Cranfield University

Integrated Review of Security, Defence, Development and Foreign Policy: Call for Evidence – submission from Cranfield University

Contents

Cranfield University

Executive summary

- Cranfield University warmly welcomes the opportunity to participate in this Call for Evidence and contribute towards a wide-ranging national security review encompassing the full spectrum of capabilities from hard military power to soft diplomatic influence, and against an ever-evolving range of malicious and non-malicious threats and vulnerabilities.
- There needs to be equivalent focus given to domestic, 'homeland' security as is given to external defence. This includes pandemics and climate change, but also low frequency, high consequence threats and threats associated with complex, networked systems, all of which will present very different sets of challenges and require different expertise.
- There is a need to look at how we are set up from an integrated government perspective, across departments, to deal with a range of possible threats.
- There needs to be an emphasis on 'connected resilience' and the impact of climate change on global security in particular should not be underestimated. Complex socio-technical systems are key to society and these are becoming ever more complex.
- International stabilisation funding will be increasingly important and stabilisation activities must also be connected to the UK homeland perspective when consideration is given to how that money is spent.
- The current national risk register framework isn't suitable for the UK's national security, simply assessing risk from a two-dimensional 'XY' perspective – there is a need for a new resilience framework to assess national risk.
- There is a need to invest in transdisciplinary science and a new cadre of transdisciplinarians, skilled in science, technology, social sciences and policy.
- The UK needs to reconsider how to integrate protection of its digital territory alongside its physical and political territory.
- The UK has a good record of exercising soft power (through its education, culture and international engagement); it should seek to extend this more widely.
- Having a strong economy which is internationally respected and attractive for business investment and engagement, with a solid underlying science and technology base to drive growth through new inventions and innovation, is also key.
- There needs to be more trust between public and private partners and academics and academic disciplines, and more tolerance of initial failures with greater diversity of participation, including small businesses.
- Closer analysis of the dynamic between the security of the economy and prosperity of economy is required, with a more harmonious connection being possible.
- We need leadership and decision-making from a dedicated national-level operation, capable of working internationally for global coordination.
- A clear overview and signposting through the science and technology innovation system is needed, including the definition of terms, processes and outcomes.
- There needs to be a wholesale focus on skills and talent in the national security sector with a broadening of awareness of the range of security sector roles and what working in and contributing to national security means, including researchers.

About Cranfield University

0.1 As a specialist postgraduate university, our world-class expertise, large-scale facilities and unrivalled industry partnerships create leaders in technology and management globally.

0.2 Our key areas of expertise and capabilities are grouped under seven main themes: aerospace, agrifood, defence and security, energy, manufacturing, transport systems and water, along with our world-renowned School of Management. Integrated thinking across these sectors is key to building a more resilient post-Covid-19 society – Cranfield has the facilities and expertise in natural capital and technology transition to inform these changes.

0.3 Cranfield University is one of the world's leading universities for defence and security education, research and consultancy. We are one of the largest providers of postgraduate education in defence and security technology and management and work on classified projects for governments and industry. Our secure site at the Defence Academy of the UK at Shrivenham, is 50 minutes away from Oxford and 15 minutes away from Swindon.

0.4 Our wholly-owned subsidiary, Cranfield Defence and Security Services Ltd (CDSS) supports our existing brand and relationships in defence, security, aviation, transport and manufacturing via the delivery of consultancy, training and test and evaluation.[1]

0.5 Cranfield prides itself on being close to business and supports the set-up and development of business at every stage from start-up to global enterprise.

0.6 We are leading the Academic Resilience and Security Community (A-RiSC), a network of over 50 UK universities formed to help Government and industry access academic experts and the latest research and knowledge in national security.[2]

0.7 Our research Grand Challenges of resilient infrastructure, smart living, green technologies and security for development are focusing on concrete and specific solutions towards the world's grand challenges of sustainability and security.[3]

0.8 Our Counterterrorism, Intelligence, Risk and Resilience Group, part of Cranfield Forensic Institute, offers a wide range of expertise in counterterrorism, intelligence, risk and resilience contexts, nationally and internationally. Expertise includes risk assessment, risk and threat modelling, leadership in transitional states and climate change and terrorism.[4]

0.9 Our International Security and Law Group promotes international security and supports states and societies in achieving peace through defence engagement, academic research, education and policy work on issues related to the multifaceted, complex nature of contemporary international and regional security environments.[5]

[1] https://www.cranfield.ac.uk/themes/defence-and-security/cranfield-defence-and-security-services

[2] https://www.cranfield.ac.uk/press/news-2019/cranfield-university-to-lead-national-security-academic-network

[3] https://www.cranfield.ac.uk/research/why-cranfield/grand-challenges

[4] https://www.cranfield.ac.uk/centres/cranfield-forensic-institute/our-research-groups/counterterrorism-intelligence-risk-and-resilience-group

[5] https://www.cranfield.ac.uk/centres/cranfield-forensic-institute/our-research-groups/international-security-and-law-group

0.10 Our Centre for Defence Management and Leadership delivers education, research and consultancy across the globe, including in some of the newest and most vulnerable civil societies in the world. Much of our programme is delivered overseas and seeks to build partnerships and strategic relationships with governments, NGOs and the international defence and security sector.[6]

0.11 We develop, evolve and apply new analytical methods and tools including modelling and simulation.[7]

0.12 The National Cyber Deception Laboratory (NCDL) aims to bring together practitioners and researchers across Government, academia and industry to facilitate research and provide guidance on the proactive defence of our computer networks through the use of deception in the context of national security.[8]

0.13 Cranfield offers a wide portfolio of defence and security courses, from taught and research-based degree programmes to short, professional development courses.

0.14 Specialist courses on building resilience include the Management and Corporate Sustainability MSc[9], Counterterrorism, Risk Management and Resilience MSc[10], Defence and Security (Leadership and Management) MSc[11], and short courses such as Leading Organisational Resilience and Leadership in Disruptive Times: a Strategic Approach to Building and Strengthening Organisational Resilience.

0.15 Our world-leading cyber qualifications include the Cyber Operations MSc[12] and Cyber Defence and Information Assurance MSc[13], educating future military leaders on the implications of operating in today's interconnected age.

0.16 Cranfield is the lead higher education provider for a 'new model' university in Milton Keynes (MK:U), developed in partnership with business to prepare students for the future world of work. One of the new BSc course design priorities is cyber security and developing graduates who can lead in a cyber environment to effectively exploit the threats and opportunities of cyber space at the organisational level. The course will specifically focus on responses to serious, present and emerging threats in the information domain.[14]

0.17 Along with the Atomic Weapons Establishment (AWE), Defence Science and Technology Laboratory (Dstl), and Defence Ordnance Safety Group (DOSG), a subgroup of Defence Equipment and Support (DE&S), we are facilitating the new Centre of Excellence in Energetic Materials (CoEEM) with the aim of delivering a UK national capability in explosives and energetic materials.[15]

[6] https://www.cranfield.ac.uk/centres/centre-for-defence-management-and-leadership
[7] https://www.cranfield.ac.uk/centres/centre-for-simulation-and-analytics
[8] https://www.cranfield.ac.uk/press/news-2019/new-cyber-deception-lab-helps-mod-take-the-fight-to-network-attackers
[9] https://www.cranfield.ac.uk/som/masters-courses/management-and-corporate-sustainability
[10] https://www.cranfield.ac.uk/courses/taught/counterterrorism-risk-management-and-resilience
[11] https://www.cranfield.ac.uk/courses/taught/defence-and-security-leadership-and-management
[12] https://www.cranfield.ac.uk/courses/taught/cyberspace-operations
[13] https://www.cranfield.ac.uk/courses/taught/cyber-defence-and-information-assurance
[14] https://www.cranfield.ac.uk/about/mku
[15] https://www.coeem.org/?action=main

Responses to the specific Call for Evidence questions

1. What are the key opportunities, challenges, threats and vulnerabilities facing the UK now? (Submissions focusing on rapidly evolving areas such as science, technology, data, cyber, and space are particularly welcome.)

1.1 The intention of the Integrated Review is to look at the security of the nation from an integrated perspective but too often we focus on defence.

1.2 Our Armed Forces do a superb job in deployed overseas operations and defending the UK from afar; yet, nowadays, there is as much danger from non-malicious threats (such as pandemics and climate change) as there is from malicious actors.

1.3 There needs to be equivalent focus given to domestic, 'homeland' security as is given to external defence. This includes pandemics and climate change, but also low frequency, high consequence threats – such as solar flares, supervolcanoes, or asteroid strikes – and threats associated with complex, networked systems (e.g. infrastructure interdependencies) and emergent/weak signal threats (e.g. new chemicals in the environment), all of which will present very different sets of challenges and require different expertise.

1.4 While important, focusing on the 'big, exciting' threats, such as asteroid strikes, also risks overlooking emerging threats which are only just starting to be recognised, such as those to the marine environment and infrastructure, encompassing telecoms, energy, carbon capture and storage, marine pharmaceuticals/therapeutics, deep sea mining, geoengineering, along with issues around fisheries and trade flows.

1.5 In cyber space, there are a range of threat actors continuously attempting to penetrate the digital dimension of the UK's economy, government and military capabilities, and an increasing threat of operations in a 'grey' zone – on the edge of conflict but ambiguous/ill-defined/deniable.

1.6 There needs to be better appreciation of the differing speeds of threats and their systemic/wicked nature. Some threats are so fast they are difficult to respond to, and this becomes more complicated when there are multiple hazards/events/threats/risks, with a variety of complex interactions going on.

1.7 It's not just a case of learning from Covid-19 and implementing measures to improve health systems and response – there is a need to look at how we are set up from an integrated government perspective, across departments, to deal with a range of possible threats.

1.8 We can't continue to rely on the Armed Forces solely to step in and deal with extraordinary events, as has so often happened with, for example, flooding, foot and mouth disease, or disruption to the supply of petrol. With Covid-19, the UK was fortunate that its Armed Forces weren't being deployed on extensive missions overseas – they need to be focused on their core role.

1.9 It is necessary to ensure we have structures, processes, equipment and forces in place to deal with homeland threats, just as we have for overseas operations.

1.10 In the defence and security realm, science and technology spending is substantial, but not linked enough to other sectors – unconnected investment and research by the Department for Business, Energy & Industrial Strategy (BEIS), the Ministry of Defence (MOD) and Home Office leads to incoherence, and this is not only problematic because of incoherence in those domains, but also the resulting complexity. There also needs to be improved links to the Department for Environment Food & Rural Affairs (Defra) in terms of environmental threats; the regulators, in terms of complex infrastructure; and the Foreign, Commonwealth & Development Office (FCDO), in terms of international aspects too.

1.11 The Dowling Review of business-university research collaboration in 2015 backs up the argument that the machinery is too complex and too fragmented.[16] SMEs and micro-businesses aren't able to navigate their way through the system – to see the benefits to themselves and the wider world – which means cutting off the largest and most diverse source of enterprise activity. Even when useful projects are given backing, the machinery of Government procurement is slow and built around inflexible systems of accountability. Success and failure is judged quickly and in black and white terms, all working against risk-taking and the eventual innovation outputs.

1.12 The Government has suggested an organisation similar to the Defense Advanced Research Projects Agency (DARPA) in the US[17], taking bigger bets on emerging technology rather than processes that split funds in multiple ways into smaller and smaller projects. In the UK, however, an agency of this kind wouldn't work in the current departmental infrastructure. A different machinery is needed; not tweaking but brave, deep cuts, realignment and a research funding approach without all the separate, overly intricate, easily disrupted moving parts.

2. What are the key global and domestic trends affecting UK international policy and national security out to 2030, and how should the government prioritise its efforts in response to these?

2.1 The rapid pace of technological advancement has directly contributed to and catalysed an increasingly complex landscape of malicious and non-malicious threats. The economic damage, scarring and disruption being caused by the Covid-19 pandemic will affect UK policy making and the UK's ability to respond to these threats, across the physical and virtual domains.

2.2 There needs to be an emphasis on 'connected resilience' and the impact of climate change on global security in particular should not be underestimated. Complex socio-technical systems are key to society and these are becoming ever more complex, exhibiting emergent behaviour and failure modes. Climate change and human behaviour can trigger complex system failures and regime shift (both in terms of politics and complex systems).

2.3 The Global Strategic Trends publication from the MOD's Development, Concepts and Doctrine Centre identifies the key drivers of change that will shape and reshape the world. The Sixth Edition (2018) lists increasing environmental stress (human influence on the climate system with far-reaching consequences such as floods, droughts, storms, heatwaves and heavy rainfall) and changing populations and evolving habits (the world population is

[16] https://www.gov.uk/government/publications/business-university-research-collaborations-dowling-review-final-report
[17] https://www.darpa.mil/

expected to grow by 2.1 billion and reach around 9.8 billion people by 2050, but with unbalanced growth) as trends that require action.[18] Increasing disruption and the cost of climate change, increasing demand and competition for resources and managing demographic change are included as focus areas that need to be addressed.[19]

2.4 Trends and assumptions that are often made may also be flawed – with climate change, for example, changes are exceeding projections and suggest the crossing of thresholds of change.

2.5 These trends mean that international stabilisation funding will be increasingly important and stabilisation activities must also be connected to the UK homeland perspective when consideration is given to how that money is spent. The key issue for the UK is how to best project overseas power offensively (through the MOD) and defensively through conflict stability funding.

3. What are the key steps the UK should take to maximise its resilience to natural hazards and malicious threats? How can we build a whole of society approach to tackle these challenges?

3.1 The current national risk register framework isn't suitable for the UK's national security, simply assessing risk from a two-dimensional 'XY' perspective. Only looking at likelihood versus impact misses a huge gulf in assessing risk – there is a need for a new resilience framework to assess national risk, including natural and malicious threats.

3.2 Assessing resilience includes looking at how to recover from an event and not just the plain financial case, but keeping in mind all five 'capitals': the value of the natural environment (as the basis of all life), human capital (skills and aptitudes), social capital (institutions and communities), and built capital (everything from our cities to manufactured goods). Financial capital is just the means of transfer between the other four.

3.3 We must be thinking in terms of connected resilience, but also recognise that some complex systems may not be recoverable. Becoming genuinely resilient – not just enhanced risk assessments and precautions, but making sure we're able to prepare for, cope and recover quickly from national crises – means looking at the big picture, all the ways in which society is connected and interdependent.

3.4 A focus on data and analytics is useful in some cases, but in terms of connected resilience, data and analytics won't always provide the 'answer'. There is a need for post normal science in this area – this may be difficult given the types of debate that are needed around defence and security.

3.5 A 'whole of society' approach to national resilience must be underpinned by a strong economy and an industrial base that works in a close collaborative partnership with Government. Universities also have a key role to play through research and tackling the well-documented physical and digital skills gaps across aerospace and defence and security sectors, exacerbated by an economy-wide STEM skills gap. To tackle these gaps and

[18] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/771309/Global_Strategic_Trends_-_The_Future_Starts_Today.pdf, p.13.

[19] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/771309/Global_Strategic_Trends_-_The_Future_Starts_Today.pdf, pp.14-15.

ensure there is sufficient resilience within our workforces to meet future challenges, the Government should work with the UK's defence and security sector and further and higher education institutions to establish an initial national strategic skills plan.

3.6 There are an increasing number of independent 'commissions/committees', which independently scrutinise different areas of government/policy and are vital to security. However, the extent to which they are joined up or considering defence and security may be questioned. These include the Committee on Climate Change, National Infrastructure Committee and Natural Capital Committee. All are key to the resilience and security of the nation. All are conducting various national assessments, which are required by law, including Climate Change Risk Assessment, the National Adaptation Programme, Adaptation Reporting Power and National Infrastructure Assessment. There is a need to engage these groups on defence and security issues.

3.7 Long-term funding for key research centres is needed as otherwise skills and expertise die off. This is a particular issue when dealing with risk and resilience, where short-term cuts to funding can have significant impact on the ability to address low frequency, high consequence threats/events such as Covid-19.

3.8 There is a need to invest in transdisciplinary science and a new cadre of transdisciplinarians who are skilled in science, technology, social sciences and policy, and have the types of understanding required to address wicked problems. This is a challenge as such individuals can be viewed by academics as being too broad in terms of their research and thinking. This and the associated difficulties with gaining funding for such research hampers career progression and puts people off such careers.

3.9 There is a need to embrace and engage researchers from different academic disciplines. This may be difficult as 'security' can be viewed in a negative light or conflict with the worldviews of such researchers.

3.10 The UK needs to reconsider how to integrate protection of its digital territory alongside its physical and political territory. For too long a civilianised intelligence-led approach to information security and cyber security has failed to secure our national capabilities from cyber attack, nor deter attackers from attempting to compromise UK systems.

3.11 Increased investment in understanding the nature of ambiguous/ill-defined/deniable threats in the 'grey' zone on the edge of conflict (linked, at least partially, to the threat and opportunity of information operations and information manoeuvre) – including prediction and countermeasures – would be valuable and reinforce the development of multidisciplinary (e.g. analysis, information technology, human sciences) and transdisciplinary skill sets.

4. What are the most effective ways for the UK to build alliances and soft power?

4.1 In a post-Brexit Britain, strong alliances have become crucial. The country will have to rethink its relations with the European Union, the US and other traditional allies. While the focus might be on economics, security and defence shouldn't be ignored. The French-British security and defence alliance that focuses on all aspects, including sharing capabilities and training, is a model to follow in that regard. The UK should consequently seek to strengthen such historical alliances.

4.2 The UK should also seek to build strong defence and security alliances with the Commonwealth, engaging actively in examining historical ties to try to start afresh. The search for allies should also encompass other nations, with whom those historical ties don't exist, to build new partnerships. Some of these alliances could be tactical or natural, and the UK should be aware of fleeting alliances.

4.3 R&D partnering can strengthen the UK's alliances and contribute to national security. In considering the UK's international policies, the Integrated Review must identify opportunities where the UK can most effectively collaborate with allies on R&D, including via multilateral organisations such as NATO and the Five Eyes.

4.4 Closer links with Global Challenges Research Fund (GCRF) funding are required, where there is a need for funding of long-term projects which allow deep working relationships to be developed rather than short-term projects/events, which do little more than provide researchers with an opportunity to visit some interesting places around the world.

4.5 The UK has a good record of exercising soft power (through its education, culture and international engagement) in Commonwealth countries and beyond; it should seek to extend this more widely. This mission is supported by Cranfield University's International Security and Law Group and the Centre for Defence Management and Leadership.

4.6 Having a strong economy which is internationally respected and attractive for business investment and engagement, with a solid underlying science and technology base to drive growth through new inventions and innovation, is also key to building alliances and exercising soft power. Cranfield School of Management is globally recognised for excellence in leadership development – connecting technology and leadership – and for its powerful industry links and real-world focus, changing the way society thinks, works and learns.[20]

4.7 The UK should be spending a larger proportion of our GDP on research and development, including investment in people. The commitment to increasing UK investment in R&D to 2.4% of GDP by 2027 and to increase public funding for R&D to £22 billion per year by 2024 to 2025 is significant but not enough – investment needs to be upwards of 5% in order for the UK to be a realistic 'research superpower', particularly when considered comparatively in relation to other larger countries such as the US and China.

5. What changes are needed to Defence so that it can underpin the UK's security and respond to the challenges and opportunities we face? (Submissions focusing on the changing character of warfare, broader concepts of deterrence, technological advantage and the role of the Armed Forces in building national resilience are particularly welcome.)

5.1 There needs to be a more integrated force across Government for defence, along with more focus on security. Security needs to be considered as equally important, but this shouldn't be achieved by reducing defence resources.

5.2 Competition in research, development and procurement isn't always good – there needs to be the flexibility to not go to competition and either form collaborative networks or go directly to the best solution which may not be the cheapest one. Giving opportunity to everyone sometimes isn't the best way to tackle an issue.

[20] https://www.cranfield.ac.uk/som

5.3 There’s a need for innovative funding to get the type of academics who are needed to provide help on these complex issues engaged. This needs to span the Engineering and Physical Sciences Research Council (EPSRC), Natural Environment Research Council (NERC), Economic and Social Research Council (ESRC) and others.

5.4 Research Councils UK (RCUK) used to hold funding sandpits where diverse groups of academics worked together and competed for funding (like Dragons’ Den combined with The Apprentice). This type of funding event is controversial but might work well here.

5.5 There needs to be more trust between public and private partners and academics and academic disciplines, and more tolerance of initial failures and greater diversity of participation, including small businesses. That means bold leadership and decision-making in order to get funding targeted to high potential, multi-disciplinary work with obvious, radical benefits for the nation. The current system, in trying to be fair to everyone, just means there are disadvantages for everyone trying to contribute and worst of all, a diminishing rate of return from taxpayers’ money.

5.6 The UK MOD has recognised how integral information is to current and future conflicts, with the Chief of the Defence Staff recently recognising that Britain is “at war every day” due to constant cyber attacks.[21] We are moving from a model of traditional state-based intercontinental engagements with kinetic capabilities to a more adversarial context where “persistent engagement” below the threshold of warfare has become the norm. With adversaries exploiting legal frameworks and the existence of the virtual domain, the UK’s approach to defence and security needs to be reconsidered to fully integrate this digital dimension, acknowledge the implications this might have for traditional concepts and characteristics of conflict and recognise what that might mean for the UK to achieve its objectives and protect its interests in today’s digital age.

5.7 There is a need for the UK to articulate with greater clarity and consistency its view of the international law parameters of “persistent engagement” – what legal rights and obligations are there when the adversarial context, below the threshold of warfare, crosses a line and infringes the UK’s sovereignty. This should be particularly tailored to encompass the cyber domain.

6. How should the UK change its governance of international policy and national security in order to seize future opportunities and meet future challenges? (Submissions focusing on the engagement of an increasing range of stakeholders while maintaining clear responsibility, accountability, and speed of action are particularly welcome.)

6.1 Answers should be viewed within the context of the increased importance of international stabilisation funding and stabilisation activities which are integrated and connected to the UK homeland security requirements.

6.2 Government departments are cylinders of excellence and their focused knowledge on particular areas and agendas is always going to be the basis for ecosystem-wide (pan-government) risk-averse decision-making. In this system only limited, piecemeal research projects appear to make sense, become able to access funding and have a chance to prove

[21] https://www.telegraph.co.uk/news/2019/09/29/britain-war-every-day-due-constant-cyber-attacks-chief-defence/

their viability; more ambitious, cross cutting, high-risk but high-potential projects, look even more remote from common sense, certainly economically. This is a big problem and an issue with international collaborative funding mechanisms such as the Newton Fund and GCRF, which are key to international defence, security and resilience.

6.3 Security depends on infrastructure and supply chains, water, food, jobs and so on – but research funding continues to come in small clusters, limited by notions of what 'security' means, generally focused on a particular technology solution, and without an overarching cohesion of purpose and direction. Where is the 'Moonshot'? Projects that involve wider perspectives and collaboration across humanities, social sciences and technology are more likely to be overlooked. The potential losses are huge so even small investments could have large paybacks.

6.4 The Home Office remit is too broad to take on the role in its current form – the department needs to be broken up and put back together again around a focus of emergency management.

6.5 Organisations like the Federal Emergency Management Agency in the Department for Homeland Security in the US have been shown to have their own flaws, but they are at least examples to learn from. The new emergency agency would need a budget reflecting the fundamental value of security, the underpinning to the life of the nation. It would need to be backed up by the UK population, in the form of a body of volunteer reserves; a fourth emergency service able to work across communities, brought together and given regular training in medical skills, crowd control, logistics, communications; a group drilled to take their place alongside emergency services and local councils.

6.6 In general, closer analysis of the dynamic between the security of the economy and prosperity of economy is required. A more harmonious connection is possible – sometimes less is spent on security which means products can be deployed faster to market, but this may leave holes in the 'back door'; cyber security is an example.

6.7 It's difficult to make a business case for the kind of changes required to foster genuine resilience, often involving low probability, but high cost. However, nations can no longer afford to keep making decisions about risk and resilience based on these kind of crude equations.

7. What lessons can we learn from the UK's international delivery over the past 5 years? Which are the key successes we should look to develop and build on, and where could we learn from things that didn't go well?

7.1 The Global Britain agenda is a critical part of delivering economic prosperity for the UK and enabling it to project influence and contribute to global security. If the UK is to maintain and build upon its international standing, a 'whole of Government' approach to international engagement must be taken.

7.2 International collaboration is extremely important for the health of the UK's defence and security sectors. Engaging with international science and technology and innovation activities and working on joint research and development and capability programmes enables the UK to develop more interoperable and exportable capabilities. There is a vital need for such research if we’re to address challenging defence and security issues associated with the environment, wellbeing and development.

7.3 As the UK transitions out of the European Union and looks to solidify new trade and institutional relationships with global partners, it is vital that a coherent picture for international engagement is presented going forwards. Long-term relationships and mechanisms that encourage and facilitate working with European partners in a way that is not impeded by the participation rules of the European Defence Fund, European Defence Industrial Development Programme, and Horizon 2020’s successor, Horizon Europe are important for the UK supply chain, collaborative innovation, and capability interoperability.

7.4 The UK’s role in NATO remains an important part of national security and our engagement with allies and partners.

8. How should UK systems and capabilities be reformed to improve the development and delivery of national strategy?

8.1 We need leadership and decision-making from a dedicated national-level operation, capable of working internationally for global coordination.

8.2 A clear overview and signposting through the science and technology innovation system is needed for everyone involved: an agreed definition of what ‘innovation’ means, in terms of the process and outcomes, and how they can best be delivered; the routes to investment available for developing science and technology, and the opportunities for government and private sector collaboration.

8.3 There is also the issue of the language around ideas: terms like ‘science and technology’ (S&T), ‘research and development’ (R&D) and ‘innovation’. All are used synonymously by both government and industry as a ‘bucket of labels’ relating to positive ingredients that bring investment, growth, new enterprise activity and revenues to UK plc. In reality, each of the terms means something very different. S&T is the outcome, the product; R&D is the work done, the conversion of money into knowledge; innovation is conversion of knowledge into money.

8.4 Mixing up the links in the chain means less clarity over the purpose of research – what is actually needed to turn all the potential contained within our universities and industry research teams into R&D that results in big answers for society. That might be novel forms of healthcare, new ways to grow food, quantum IT or new ways to move between two places.

8.5 There also needs to be more common ground and sharing of what the priorities are for science and technology; the associated roadmaps for delivering change; and sharing of insights into the context, in terms of technologies and markets, access to data and facilities that will accelerate development and testing.

8.6 Regular communications and a two/three-way dialogue between Government, industry and academia on the ecosystem for innovation would go a long way in ensuring real understanding and appreciation of the changing landscape of needs. It is also needed to develop synergies between academic, Government and industry research and would lead to improved collaboration and reduce the risk of duplication of research, but it requires openness.

8.7 Current Government frameworks for procurement, intellectual property and commercialisation aren't conducive to innovation: complex systems of decision-making around acmes to funding, regular changes in team members. Fundamentally, there needs to be more tolerance to risk and 'failure' as part of an innovation process.

8.8 Narrow commercial, and academic/research, perspectives will be the enemy to the UK's ability to cope with future crises. We've built organisations that are razor-sharp in terms of conversion of resources, mapped tightly against a clear business case. But that also means operations are razor thin. The Covid-19 pandemic has exposed everything that's brittle about making efficiency the priority for both private and public organisations. We need to be proactive in our preparation, rather than reactive.

8.9 In Government, business and organisations generally there needs to be an opening up to wider perspectives. Sharing of knowledge for a broader understanding of interdependence/collaboration across sectors; and that's where universities can play a useful role as 'big picture' hubs, with their communities of expertise across disciplines, business sectors and technologies in a 'safe-sandpit' to experiment within.

8.10 The modern defence market and industrial sector requires skills and competencies that meet the needs of evolving, dynamic organisations. Innovative education and training is needed to create an open-minded, pragmatic and flexible workforce with digital skills (such as in artificial intelligence or cyber defence) and also skills for the digital age – the latter being linked to the Industry 4.0 agenda – along with a sound understanding of the social and environmental sciences and policy.

8.11 There needs to be a wholesale focus on skills and talent in the national security sector – children may not be familiar with or consider roles in 'security'; some may say they are interested in a future career in defence (for example, in the military) but there is a need to broaden awareness of the range of security sector roles and move the perception of the future workforce away from a purely 'James Bond / secret agent' interpretation of what working in and contributing to national security means. This includes educating researchers, and particularly talented PhD students, on the vital need for such research, although, as noted above, may be difficult due to conflicting worldviews and moral standpoints.

11 September 2020