GLOBAL STRATEGY FORUM

EDITION No. 17 - JUNE 2020

The 17th in our series of expert comment and analysis, by General Sir Richard Barrons, Commander Joint Forces Command (2013-2016), now Co-Chairman of Universal Defence & Security Solutions, and GSF Advisory Board member. As always, the views expressed are those of the author and not of Global Strategy Forum unless otherwise stated.

Weaponising The Nerds: Artificial Intelligence For UK Intelligence And Policymaking

There are 58 million smartphone users in the UK and about 90% of households have some flavour of home computer. Perhaps only 10% of the population is not assisted by the Artificial Intelligence (AI) that brings most of us our information from Facebook and Google, our stuff from Amazon or eBay, our telly from Netflix, and the unfiltered opinion of anybody with thumbs from Twitter. These are amongst the wonders of having 100,000 times more computing power in our pocket in 2020 than landed man on the moon in 1969. Another wonder is that everybody who does carry a smartphone is a sensor, taking photographs, registering movement and location, recording contacts and purchases, and communicating facts and opinion – inexorably contributing to the 4.4 Zettabytes (a Zettabyte is 1 with 21 noughts after it bytes) of data so far that is piling up around the world.

The internet is not all pictures of cats, although there are 85 million cat videos on YouTube alone, and only 4% of the web is pornography. With 1.75 billion websites and counting, the internet is a store of information so large and growing so fast that no one person could ever sort through it for a vital nugget. AI can do that. The internet is only really useful when AI manages it for us. So AI is truly vital to getting the intelligence needed by Governments and Armed Forces and to making policy. It must be time we worked how to do this well and got on with it.

Intelligence is conventionally grounded in a well-refined, analogue way of working in which trained analysts build expertise in particular subjects, providing general insight and answering questions. When faced with a new situation or a specific question an analyst will design a collection plan to try and answer it. This may rely heavily on the three traditional secret intelligence sources of: communications intelligence (listening to telephone conversations or remotely poking about unobserved in computers); human intelligence (just chatting to people who know or persuading others to reveal or steal what they should not); and image intelligence (what can be 'photographed' from the sky or space with cameras, lasers and radars).

A good analyst will invest in a network of fellow experts and be an assiduous reader of what is freely written and disseminated. We already have ever-better software to catalogue and connect pieces of information, greatly stimulated by the need to uncover, understand and target well-concealed cellular terrorist networks, especially since 9/11. This system leads to the writing of erudite reports, peer-reviewed material - perhaps with some images attached. And whilst all of this is going on, the Minister in her office and the General in the field still get first sight of an event and the first explanations from the TV, and still Google the internet from their phones for more, quicker (and unverified) information.

The case for transforming support to intelligence and policy making around Digital Age capability is clear: there is so much more data to be found via the internet and other sources than closed government systems can ever deliver. Not only so much more, but also in many cases both available and useful in real time.

If you want to know what is happening on Regent Street you could ask someone to go and take a photograph and write a report, ring up some shopkeepers, ask Transport for London (TfL), and fly an aircraft over it. Or you could tap into the picture of every mobile phone on the street in real time, the data from TfL that shows bus information in real time, the street CCTV that shows the street right now and could be linked to facial recognition, the private security CCTV in each shop, and maybe footage at 2m resolution from a commercial low earth orbit satellite that is passing overhead. This data is created all day every day, so when routinely collected and fused by AI over a period it will reveal patterns that are instructive and predictive, making it possible to detect the unusual as it happens.

We need to convert the business of intelligence and policymaking from reliance on the closed, secret government-owned systems to an intelligence system that operates more like a newsroom. This is a capability that constantly monitors what is going on in relevant parts of the world through the mass of open-source information and pushes this awareness to decision-makers in an intuitively useful and convenient way (such as to their phone) – as well as answers their questions. Doing this well requires: access to as much data and in real time as possible; the technical capability to collect, fuse, analyse, and present much of it automatically and without human intervention; the visualisation, modelling and simulation to display and interrogate the information; and the secure networks to convey intelligence and information to users.

Almost none of this removes entirely the need for some humans to own and direct the system, to make judgements about its product and to decide what to do. Machines will remove quite a lot of human labour currently involved in collecting, collating and presenting data, but they will not replace the intuition, creativity, and capacity for lateral thinking of a skilled analyst, policymaker, or minister.

Not much of this transformation process in Government will mean breaking entirely new ground because the technology in whole or in part is already well established in other sectors. Artificial intelligence is led by the major information technology companies as the key to their commercial success. This is how 3.5 billion Google searches a day are turned into individually targeted advertisements for 4.4 billion internet users in hundreds of languages, and why Amazon spends $22bn on R&D each year.

Cloud technology is led by companies such as Amazon, Google, Facebook, HP, and Oracle, as (so far) only companies of this size are able to offer large customers (including the CIA and US DOD) scalability, access to constant innovation, and layers of security. It does seem likely, however, that sensible concerns about where data travels and where it is stored will lead to a preference for sovereign data storage in some cases, so that governments are sure that sensitive information only passes along limited and secure pathways to a place they control. UK Govt already has a clear policy encouraging the adoption of Cloud technology, but some degree of UK-based Cloud architecture for Government is likely to be necessary, perhaps spurred on by the international chill created by the COVID 19 pandemic.

In adopting AI, the challenge for UK intelligence providers and policymakers is to recast themselves around technologies they have never had and do not lead in, by working with technology experts some of whom don't think or care much about government. Innovation in Cloud, processing power, AI, simulation etc., is coming from a mix of very big companies, small and medium-sized enterprises, and universities. Most of the engineers leading the way are youthful, many also subscribe to a technocratic, liberal and individualistic culture that is rarely interested in public policy and certainly not defence and security matters – even sometimes prejudiced against it. Google withdrew from the US DoD's AI Project Maven (worth only $10m) in June 2018 as a result of employee pressure.

Yet the very worst approach now would be to try and retrain civil servants or military personnel to become competitive in building their own bijou Cloud, algorithms and models. There are some very good experts in Government science posts, in Dstl and GCHQ, but relying on reskilling beyond these would be like trying to build a jet fighter in a garden shed with instructions found on the internet and parts sourced at B&Q. Better answers are already functioning in the private sector.

The level of technological understanding amongst non-technical officials who will need to lead this transformation is patchy, as it is in many other long-standing institutions, and not helped by the way Whitehall generally does less well at pan-Department coordination than it does when working inside clear Departmental boundaries. Data is still sometimes seen as something best managed by keeping one's own supply secure and isolated. This has led to Departments having exclusive data sources and bespoke visualisations - and therefore competing sets of situational understanding and conclusions. Instead of one big, build once and use many times Government data store we still have many little data compartments scattered up and down Whitehall, even if these too are actually stored in a Cloud somewhere rather than on a server under the stairs.

The power of AI is only unlocked by accessing as much data from as many sources as possible: new insights and options can be drawn by AI examining far more data than a human could possibly stomach to detect hitherto unfathomable correlations and connections. This is why China, with access to the data arising from the thoughts and habits of 1.4bn people, can find immense commercial opportunity and understanding in a way that countries of just a few 10s of millions and more restrictive data laws cannot. Similarly, there can be too much focus on algorithms and too little on the data these algorithms explore. A

brilliant algorithm working on an egg-cup's worth of data is not progress. But algorithms are also not straightforward: they inevitably reflect the bias of the authors and their usage, so different algorithms applied to the same data sets will usually lead to different conclusions. Should intelligence and policymaking be supported by algorithms that match the inclinations of the officials who employ them, or be carefully selected to balance them, or should there just be a way of exposing the differences?

How can the best private sector expertise be drawn into supporting intelligence and policy? It means aligning the public servants (who understand the problems they need to solve and have immense subject matter expertise but limited capability in digital tech), with technology and technologists (who can innovate and develop at great pace and originality, but often have little feel for specific subjects). The conversation between them is much more about breath-taking application than breath-taking innovation. This conversation needs to avoid being either only with the big, conventional suppliers in suits or only with small companies dressed for the beach. Major, established players have highly skilled and well organised technical expertise and deeper pockets, smaller players provide different sorts of creativity and innovation. Both have a role to play in new and more agile capability and service delivery formats based on enduring collaboration.

What options are there for organising this collaboration? It would be possible for HMG to buy a suitable firm or hire talented individuals and make them public servants (on a special pay scale no doubt) but ownership in this way will be expensive, limit scalability and exclude access to wider innovation. More likely models include either buying capability in as a contracted service or forming a joint venture. Both models will have some challenges in common.

First, who owns and benefits from the IPR that a combined effort will develop? The government side brings its understanding, its definition of the problems to be addressed, and leads on the conclusions to be drawn; industry brings access to wider data sources, algorithms to choose from and the ability to refine them. After a period, once data sources have been better sourced and structured and the algorithms have 'learned' to the point where they are uniquely identifying features, patterns, and anomalies and recommending better options, a very valuable capability will have been created. This is valuable both in terms of its exportability to other users (public and private) and valuable as an intelligence target for hostile actors. Should the commercial partner be allowed to take what has been created and sell it elsewhere, and if so should HMG also see a financial return – or expect the service it receives to be free or at least heavily discounted as a quid pro quo? Industry will bid for this work for the return to shareholders and officials will judge value by effectiveness and efficiency – and both parties have an interest in making a partnership work.

Second, how is the security and cyber resilience of such an arrangement to be assured? Will all the technical engineers who build the applications that are brought in from the private sector have to be vetted to an enhanced level? The time and cost considerations will be substantial, and many of the engineers needed may resent the intrusion. It is equally important to be sure about the integrity of: the data that is sourced; where it is stored; the AI that manages it; the outputs that occur; and the distribution of that output. Any hostile power will certainly be interested in fiddling with data sources, interfering with what

is done with it, and seeing what the results are. There does seem to be no alternative to more private sector expertise becoming formally vetted, which of course already happens now with many defence and intelligence contractors.

Yet if a great deal of data is open source and freely available, at least some of the support can be done 'outside the wire' and drawn up into higher levels of classification on a one-way journey. This needs a more thoughtful approach to digital security risk management than a one-size fits all model can confer.

What would a model for bringing AI into intelligence and policy making look like? Here are some broad conclusions:

- It requires commitment to a transformative, disruptive process that over time puts data and digital technology at the heart of intelligence and policy-making, building new organisation and method around it. This will bring the pains of dislocation as well as the joys of revelation.

- This can only be done with the secure Cloud, AI, visualisation, and networks capable of exploiting the vastness of data that is mostly connected to the internet. This needs private sector expertise.

- It requires Government to partner with commercial technology providers in a committed, collaborative arrangements with well-defined terms for sharing benefits and accrued value. It cannot be a distanced, transactional arrangement.

- Information security and cyber resilience will be a core requirement, based on an intelligent and agile risk management approach.

- There must be a structured approach to the education and training of officials (and politicians) to understand the potential of AI for their work so they can partner better and make maximum use of the power about to be put at their disposal.

HMG could do none of this, leaving the exploitation of data in a data-centric world to others, but then explain to us how this makes us safer, more prosperous and better governed?

General Sir Richard Barrons
June 2020

Commander Joint Forces Command (2013-2016), now Co-Chairman Universal Defence & Security Solutions