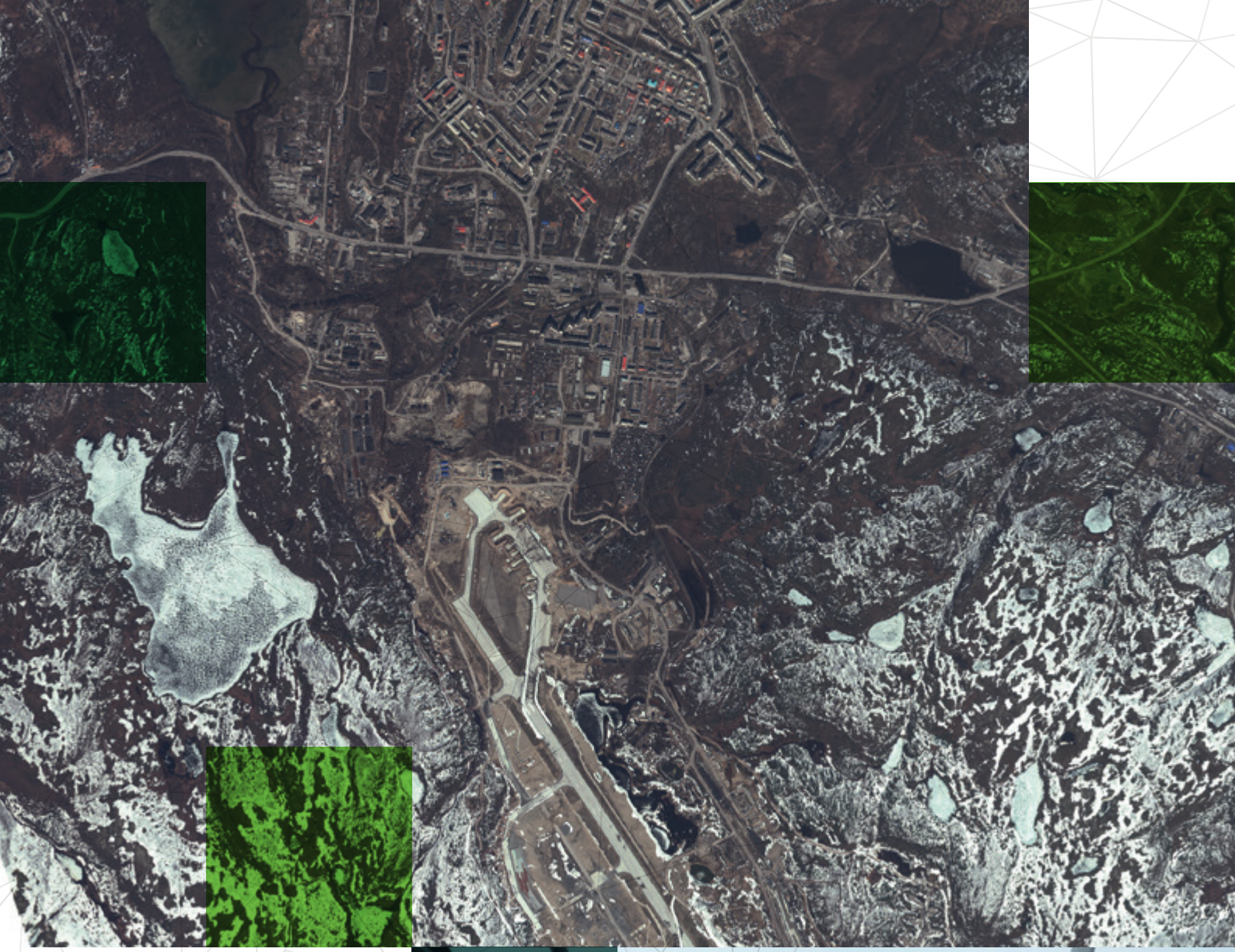
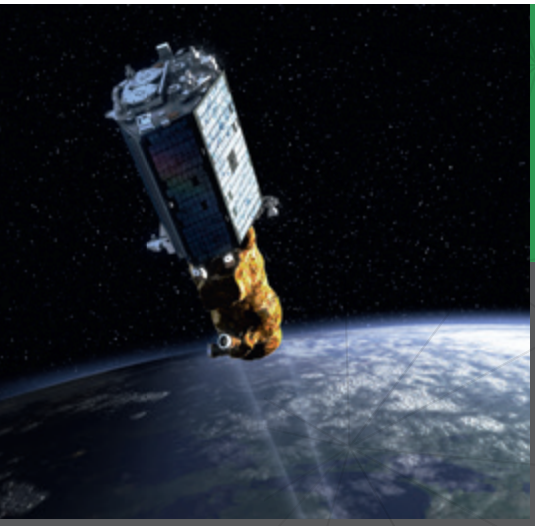


Intelligence as a Service.
Time to Change the Approach?

By Sean Corbett, CB, MBE.
Director of Defence, Security and Intelligence.

earthi



Industry has something game-changing that Defence Intelligence needs. But has that sunk in yet?

By Sean Corbett, CB, MBE.
Director of Defence, Security and Intelligence.

Across all areas of defence, the need for Government organisations to work more closely with industry is increasingly acknowledged, including within the intelligence community, as highlighted in the recent Open Source Analytics and Disruptive Technology for Defence Transformation conferences in Washington DC and London respectively. The complexity and global nature of the contemporary threat environment is placing unparalleled demands on resource-strapped defence, security and intelligence organisations, requiring innovative approaches to ensure information advantage is maintained.

The continued proliferation of violent extremist organisations, the 'return' of the nation state as a potential adversary, and the unpredictability of rogue states as intelligence problem sets, are simply too big, complex and fast changing for any government to fully monitor using internal resources alone.

The blurring of state and non-state actors and with it the inability to identify clear accountability has further complicated the landscape. Add this to the ease of access to ever more sophisticated technology and social media to proliferate fake-news for propaganda and dis-information, and the challenge in maintaining the level of understanding necessary to counter these threats is at an all-time high.

Intelligence analysis is an inherently labour-intensive discipline, and not always seen as 'core business' within defence, or at least not heavily prioritised for resource allocation and investment. The ability to collect information now significantly outstrips the ability to process, exploit and disseminate what is gathered. The tyranny of the 'now' is particularly keenly felt in the intelligence world, as a huge proportion of available capacity is understandably focused on immediate and short-term threats. The time and resources available to devote to horizon-scanning, indicators & warnings (I&W), and in building and maintaining the foundational intelligence, are therefore at a premium. Whilst these activities provide the critical underpinning from which confident intelligence assessments are derived, we cannot rely on increased

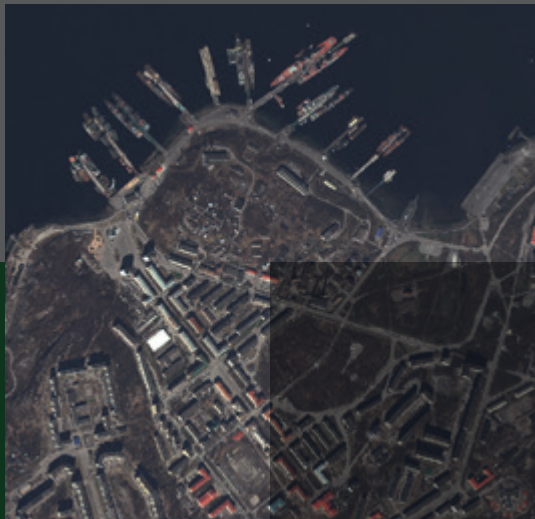
defence budgets. A different approach is therefore required.

One tool to ease this burden is the harnessing of Big Data, Machine Learning (ML) and Artificial Intelligence (AI). Effectively integrating these technologies is, however, complex, time consuming and requires individuals with a range of deeply specialist skills, including coders, developers, data scientists and visualisation experts.
The military is not particularly well suited to recruit, train, manage or retain these specialists, nor are they able to compete with the commercial sector for the remuneration expected as such specialist skills are also in short supply in industry. Unsurprisingly therefore, the commercial sector is significantly ahead of defence in developing applications of these new technologies.

To underscore this point, commercial investment in research and development in the US totalled $357 billion in 2016, more than doubling the $130 billion invested by federal organisations. Intelligence is only as good as the data from which the analysis is derived, and an eye-watering amount of resource and money is expended by many government defence and intelligence organisations to collect “exquisite”, highly discrete and sensitive data. Government-owned data collection will continue to be critical, but it is being augmented (and expected to be overtaken) by the amount of highly detailed information now available in the open source domain. Commercially-owned open source intelligence (OSINT) data collection platforms, social media and third-party data feeds, as well as data- mining of the internet, will become an increasingly important mainstay of intelligence in the future. When validated and verified, publicly available information is therefore increasingly relevant and valuable to the analyst. It has the added benefit of starting as unclassified data from the outset, which can then be protectively marked as “exquisite” data is added. This can significantly help in enabling dissemination to those who need it.

There will, of course, always be the national security argument about protecting sensitive information and an understandable need to protect where the intelligence gaps may be. However, there are well-founded mechanisms in place to enable both individuals and companies to become suitably accredited. No-one is saying that the most sensitive, timely and operationally compartmented intelligence requirements should be out-sourced. Yet there is a huge amount of the more mundane, but nonetheless, important foundational intelligence that simply does not get covered due to competing high priorities. This foundational intelligence is often the most time consuming and resource intensive to produce and that would be entirely appropriate to out-source. The argument to leverage the commercial sector is therefore compelling.

And yet progress in defence partnering with industry to provide intelligence as a service remains embryonic at best. Why is this so?



It would be easy (and largely accurate) to point to policy limitations; there is simply no formal mechanism whereby a U.K. Ministry of Defence (MoD) organisation can easily set an intelligence requirement, compete it (or not) and write a contract for services. The US Department of Defence (DoD) has similar challenges and an even more complex bureaucracy, with the added constraint that, by and large, they will only deal with US companies and US personnel. In the UK, the lack of a fit-for-purpose policy drives us back into the MoD procurement process, designed in a different age, and focused on big capital projects. While this may be entirely appropriate for the purchase of ships, armour and aircraft, it is completely inappropriate for small, time-sensitive programmes, particularly when applied to services (one-off or recurring) rather than equipment. Innovation is strangled by legacy procurement processes, and the time required to get projects underway. These limitations have been recognised for a while now and although we are adept at 'admiring the problem', we have yet to adequately address it.

Having recently attended back-to back conferences in the US and the UK that touched on these issues , each identifies strikingly similar constraints and there is a lack of clarity in how to approach the issue in both countries. The default setting on each side of the 'pond' is to set challenges to industry to address specific problem sets as capability demonstrators. While this approach is great for pilot projects and small discrete problem sets, it does not adequately address the provision of intelligence services and there has, for now, been limited success in translating these pilots into something more enduring.

But for all the policy constraints, the challenge is as much cultural. There remain a few intelligence analysts (thankfully an ever-decreasing number) that do not recognise publicly available information as a legitimate data source. To this is added an inherent mistrust of those not 'in the club' and an inherent aversion to sharing intelligence gaps and requirements outside of the community, let alone trying something new in a controlled environment. To an extent this is understandable, since security and the 'need to know' principle' is indoctrinated into every intelligence specialist at the earliest stages in their career. But behind this, there is also a sense that not being able to address a particular intelligence query internally is an admission of failure.

It would, however, be unfair to put all the onus solely on defence and there is a real obligation on the commercial sector (Enterprise and SME) to demonstrate in very clear terms the value-add it can bring to the party, both in terms of answering the question in a simple and clear manner, but also sharing the risk as a co-investor. In a highly competitive sector, it is easy to over-promise and under-deliver. The more compelling the capability, the more likely it is to be taken up by defence. But to demonstrate this within the intelligence world is best achieved if we can apply it to a real problem set or, in commercial parlance, 'use-cases'. For now, this simply isn't happening and the lack of

engagement in articulating relevant problem sets makes the requirement guess work and therefore the ability to demonstrate added value difficult; the proverbial 'chicken and egg' situation. Industry also needs to ensure it fully under-stands the policies, processes and constraints under which the MoD must operate and work in partnership to determine the art of the possible, rather than merely lament the lack of opportunity.

In summary and having now seen this issue from both ends of the telescope, there is urgent imperative and major opportunity for the defence intelligence community to partner with trusted industry innovators to address current and future intelligence challenges. By focusing on the less sensitive, foundational and strategic intelligence areas, industry can release defence resource to cover the operational, time-critical and sensitive issues. In partnership, there is a much better chance of effective horizon scanning and anticipating future threats, thereby helping to maintain the information advantage that is so critical in today's information environment. To achieve this though, is going to require a more agile approach, increased trust and ultimately a mind-set change that looks at industry as a potential asset rather than irrelevant or even a threat. We are nowhere near that true strategic partnership yet, but now might just be the right time for us to seize the initiative.

If you wish to learn more about Earth-i's Defence, Intelligence and Security programme, or to discuss this article in more detail, please contact: enquiries@earthi.co.uk

About Sean Corbett

Air Vice Marshal (Retired) Sean Corbett joined Earth-i after thirty years' service as a professional intelligence officer in the RAF. He brings significant operational experience and leadership and a deep understanding of the UK defence intelligence environment. He has unparalleled international credentials within the defence intelligence community, having worked at senior levels in NATO and most recently as the first non-US Deputy Director of a US Intelligence Agency. As the Deputy Director for Commonwealth Integration at the Defence Intelligence Agency he focused on the sharing of intelligence between Australia, Canada and New Zealand, the US and UK.

At Earth-i Sean is working with the UK's Ministry of Defence and other military and security organisations, both within and outside the UK.