GLOBAL STRATEGY FORUM

EDITION No. 15 - JUNE 2020

The 15th 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.

A Digital Age Defence Industrial Policy For The UK

The UK has a long history of making and selling defence equipment and services. This has met the changing needs of the Armed Forces over time to protect the country and support vital interests abroad, always maintaining sovereign independence in a few essential areas. Defence industry has also provided stable and often highly skilled jobs, perhaps 135,000 are directly employed now, and led to successful exports (£9 billion in 2017).

The industrial horizon, however, now looks more difficult. Current UK defence spending funds only a very small number of technologically advanced platforms, many with only limited export potential, and the trend is for further reductions. The US cuts an ever-larger swathe through major equipment purchases in Europe, with equipment such as the F35 fighter, P8 anti-submarine aircraft, and Apache attack helicopter, winning on both price and performance. European defence collaboration has struggled to overcome the fondness for protection of comparatively inefficient national programmes and industries, and battled unsuccessfully for cost-effective compromise in programmes such as Airbus' A400M transport aircraft. China, Russia and India sell ever-improving materiel at lower prices and with fewer constraints.

There are already areas of contemporary defence technology where UK industry is not fully keeping up – partly because the MoD is not funding them. Long-range precision conventional ballistic and cruise missiles including the hypersonic generation; space-based surveillance capability; AI-enabled command and control; and advanced unmanned and autonomous platforms at sea, on land and in the air are some of the capabilities taking centre stage where UK is not leading. The industrial deficit is also partly because confrontation and conflict have acquired new forms of expression through cyber warfare and information exploitation, where different industry is required in what is now a global competition. UK Defence industry will need more than a trickle of business around evolving the diminishing numbers of high-end conventional platforms to sustain the defence and security of the country, ensure commercial longevity, and contribute to national prosperity.

The new way forward on defence industrial policy is staring us in the face. We know that combinations of digital age technology will transform defence and security capability, operations, and organisation just as it transforms how we live, work and play. We are in the foothills of the profound transformation brought by the AI industrial revolution, through well-conceived combinations of data, cloud, AI, connectivity including 5G, processing power, autonomy, robotics, material science, nanotechnology, bioscience and many other technologies. These disrupt and define what being competitive and resilient looks like in almost all parts of 21st century endeavour.

The forthcoming UK Integrated Review of foreign policy, defence and security is an unmissable opportunity to re-cast UK defence industrial policy for the Digital Age. It is the door to resetting capability for the risks that we face at a sustainably affordable price, especially important in a fiscal climate dominated in the short term by deep recession. The same advantages in operational effectiveness and resource efficiency that digital technologies bring to other industries apply equally to defence and security. The risks and costs of persisting with defence equipment and services that are steadily over-matched and obsolescent are clear, so a renewed common effort driven through a new Defence Industrial Policy is essential to put the UK back on the path to security and prosperity. How do we make this happen?

First, this has to be led by politics. There must be a solid recognition that the current Defence Industrial Policy, where it exists, is neither going to deliver the capability that the Armed Forces need in the 21st century nor going to sustain jobs or exports in the way that it has in the past. Only Government has the convening power to set UK defence policy, integrate it with our collective security arrangements such as NATO, and resource and incentivise the goods and services that are required. Only government can lead and *impose* the drive for essential modernisation and transformation as it will cause significant short-term dislocation and disruption of long established and economically significant industries. Government will need to lead the way through necessarily disruptive transformation which will be hard pounding for the Armed Forces and for industry and resisted in some quarters of both.

With major prizes in security and prosperity in prospect this is both hard and non-discretionary; doing nothing will certainly mean ever-poorer outcomes as the rest of the world moves on past the UK military and industry wilfully marking time. In short, the Integrated Review should lead to the Government bringing together the Armed Forces, industry, research and academia, and civil society in common support of the most profound transformation of defence and security for over 100 years.

Second, the new Defence Industrial Policy must be grounded in how the decisive digital technologies are generally led by the scale of investment in research and development that comes from the private sector, absolutely dwarfing what most governments are able to provide. Google alone spent $26bn on research in 2019, the MoD spends about £1.8bn a year. We need a Defence Industrial Policy which is about the intelligent *application* of combinations of technologies that are for the most part rapidly developing outside defence and security. There are, of course, exceptions to this where the requirement is so specialist that only a government can provide the necessary investment. Nuclear weapons, missile-firing submarines, offensive cyber tools, and some space-based capability are all relevant examples.

UK industry must lead in bridging between the technology to be found in the private sector and

the challenges faced by the UK intelligence services and Armed Forces. An important aspect is to set a Defence Industrial Policy that incentivises industry to produce *propositions* for better ways of delivering defence and security outcomes, instead of mostly waiting for their customers, the Armed Forces and intelligence services, to write a full specification based on quite limited and prematurely bounded understanding of what is becoming possible. We will need contracts that establish an enduring, evolving *partnership* rooted in constructive discussion, rather than traditional transactional arrangements based on specifications laid out in great detail in advance as both the start and immutable end-point. In many cases this will mean contracting for capability or services, not just buying a thing.

Third, a new Defence Industrial Policy cannot just be about producing Digital Age military hard power. Our defence and security now rests on sophisticated integration of military hard power, public sector soft power, private sector soft power, and greatly strengthened national resilience in the face of both physical and cognitive attack. We need to invest in how the Armed Forces are equipped, organised, trained and supported, but we also need to invest in hybrid campaigning tools such as AI-enabled intelligence and situational understanding, offensive cyber, and social media tools.

We must also support how resilience is built into all forms of our Critical National Infrastructure, business continuity, government continuity and daily civil life against a wide range of threats, from missiles to pandemics. Emerging digital capabilities such as data-based surveillance, situational understanding, decision support, information security, planning tools, networks, visualisation, modelling and simulation are often this century's spear-tips and as important to Defence and its supporting Industrial Policy as frigates.

Fourth, it follows that a digital age defence industrial policy will be a blend of products and services. It will still be important to make things that sail, drive and fly, but most of these things will be the platform wrappers for information. In constructing information-centric capability we will need to promote all forms of engineering, soft and hard. We will also need expertise in the application of technology through new methods, ways of operating and new organisations. This is not just about different kit. The effectiveness and efficiency advantages of new technology are only secured by moving beyond *accessorising* current ways of working. We must arrive at new solutions in which people and machines are blended in an optimal way. This means that a Digital Age Defence Industrial Policy will draw together not just the current industrial champions and capability integrators such as BAE Systems, Babcock, Rolls-Royce, BT Defence, and QinetiQ, but also the technology-oriented services found in the major consulting houses and the capacity for niche agility and innovation championed by university research and SMEs. All are a vital part of the discussion to be convened by Government in a national effort.

Fifth, it is not possible to keep pace with rapidly advancing digital age technologies with conventional approaches to the acquisition and support of military equipment. An absolutely vital part of a Digital Age Defence Industrial Policy is the acquisition reform needed to enact it. This is hardly a new thought, but progress to date has been mixed as the MOD and industry struggle to find a new formula whilst also battling with existing contracts and unmanageable resource challenges. Many other potential contributors, particularly SMEs, remain outside the acquisition fence, unable or unwilling to meet the extensive bureaucratic challenges of existing ways of contracting. It will, nonetheless, need restating that whilst acquisition reform is an essential part of a new Defence Industrial Policy it is clearly not the

sum of the problem. The right capability needs to be acquired in the best way, it's not just about how to do the shopping.

Sixth, this new deal won't work without a commitment to experimentation - and that with experimentation comes the inevitability of some failure. Otherwise there would be no need to experiment. As Defence and Security will already be the beneficiaries of massive private sector investment, Government money can be focused on experimentation in the adaptation and application of technologies that have generally been matured elsewhere. They should reduce the challenge, but nobody is going to invest in how combinations of digital is technology may transform defence and security unless the risk is well ameliorated with some public and private sector money for experimentation. The MoD's shared investment with Improbable and CAE(UK) in a Single Synthetic Environment Technology Demonstrator is a good example.

Seventh, there is a broad conceptual outline for what this modernisation and transformation of defence looks like, so a Defence Industrial Policy can be constructed around an evolving framework of what Armed Forces and intelligence services around the world are already looking for. There has to be a start somewhere so early moves may feel like random shots, but an important element of the present opportunity for the UK is to produce an industrial policy that delivers Digital Age strategic capability coherence over time, as well as fosters rapid and competitive innovation. The major elements of this framework are likely to be:

- All capability will be founded on a common digital backbone that underpins new levels of operational effectiveness at platform, Single Service, Joint, Inter-Agency, and Combined (multi-national) levels. This backbone is a combination of data in secure cloud, AI, secure and resilient networks where bandwidth is no longer a constraint, and the visualisation and modelling-based decision support, planning, and training enablement a very large scale, complex 'Single Synthetic Environments (perhaps better known as Digital Twins).

- Intelligence, Surveillance and Reconnaissance (ISR) will change from the conventional reliance on generally closed, secret systems for human intelligence, communications intelligence, and imagery in support of human analysts. ISR systems will be built around access to as many sensors and sources of data as possible. Much of this will come from data that is freely available or can be purchased and supplemented by closed sources. Sensors will include not just the high-end systems operated by Armed Forces, but also networks such as commercial low Earth orbit satellites, commercial radar and 24/7 news. All of this data will be managed by AI, freeing up human analysts for more creative and insightful work as situational understanding is pushed to decision-makers in near real time 24/7. Defence Industrial Policy needs to focus on how technology is adapted and applied in this area and how it keeps pace with the rapid rate of change: just helping analysts write better essays is not enough.

- Command & Control (how leaders and their HQs organise and operate at all levels) will change in the most profound way for 150 years, as data, AI, connectivity and simulation disrupt the long-standing conventional approaches of a traditional 'General Staff'. The number of headquarters, their size, location and operating models are as open to change as any other institution, indeed the lessons from how other organisations have already adapted (such as banking and large-scale industry) will be highly instructive. Main headquarters will be static and back underground, all types of HQs in the field will have far smaller, agile footprints if they are to survive.

- Military forces will transition from a conventional model rooted in people manning equipment (ships, tanks and aircraft) to an ever-evolving mix of manned, unmanned and autonomous capability. This will offer routes to expanding the size and footprint of a deployed force over time by exchanging a small force of high-end manned platforms for a larger force of smaller and often personnel-free networked platforms bearing sensors and weapons. Where this leads to fewer people in harm's way there will be less risk to life and where it leads to needing fewer people overall there will be major savings in support costs, including pensions. Where equipment is smaller, less complex and more resilient through not having to support people, there will be savings in acquisition, training and support costs. Substantial numbers of people will still be required of course, just in a different way with as much risk as possible placed on machines. This transition is the biggest opportunity for UK Defence Industrial champions to lead in building new equipment mixes, stealing a march on global competition.

Eighth, there are some important ethical and legal considerations that need to be at the heart of a 21st century Defence Industrial Policy. Some of this is not new, such as where limits are to be set on equipment exports. Some of it is new, such as how to handle the developing prominence of lethal autonomous weapons systems, whether these exist primarily in the hands of opponents, are reserved for self-defence purposes only, or become a more routine part of the military inventory. UK policy will have to go further than just regretting or denying the existence of technology that is open to exploitation worldwide.

In summary, if the UK can launch a coherent Digital Age Defence Industrial Policy as part of the Integrated Review the potential prizes are very substantial. It will chart the path to restoring effectiveness and efficiency in defence and security. It will transition industries and the constituencies that support them from clinging to the tail-end of conventional, industrial age capability to setting the pace globally in the application of new technology. This will bring greater security and also influence with friends and opponents alike. It will promote skilled jobs sustainably linked to the Armed Forces and to substantial export prospects. None of this will happen unless government provides the leadership and incentives to draw together all those who have something to contribute, but industry and others can at least now help get the ball rolling.

General Sir Richard Barrons
June 2020

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