A Question 4 Moment

A PERSPECTIVE ON CHANGES TO THE CHALLENGES AND IMPERATIVES WITHIN THE SINGLE INTELLIGENCE ENVIRONMENT

The title is drawn from military doctrine for the Mission Analysis and Estimate process which shapes the development of an operational or tactical plan. Question 4 of the Mission Analysis reviews changes to the situation and has entered common parlance beyond this formal usage as a ***Question 4 moment.***

Abstract

A Leidos thought-piece developed in association with Jon Rigby, Rob Jones and Ross Bailey; they argue that there has been a post-Afghanistan paradigm shift which, when combined with the transformative effect of digital technology and social media, has challenged the defence intelligence community. Yet, the responses to this shift in the geo-political, socio-economic and technological plates should be bold but achievable; however, it will require the current commercial and acceptance processes to be adapted which will allow for innovation, agility and contracting for outcomes, as opposed to against the minutiae of system requirement documentation.

They will address the challenges faced in a World of large-scale open-source data and the need for timely access to that data; the need for agility and focussed spending on capability and new technology to maintain situational awareness; and the importance of achieving interoperability and sharing of data through trust, with consideration of the necessary security constraints within which we operate.

The answer to the Question 4 (what has changed?), they contend, is that the combination of a fundamentally new World (brave or not) and the potential to leverage new capabilities should catalyse a change to the Single Intelligence Environment (SIE) strategy – not to the ends, or fundamentally the ways, but rapid and targeted interventions to the means of delivery.

Introduction

Should the advent of 2018 be characterised as the end of the beginning of the quest for the SIE? Almost certainly. The formation of Joint Forces Command (JFC) and the transformative impact of Wyton and other intelligence centres has created a template for intelligence integration (previously seen temporarily and only on operations) to be made repeatable and sustainable. Many challenges remain, not least the integration at the data level of Geospatial Intelligence (GEOINT) – a key foundation upon which intelligence capabilities are based - and indeed the other Ints that make up the SIE. Meanwhile, politics, the information and technology landscape and the expectation of intelligence consumers ("from Whitehall to the fox-hole") continues to evolve. The community cannot afford the luxury of pausing and consolidating this first phase. Continued agility and steady, incremental steps in concepts, enabling technologies and, in equal measures, bold, agile and innovative leadership is required to build on the current, firm foundations. More of the same (great as it is) is not going to be enough.

Vision

The Defence Intelligence (DI) mission remains largely unchanged – essentially to optimise the use of intelligence and information in support of better decision-making across defence.

Context

In this paper we suggest that the last three to four years has seen an exceptional period of rapid, generational change that offers the stiffest of challenges for Western society, be that democratic governments, departments of state or the general population. Whilst the geopolitical environment bears many of the hallmarks that we would recognise from the Cold War and previous terrorist campaigns, the transformative impact of digital technology and social media has catalysed a New World for the intelligence community and the society that it serves. In looking at the impact of these causes, we have matched some with the UK defence information benefits framework (effectiveness, efficiency, agility, compliance) to provide some structure for our context.

Table 1. Causes and Impacts of the Question 4 moment

Cause	Impact
The normalisation of democratic protest, Brexit, the £/$ exchange rate.	**Efficiency**
Fake news; policy through social media; the personalisation of everything; human rights vs state surveillance.	**Agility; Compliance; Privacy** *(Judgment)*
"Fast and Big" data everywhere; AI and machine-learning; social media; cloud; human rights vs data monitoring; the power of aggregation; retrospective intelligence at public enquiries (Manchester, Grenfell). The loss of the State's monopoly of intelligence. The validation of open source information, and its integration with verified, unique and high-end intelligence.	**Effectiveness; Compliance; Differentiation** *(De facto Information Inferiority?)*
Superpower realignment; creaking nuclear monocrop economies. Western retreat from global engagement.	**Agility; Effectiveness** *(for new/old missions)*
Future role of the military against diverse threat environment? Interface and boundary between security, law enforcement and military.	**Efficiency** *(Pressure on department; increase support to homeland security?)*
Technology – Defence imperatives – Defence Enterprise Architectures, Evergreen, removal of vendor lock-in. Potential of agile and enabling architecture: infrastructure, platforms, applications, security.	**Effectiveness; Security, Compliance.** *Aspirational – will delivery meet required timescales?*

Table 1. Causes and Impacts of the Question 4 moment

Individually, many of these causes at Table 1 offer new and pressing challenges to UK Defence; together they amount to a post-Afghanistan paradigm shift, which provides, in military parlance, a Question 4 moment. This may provide an imperative to pause and reflect on the Impacts and both the inherent risks that may need to be mitigated, and the opportunities that may need to be realised, in shaping future responses.

Factors

We believe that the responses to this shift in the geo-political, socio-economic and technological plates should be bold but achievable; they will demand vision and leadership both to harness resources within the UK's defence and security domain, and to further develop trusted partnerships with allies, across departments and with industry. The department may have simply to stop doing some activities[1] to find the headroom, within resources, to invest in the technology necessary to enable the level of transformation required in this new paradigm. We have framed our arguments around eight principal factors:

1. **INNOVATION** On operations and in industry the rapid evolution of technology to meet customers' needs is the norm. ***The agile development of software is the foundation of the mo*****dern economy and the acceptance that failing fast is better than not competing is a business imperative.** It is a given that a programme requirement will change or evolve over time. A customer could move towards a hybrid (i.e., in-house, partner, contract) and layered supply-chain model which would enable: advantage to be taken of industry's investment in technology for the wider market; the rapid commoditisation of this technology into products and services which may be packaged to meet an evolving requirement; and further, incentivisation of Small and Medium Enterprises (SMEs) through assuring them of access to opportunity and contracts. This way, participants in the supply chain may meet the demands of changing circumstances and innovation can become a given. On operations, militaries generally evolve to this agile model when the alternative is losing lives, battles and wars.

2. **MANAGED-RISK SOLUTION** Maintaining momentum and responding rapidly to changing circumstances is all. Whilst an ambitious, long term strategy is essential to deliver the required transformation. In the immediate term, low-risk and assured capability delivery is essential. The need and opportunity abound (not least in Imagery Intelligence (IMINT), GEOINT and Electronic Warfare (EW) to deploy tried, trusted and tested solutions which has always been preferred by the military. Interoperability, fundamental to intelligence operations, can be achieved by procuring common capabilities. ***Partnering and streamlined commercial arrangements are cheaper for both defence and industry, and with appropriate assurance and competition, result in greater understanding and innovation. Time and money spent on bids could be spent on capability instead.*** The ability to negotiate national security and export constraints is a challenge, but far from insurmountable.

3. **ALL COLLECTORS AND DATA SOURCES** This is not just about a centralised exploitation of intelligence and information capability: it looks to the boundaries and includes all collection capability. Turning to the Defence Lines of Development (DLOD[2]s), ***one of the first tasks is to review/produce a dynamic concept of operations, against which to set and monitor user requirements, rather than defaulting to the minutiae of system requirements.*** Much of Wyton's success was achieved by placing an emphasis on conceptual, infrastructure, policy and people levers, whilst making pragmatic but relatively small improvements in technology; however, ownership and accountability of the DLODs is in need of a refresh.

4. **INFORMATION *AND* INTELLIGENCE (I2)** Highly-trusted (sometimes termed "exquisite") intelligence sources and analysis will retain their value and can be game-changing, providing a decisive information advantage. The reputation of intelligence organisations is everything, so invariably the accuracy of their 'stuff' is exemplary. ***However, the pace and spread of events may outstrip an organisation's ability to collect and analyse, so the default source for decision-making has to be basic, open-source information.*** If we consider key components of intelligence to be timeliness, accuracy and relevance, a piece of open-source which is, say, 40% accurate but on time, can be better than a late but 'assured' assessment. Policy changes will be needed to

[1] Noting the Rubicon was crossed with the capability holiday for long-range, airborne maritime patrol

[2] DLODs – Training, Equipment, Personnel, Information, Doctrine and Concepts, Organisation, Infrastructure, Logistics (TEPIDOIL).

Consider the change in the rules and decision-making construct in a non-elective war. It has always been preferable to task something operated by someone you absolutely trust, something highly 'assured'. This is often too late/ too polite, so this strand encompasses the assurance of information, the judgment of analysts and decision makers. It is about a winning advantage and taking risk by using decidedly 'unassured' information.

clearly define both what information and intelligence are, and how it should be validated and used. For example, targeting will still require the highest levels of assurance and accuracy. The reality is that today's commanders will reach for their iPhone, just like yesterday's commanders reached for CNN. The intelligence community must recognise, lead, support and adapt to this reality. The need for professional analysis and interpretation hasn't changed, just the source of the data. Just because open source data is…open…. it does not make it easy to process and to transform it from data to intelligence; however, the leverage created by investing in open-source solutions is fundamentally greater than investment in high-end intelligence solutions.

5. **LEVERAGING NEW TECHNOLOGY** A new paradigm demands appropriate platforms to host new applications and allow extensible storage, taking advantage of open-source capabilities and an open, cloud-enabled data approach which readily supports automated data analytics; moreover, virtualisation offers efficiencies at the enterprise level. Security has been an essential factor behind the design of intelligence technology and has been a constraint on innovation, integration development and design. New security technologies and policies should make the adoption of modern architectures and technologies possible. ***However, moving to new environments is not a simple drag and drop into place.***

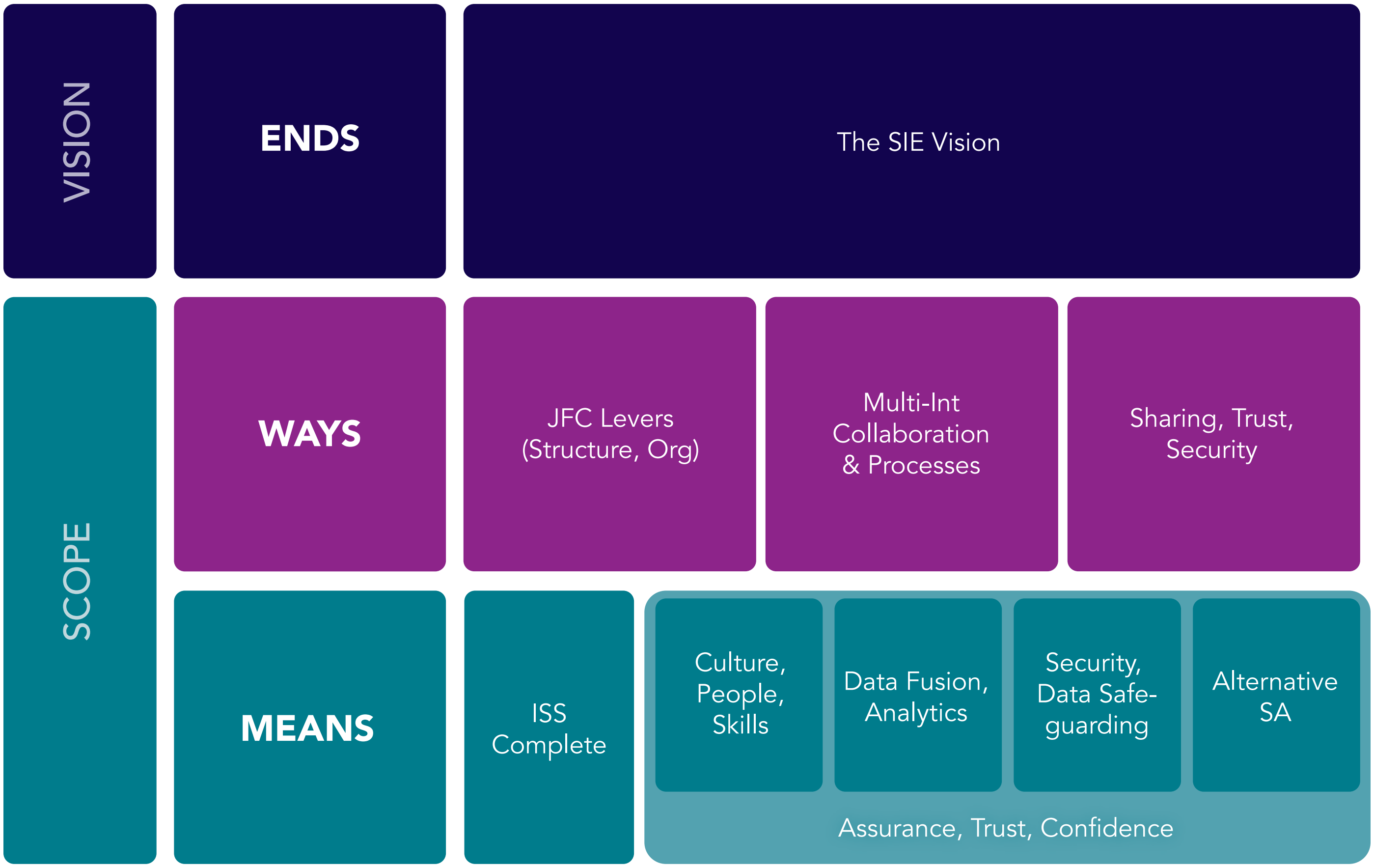
6. **TIMESCALE OUT TO 2022** Stretching an analogy – possibly to breaking point - that the SIE vision is akin to a start-up enterprise, experience in industry might suggest that it takes three years for a commercial entity to start up, and two years to normalise. If we agree the **Question 4 moment** is now, the timeframe for transformation after a rapid review is from now until 2022. Can UK Defence, however, continue with traditional acquisition cycles and requirement specification to hit this target? It is telling that the FinTech sector is not mirroring Defence's approach. ***The baseline created by the current defence capabilities delivering Open Source Intelligence and (OSINT) and IMINT creates opportunities for further integration, development and innovation.***

7. **EXISTING PROCESSES AND REALITIES** ***There is no need to reinvent the wheel;*** but we do need to change from steel to alloys…and change our tyres. Most of the necessary processes are in place, or at least available, as are some examples of bold policy changes. Much can be achieved through clear vision and leadership to optimise sub-components of the SIE and indeed to be transformative.

8. **DEFENCE *AND* SECURITY** A more agile approach could mean at times, large chunks of the military sustained in support of police, agencies or other departments to address national priorities. This may be based on specific skills or on the agencies and police being overwhelmed. Whatever the scenario, it should be based on national priorities, not departmental ones, and embracing a truly ''comprehensive approach.'' The same principle holds with NATO and other extant partnerships and burden-sharing agreements. ***Interoperability must* be considered at source, whilst maintaining releasability policies and intelligence-sharing relationships.** The tasking of Defence collection resources in support of Civil Power or Authority is not unusual. So whilst the alignment of data assets and analysis is likely to become the norm within the highly integrated intelligence community, the efficiencies and effectiveness that will accrue through wider data interoperability should not be ignored.

Deductions

Having framed the factors we can turn to the deductions as they pertain to the SIE. We have chosen to present them within a Strategy framework to reinforce our overall message and show the relationships between the deductions – illustrated at Figure 1.



VISION

ENDS

The SIE Vision

SCOPE

WAYS

JFC Levers (Structure, Org)

Multi-Int Collaboration & Processes

Sharing, Trust, Security

MEANS

ISS Complete

Culture, People, Skills

Data Fusion, Analytics

Security, Data Safeguarding

Alternative SA

Assurance, Trust, Confidence

Figure 1: Factors arranged under a Strategy framework

ENDS

As stated, the ***Ends*** – our vision – are clear: loosely, to optimise Defence's intelligence effort in support of whatever it may be tasked to do. We have brigaded nine deductions under ***Ways*** (actions) or ***Means*** (resources).

WAYS

1. **SHARING, TRUST AND SECURITY** ***The fundamental enabler of the enterprise is the ability to collaborate through sharing your and others' data securely at pace.*** This requires establishment of Trust through technical means, access protocols, safeguarding policy and through organisational and human relationships. A step change in analysis through applied analytics of shared, unstructured data is possible. Security policies, identity and access management, audit and monitoring are essential to enable this step change – and if executed well and widely will enhance security by default. Data ownership issues have generally precluded other than the slow and inefficient fusion with 'product', rather than source data; modern security and audit will assure data owners that their policies are applied rigorously and **most fundamentally** that their sources are protected. If we don't, in addition to the operational damage, retrospective intelligence pictures that are now being offered in public enquiries, e.g., Manchester, would raise difficult questions. Secure storage is required for huge data lake(s) but some source-protect material will be kept outside; this must encompass big data and could be an additional network at a DI node.

2. **JFC LEVERS; STRUCTURE, ORGANISATION** ***With all the information levers, critically including the Senior Responsible Owner, in one command chain, there is the possibility of continuing to address previously intractable problems, such as making agile acquisition work.*** Structures and Organisation present culturally challenging issues where human nature instinctively defends beloved stovepipes or fiefdoms. The enduring and very recent fiscal pressures, along with the gravity and span of threats suggest time to look at pan-Defence **Effectiveness** and **Efficiency** of its intelligence components. The sum of the parts is traditionally less than it should be. A piece of work to deliver a Blueprint to look at DLOD efficiencies – Organisation, Training, Personnel, Logistic synergies - across the principal air ISR collectors, is an example of the user addressing some of these intractable issues. Location, organisational, technical and structural changes have taken place to integrate IMINT, GEOINT, OSINT and Signals Intelligence (SIGINT) (irrespective of collection source) at all other stages in the cycle – more can be done within Defence, cross government and between allies to integrate at the data-level.

3. **MULTI-INT COLLABORATION AND PROCESS** Single-Int is no longer relevant for most tasks, where the baseline could be open-source as the norm, with the Intelligence community providing added value. ***Aligning the different processes for the different Ints must be an enabler for fusion at pace.*** The Intelligence Cycle must be adapted for the needs of the task, be it rigid (say for timed collect or operational security) or 'free play', when the task is less critical. Every platform a sensor is largely an unfunded aspiration, so needs connectivity, innovation and agility to realise the potential value in 4th generation platforms. The intelligence cycle needs to plan for failure when a collector has a primary strike role; reachback is highly efficient but cultural attachment to having high grade analysts forward is expensive. These process changes must be enabled by the technology, which must provide a stable but agile exploitation solution to accommodate the needs from the tactical to the national analysis.

MEANS

4. **INFORMATION SYSTEMS AND SERVICES (ISS) *COMPLETE*** The move of an organisation providing the means of acquisition into Joint Forces Command has been hugely positive, and great things have been achieved. However, there is now the need for the technology to enable the agility, pace and scale demanded by the new level of challenge. This means modern architecture(s), stable infrastructure, agile app development and extensible data storage; these can only be introduced ***with a more-determined focus on agile commercials, moving from contracting against requirements to contracting for outcomes and benefits. Innovation must be embedded early and at the appropriate levels in the supply chain with opportunity to create interventions; critically, delivery stovepipes must be broken***. These are difficult, and some may feel somewhat esoteric, however, ignoring them should not be an option if the information battle is to be contested fully. Adoption of agile security-protection techniques, as applied in the more evolved commercial sectors is fundamental.

5. **DATA FUSION AND ANALYTICS** Bluntly, algorithms can do the mundane better than regiments of analysts; Artificial Intelligence(AI) and machine-learning offer huge leaps in **Effectiveness** and **Agility**, while the **Efficiencies** both in manpower cost reductions and in freeing staff to employ judgement on a managed deluge are hugely appealing. If anything encapsulates the paradigm shift, it is the nearing of big data (BD) and AI as normal. Western liberal democracies will need to decide how to confront states or actors with a different tolerance level for data privacy and state-level surveillance, who therefore may come to enjoy an exponential information advantage. ***While 'BD&AI' will not guarantee information dominance, not pursuing both with vigour will likely lead to failure.***

6. **CULTURE, PEOPLE, SKILLS** Intelligence analysis is not and cannot be immune from the impact of data-science and AI. ***Agile application development, data analytics and access management can industrialise analysis, but call for a fundamentally different skill-set and approach.*** This should not remove the need for insight, judgement and subject-matter expertise. However, the days of high-end analysts engaged in collation and information management must cease: it's just too wasteful. Looking forward, the multi-int team will continue to incorporate general and int-specific analysts. It should also incorporate a high proportion of data scientists, access managers and auditors and software engineers. Defence has a plethora of high-quality intelligence analysts but is it ready to exchange two-thirds of them for data scientists (DS)? Or at least provide one DS for every team? And if it were ready culturally, is it able to attract and retain the right talent…or vet what will largely, increasingly, be unconventional millennials? A risk-based approach to personnel security will be essential for the latter; the former may be more of a challenge but developing a world-class reputation and having vitally important, exciting and challenging missions, in lieu of pop-star wages, works for some organisation. As for retention, if short spells of work is just how millennials work, then agile management of the workforce will be tested. Furthermore, ***looking at simple commercial alternatives, such as outsourcing of lower-grade or less-secure products that do not need to be held at the highest levels of the enterprise, should be considered.***

7. **SITUATIONAL AWARENESS (SA): A NEW PARADIGM** The pursuit of the most timely and accurate Situational Awareness is at the behest of the data deluge with which analysts are over-faced. It is a critical enabler for commanders' decision-making and sets the context for everything. Open-source should be the baseline, some of it more assured than some decidedly unassured but unique data. ***However, the use of crowd-sourcing offers great potential as long as risks are understood and a degree of assurance is attached to any assessments.***

Perhaps, light-heartedly, analysts in certain roles could be given Monopoly money, where they have, say, 3 x £500s and unlimited £1s. They can use the £1s for open-source searches and info; they can only task prized Int assets three times. This would encourage the inversion that has been suggested for years (80%+ from open source) and avoid wasting high-value collect on mundane baseline tasks. Or use the cricketing Decision Review System, whereby if you task inappropriately you lose an umpire review: three and you're out and confined to Wikipedia!

8. **SECURITY AND DATA SAFEGUARDING** Disseminating intelligence, whilst appropriately protecting your source, is a fundamental skill of the intelligence analyst and leader. Ultimately, lack of appropriate security and safeguarding can deny access to vital sources, data and intelligence, so these are must-comply issues. ***Personnel security needs a robust, end-to-end system of access management, audit, vetting, counter-intelligence and insider-threat protection.*** Data fusion cannot work with ring-fenced, unconnected, high-side systems. Equally, whilst fully open and connected architectures may be unrealistic, the need to federate across boundaries and the aspiration to be as open as possible both technologically and commercially must be maintained. Aligned security policy, standards and implementation can enable the individuals to access the data that they need (perhaps with source protection) to do their job. There is an overhead, but it is one that enables sharing – rather than prevents it.

9. **ASSURANCE, TRUST, CONFIDENCE** Human nature and individual bias means that the cavalier may be wholly assured by some information that patently has no assurance – think fake news - whereas the serial doubter will trust nothing. ***We need to develop a system, culture and training where the development of trust, assurance and confidence are enabled by technology and protocols. Such a campaign would enable a more uniform and rational level of risk-taking, and establish a culture where it was acceptable for decision makers to make mistakes.*** The increasing (or are we there already?) inevitability of having difficult, controversial and – with hindsight - poor decisions investigated by frankly anyone, benign or not, with authority or not does not suggest the need for evidence-based decision-making: it compels it. That means managing risk, sometimes with very little information; but it never means just a hunch, a guess or a gamble. Without taking the fun and flair out of a military career, the reduction in gambling would assuage most senior commanders. On the technical side, the assurance can be semi-automated by tagging open-source material, attributing different values to different grades of material. Clunky now perhaps but AI and self-learning offer real opportunities.

Table 2: Risks and Opportunities attributed to Q4 Deductions

Factor	Risk	Opps
WAYS		
1. Sharing, trust, security	Security protocols block transformation; Defence becomes more risk averse.	Some enablers such as security policy and collaboration agreements exist. These are not yet systemic; remaining exceptions rather than the rule.
2. JFC Levers, Structure, Organisation	Fiefdoms, culture and ownership stifle progress; complacency.	Re-energise drive for trusted partnerships with industry. Speed it up.
3. Multi-Int Collaboration and Process	Slavish adherence to process within worthy stovepipes.	A multi-step process can be lightning fast if culture and leadership right. Must be pan-organisation.
MEANS		
4. ISS Complete (Information Systems provision)	Architecture: tie to ISS. Current architecture cannot support this.	Parallel with private equity which throws cash at first two years CAPEX, but hates OPEX
5. Data Fusion and Analytics	Aggregation and AI appear threatening.	Speed, span, accuracy; a DevOPS approach to government/industry-developed tools.
6. Culture, People, Skills	Unable to attract/retain Web 3.0 talent.	Multi-skilling; new types of employee; sell being part of world-class organisation.
7. Alternative SA: A new paradigm	Incomplete/late/lose, or infringe human rights, lose trust.	Good enough within newly defined bounds (of being poorer!)
8. Security and data Safeguarding	Denial of data access; lack of agility.	Must do; compliance.
9. Assurance, Confidence and Trust	Culture/confidence to make mistakes? Easier to plod on dutifully?	Algorithms and AI vs analyst: speed v assurance/judgement.

Table 2: Risks and Opportunities attributed to Q4 Deductions

So what?

We cannot help but be proud of what has been achieved over the past ten years and how Defence Intelligence has organised and sustained itself around a new paradigm. Despite the financial challenges facing Defence, most of the leadership, levers, programme and vision are in place to continue this progress. Modern data-analytics and integrated and agile intelligence capability was a known challenge five years ago and remains so; it does not justify in itself the declaration of a "Question 4 moment". However, the World is a more dangerous place than it was and disruptive technologies are changing the way that people think, decide and act. At the same time opportunities exist to leverage new technology and practices; and to reinforce recent success.

The answer to our Question 4 (what has changed?) is that the combination of a fundamentally new World (brave or not) and the potential to leverage new capabilities should catalyse a change to the SIE strategy – not to the <u>ends</u>, or fundamentally the <u>ways</u>, but rapid and targeted interventions to the <u>means</u> of delivery.

Points for Discussion

Factor/Deduction	Statement
FACTOR Innovation	***The agile development of software is the foundation of the modern economy and the acceptance that failing fast is better than not competing is a business imperative.***
FACTOR Managed-risk solution	***Partnering and streamlined commercial arrangements are cheaper for both defence and industry, and with appropriate assurance and competition, result in greater understanding and innovation. Time and money spent on bids could be spent on capability instead.***
FACTOR All collectors and data sources	***…one of the first tasks is to review/produce a dynamic concept of operations, against which to set and monitor user requirements, rather than defaulting to the minutiae of system requirements.***
FACTOR I2	***However, the pace and spread of events may outstrip an organisation's ability to collect and analyse, so the default source for decision-making has to be basic, open-source information.***
FACTOR New technology	***However, moving to new environments is not a simple drag and drop into place.***
FACTOR Timescale to 2022	***The baseline created by the current defence capabilities delivering Open Source Intelligence and (OSINT) and IMINT creates opportunities for further integration, development and innovation.***
FACTOR Existing processes and reality	***There is no need to reinvent the wheel.***
FACTOR Defence and security	***Interoperability must be considered at source, whilst maintaining releasability policies and intelligence-sharing relationships.***

Discussion

Can Defence adapt to a 'black box' mentality where failure is embraced as a way of learning lessons and ultimately delivering capability more rapidly?

What incentives are there for both Defence and Industry to adapt to an agile supply chain model? How does it develop an innovation mind-set?

Is the current acceptance process fit for purpose? Are DLOD leads stood up and accountable? How can the CONOPS and Benefits Management methodologies be used to underpin the acceptance process and drag the user out from under the minutiae of SRs?

Is Defence willing to adopt open-source first as an approach, with more detailed / secure source used later? (And targeted?)

How can Defence balance the perceived need for advanced technologies with the ability of their incumbents within the supply chain to provide a 'two-inch putt' to move them forward along a progressive pathway?

Should re-use of existing solutions be considered first for expansion of capability to prevent many systems providing overlapping capability, e.g. expansion of IMINT to multi-int?

Does the procurement process allow the constraints of COTS to be accounted for early enough in the lifecycle?

Shouldn't Defence make better use of what it has to form the baseline for what comes next? Can defence look to partners for some of the answers?

Who has responsibility for interoperability in a world of COTS and disaggregated procurements?

Points for Discussion

Factor/Deduction	Statement
WAYS Sharing, trust and security	***The fundamental enabler of the enterprise is the ability to collaborate through sharing your and others' data securely at pace.***
WAYS JFC levers	***With all the information levers, critically including the Senior Responsible Owner, in one command chain, there is the possibility of continuing to address previously intractable problems, such as making agile acquisition work.***
WAYS Multi-Int collaboration and process	***Aligning the different processes for the different Ints must be an enabler for fusion at pace.***
WAYS ISS complete	***…with a more-determined focus on agile commercials, moving from contracting against requirements to contracting for outcomes and benefits. Innovation must be embedded early and at the appropriate levels in the supply chain with opportunity to create interventions; critically, delivery stovepipes must be broken.***
WAYS Data fusion and analytics	***While 'BD&AI' will not guarantee information dominance, not pursuing both with vigour will likely lead to failure.***
WAYS Culture, people, skills	***Agile application development, data analytics and access management can industrialise analysis, but call for a fundamentally different skill-set and approach…… looking at simple commercial alternatives, such as outsourcing of lower-grade or less-secure products that do not need to be held at the highest levels of the enterprise, should be considered.***
WAYS SA – a new paradigm	***However, the use of crowd-sourcing offers great potential as long as risks are understood and a degree of assurance is attached to any assessments.***
WAYS Security and data-safeguarding	***Personnel security needs a robust, end-to-end system of access management, audit, vetting, counter-intelligence and insider-threat protection.***
WAYS Assurance, trust and confidence	***We need to develop a system, culture and training where the development of trust, assurance and confidence are enabled by technology and protocols. Such a campaign would enable a more uniform and rational level of risk-taking, and establish a culture where it was acceptable for decision makers to make mistakes.***

Discussion

Is this a cultural or technological issue? Or process?

How do ISS provide the necessary commercial flexibility to enable JFC to get what they want delivered?

If GEOINT is the foundation, how are the multiple Ints aligned to a consistent framework and process?

How should Defence break existing commercial strangleholds in critical capability areas?

Without exploiting Big Data will Defence 'drown' in data overload? What areas on INT / INT process will Defence allow AI to support?

Which elements of the DI capability could be outsourced to industry to deliver? How can industry help more broadly in line with a whole force approach?

Can Defence use crowd-sourcing in a similar manner to every soldier is a sensor? Will it allow analysts to focus/target on specific areas?

Do advances in commercial standards for security and a shift towards open source mean a fundamental reconsideration of the security principals and constraints applied to military capability? Consider responses to protect against the insider threat?

How can a system of confidence tags be applied to data to support assurance and trust? How does this change as data is fused?

About the Authors

Jon Rigby retired from the Royal Air Force in 2015. His last appointment was as Director of Cyber, Intelligence and Information Integration (DCI3). He acted as Senior Responsible Owner for a variety of information, intelligence and cyber programmes and commanded Joint Force Intelligence and Cyber Groups. He was responsible for the delivery of the Wyton intelligence centre and, with partners (and Ross Bailey!) the transformation of the Joint Services Signals Organisation. Jon is now a director in AlixPartners' Digital practice, co-leading the cyber practice and working primarily with Private Equity funds.

Rob Jones is a retired Army Officer who developed the ISTAR capability strategy in 2006, providing a high level vision from which much of what is discussed in this paper was developed. He has worked in the commercial world for the last twelve years, latterly establishing and then running the Programme Support Office for a major Unmanned Aerial System programme in Army HQ. Rob is a Director and Managing Consultant for XL Innovate Ltd.

Ross Bailey is a retired RAF Intelligence Officer who, for the last ten years or so of his career, led the development of an intelligence vision, its concepts, doctrine and delivery, in senior operational, command and staff appointments. On moving to industry in 2013, he continued to support Defence's quest for innovation and transformation in the intelligence and information domains. He is now a semi-retired independent consultant and triathlon coach.

FOR MORE INFORMATION

Andrew Radley
Business Development Director
+44 (0) 7773 058 807
Andrew.Radley@leidos.com

VISIT US ONLINE

leidos.com/SIE

in Leidos
f LeidosInc
YouTube LeidosInc
LeidosInc
@LeidosInc