Royal United Services Institute
for Defence and Security Studies

Occasional Paper

Intelligence, Surveillance and Reconnaissance in 2035 and Beyond

Peter Roberts and Andrew Payne

Intelligence, Surveillance and Reconnaissance in 2035 and Beyond

Peter Roberts and Andrew Payne

RUSI Occasional Paper, February 2016

Royal United Services Institute
for Defence and Security Studies

Over 180 years of independent defence and security thinking

The Royal United Services Institute is the UK's leading independent think-tank on international defence and security. Its mission is to be an analytical, research-led global forum for informing, influencing and enhancing public debate on a safer and more stable world.

Since its foundation in 1831, RUSI has relied on its members to support its activities, sustaining its political independence for over 180 years.

London | Brussels | Nairobi | Doha | Tokyo | Washington, DC

Published in 2016 by the Royal United Services Institute for Defence and Security Studies.

RUSI Occasional Paper, February 2016. ISSN 2397-0286 (Online); ISSN 2397-0278 (Print).

Printed in the UK by Stephen Austin and Sons, Ltd.

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org

RUSI is a registered charity (No. 210639)

Contents

About the Project

This research project was enabled by generous support from Boeing Defence UK and Lockheed Martin UK, both of which also shared deep knowledge regarding the ISR domain beyond simple platform information. Other companies to participate included L-3, CSC, Atkins, Raytheon, Saab, Roke Manor Research, UTC Aerospace Systems, Luciad, Sony Computer Entertainment, Kuju, Kongsberg Satellite Services, QinetiQ, 3SDL, USAF Air Combat Command, USAF 25th Air Force, 480th ISR Wg, the BICES Group Executive, Rockwell Collins, Northrop Grumman, Airbus, BAE Systems and Hewlett Packard.

Introduction

THE VAST MAJORITY of intelligence, surveillance and reconnaissance (ISR) capabilities interact with or rely on part of the electromagnetic spectrum. That spectrum ranges from waves with the longest wavelengths (and least energy), through radio waves, microwaves, infrared radiation, visible light, ultraviolet radiation and x-rays, to gamma radiation at the other end of the spectrum. Some ISR tools rely on one area of that spectrum – for instance, infrared only; others exploit radio frequency (RF) energy to send messages between nodes, for example between the sensor and the analyst.

Historically, the military has been the dominant actor within this electromagnetic environment (EME), driving advances in communication and sensor technology that exploited frequency and wavelengths to suit its own specific needs. However, the commercialisation of the EME for communications and civil usage has driven the military into smaller areas of the spectrum, although it still – potentially – needs to understand all of it for intelligence-gathering. The spectrum has become congested, at both the domestic and global level, and the freedom that militaries once enjoyed in dictating the areas of the EME that they would dominate is now severely constrained by national and international regulation, with considerable implications for future military operations, both day-to-day and combat.

This paper has been written in response to a request made by the UK's Joint Forces Command (JFC) in 2015 for an evaluation of the ISR strategy requirements of the Ministry of Defence (MoD) in 2035 and beyond. A further, key consideration is that the intervening twenty-year period is also expected to see the emergence and integration of additional technologies.

The relationship between ISR and the EME is central to this question of future strategy and military needs. As such, the research project was broken down into three distinct phases. First, the project examined how the EME might evolve by 2035, and how the interplay between the EME and ISR might alter. Phase 2 focused on the issues of emerging and disruptive technologies and how these could shape or be shaped by the future EME, as well as attempting to understand whether such technologies could be nullified by other factors. Finally, phase 3 focused on human and organisational factors, and their impact on the successful execution of future ISR operations.

A Note on Methodology

Having conducted a broad literature review to understand the published research in this area, it became clear that the relevant expertise resided primarily within industry rather than academia. Companies, however, were nervous about exposing their research, findings and future areas of investment – in other words, the sources of their competitive edge – to a broad audience. What was required, therefore, was a wide, bilateral engagement with industry and international militaries in an attempt to understand future technological trends and investment

patterns. Those individuals engaged with included military operators, representatives of military research and development (R&D) companies, cyber consultants and actors within the civilian gaming industry, amongst others. The initial findings were examined at two workshops whose attendees were drawn from the academic, military and industrial sectors, and the findings were peer reviewed by more than fifteen organisations and experts across the science-and-technology domain, including social-media providers as well as relevant research groups in the UK and abroad.

It is the outcome of this process – the tested and refined findings – which are presented in this paper in response to the JFC's initial question. It should be noted, however, that intellectual-property rules and bilateral agreements with companies over research domains prevent attribution in this paper. In addition, specific equipment types cannot be identified. Looking ahead to 2035 and beyond, these unattributed perspectives and findings nevertheless help to draw out broader themes and conclusions regarding the ISR strategy requirements of the UK MoD.

Key Factors

The project was shaped by seven critical factors that emerged as the research was undertaken.

Most importantly, there was an apparent divergence between the perspectives of militaries in the US, UK and most other European countries, and those in the rest of the world regarding how future military operations will be conducted. The former group continues to place information at the heart of future conflict. The latest expression of this is to be found within Commander JFC's 2015 'Warfare in the Information Age' paper,[1] which follows on from RUSI's own analysis.[2] By contrast, other nations, including Russia, China, France, Iran and India, continue to place greater emphasis on (and dedicate greater resources to) generating military mass. Indeed, the US Army argues that the greatest challenge to its own information-centric forces in 2035 will be the scale of an enemy's capability; moreover, technology will not always be able to solve issues of scale in combat.[3] Certainly, the outcome of conflict between a numerically superior force and a technologically enabled force could theoretically favour the smaller, more-advanced actor, but such a result is not a foregone conclusion.[4] Growing emphasis on the disruption of critical information is a clear trend on the part of adversaries, as noted by RUSI in 2014.[5]

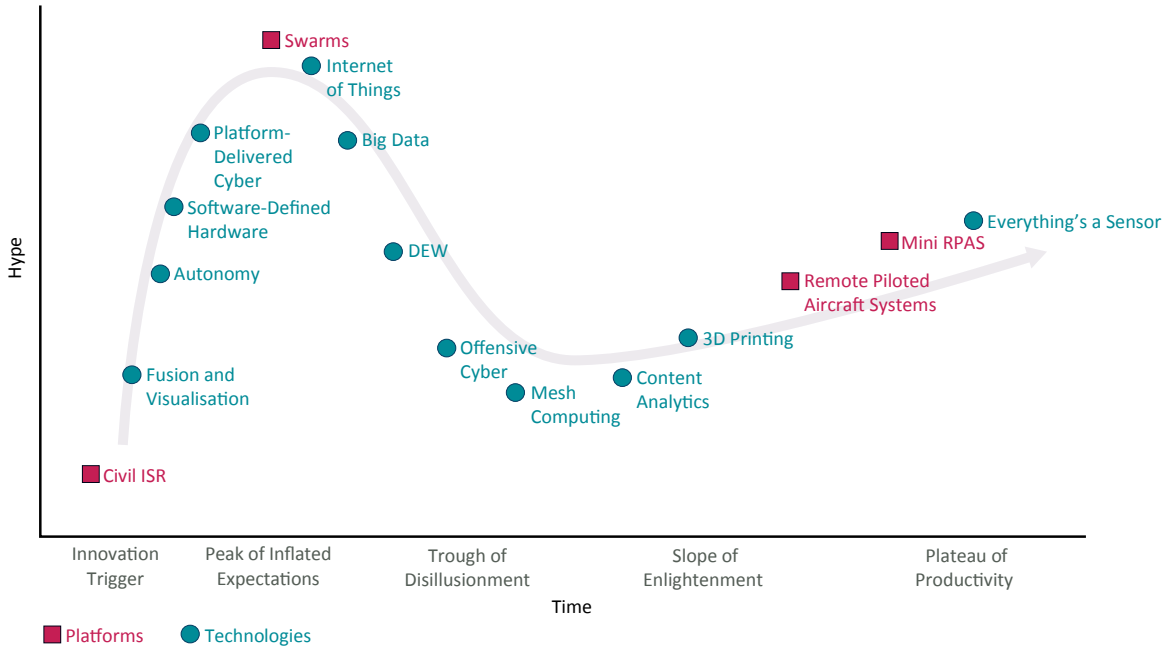
1. Richard Barons, 'Warfare in the Information Age', Joint Forces Command, Ministry of Defence (MoD), 2015. This paper is not publicly available.
2. Peter Roberts and Bill Robins, 'Maginot Line or Manoeuvrism? The Choice for Information Enabled Warfare', published in the conference brochure for the RUSI Defence Information Superiority Conference, 16–17 September 2014, London.
3. John W R Lepingwell, 'The Laws of Combat? Lanchester Reexamined', *International Security* (Vol. 12, No. 1, 1987), pp. 89–134. The debate about the role of technology in combat operations explored in this article remains the basis of US Army thinking.
4. General HR McMaster, comments made at the RUSI Land Warfare Conference, London, 30 June 2015.
5. Roberts and Robins, 'Maginot Line or Manoeuvrism?'.

The second critical factor, derived from numerous discussions with industry experts, is the tendency for largescale technological change to occur, on average, every seven years, with considerable implications for society more broadly, but also specifically for the defence and security sector. This is particularly important in terms of defence procurement and doctrine. For example, while the MoD might continue to focus on operationalising the concept of Big Data as well as incorporating social media and coding skills, these are expected to be normal business within ten years, with focus shifting to the veracity of the information and data rather than the collection itself thereafter. Such patterns are not necessarily new: transformative change within militaries has been called for in every generation, whether as a result of the advent of specific technologies or with the rise of new doctrine. When these combine, the call goes out for a Revolution in Military Affairs – evident, for example, in the buzz around network-centric warfare in the mid- to late 1990s, which was manifested in significant investment by Western militaries. Yet, ultimately, such changes have rarely had the expected impact on military affairs or on the experience of combat.

The third factor is the identification of phases in technological development linked to expectations and actual utility. Usefully, civilian companies have already mapped such research into formats such as Gartner's 'Hype Cycle'.[6] By transposing ISR technologies and emerging science onto the hype cycle it is possible to show the interplay between levels of expectation and the progress of time; Figure 1 on the next page could be an interpretation of how this area is developing. While this example is illustrative, the key factor is recognising that the curve represents the hype surrounding technologies and their failure to live up to their initial billing.

6. More information about the Gartner Hype Cycle can be found at <http://www.gartner.com/technology/research/methodologies/hype-cycle.jsp>, accessed 21 January 2016.

Figure 1: The Development of ISR Technologies, Mapping Hype against Maturity (Based on the Gartner Hype Cycle).



Fourth, recent operations in Iraq and Afghanistan placed great emphasis on information and data, but these operations were conducted within a relatively uncontested information space and benign connectivity environment. This is a key point that the MoD has yet to openly acknowledge. Commanders were able to rely on and trust the information provided to them without any cause for doubt. However, commanders at all levels also noted the increased complexity of the decision-making environment due to the volume of information available to them, necessitating analysis of apparent issues such as information fatigue and decision paralysis.[7] These experiences raise some important questions. Western militaries may have historically focused on acquiring information about the capability and intent of an adversary – rather than about its motivations – but renewed and growing interest in cultural understanding and behaviours is likely to continue.[8] In contrast, others engaged in more aggressive forms of warfare have noted that the acquisition of such information and understanding has not been decisive in military campaigns; it did not prove critical, for example, in the Sri Lankan armed

7. See, for example, Alex Mintz and Carly Wayne, *The Polythink Syndrome: U.S. Foreign Policy Decisions on 9/11, Afghanistan, Iraq, Iran, Syria, and ISIS* (Stanford, CA: Stanford University Press, 2015); Valerie M Hudson, *Foreign Policy Analysis: Classic and Contemporary Theory* (Lanham, MD: Rowman and Littlefield Publishers, 2013).
8. British military doctrine defines a threat as a mixture of an actor's intent (political and military will) and his capability to successfully pursue that intent. Evaluation of intent has not usually included an examination of the motivations for undertaking action or the cultural and behavioural considerations that shape an adversary's decision-making.

forces' (ultimately successful) twenty-five-year campaign against a determined adversary.[9] As such, the UK orthodoxy of an information-centric approach may not necessarily be valid. Indeed, one can deduce that there are key differences between the theory of an information-centric campaign and the reality of war-fighting in practice, yet such considerations do not necessarily shape procurement or balance-of-investment decisions.[10]

The fifth critical factor is that military tools derived from defence R&D have often been transferred into the commercial sector – the Internet being the most-cited example. Commercialisation of military equipment became the de facto position of commercial and military organisations. More recently, however, industry has been at the forefront of technological innovation and in the exploitation of new technologies, leading to a broad reversal of positions – with the military now often seeking to militarise commercial solutions for martial purposes. In the West, the investment in science and technology by industry is far larger than that undertaken by armed forces and ministries of defence, which are increasingly seen by traditional industrial partners as an insignificant customer from which there are smaller profits to be made.[11] There are, of course, areas in which the US military in particular has led the way, for instance in the application of sensors, in robotics, in global networks and in the exploitation of space. Arguably, the National Security Agency (NSA) and CIA have also led on the application of Big Data. In short, the number of areas in which the military is leading technological development is decreasing, but the competitive nature of military operations will always drive a requirement to be at the cutting-edge – or, at the very least, to gain an advantage over potential adversaries. Given the growing pre-eminence of industry in technological innovation, however, the result is a tension between companies wishing to protect their competitive advantage and the state, which seeks to enhance national security by exploiting new technology – and to do so as the sole customer. Within this paradigm, companies are loath to expose developing technologies and investment strategies without stringent intellectual-property agreements.

Sixth, expectations about the potential of the cyber and virtual domains are currently at their peak. There is no doubt that these domains are important, but the Western emphasis on integrating them into ISR capabilities and using them directly as weapons is driven by an infatuation with technology rather than being rooted in a sound, desirable concept of future warfare. By 2035, it is unlikely that cyber-capabilities will be seen as standalone solutions or silver bullets. Instead, the effective exploitation of these domains is more likely to involve the integration of cyber into military ISR operations and the use of cyber-capabilities to complement other weapons – in other words, the exploitation of the cyber and virtual domains

9. Raj Mehta, *Lost Victory: The Rise and Fall of LTTE Supremo, V Prabhakaran* (New Delhi: Pentagon Press, 2009); Paul Staniland, *Networks of Rebellion: Explaining Insurgent Cohesion and Collapse* (London: Cornell, 2014).
10. UK MoD FinMilCap Balance of Investment processes, as detailed within UK MoD Defence Acquisition System Guidance, available at <https://www.gov.uk/guidance/acquisition-operating-framework>, accessed 21 January 2016.
11. Van Iersel, 'Opinion of the European Economic and Social Committee on the "Need for a European Defence Industry: Industrial, Innovative and Social Aspects" (Own-Initiative Opinion)', *Official Journal of the European Union*, EU: 2012/C 299/04, 4 October 2012, <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012IE1590&from=EN>, accessed 21 January 2016.

will likely develop along the lines of current Russian and Israeli doctrine. It is also likely that there will be diminished emphasis on virtual training and simulation on the basis that these are proving inadequate in terms of both their representation of reality and their flexibility. Indeed, during recent campaigns in Afghanistan and Syria it was found that non-virtual training was more representative of conditions in conflict than anything provided virtually (even in the holographic sphere).[12]

The final critical factor is the reality that the requirements for interoperability will continue to shape, and have an increasing impact on, ISR. However, it can be concluded from the research undertaken for this project that uninterrupted ISR interoperability across joint, integrated and multinational domains is not likely to be achievable even by 2035. Meanwhile, the decline in the number of UK forces will make it all but impossible to deploy them outside of a coalition design in operations larger than small-scale engagements. At some stage before 2035, this will become clear, forcing the UK to make decisions over the areas of capability that it might best contribute to in order to support vital national interests – decisions likely shaped by the residual desire to be able to undertake sovereign action without third-party assistance. Choices about primary operating partners – be they government agencies, organisations or other militaries – will thus become the driver for future change in the UK's ISR capabilities.

A Note on Scope

It is not the aim of this paper to identify what the world will look like in 2035 – there are many different views on this already. The MoD, for instance, has already taken a view on this, as set out in such publications as DCDC's 'Future Operating Environment 2035' and 'Global Strategic Trends – Out to 2045'.[13] Less formulaic views are taken by other nations (see, for example, the assessments published by the Pentagon's Defense Technical Information Center[14] and the Center for New American Security[15]) and by other bodies (Lloyd's Register's Strategic Research Group, QinetiQ and the University of Strathclyde, 'Global Marine Trends 2030'[16]). Neither is it the objective of this paper – or the research underlying it – to draw a path from the ISR-related environment envisaged in 2035 back to today; this is a task for front-line commands should they choose to accept the paper's conclusions.

The paper does, however, seek to identify key trends within and changes to the ISR environment over the next twenty years in order to facilitate outline planning for capabilities that might be required in future. A detailed extrapolation of expected change is unlikely to be perfect; as such, a more fruitful approach is to indicate areas of R&D that are worthy of longer-term examination.

12. General McMaster, comments made at the RUSI Land Warfare Conference.
13. Development, Concepts and Doctrine Centre (DCDC), 'Future Operating Environment 2035', 1st edition, November 2014; DCDC, 'Global Strategic Trends – Out to 2045', 5th edition, April 2014.
14. Defense Science Board, US Department of Defense, 'Study on Technology and Innovation Enablers for Superiority in 2030', October 2013.
15. Paul Scharre, 'Uncertain Ground: Emerging Challenges in Land Warfare', 1st edition, Center for New American Security, December 2015.
16. Lloyd's Register – Marine, 'Global Marine Trends 2030', <http://www.lr.org/en/marine/projects/global-marine-trends-2030.aspx>, accessed 21 January 2016.

Other reports examining the key trends in defence-related scientific development over the same timeframe have focused on biometrics, robotics, artificial (or augmented) intelligence, nanotechnology and energy (re)generation (known as BRINE).[17] It is certainly possible that these technologies might continue to be deemed the cutting-edge of defence science and technology post 2035, but it is more likely that developments in such areas will have already been integrated and exploited for military and security purposes.

In any case, the use of ISR tools, permissions enabling their use, their limitations and potential exploitation pathways are going to be shaped by the environment in which they are deployed – the most important of these arguably being the EME.

17. Antulio J Echevarria II, 'Strategic Implications of Emerging Technologies', Strategic Studies Institute, US Army War College, <http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB927.pdf>, accessed 21 January 2016.

I. The Electromagnetic Environment

IN 2035, MOST ISR functions will continue to be performed within an EME, and will require a strong and resilient network; but that environment is already changing rapidly, and not in the linear way assumed by many studies of broad future trends. Such conventional thinking sees merely an expansion of current networks and the Internet into new populations in much the same way as has previously been experienced; it does not take into account evidence of a fracturing global information domain.[18] Indeed, leading-edge thinking sees the EME changing radically over the coming twenty years, shaped by governance regimes, sovereign approaches and privacy concerns as much as by advances in technology. Recent research, such as that undertaken by Jason Healey and Barry Hughes, has examined individual areas of the EME, such as the Internet, and how these might change from their current form: broadly, the expectation remains that the communications domain will be increasingly shaped by governance regimes, accessibility, cost and penetration across populations.[19] Assured access will become ever-more central to the utility of technology; yet increasingly, in some parts of the world such access will likely be contested, putting basic assumptions about information reliance into question. Given that it is difficult, if not impossible, to predict with any certainty how these various factors will play out by geographical area and over an extended period of time, it is a useful exercise to consider what might be called the 'extreme' potential EMEs of 2035 in order to better define the potential future of ISR.

The Extremes of the Future EME

In the twenty years prior to 2035, many essential activities will become heavily reliant on mobile communication, each requiring a degree of assured access to the right parts of the electromagnetic spectrum. The Internet of Things will entail tens of billions of connections, a large proportion of which will be connected wirelessly. It is likely that demand on the EME will come primarily from the civil domain – as will efforts to regulate and manage its use. The military is likely to have been squeezed out of much of the spectrum on a day-to-day basis even in peacetime,[20] replaced either by other government users or by telecom operators to which governments have sold the hugely valuable licences. On current trends and predictions, much of the global population will live in megacities characterised by intensive usage of the electromagnetic spectrum and

18. For a comparison, see, for example, DCDC, 'Future Operating Environment 2035', 1st edition, November 2014 versus research published by Jason Healey and Barry Hughes, 'Risk Nexus: Overcome by Cyber Risks? Economic Benefits and Costs of Alternate Cyber Futures', Atlantic Council and Zurich International, 2015, <http://www.atlanticcouncil.org/cyberrisks/>, accessed 21 January 2016.
19. Healey and Hughes, 'Risk Nexus'.
20. A specific requirement of equipment procurement is to train with the equipment in peacetime. If militaries are prevented from training with new systems due to frequency regulations, the acquisition becomes less likely.

the criticality of connectivity to daily life. The military and security services will require the ability to operate in such a congested environment, and alongside these other users, without causing accidental disruption. They will also need to operate in austere environments where the spectrum is much less densely occupied but also less well governed, something reflected in the MoD's intent to establish a single information environment (SIE) supported by a resilient mesh of related networks. This would allow for greater autonomy, but it would not diminish the need for governance and regulation, even though it would reduce the necessary level of bureaucracy (flatter governance structures will require contractual performance but without layers of administration and scrutiny to ensure compliance).

These two physical operating environments – the intensive and the austere – form the basis of the two extreme potential EMEs of 2035. The first, desired by telecoms and technology companies and many Western governments, sees a better-ordered, governed and deconflicted environment that is designed, regulated and policed effectively. Governments recognise the electromagnetic spectrum to be a highly valuable resource, essential to both the sustainment of advanced societies and to the development of poorer countries. The Internet of Things may become so intimately woven into the fabric of society, trade and national and global economies that it – and the communications that host it – will potentially be designated by the UN as Global Critical Infrastructure and be governed actively by new and empowered agencies. In this scenario, ubiquitous mobile connectivity is enabled through low-powered, spectrum-efficient waveforms and open architecture. Spectrum reuse is mandated, planned and exploited. The security of the EME is delivered by national and international protocols and standards which rely on monitoring, legislation, co-operation and deconfliction with industry and an assumption that encryption (at the commercial, industrial, military and government levels) is sufficiently robust to enable the level of security that underpins a permissive trade and communication dynamic. For the purposes of this report and as a concept for debate, this fundamentally communal scenario is named 'The Village' and invariably carries a significant cost overhead that is associated with infrastructure, including renewal, governance and policing. That fact alone may prevent many developing countries from following such a path.

An alternative extreme (labelled 'Favela' for ease of discussion) sees a multiplicity of potentially disconnected networks where connectivity is patchy, intermittent and conducted peer-to-peer, with constantly changing and evolving mediums of communication. In this scenario, the proliferation of inexpensive wireless-communication technologies is exacerbated by the ability of individuals to create their own network devices using fourth-generation 3D printing, exploiting the emerging technologies of today that will be ubiquitous by 2035, such as graphene-based technologies. Architectures will be highly dynamic, ad hoc, poorly maintained and unreplicated but, importantly, also inexpensive. Regulations might exist but are ineffective, the vast majority broken, ignored or abandoned and divergent from any international standards, which are unenforceable. The increasingly important global economic powers – China, India and Russia, for example – do not acknowledge the authority of existing international bodies regulating the electromagnetic spectrum and have established their own competing regimes. The spread of conformist, engineered networks, managed services and assured connectivity is slow and highly localised. Experience of one architecture does not necessarily assist in mapping others.

The environment is chaotic and not easily moulded by centrally planned investment. It exploits legacy and nationally provided infrastructure without accountability, monitoring, assurance or governance. Interception and identification are very challenging due to the volume and variety of traffic across the spectrum. Even if intercepted, new processing technology enables inexpensive open-source encryption that is likely to be exceptionally difficult to compromise, even by government agencies.

Such scenarios, although extreme, are not based on blue-sky thinking: elements of these environments exist today – as in Mali, for example. In 2014, the country experienced 17 per cent growth in internet penetration, and by the end of the year more than 75 per cent of the population had access to the Internet, mostly in the mobile-connectivity domain, which benefits from some of the cheapest data and roaming rates in the world.[21] The side effect of such rapid growth is that the networks have become a sophisticated yet chaotic environment driven by private investment, commercial opportunity and a lack of enforced governance. Somalia was likewise able to leapfrog technological boundaries and establish networks without the constraints of (and order provided by) state-driven competition, spectrum sell-offs and regulation. Rather, networks and domains evolved without the restraint or influence of an established state-based infrastructure based on affordability and need; people without land-line communication gained internet connectivity via mobile devices without first experiencing access through desktop or laptop devices. Such rapid and revolutionary (rather than evolutionary) technological development occurring at the commercial level means that state-driven regulation and processes cannot keep up – and the result is regulatory chaos and a move away from assured access. The EME in the UK, by contrast, is tightly governed through the management of technological progress and adherence to state and international regulatory frameworks, and it benefits from a population that keeps up to date with, but not ahead of, the information curve. There is some danger in expecting similar conditions in other countries when undertaking expeditionary operations that rely on presumptions of access, assurance and governance.

A ubiquitous EME design is unlikely to be available and operators will need to differentiate according to the type of operations and different requirements. Treating ISR as a service (that is, the fulfilment of reconnaissance requirements by commercial entities rather than military forces) might be an efficient approach when analysing migrant flows across the Mediterranean, for example – and would free up military assets to perform other activities. Other ISR operations might be conducted in support of deterrence (for instance, against advanced militaries from developed nations) and are therefore long-term and technical in nature, requiring specific assets and technology. Further differences might relate to the notice at which ISR assets are required and deployed: it might not be possible to find commercial solutions at very short notice in order to perform activities that would otherwise require a military surge (probably in developing nations).

21. See, for example, data available at <http://www.internetlivestats.com/internet-users-by-country/>, accessed 21 January 2016.

Furthermore, while global regulations are being established and more widely communicated – for example, through the UN's International Telecommunications Union (ITU) – fewer states are adhering to them and commercial practices are becoming more flexible and are moving into new areas in order to exploit potential market and competitive opportunities. Google, for instance, will shortly trial dynamic spectrum management for commercial users. This would allow for assured access to voice and data worldwide, without interruption to users, but it would do so by spreading connectivity over available transfer mediums, be they microwave, satellite or analogue.

This does not preclude states from maintaining well-governed EMEs, but clearly uniformity across EMEs is impossible – something that commercial entities are already seeking to exploit through new technologies. Once again, industry is leading militaries in these areas, which represents an opportunity for military leaders to reduce costs if they are willing to accept the increased risks of non-availability, and if doctrine moves away from the current centrality of information to military operations.

It is nevertheless feasible to build a mesh of related networks that are well governed and have a degree of autonomy without the chaos and competition inherent to the favela scenario outlined above. The current UK Chief Information Officer is attempting to build this approach into UK force design structures and, if successful, could go some way to mitigating favela-type environments in 2035 and beyond.

Deductions

Commercial or Niche Spectrum Management?

Deployed forces are likely to experience EMEs ranging between the two extremes outlined above and, as such, ISR equipment and processes will need to be sufficiently flexible to meet ISR requirements set by commanders and to exploit the different opportunities presented by these environments. This will be all the more necessary given that it is unlikely, in the absence of a globally ubiquitous EME, that the same parts of the electromagnetic spectrum will be available in any two areas of operations. Certainly, Western militaries will have to be able to fight in the favela scenario, even if they routinely operate in EMEs more akin to 'The Village'. Mutual interference will therefore exist and dynamic spectrum management for ISR, indeed for all military uses, is almost certainly going to be required.

It is also highly likely that commercial spectrum users will have similar requirements, which will only add to demands on EMEs. However, there may also be advantages to be gained by the military from this situation. Congestion in the spectrum affects all users, both commercial and military, in broadly the same way, meaning that commercial organisations will also need to be able to operate in the favela scenario. Commercial tools developed to do so may well prove of use to the military too, should the MoD be willing to accept the risks in terms of their future availability and suitability. There will also likely be increasing opportunities for collaboration in the development of suitably 'clever' technology through which to exploit a range of EMEs.

Such an approach also allows military forces to hide their own EME activities within the larger commercial demands, reducing the vulnerability inherent to such discrete and targetable activities by becoming part of the white noise.

A radical shift away from extensive reliance on the electromagnetic spectrum might also offer competitive advantage to the military. The alternative is procuring niche tools that serve distinctly military requirements, but this may well prove difficult given the trend towards integration – in the form of joint, interagency and multinational efforts – which appears set to widen the scope of ISR requirements.[22]

Information Assurance versus Quantity and Quality of Information?

Whatever degree of EME congestion and contest that deployed forces will experience, by 2035 there is likely to be as great a focus on the veracity – and hence reliability – of the information gathered by ISR systems as on accessing the information itself.

Historically, secret intelligence – particularly that which has been gathered covertly (for example, through HUMINT or National Technical Means) – has been regarded as providing the most reliable representation of 'ground truth'. Much of this intelligence has been transmitted around the world relatively discretely via the RF component of the EME. By contrast, open-source intelligence – freely available via the Internet – is treated with scepticism. By 2035, an increasing challenge for ISR managers will be to decide how to assign value to the different sources of information with greater confidence: should a Wikistrat assessment – crowdsourced from a pool of more than 2,000 experts worldwide[23] and rated highly by academics and regional experts – be deemed as valuable as a single-source report from a covert agent?

Correlation of ISR data across the full range of sources, using multi-level comparative analysis, will be needed – in combination with cryptographic methods – in order to provide confidence in veracity. The use of operationally responsive but inexpensive low-orbit satellites to provide relatively covert confirmatory sensor feeds will be critically important where other forms of ISR access are denied. Problems in assessing the validity of information and intelligence delivered to the commander or deployed forces will largely be determined by future developments in cryptography; another factor will be whether developments in this field (such as quantum encryption) prove to be an advantage in defending information or in attacking it. Enemies seeking to achieve asymmetric effects against Western countries will use the age-old methods of camouflage in the EME and on the Internet, as well as deception and misinformation (particularly via social media) to sow doubt, to disguise true intentions and to cause indecision. This might be

22. Comments by General Sir Nicholas Carter (Chief of the General Staff), Professor Sir Hew Strachan (Professor of International Relations at the University of St Andrews), Lieutenant General (Rtd) Sir Graeme Lamb (Senior Associate Fellow at RUSI), Lieutenant General H R McMaster (Director, US Army Capabilities Integration Center, Sir Christopher Meyer (Senior Associate Fellow at RUSI), and Lieutenant General Mark Poffley (Deputy Chief of General Staff, British Army) at the RUSI Land Warfare Conference, London, 30 June–1 July 2015.
23. See <http://www.wikistrat.com/>, accessed 21 January 2016.

particularly effective against Western democracies where politicians appear reluctant to commit to war-fighting if there is ambiguity or doubt about the enemy's intentions. In military terms, challenges and opportunities associated with such activities in the physical and signals domains may also be replicated in EMEs. As such, should the West continue to pursue 'informationised warfare' rather than, for instance, mechanised warfare,[24] early research into the portability of such activity should be accelerated to ensure the delivery of potential benefits to commanders and deployed forces.

Discriminatory Capabilities

Regardless of whether an EME is actively contested, increasing congestion – due to the civilian sector's exploitation of frequencies traditionally reserved for military use – will make it ever-more important to understand what is happening in the EME in order to limit the likelihood of deception. In addition, as potential enemies increasingly rely on information operations and on the cyber-domain as an operating environment, it will be necessary to discriminate enemy action from benign activity to prevent an adversary from hiding in the white noise of day-to-day activity.

Predicting the Nature of an EME

Approaches using linear prediction tools to predict the likely EME of a given area of interest will be flawed, given that commercial solutions have enabled both states and individuals to jump technology generations and bypass historical challenges of ageing infrastructure. Somalia, for example, has one of the highest growth rates in internet and mobile-computing penetration despite the lack of fixed infrastructure. Military prediction tools did not foresee such an eventuality in 2001.[25]

Looking ahead, there will be an increasing number of states that rapidly shift from one EME generation to another driven by commercial availability, consumer demand and reducing costs – frustrating military planners and those attempting to design forces for future contingencies. Monitoring such changes will be resource intensive for the MoD. However, commercial providers will be able to provide faster and more accurate information on demand about network and system architecture in areas of interest. Early partnering by the MoD with these commercial actors can deliver disproportionate benefits to military commanders and deployed forces.

24. See, for example, Dean Cheng, 'PLA Views on Informationized Warfare, Information Warfare and Information Operations', in Daniel Ventre (ed.), *Chinese Cybersecurity and Defense* (Hoboken, NJ: John Wiley and Sons, 2014).
25. Interview by Peter Roberts with Commander CJTF-HOA, Djibouti, 2003; Defense Science Board, US Department of Defense, 'Study on Technology and Innovation Enablers for Superiority in 2030', October 2013, <http://www.acq.osd.mil/dsb/reports/DSB2030.pdf>, accessed 21 January 2016.

The Reality of Stand-off ISR

The highly differentiated nature of EMEs and the variety and diversity of domains in which military forces might be deployed will make reliance on open-source information and commercial ISR very attractive, particularly because commercial systems will almost certainly continue to grow at a pace that outstrips military capability.[26] These systems are also likely to have the ability to penetrate areas of interest faster than the military could deploy. However, the exploitation of commercial capabilities will not meet every data requirement of a commander or deployed force; moreover, the military is also extremely likely to continue to need its own platforms and sensors that perform niche or strategically vital tasks. Those systems will need to have a high degree of flexibility, be rapidly deployable and provide persistent coverage in order to meet information demand.

The nature of the EME in which ISR operations are conducted will also depend on whether this is done at range or in close proximity. This applies to all aspects of the ISR cycle (Direct, Collect, Process and Disseminate), but especially to the Collect phase when platforms such as remotely piloted aircraft systems (RPAS) are being used in remote and dispersed operations. Such assets are likely to become extremely important to a deployed force and could buy significant leverage within a coalition. This is equally true where this is a unique capability or where an identical capability is possessed by an ally. In the case of the latter, this could enable strategic burden-sharing across ISR activities, with all the attendant advantages of operational and cost efficiencies as well as greater ISR coverage. Such niche military capabilities that have been adapted in line with technological advancements (akin to specialist SIGINT aircraft today) will thus become strategic and highly political assets. However, these platforms will be required to operate at stand-off range, given the nature of the networks against which they will be required to operate and the vulnerabilities they will be intended to exploit. As a result, by 2035, it is likely that such capabilities will continue to comprise a system of manned and unmanned platforms in order to mitigate the risks of deployment closer to the line of engagement.

Dispersal

Contested EMEs, specifically where connectivity is congested or cannot be assured, pose problems for current doctrines of dispersed operations that are reliant on reach-forward or reach-back for information, data, intelligence and command and control. Current aspirations and plans for ISR foresee much of the collection completed remotely and the results of the subsequent analysis available in the cloud for all who may require them. This methodology may founder in EMEs where such activities and connectivity are prevented or frustrated. If this vision is to be realised, therefore, the networks and cloud capabilities upon which it rests will have to be both robust and scalable in order to support deployments in austere locations as well as established home bases. The divergent EMEs of 2035 will require different approaches,

26. Google will use UrtheCast cameras onboard the International Space Station to release near-real-time images of the earth six times per day at 1-metre resolution during 2016. Jeff Kearns and Gerrit De Vynck, 'UrtheCast Acquires Deimos to Double its Space-Imaging Capacity', *Bloomberg Business*, 22 June 2015.

harnessing onboard analysis and closer, guaranteed connectivity to the customer of the ISR. Systems in which the analysis is done onboard instantaneously will generally rely on highly sensitive technology which should not be allowed to fall into enemy hands. Analysed data is also likely to be more highly classified than raw. Thus, there will also be a requirement for higher-grade cryptographic capabilities onboard. These will both be significant considerations when decisions are taken about how and when to analyse the data.

Critical National Infrastructure

The enemy will continue to seek affordable competitive advantage – so as to sidestep any early conventional military confrontation, which would entail great risk – by attacking critical national infrastructure (CNI). Such an attack may be discriminate (significant collateral damage is avoided) or indiscriminate (significant collateral damage is accepted) in form. A key element of defensive ISR post 2035 will be the ability to recognise when an attack on CNI is underway in time to deploy countermeasures before the infrastructure completely collapses. Alternatively, should the UK conduct an attack on an enemy's CNI, it is likely to undertake highly discriminate action designed to eliminate a threat while incurring the minimum number of casualties. In such instances, highly accurate ISR on the enemy's CNI will be required to pinpoint the most effective way of crippling it while minimising the number of civilians killed. This will require close co-operation and interoperability with national civilian intelligence agencies and those of key international partners.

Conclusion

The EME is the 'physics context' for – and is therefore central to – all ISR activity. Each of the deductions from the 'extreme' EMEs outlined above will be shaped by advances in technology and scientific breakthroughs. Accurate and rigorous research about potential developments in these areas is necessary to provide decision-level evidence for procurement decisions – and, more importantly, in shaping future doctrine and operating concepts. This is especially critical regarding key assumptions such as the availability of a robust, high-bandwidth network or issues such as strategic burden-sharing with close allies. By examining future technologies, including potentially disruptive ones, more detail can be added when sketching out the possibilities for ISR in 2035 and beyond.

II. Technology

A SIGNIFICANT CHALLENGE IN shaping ISR strategy post 2035 is the unpredictable and rapidly evolving nature of the technological landscape. Computing power and the number and diversity of its applications have grown remarkably over past decades and there is no evidence to suggest this trend will change markedly before 2035. This, coupled with the rapid exploitation of computing capabilities in the civilian technology sector, makes technology horizon-scanning exceptionally difficult. An illustrative example of exponential advances in technology is the mobile telephone. The first use of a mobile phone in the UK was on 1 January 1985; thirty years later, a simple telephony device has turned into a miniature, high-powered computer which is also a camera (both still and video), a multimedia player and a GPS navigation system, as well as being a phone.

Whilst predicting the future of technological advance is fraught with difficulty, a number of common themes that may come to shape it have emerged from the research underpinning this paper.

Common Themes of Future Technology

Networks

There is an assumption on the part of commercial operators that all military operations will require an assured, high-capacity, agile and ubiquitous network in 2035 and beyond. Cloud computing is already in its first generation. By 2035 a fifth-generation ISR cloud operating environment is likely to be in place.[27] This will shape some of the technologies under development; it is also likely that militaries will want their own cloud-computing networks, rather than being reliant on those commercial-transfer mediums and networks already in place. An intelligent approach to this issue will see a core of sovereign networks and a wide range of commercial, global links used in combination. Each network will have its own approach to resilience and intelligent militaries will be able to swing between them as required.

Mesh Computing

Building on the concept of cloud computing, a common theme amongst a number of ISR companies engaged with as part of the research process was the potential of mesh computing – where the ISR data is sent to wherever the processing capacity is, regardless of the network and potentially without the requirement for centralised infrastructure. In short, this processing capacity is not necessarily in the same unit, the same country or, indeed, on a dedicated ISR network. It does, however, rely on an efficiently managed and assured network, as well as automation tools to split the data across networks/units and then re-stitch it once it comes

27. Interview with senior personnel from USAF Air Combat Command.

back together post processing. The benefit of mesh computing is that it makes the maximum use of the processing capacity that exists; however, it also relies on assumptions of assured access and connectivity, excellent capacity-management systems and the ongoing centrality of human judgement in terms of analysing and prioritising the information gathered. This capacity-management issue will be returned to in Chapter III, which focuses on human and organisational factors.

Analytics

It has been claimed that 90 per cent of the data in the world today has been created in the last two years,[28] and this growth in volume of data is increasing exponentially. Whilst Big Data analytics is already a reality, the majority focuses on volume, not value – a significant gap in this area. By 2035, it is probable that analytics will have matured to the point that the value of individual reports, not just their aggregated value, can be identified (this will be an important step forward, as trend analysis that relies on sheer quantity of reports risks missing individual reports of greater value). For this to happen, however, further financial and conceptual investment will be required. An increasing emphasis on data analytics by 2035 will necessitate a change in the nature of an analyst's skill set, with a significant increase in the demand for data scientists over the more traditional British analytical art, which has previously relied on behavioural and social-science skills instead.

Fusion and Visualisation

In addition to advanced Big Data analytics, as outlined above, it is envisaged that a post-2035 ISR capability will require substantial developments in fusion and visualisation tools. Indeed, gathering the related data sets together is not the totality of the problem; the work involved in translating them into a useful and usable format, in order to minimise the need for human interpretation and interpolation, is essential in increasing the utility of Big Data. The latter in particular will require significant work with regards to the recruitment, training, development and retention of personnel, as a post-millennial generation will embrace and interact with data sets in a completely different way to the pre-Internet generation, with each generation potentially learning a whole new set of coding skills.

Autonomy and Robotics

The issue of autonomy and robotics in ISR links to both analytics and collection platforms. Several companies have stated that in a data-deluged environment human analysts will need machine augmentation while the automation of certain analytical functions will be necessary if the maximum use is to be made of scarce analytical resources. The use of automated data-fusion techniques and first-line automated movement analysis would be important steps. Embryonic automated capabilities already exist in fields such as imagery-based analytical tools to count tanks, for example, but these are still relatively crude and unreliable. In addition to these

28. IBM, 'What is Big Data?', <http://www-01.ibm.com/software/data/bigdata/what-is-big-data.html>, accessed 21 January 2016.

toolsets (once mature), technology to identify intent from the body language and behaviour of individuals, as well as automated gisting,[29] will play a key role post 2035. Autonomy and robotics will also likely be significant in enabling ISR persistence as well as in increasing the granularity of data sets, as sensors 'learn' what they are observing and highlight the salient events autonomously.

Sensors

A common theme that emerged from interviews and workshops is that no breakthroughs are expected with regard to sensing technologies, although significant development is nevertheless expected in terms of multi-spectral sensing,[30] miniaturisation and the collection of higher-fidelity images and data. Whilst what can be detected or 'sensed' may not change significantly, the opportunities afforded by multi-spectral and miniature sensors will place new demands on collection-management capabilities, as novel capabilities increasingly cascade to tactical levels of operation. The fusing of currently disparate sensor technology in particular has profound potential, especially when augmented by analytical tools and autonomy with self-cueing sensors. (Today, such a process might involve the overlaying and analysis of electro-optic and infrared imagery, signals-intelligence feeds, electromagnetic sensors, communications intelligence, historical positional information and behavioural information – a process that would use significant manpower to turn a variety of information feeds into usable intelligence.) The future will see an ability to trigger a longer 'stare' at something as a result of an autonomous decision-making process, thus saving time and man hours.

Applied Civil ISR Capabilities

All interviewees expressed the opinion that any technological breakthroughs are likely to come first in the civil sector. This marks a significant change in the relative power of civil versus military technologies. The timely and successful adoption, application and exploitation of civil technology will be an important component of ISR strategy in 2035 and beyond. This can happen throughout the ISR/intelligence cycle and can cover everything from the use of civilian radio and telephone masts to conduct passive collection, to the use of broadcast-media technologies to archive data and conduct full-motion video analysis. The ability to embrace and exploit emerging (and at times fleeting) civilian technology, applying it to the military problem set, is arguably the greatest ISR technology challenge facing the military in the post-2035 timeframe.

Multiplicity of Platforms

A plethora of platforms, from nanosatellites to autonomous surface and sub-surface vehicles, will come into operational use in the post-2035 timeframe. Many of these will primarily be civil platforms that are adapted for use in a secondary, military capacity. This increase in the use of civil platforms to host either military or civil ISR capabilities is likely to force military ISR towards

29. Gisting is the SIGINT technique which provides the general meaning of a conversation rather than a literal, word-for-word translation.
30. Multi-spectral in this case includes both the electromagnetic and acoustic spectrums.

open standards. Progress is already being made in this area, driven by costs and the need for agility. By 2035 this situation will be more mature.

Enabling Technologies

A number of generic enabling technologies have emerged which are also applicable to MoD activity, including ISR. These include new battery technology and low-power, low-bandwidth ubiquitous networks. In addition, software development was highlighted as an area in which there is major potential for improvement using advances such as automated coding.

These developments are predominantly evolutionary in nature. In addition to these, there are a number of revolutionary or disruptive technologies also envisaged for the post-2035 timeframe, whose potential effects are not yet understood. Examples include:

- Quantum computing
- Artificial or augmented intelligence
- Context-aware computing
- Synthetic biology
- Photonics
- Gravity sensing.

Technological Characteristics and Challenges

In addition to the above mixture of evolutionary and potentially disruptive, revolutionary capabilities, the research identified a number of common technological characteristics and challenges relating to ISR in 2035 and beyond. These include but are not limited to the following.

Open Standards

The use of open data standards will enable the MoD to exploit civilian technology, to make better use of its technological resources and to increase interoperability with partners.

Sensor-agnostic Platforms

The ‘plug-and-play’ approach – with platforms being sensor-agnostic and multi-mission – is superficially attractive but usually means that platforms themselves become scarce assets as fewer are purchased to perform multiple missions. As such, a decision to procure fewer multi-role platforms might preclude tasking on concurrent, geographically displaced operations, or it might necessitate a campaign design that requires mass ISR collection over large areas.

Exquisite versus Ubiquitous ISR Technology

Previous developments in military ISR capability were often undertaken over many years and in great secrecy before being very slowly rolled out to the wider military. The creation of the first

digital imaging sensors by Kodak for the US space-imaging programme is an excellent example of this. This exquisite-technology model has historically been the norm for much of the military's ISR capability; but although it did indeed give rise to significant technological innovation, it also came at an extremely high financial and operational cost. The latter became an issue as the high cost of exquisite technology frequently resulted in a very thin spread of deployed capability. Underpinning this situation was the lack of an affordable civil alternative.

However, as previously highlighted, the 2035 era will see the majority of ISR developments happening in the civil sector. Opportunities for the direct transfer of civilian applications to military ISR are likely to be very limited; appropriate, advanced commerical technologies will first have to be identified and then mapped to military requirements. Nevertheless, the possible transfer of affordable civil technologies may well see the substitution of high numbers of ubiquitous, cheap civil ISR capability for small numbers of exquisite military ISR capability. The necessary human skill will be to be able to spot the potential military ISR application of emerging commercial technologies.

Superficially, this is an enticing prospect and indeed has some merit: the use of ubiquitous civil ISR capability would certainly allow for greater operational flexibility as ISR capabilities could be more effectively massed. However, it comes with the risk that not all military requirements can be met by technology developed for the civilian market – for example, in the areas of hardened space surveillance systems, underwater hyperspectral reconnaissance sensors and signals-intercept technologies. A balance will therefore have to be struck between a proliferation of ubiquitous civil technology and also ensuring that any niche military needs not met by the civil sector can still be met by exquisite military ISR technology.

Secondary Customer Status

The major investment in ISR will come in the civil sector, not the military sector. Consequently, the MoD will have to focus on adapting technology rather than on driving technological innovation itself. This will require significantly enhanced operational evaluation capabilities within the MoD and a willingness to experiment and field newer capabilities early, accepting that some will not work. A doctrine of 'fail again, fail better'[31] will be important in ensuring both a greater ability to embrace civil technology and an increased ability to recognise what success and failure look like at an early stage.

Governance and Acquisition Processes

Extant differences in governance structures and norms between the MoD/government and industry will increasingly create problems in the future. The differences between acquisition processes across government, for example, are unlikely to deliver a coherent approach that enables integrated operations such as those outlined within the UK 2015 SDSR.[32] This

31. Samuel Beckett, *Worstward Ho* (New York, NY: Grove Press, 1983).
32. The system utilised for developing the MoD's IT requirements is the CADMID cycle (Concept, Assessment, Development, Manufacturing, In-Service and Disposal). This is in contrast to the

is particularly true with regard to spectrum management and information management and security, where divergence of processes across government has often necessitated increased resources to mitigate differences. In 2014, for example, the MoD had to pay the Treasury a significant sum for using frequencies in parts of the electromagnetic spectrum that had just been sold to commercial telecoms companies. Governance issues will also assume greater significance in relation to contracted ISR services, such as the use of commercial satellite imagery for targeting or the harvesting of open-source intelligence (and the questions over privacy rights that this raises). In addition, longstanding governance structures and legacy acquisition procedures also make it difficult to embrace and exploit new technologies. This calls for greater responsiveness by technologists, a more dynamic, fast-track C4ISR acquisition process and a much better dialogue between the defence industry and the intelligence communities – a series of processes that fall under the Whitehall governance remit.

Broader Technological Challenges

Ethical, Moral and Legal Considerations

The debate over automation and remotely piloted vehicles in ethical, moral and legal terms is only just maturing, and is characterised by divergent national views on use and employability. Whilst the US appears broadly content to pursue greater technological autonomy of its military equipment and processes, there seems to be less willingness to do so in Europe.[33] Policy decisions and court rulings on such questions today could have profound impact on the employment of autonomous processing as well as autonomous and unmanned vehicles in the future, but have only come to light after nearly a century of unmanned flight.[34] It is certainly likely that as public understanding of the scope and potential of ISR increases, similar questions will be posed regarding the armed forces' capabilities in this regard, with one potential outcome being the restriction of the use and exploitation of such tools, even within a military capacity.

Permissions to Operate

As rulings are established and societal attitudes towards ISR develop, it is also likely that the use of military ISR technology will require political approval, as is currently required with regards to the police and security services. Certain ISR capabilities such as communications intercept are governed by a robust legal framework but new capabilities and activities such as the data mining of open-source information and imaging may require new and specific permission. It is likely that ISR missions will therefore need a new set of deployment rules, along the lines of those

Cabinet Office's digital-service delivery model, which follows the five-step Discovery, Alpha, Beta, Live and Retire structure.

33. The European Commission made its Riga Declaration on remotely piloted aircraft systems in March 2015. The European Aviation Safety Agency published its 'Concept of Operations for Drones' in May 2015, and the Joint Authorities for Rulemaking on Unmanned Systems agreed its new Terms of Reference in mid-April 2015, <http://uvs-info.com/index.php?subid=10229&option=com_acymailing&ctrl=url&urlid=279&mailid=249>, accessed 1 February 2016.
34. John Keane and Stephen Carr, 'A Brief History of Early Unmanned Aircraft', *John Hopkins APL Technical Digest* (Vol. 32, No. 3, 2013).

for the use of force, known as rules of engagement.[35] While harmonising such a process early would be advantageous, the key for commanders will be in understanding the permissions and freedoms that all ISR providers across a coalition have and then employing them appropriately.

The Limits of Commercial ISR Tools

The development of commercial tools will continue to lead military R&D in nearly every area. The depth, persistence and variety of commercial tools will increase, costs will be reduced, delivery timelines will shorten and refresh rates will be greater. However, industry will almost certainly neglect areas of technology or battlespace where there is little financial gain or in which there is limited interest. As such, militaries and defence ministries will need to fill these niche-capability gaps, meeting the associated developmental costs. Given the expectation of diminishing profit margins in these areas, there will probably be fewer traditional suppliers to choose from and the MoD ISR community will need to become a far better customer in order to continue receiving the preferential treatment it has thus far experienced. Conversely, there might also be many more ad hoc providers prepared to undertake ISR processes and sell their services to a broader customer base – including, but not limited to, the military, with other potential customers such as oil and gas companies, extraction firms, the agricultural sector, fisheries and so on – thereby spreading their costs.

Achieving a Competitive Edge

In Favour of Offensive or Defensive ISR?

Uncertainty over what technology will become available, when and what impact it will have on operations – and indeed on ISR requirements and capabilities specifically – is not new. The real question for the future is how technological changes will provide net advantages to defensive or offensive military operations, and whether such net impact could be decisive.

Such debate is perhaps at its most mature on the future of commercial quantum cryptography (the exploitation of quantum mechanical properties to perform cryptographic tasks). While it can be argued that a breakthrough in the availability of infinitely powerful encryption devices will ensure complete privacy and deny access to state intelligence agencies to all forms of communication, rendering some forms of intelligence-gathering impossible, it is equally possible that such an advance would see a return of intelligence professionals to an ISR domain that is not reliant on encrypted communications (such as geospatial analysis and HUMINT). There is a *post hoc* fallacy to prediction is this domain,[36] and therefore it is unwise to guarantee an outcome one way or another. However, the most likely outcome is a continuation of historical trends that have seen net advantages accrue to both offensive and defensive ISR activity, but that none will prove sufficiently decisive to transform intelligence and military activities as a whole.

35. The UK documentation for rules of engagement is Joint Service Publication 398, which already governs the use of electronic-warfare tools by the military.
36. Sir John Scarlett, remarks made at 'SDSR Breakfast Briefing: Pan-Governmental Intelligence and Information', RUSI, London, 4 February 2015.

Indeed, technological advancement alone will be of limited use to the military in creating a competitive advantage in the ISR domain. The critical changes are likely to rest on how ISR professionals deal with the information such technology will provide access to, as well as in the organisation at the operational level and the processes built around these capabilities.

III. Human and Organisational Factors

WHILE ISR IN 2035 and beyond will be both enabled and frustrated by the EME and technological development or breakthroughs, the key terrain will be the role and activities of humans and the organisation within which they work. Some specific issues in this area were drawn out from the research undertaken in phases 1 and 2 of the project, which examined the potential evolution of – and the impact of emerging and disruptive technologies on – the EME. This section homes in on the human and organisational factors in more detail, drawing out thematic issues that are central to MoD plans to maximise its investment in ISR.

Agility

Although the structural issues underpinning MoD procurement challenges are beyond the scope of this paper, it is worth highlighting that every technology company engaged with during this research project expressed the view that the MoD process builds delay and cost into contracts, with the bureaucratic and cost burden remaining the same irrespective of the size of the contract. The prevailing view was that these processes make the MoD a highly inflexible and unappealing partner. There is a significant mismatch between the rate at which industry is able to develop technology and the pace at which the MoD is able to contract, embrace and exploit it – with one interviewee suggesting, for example, that a major MoD intelligence system was only upgraded to Windows 2003 in late 2014.[37] Such a lack of synchronisation in gearing is only going to be exacerbated as technology develops.

The current MoD procurement model does offer options – such as the Urgent Operational Requirement process – through which to procure equipment at pace, but this is the exception rather than the norm. In a post-2035 hi-tech ISR environment, the reverse is likely to be true: the routine and long-term procurements of today will be the exception as new technologies will have to be brought into service at pace.[38] The revised (2015) commercial model for Joint Forces Command might, eventually, underpin the MoD's communications networks sufficiently to enable ISR users to be more agile in future, but so far has yet to deliver a coherent approach. Other approaches have had more success. The Acoustic Rapid Commercial Off-the-Shelf Insertion sonar upgrade process now used by the navies of both the UK and US is an exemplar of how spiral development – pioneered by the UK's Defence Intelligence Staff at the end of the twentieth century – can be made to work very powerfully.

37. Interview with MoD employee, May 2015.
38. The corollary to this is that these technologies will also have to be taken out of service at pace, so a more flexible view of capability will be required.

In addition, much has been made in recent years of delivering systems and networks that are both agile and resilient. Even if providing both were financially possible, conceptually these two requirements may be lead to dissimilar solutions. Agility in ISR terms might best be provided by a single domain or network with a common architecture and operating system. Such an approach, however, presents a single target vector to adversaries that runs counter to the principles of resilient systems that have multiple architectures, sensors and networks. These differentiated systems create a form of resilience and redundancy by default, complicating the challenge to the aggressor. Agility and resilience are not, therefore, mutually supporting when undertaken in an environment of resource austerity. By 2035, advances in technology are unlikely to have overcome this hurdle: single systems, indeed single paths in any domain, will be less resilient to attack and harder (and more costly) to defend.

Capacity Management

As concepts such as mesh computing evolve, it will not just be the technological networks and network infrastructure that will need to be carefully managed. A data-deluged analysis community will also need to be carefully managed in order to maximise its capacity. Consequently, a post-2035 ISR strategy will require the ability to send tasks to where the analytical capacity exists. This poses significant challenges in terms of personnel management, tasking authority, management procedures and career structures. More will need to be done to increase the return on investment in training analysts and to ensure that analysts are actually used for conducting analysis. It is also important to note that post 2035, it is likely that an increasing amount of ISR activity will be contracted to non-governmental entities, whether they be behavioural scientists, human geographers, open-source intelligence analysts or platform or sensor operators. This will help to create flexibility within the MoD's ISR capacity.

Understanding

While technological advances will drive many of the developments in ISR by 2035, and particularly in data exploitation, there will remain a requirement to understand the operating context at a human level. Contemporary conflicts have shown the importance of having an understanding of tribal dynamics, for example. Such matters of human geography and ethnolinguistics may continue to be important for the execution of military operations in the future. Developing and sustaining this type of understanding is exceptionally challenging, especially within the military, and it is likely a balance will have to be struck between maintaining a core, in-house capability and knowledge of the civil and academic marketplace for this type of expertise.

Legal Issues

For the MoD to exploit the ISR capabilities available in the post-2035 timeframe, new legal frameworks will need to be put in place that set out how civil ISR capabilities can be used for military purposes, where any liabilities may lie and any privacy issues that may arise. In addition, current legal frameworks covering, for instance, intercept capabilities will also likely require regular revision in order to cover rapidly evolving technologies.

Within an increasingly legalistic framework of military campaign design, commanders may also have to better articulate and minimise risk before deploying forces. Such a move would require commanders and troops to have access to the best possible information and intelligence before being put (or putting others) in harm's way, increasing the importance of and requirement for pre-deployment ISR. It will also be necessary for deployed troops to have a similar level of access to ISR as the political and operational decision-makers, so that they are continually aware of the risks in the deployed environment.

Human Factors

The ISR operators[39] of the post-2035 timeframe may require a very different skill set to their counterparts today. The balance of capabilities between analytical art and analytical science is likely to change markedly as analysts will need to be increasingly adept at using data-mining and fusion tools. That said, the purpose of the analysis will remain the same: to influence, inform and empower commanders at every level of military operation. Consequently, some traditional analytical skills will still be required, although analysts may well benefit from additional training in behavioural science to improve their ability to distil complex analytics into a message that the commander they support better understands.

In addition, the new generation of ISR operators will have a very different way of thinking about, visualising, exploiting and utilising data. Consequently, training for ISR operators post 2035 will need to be far more attuned to their extant abilities and needs, as well as to the specific technology they will be using. The key issue by 2035 will be that the high-volume 'data deluge' will be handled autonomously, as will the very rapid-reaction challenges that are beyond human capacity. Therefore, analysts will need to understand how the computers running the automation are programmed in order to understand, in turn, what the solutions provided actually mean. These are sometimes referred to as cyber-physical systems.[40]

On-Demand ISR Services

A model of ISR provision – currently embryonic in form and being developed only within the civil domain – is on-demand ISR services. Under this model, the first step is for customers to specify their requirements; the collection of these requirements is automatically identified and the information is then fed to the customer. Breaking away from the process-driven frameworks currently employed by militaries (which automatically fuse the data collected and alert analysts to data requiring their attention) could see the establishment of a more flexible set of rules. This would allow the military customer to use these capabilities more intelligently according to the case in hand, thereby maximising the utility of the end product. For example, the combination of space-based sources (RADARSAT) and the global Automatic Identification System (AIS) data

39. The term 'ISR operators' includes all those who are engaged in ISR operations. This includes platform operators, network engineers and analysts.
40. Radhakisan Baheti and Helen Gill, 'Cyber-Physical Systems', in Tariq Samad and Anuradha Annaswamy, 'The Impact of Control Technology: Overview, Success Stories and Research Challenges', IEEE Control Systems Society, February 2011, pp. 161–66.

can be used to fill capability gaps in C4ISR in the maritime domain and has tremendous potential in delivering a modern, user-driven capability. In addition, on-demand ISR services may also help to address the increasingly complex collection-management issue. The possibility of a subscription-based ISR service available on demand – with customers shaping the end product more directly – has significant allure. However, it does come with significant challenges in terms of role-based access controls, automation, filtering, fusion and the ability to move a myriad of different ISR data sets around a common network.

Potential Impact

The impact of the factors outlined above on the 2035 ISR landscape will be significant. It may be that some of the potentially negative consequences will be partly addressed by technology, but the conceptual challenge posed by a dynamic ISR and data environment to traditional military command structures should not be underestimated. Potential information-flow requirements should inform both the network construct and also, crucially, the command structure. Agile management of the system capacity – both human and machine – should ensure that, in the 2035 ISR environment, more can be done with less and, critically, that the capabilities available are utilised to the maximum extent.

Conclusions

THE BRITISH MILITARY continues to assign great significance to technology in conducting operations and planning for future conflicts. Yet, as highlighted by many military leaders and scholars, a reliance on technology does not in itself guarantee victory. Nevertheless, while technological superiority and victory are not inextricably linked, the former has remained an important factor in fighting, particularly when time, space and scale are limited. Placing too great an emphasis on it at the expense of tactics, training and procedures is not wise, however; and to do so without the investment in mass to exploit the information is to court disaster: the ultimate humiliation is to know everything and to be able to do nothing.

These statements are especially valid for ISR in 2035 and beyond. It is certainly possible to achieve technological advantage within that timeframe against peer adversaries, but there is risk in assuming a linear development in the EME. Over-reliance on technology to deliver ISR might be undone quite easily in a contested and congested environment when data, and thus perceptions and actions, become easier targets for an adversary to shape and change. A commander who is entirely reliant on analysis conducted remotely, for example, might be lost if that connectivity is undone – or worse – when the product he receives is in fact written by his enemy. A balance is therefore necessary between reach-forward and reach-back analytical activity with the relative risks and advantages of both being an explicit part of any estimate. In addition, a far more effective capacity to embrace and exploit emergent and fleeting civil technologies is required. Critically, in the post-2035 landscape this will have to be done at tempo, with capability being rapidly delivered.

In reviewing the research, several questions need to be addressed in order to forge an ISR strategy for twenty years hence.

First, is it more effective to procure equipment with a lifespan of twenty years which is at risk of becoming obsolescent; or is it better to wait for an operation and purchase the latest technology at that stage? This decision must take into account risks to training, the development of tactics and interoperability with allies, as well as wider consideration of whether a force designed on the basis of last-minute procurement forms a worthy deterrent between campaigns.

Second, and largely dependent on the answer to the first question, is the balance struck in the investment strategy between platforms and payloads. A longer-term commitment to rely on common payload size, common connectivity and open architecture would open up significant benefits to the manufacturers of sensor payloads and platform designers. Making such a decision would mitigate risk in the procurement of long-life platforms and enable them to be rerolled while also increasing their utility across the spectrum of military tasks. In the absence of such a commitment, military budgets may continue to be constrained by large, generational purchases of capabilities that risk becoming obsolete within a decade; resilience would also be a matter

for concern if a common standard were to come into use, as it would provide a clear target for adversaries – and the cost of defending it would rise proportionately.

This points to another key factor: the risk appetite of militaries and governments. Any strategy for ISR in 2035 and beyond will need to determine how much emphasis should be placed on sovereign capabilities, and the willingness to purchase and integrate commercial technologies, foreign military equipment and non-Western ways of operating within the force design. This is not an easy conundrum to solve, but could be answered by outlining the future command and information structures around which functionality and technology could be integrated.

Even once technologies have been embraced, the legal, moral and ethical dimensions of their use are likely to continue to vex commanders and force designers. This post-2035 ISR landscape will be further complicated by the absence of homogenous rules, governance and freedoms across allies and coalition members: these factors are more likely to be shaped by the strategic culture of each state, associated with its ambition, vital national interests and political outlook. In this way the use of ISR assets and the associated data might be akin to the differentiated rules of engagement employed by states for the same mission. Understanding and exploiting these differences will be important for a commander in succeeding on operations.

The employment of ISR capabilities, and the processes underpinning their use, will continue to morph. Regardless, it is likely that their utility will never be maximised in the UK due not only to conceptual concerns, but also to the lack of appetite on the part of British citizens for the intrusion of such capabilities into their lives – although, by and large, they do not appear to have such qualms over the use of such capabilities in relation to (potential) adversaries. Such restrictions will surely frustrate commanders who will know the potential of such ISR capabilities but will be unable to exploit the knowledge they might provide during operations – unless views on this matter in the UK shift markedly. Acceptance of – and permission for – the use of ISR tools will need to become embedded within the political culture relating to conflict and security. In this regard, conflict and operational experience of the benefits of ever-more advanced ISR capabilities will likely facilitate a mature debate on the subject, ultimately resulting in more lenient permissions being granted to operational commanders. If there are fewer military deployments, this will stymie such advances.

Finally, there remain decisions to be made over the relative importance of the six domains[41] within the UK's defence efforts. In relative terms, UK ISR capability in the space and maritime domains is marked by underinvestment. Whilst the current hype over cyber-capabilities places the cyber domain at the centre of plans for future capabilities, there remain several key aspects of ISR in the post-2035 timeframe that will need to be addressed, not by technology but by

41. The number of domains used by states differs according to their respective doctrines. The historically ubiquitous air, sea and land have seen additions of space, cyber, information and cognitive domains by various countries over the last decade. While the conceptual debate continues, there remain concerns that ISR capabilities are expected to deliver in all domains but cannot necessarily do so in reality, giving rise to the dilemma over where to invest limited resources.

an adaptive command capability that has the authority to send ISR tasks to wherever the execution capacity is. That execution covers the full ISR cycle from Collect right through to Process, Exploit and Disseminate. Implicit in this is the technological ability to send tasks to the available analytical capacity, or to be able to do without. While this requires common standards and tactics, techniques and procedures, it will be important that these open standards are not turned into dogma, which might prevent niche technologies from being exploited by the military. Acknowledging this makes clear that ISR solutions are unlikely to have ubiquitous capability across the world, and niche military solutions must continue to be fielded in support of the UK's vital defence and security interests.

Key Findings

- A post-2035 ISR strategy will require the ability to send tasks to where the collection, processing and analytical capacity exists. This approach to capacity management stretches across single-service boundaries, across government, across industry and amongst key allies
- Technological breakthroughs are likely to come in the civil sector first, rather than in the military sector. Thus, capability brokering – in order to embrace and exploit civil technology – will be an important component of ISR strategy in the post-2035 timeframe
- There is a significant mismatch between the rate at which industry is able to develop technology and the pace at which the MoD is able to contract, embrace and exploit that technology. The question of how the military can best mitigate this discrepancy and harness new capabilities at speed will need to addressed in order to improve its effectiveness within the ISR field
- The increasing use of civil platforms to host either military or civil ISR capabilities is likely to force military ISR towards open standards
- While Big Data analytics is already a reality, the majority focuses on volume not value. It is possible that in the 2035 timeframe analytics may have matured so that is used to identify the value and veracity of individual reports
- Increased data volumes will require big developments in fusion and visualisation tools
- Human analysts will need machine augmentation and the automation of certain analytical functions in order to deal with quantities and complexity of the information provided by advanced ISR
- Autonomy and robotics will also likely play a significant role in enabling persistence as well as in increasing the granularity of data sets
- No breakthroughs are expected in sensing technologies, although significant development is expected in terms of multi-spectral sensing, sensor fusion and miniaturisation
- In a post-2035 hi-tech ISR environment, it is probable that the routine and long-term procurements of today will be the exception, as new technologies will have to be brought into service at pace
- An increasing amount of ISR activity will be contracted to non-government entities
- The post-2035 training for ISR operators will need to be better attuned to the needs of personnel and the technology they will be using, with a greater requirement for personnel to be trained in scientific data analytical techniques.

About the Authors

Peter Roberts is a Senior Research Fellow at RUSI who runs two research programmes: Sea Power and C4ISTAR. He was previously a warfare officer in the Royal Navy who served with each of the British armed services, and with international allies in the intelligence and surveillance domain. He is a visiting lecturer in strategy at the University of Portsmouth School of Business and Law, and is a Fellow of the Chartered Management Institute.

Andrew Payne is a Visiting Fellow at RUSI. He is an RAF intelligence officer with more than twenty years' experience in the ISR domain. Andrew has a Master's degree in International Relations and Affairs from Leeds University.