

BLIND SPOT

Daryl Flack *shines the spotlight on the UK and Europe's defence deficiencies and wonders if strategic autonomy is failing*

Strategic autonomy has become one of the defining themes of modern defence policy across the UK and Europe are now putting significant money behind it. Russia's war in Ukraine, pressure on ammunition stocks, persistent cyber threats and concerns about industrial capacity have forced governments to look again not only at how much they spend on defence, but at where military technologies come from and how quickly capability can be produced, adapted and sustained.

The UK's Defence Investment Plan is a good example. It sets out almost £300-billion of defence spending over four years, including more than £5-billion for drones and autonomous systems. Germany, meanwhile, has undergone an extraordinary change in defence posture and is now the largest military spender among European NATO members.

There is clearly a defence investment race underway, but there is also a potential blind spot. Governments are spending billions strengthening sovereign defence capability while many systems they are buying remain dependent on globally sourced components, firmware, software and digital infrastructure that can become extremely difficult to trace beyond the first few tiers of the supply chain.

There is a tendency in defence to think about sovereignty at platform level. Is the drone British? Is the aircraft European? Was the system developed by a UK company? But those questions tell only part of the story.

A finished system may come from a British or European supplier while the processors, cameras, communications modules or firmware inside it originate somewhere entirely different. Go down another tier and provenance can become considerably harder to establish.

Modern defence capability has effectively become a giant systems-integration exercise played out across global technology supply chains. Defence organisations may have a relatively strong understanding of their Tier One suppliers and the companies directly responsible for delivering critical capability, but visibility often deteriorates significantly at Tier Two and Tier Three, precisely where smaller technology providers, specialist manufacturers and software dependencies can introduce cyber, geopolitical and operational risks. The recent reporting around cameras intended for Royal Navy K3 Scout uncrewed surface vessels brings this blind spot into sharp focus.

Routine cyber testing reportedly identified third-party camera components sending automated 'heartbeat' communications to an IP address in China. Importantly, the Ministry of Defence said its investigation found no evidence that MoD data or systems had been accessed, compromised or transmitted externally and internet connectivity to the affected cameras was removed.

Based on what is publicly known, this is not evidence of classified info being stolen. The more interesting point is how far down the technology stack organisations need to look before they can understand their dependencies.

Camera components on Royal Navy K3 Scout vessels was discovered to be sending data back to China

An unvetted external communications path appears to have existed inside technology intended for a military platform. In a defence environment, that should lead to some fairly basic questions: why is the connection there, what info can be transmitted, who receives it and what else could the component theoretically communicate?

It is easy to dismiss heartbeat telemetry because it appears innocuous. A device effectively saying "I'm alive" may reveal very little in isolation, but intelligence rarely comes from one perfect piece of information. More often, it is created by combining apparently insignificant fragments until patterns begin to emerge.

Basic telemetry can potentially disclose device presence, uptime and temporal patterns. Depending on the architecture and metadata available, an observer might learn when a device comes online, how long it remains active or whether its use follows a pattern. Combine that with other sources of intelligence, including OSINT, SIGINT or knowledge of exercises and deployments, and seemingly mundane signals can potentially contribute to a much richer picture.

That does not mean the K3 Scout incident exposed Royal Navy locations, personnel or operational movements; there is no public evidence to support that conclusion. It does however, demonstrate why assurance cannot stop at asking whether obviously sensitive information left a system. Defence organisations also need to ask what somebody could potentially infer from the information that did.

This is particularly important with cameras and other connected sensors because of what those components are capable of collecting. If an unexpected communications path is discovered, the assurance question should not simply be what has so far been observed travelling across it, but what the architecture could have allowed the device to transmit under different circumstances.

These questions are becoming more pressing because defence organisations are simultaneously being encouraged to embrace exactly the types of technologies that create more complex supply-chain dependencies.

Ukraine has demonstrated the extraordinary military value of relatively inexpensive unmanned systems for reconnaissance, targeting, electronic warfare and strike. They do not replace sophisticated missiles or high-end platforms, but they are changing the economics of conflict by providing capabilities that can often be produced, modified and replaced much more quickly.

The contrast with missile warfare and defence is particularly striking. Ukraine continues to face pressure on supplies of sophisticated air-defence interceptors as Russia conducts large-scale missile and drone attacks. A Patriot PAC-3 MSE interceptor, for example, costs millions of dollars and depends on complex manufacturing capacity that cannot simply be expanded overnight.

It is not a straightforward comparison between cheap drones and expensive missiles because they perform very different roles. Future militaries will need exquisite capability, but they will also need systems that can be manufactured at scale, replaced rapidly and modified as battlefield conditions change.

That helps explain why the UK is putting billions into drones and autonomous systems, but it also exposes a tension at the heart of strategic autonomy. One reason emerging defence technologies can be developed quickly and relatively cheaply is that manufacturers integrate commercial off-the-shelf components rather than designing every processor, camera and communications module themselves. The global technology ecosystem that makes rapid innovation possible can therefore create the very dependencies governments are trying to reduce.

The drive for strategic autonomy creates a difficult tension between the speed of commercial innovation and the assurance expected of military systems. For smaller defence technology companies in particular, switching to a sovereign or trusted component can mean higher costs, longer lead times, redesign and additional certification. Requiring complete provenance of every component risks slowing the very innovation governments are trying to encourage, which makes proportionate, risk-based assurance increasingly important. A connected, programmable camera, for example, warrants considerably greater scrutiny than a passive component, even where both have overseas provenance.

This challenge becomes more complicated as defence moves further into artificial intelligence. Autonomous platforms, sensor-fusion systems and battlefield decision-support tools increasingly depend on AI models, data pipelines, software libraries and continuous updates. Assurance therefore needs to extend beyond where a physical component was manufactured to how a model was trained, where its data originated, who can update it and how its integrity is maintained throughout its operational life. A manipulated dataset or compromised model could ultimately matter just as much as a questionable hardware component.

STRATEGIC AUTONOMY EXTENDS FAR BEYOND WHERE A PLATFORM IS ASSEMBLED OR BUILT

Quantum technologies present a similar, longer-term challenge. Quantum sensing has potential applications in navigation and detection, while sufficiently capable future quantum computers could have profound implications for some of the cryptography relied upon today.

The underlying problem is that a military platform may remain operational for 20 or 30 years while the digital technologies inside it can change dramatically in a fraction of that time. Defence procurement therefore needs to become more adaptable, using modular architectures, software-defined capability and continuous assurance so that technology can evolve without forcing an entire platform through lengthy redesign and procurement cycles. Defence organisations also need to challenge the assumption that the adversary will always look like another military.

The boundaries between state actors, cyber criminals, proxies and individual operators are increasingly blurred, while AI has the potential to make some sophisticated capabilities accessible to a much wider range of actors.

Rogue agents are useful to think about in this context. Individuals, criminal organisations, state-backed proxies and, increasingly, AI-enabled agents capable of automating parts of reconnaissance and cyber activity. The point is not that autonomous AI has suddenly replaced human adversaries, but that automation

can increase the speed and scale at which established techniques are deployed.

Attackers have already adapted to interconnected ecosystems. SolarWinds demonstrated how a compromised trusted software update could affect government and private-sector organisations, while MOVEit demonstrated how vulnerabilities in widely deployed software could have cascading

FUTURE MILITARIES WILL NEED EXQUISITE CAPABILITY THAT CAN BE MANUFACTURED AT SCALE

consequences across many organisations. More recently, security incidents and testing involving AI systems from Anthropic, OpenAI and Meta have highlighted the growing ability of AI agents to identify vulnerabilities and, where controls fail, interact with systems beyond their intended environments. As those capabilities mature, the potential for nation states to direct autonomous AI towards reconnaissance and cyber operations is becoming increasingly difficult to ignore.

An adversary does not necessarily need to defeat the most heavily protected military platform if a supplier, software dependency, subcontractor or trusted relationship provides an easier route. Supply chains have become strategic attack surfaces, making an understanding of who and what you trust increasingly important.

None of this means international defence supply chains are inherently a weakness. In many cases, they are precisely what makes advanced capability possible. The F-35 Lightning II combat aircraft programme is a good example. Led by the United States but developed and sustained through an international network of partner nations and suppliers, including the UK, it brings together specialist manufacturers, technology providers and maintenance networks across multiple countries. British companies contribute important components and technologies to the aircraft, demonstrating how expertise and industrial capability can be shared across an international programme.

That interdependence brings significant advantages, but it also creates dependencies that need to be understood. Disruption affecting a specialist supplier, component or part of the sustainment network can have consequences elsewhere, particularly where alternatives are limited or difficult to introduce quickly.

This is why strategic visibility should increasingly be treated as a defence capability in its own right. Component provenance, firmware validation, software and hardware bills of materials, and architectural controls such as network segmentation can all help organisations identify where the greatest risks sit. Perfect knowledge of every component is neither realistic nor desirable if the cost and delay undermine innovation; assurance needs to be proportionate to the strategic risk.

So, is strategic autonomy failing? Not necessarily, but our definition of it may be. If it means manufacturing more platforms domestically while remaining unable to see critical dependencies several layers beneath them, increased defence spending risks creating the appearance of autonomy without necessarily delivering it.

Strategic autonomy extends far beyond where a platform is assembled or which flag sits above the company that built it. As defence becomes more connected, autonomous and software-defined, it will increasingly depend on understanding the technologies within those platforms and the supply chains that sustain them. Essentially, autonomy will require a careful balance between managing international dependencies and having the resilience to respond when circumstances change ●

Daryl Flack is Partner at Avella Security.



Ukraine has demonstrated the extraordinary military value of relatively inexpensive unmanned systems