiers working together under fire, iterating week by week.

And remember Claesson's single word. Not 'soon.' Not 'within two years.' Now.

You are at the beginning of careers that will unfold against the backdrop of the most consequential security challenge Europe has faced since 1945.

The research you do, the collaborations you build, the frameworks you design, and the courage you bring to engaging with uncomfortable problems — all of it matters.

The tools Churchill asked for in 1941 were built by engineers, manufacturers, scientists and women who had taught themselves to fly.

The tools we need now will be built by people in rooms like this one.

Carpe diem. Seize this moment — boldly, decisively, and collectively. The timeline is not generous. But the opportunity is real.

Robin Ashby is Director General of the UK Defence Forum and Secretary General of Eurodefense UK..The conference was organised by the Manchester University Ukranian Society