Written evidence submitted by Office of the Chief Scientific Adviser for National Security (OCSA) on behalf of the Cabinet Office

Building the S&T Edge

This evidence note gives an overview of science and technology (S&T) in support of mission, capability and strategy in key organisations within national security. It sets out an analysis of the strategic context, provides a short account of the S&T system, and outlines the S&T programme currently being undertaken. The evidence concludes by pointing to some important next steps that are relevant to the JCNSS Call for Evidence. Necessarily, at this classification, there are significant constraints on the evidence that can be presented, we have nevertheless sought to provide as informative account as possible.

The Chief Scientific Adviser (CSA-NS) for National Security is Professor Anthony Finkelstein CBE FREng. The CSA-NS is a senior strategic and operational leadership role with responsibility for: undertaking science, research and innovation programmes in support of the National Security Community; providing advice on strategy to the senior leadership of the National Security Community; working with other Chief Scientific Advisers (CSAs) across HMG and providing technical advice on key national and international challenges; undertaking such sensitive work, in the UK and overseas, as is required in support of the national security mission.

I STRATEGIC CONTEXT

1. The pandemic, and the international response to it, has shifted the context for Science and Technology (S&T), and for much else, irreversibly. S&T is ever more central to how the UK secures economic recovery, resilience, future prosperity and security. These are **our assumptions** about the new realities we face.

2. The pandemic underscores the significance of S&T as a domain of **strategic competition between states**. While universities and research institutes have collaborated across borders to rapidly innovate treatments, some states are putting their national interest first in acquiring and deploying life-saving medical technology.

3. States that have fared best possess three characteristics: a **strong national research base**; effective, scaled **collaboration between government and private sector** to translate research into rapidly deployable medical technology and ramp up manufacture; and **strong societal support** for and compliance with an evidence-led, government-directed approach to managing the pandemic.

4. Global supply chains for critical national infrastructure systems have suffered disruption. **Highly digitised, technology-enabled sectors are adapting quickest**, maintaining higher levels of resilience and productivity. **We cannot retreat from**

highly optimised global supply chains, success in gaining benefit from them comes from intelligence and foresight.

5. There is an acceleration in further **digitisation of services.** Big Tech companies are rapidly extending the range of services they supply to citizens, increasing their dominance; but these companies are also taking a greater role in providing **social goods**, working collaboratively with governments in the crisis response to ensure resilient and equitable supply of essential goods and services to citizens; and using their data to inform government interventions.

6. The rapidity of the UK's move to greater online working and digital services has **increased exposure to cyber harms,** particularly among individuals and small businesses. Online manipulation by state and non-state actors is rising substantially. Domestic extremists and terrorist groups are finding a fertile audience in the large population who are socially isolated and mentally vulnerable as a result of extraordinary social distancing measures.

7. **Geopolitical competition in S&T has intensified. China is recovering rapidly,** in both health and economic terms, and is leveraging a strong economic position and asserting a global health leadership role to bolster its international influence. China is seeking to **increase its dominance in key emerging technologies** through targeted foreign direct investment, intensified competition for talent, and an advantageous position in funding available for R&D. It is maximising the fusion of its defence and civil innovation capabilities. **The US will necessarily focus much of its attentions on rebuilding its own economy. It is cohering a National Technology Strategy with success in great power competition as its primary goal.**

8. Government decision making is increasingly conducted at **lower classification, remotely, and with much greater emphasis on data** to underpin decision-making. But HMG needs to invest further in the skills, particularly with regard to science and data, necessary to understand, assess and develop coherent policy.

9. The National Security Community has, like most areas of government, had to make decisions on what lines of activity to place emphasis on, and which underpinning systems to prioritise. It is adopting much more flexible deployment models, placing a premium on **knowledge management systems**. Opportunities for high-side insight to inform government decision making are narrowing, forcing a reappraisal of how we supply valuable **insight at the point of decision-making**.

10. Disruption is bringing opportunity: by scrutinising lower-value activities, the National Security Community is creating space and appetite to innovate. A move to much more low-side, remote working is building **demand for commercial tools and platforms** to enable the change; opening **scope to experiment** with data analytics; and engendering **more policy flexibility.** Teams where adoption is greatest are seeing better productivity and resilience.

11. **Behavioural science** is playing a critical role in delivering the most profound and

rapid shifts in societal behaviour that a British government has ever sought; and in supporting the resilience and welfare of our people. The value of behavioural science as a tool in support of national security is increasingly appreciated.

II RESPONSE

12. In this new context, against a tough economic backdrop, national strength in S&T becomes more critical than before - as a foundation for our economic recovery, our resilience, and our national security. The 'Integrated Review' has provided a strong policy framework that shapes the National Security Community response. The key elements are set out below.

13. **Make a strategic choice to retain the UK's position as a Tier 1 player in S&T – a "Science and Technology Superpower" – in a more competitive global context. Orient our business to enabling this.**

- Place much more focus on establishing foresight in critical emerging technology areas and interrogating the implications for UK prosperity, security, society.
- Support difficult HMG choices on where the UK can realistically establish and hold a lead in these critical technology areas, within economic and social constraints.
- Focus on extracting hard power and soft power advantage from the UK's S&T strength

14. **Focus on global grand challenges.**

- Recalibrate towards the most serious threats and risks to UK security and resilience. Use our national security capabilities to tackle global strategic challenges: climate change; demographics and migration; health security.

15. **Leverage S&T strength for international influence.**

- Prioritise work to shape international rules, norms and standards to UK advantage.
- Invest in areas where UK national security S&T strength underpins critical alliances and partnerships.
- Understand competitors' strategic R&D, and how they intend to leverage their S&T strength for influence, as a core requirement.

16. **Support and sustain the innovation economy. Build on momentum in government and private-sector partnership, including with Big Tech.**

- Supply effective, targeted incentives and support for technology areas where the UK wants to establish a leading position and where national security partnership is best placed to deliver it.
- Develop and scale national security capacity to partner and co-develop with the UK private-sector.
- Identify where the UK needs to ensure sovereign capability for our security and resilience, and supply incentives and support.
- Better protection of UK innovation assets from espionage, predatory FDI, and market failure.

17. **Drive efficiency in our S&T investments across the National Security Community.**

- Choose strategically critical areas where the National Security Community will leverage collective UK resources (including UKRI and 'ARIA') for world-

leading advantage.

- Be clear about the bespoke/niche capabilities we cannot do without for our national security needs.
- Cut 'nice to have'; strip out duplication across departments; look hard at work that is not keeping pace with private sector innovation.
- Join up the innovation mechanisms across National Security Community and wider government, using them in concert.
- Exert more rapid and rigorous evaluation of performance of these mechanisms in driving prosperity or security outcomes, and quickly dismantle mechanisms that don't prove benefit.

18. **Supply the science, partnerships and skills to enable national security's accelerated digital transformation: for greater productivity, efficiency, better collaboration and to enable us to distribute and flex our workforces differently.**

- Enable this accelerated transformation through the supply of research, skills and tools in Data science/AI/ML; Privacy Enhancing Technologies and Behavioural Science including behavioural analytics.

19. **Take a mutually-reinforcing approach for S&T and cyber – supporting our growing industrial base, take a deliberative and proactive stance on strategic advantage in critical technologies, pursue economic opportunities and, where needed, mitigate the risks of dependence on non-allied sources of supply.**

- Deploy the Own-Collaborate-Access framework to guide strategic decisions, being clear about where the UK has the potential to 'own' the end-to-end development of a technology, where it should collaborate or partner to achieve shared beneficial outcomes, and where it should seek to access a technology through options, deals and relationships.
- Improve our ability to anticipate, assess and act on the technological developments most vital to the UK's cyber power (e.g. those that give rise to new cyber security risks, create opportunities to enhance defensive or offensive capabilities, or could transform the nature of cyberspace).
- Mitigate the cyber security risks of dependence on global technology and ensure UK users have access to trustworthy and diverse supply chains.
- Develop and maintain sovereign or allied capability in the security technologies most vital to our cyber power (where the UK has the potential to lead, or reliance on non-allied sources of supply poses unacceptable security risks).
- Project a vision of technology that reflects our values and interests as a cyber power and work to promote and defend this through the multistakeholder international system

20. **Build S&T skills throughout the system to meet the national need**

- Equip government decision-makers with S&T skills, with a particular focus on data literacy.
- Build a pipeline of skills available to national security S&T through the education system and in our leading universities and research institutes.
- Keep skills sharp in our workforce through partnership with world leading innovators.

III S&T SYSTEM

21. The National Security Community has significant S&T capability and resources placed across all the relevant organisations, including those within HMGCC, CPNI and NCSC. Details of these organisational capabilities and infrastructure are mostly classified. The Chief Scientific Adviser for National Security (CSA-NS) provides scientific and strategic leadership supported by senior staff. The CSA-NS sits on the boards of the relevant organisations and meets regularly with the heads of the organisations. The CSA-NS is supported by a Science Advisory Council (SAC) and associated Expert Community, comprising distinguished external scientists and engineers, that plays an important role in assurance and in the evaluation of programmes.

22. The National Security Community uses a blend of intra-mural and extra-mural research, with security requirements and the need to maintain secrecy requirement often a key factor in how work is commissioned and / or delivered against research requirements. It maintains an independent capability to commission research and to undertake independent research 'in- house' in areas that are highly sensitive or where a sovereign government capability is required. Existing programmes attract substantial external funding from across HMG and international partners generating strong leverage and public value.

23. The National Security Community has adopted a unique 'Science Plan' process. Each key area of operations, including, corporate, has a tailored Science Plan that is 'co-owned' between the operational and S&T functions. The Science Plans, where already in place, are reviewed annually and there is an ongoing process of stakeholder engagement. Each area of operations is required to assign points of contact and commit to resourcing their component of the Science Plan. R&D is very closely mission aligned with S&T experts moving between operational and R&D roles. R&D is frequently undertaken by multidisciplinary teams in operational settings. The use of Science Plans alongside specific 'requirements capture' exercises act as the principal means to formulate research priorities.

24. The National Security Community makes significant use of industry partners (both large and small). Much of this work is undertaken within agile research hubs managed by industry partners as part of a framework. This is an innovative and highly successful arrangement which has proved effective for 'near-in' innovation.

25. HMG has also established a unique government capability – the National Security Strategic Investment Fund (NSSIF) – for stimulating private sector R&D and innovation, using strategic venture capital (delivered by commercial venture capital partners) in conjunction with HMG technical expertise and support, piloting leading to early procurement. We also work with established international partners to generate commercial insight. This work exemplifies the 'business-science' approach championed by the Government Chief Scientific Adviser.

26. The National Security Community has a cadre of senior programme managers with project and expert finance support. Project outcomes are reviewed and project progress

closely managed. Quality and scientific assurance is the responsibility of the CSA-NS. The National Security Community subscribes to the Research Integrity Concordat though applies some derogations to reflect legal, security and other considerations. The community has an ethics and oversight system that meshes with its approach to research integrity.

27. The National Security Community works closely with existing Public Sector Research Establishments (PSREs), most notably Dstl but also AWE, HSE Science and Research Centre (Buxton), National Physical Laboratory (NPL), Met Office and others.

28. The National Security Community undertakes significant R&D in collaboration with UKRI and plans to significantly extend this collaboration. For example, it has substantial collaborations with UKRI programmes in the areas of Cryptography, Cyber Security and Quantum Technologies. The National Security Community also supports its own programmes managed through UKRI such as the Economic and Social Research Council (ESRC) Centre for Research and Evidence on Security (CREST) and the NCSC-EPSRC Cyber Security Research Institutes. NSSIF is developing a close relationship with Innovate UK. The National Security Community has, with HMG partners, established AMETHYST, a joint Board, to provide strategic direction for stakeholders and to collaboratively shape research relevant to national security.

29. The National Security Community funds projects, collaborations and maintains strategic relationships with almost all of the leading UK academic and Research Institutes. It has particularly important relationships with The Heilbronn Institute for Mathematical Research (HIMR) and The Alan Turing Institute (ATI). It also works closely with the National Academies most notably the Royal Academy of Engineering who, for example, operate the IC PostDoc Scheme. The community funds some research in Think Tanks such as the Royal United Services Institute (RUSI) and Chatham House.

30. The National Security Community operates an ‘in-house’ Masters Degree provided by a leading UK university that gives a post-graduate level introduction to the S&T relevant in security and intelligence for policy and operational staff. This scheme has been extended across HMG.

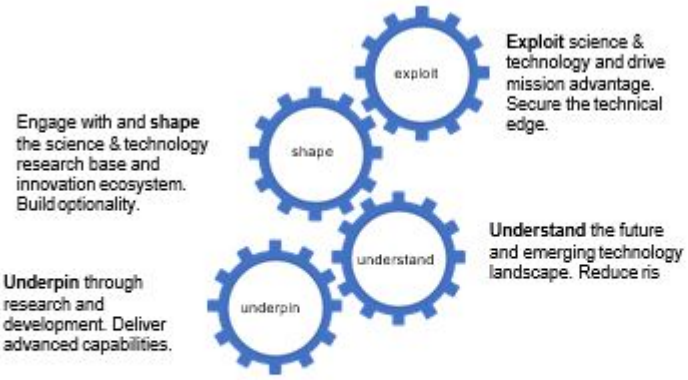
31. The National Security Community engages in significant international collaboration with 5- EYES and other international partners. These collaborations yield very large leverage and have enabled the development of highly significant capabilities and efficiency savings.

IV PROGRAMME

32. The National Security S&T programme (STEP) has secured substantial 4-year funding as part of the Comprehensive Spending Review 2020. The programme has 4 interlocking strands: Underpin (U), Understand (U), Shape (S) and Exploit (E). Conveniently forming the acronym U- USE. The overall programme is structured as a connected innovation system (the ‘gears’ in the figure above represent this).The strands

are as follows:

- **Underpin** through research and development programmes and deliver advanced capabilities.
- **Understand** the future and emerging technology landscape and reduce technical risk.
- Engage with and **Shape** the science & technology research base and innovation ecosystem, building optionality.
- **Exploit** S&T 'pulling through' to drive mission application and securing technical advantage.



33. Key elements of the programme, significantly limited by the classification of this evidence note but sufficient to indicate the broad scope of the work, are set out below.

34. The *Underpin* strand comprises:
    - **Big Bets.** Focused research programmes targeted on high impact Horizon 3 S&T, for example behavioural analytics, privacy enhancing technologies, low-cost space technology, augmented reality and so on.
    - **Experimental Facilities.** Development of advanced experimental and scientific facilities and testbeds, for example a near-field antenna measurement chamber to assure 5G capabilities. These facilities enable classified research programmes but can also support testing and co- development of commercial solutions.
    - **Protective Security.** Research to underpin the National Technical Authorities' (CPNI, NCSC, NACE) protective security missions, for example the CPNI drones protective security programme, NCSC work on smart cities and NACE work on intelligent RF monitoring.
    - **Behavioural Science.** Behavioural science confers a strong UK advantage and is in high demand by national security mission. Key areas of work include behavioural effects, behavioural analytics and an insider threat.
    - **Cryptography.** Building on UK excellence in crypt, including mathematics, taking advantage of the Heilbronn Institute for Mathematical Research (HIMR) and high-performance computational support to tackle the very significant new challenges posed by emerging future technology and global communications

trends.

- **Vulnerability Research & Data Science.** Building capacity in these key areas.

35. The *Understand* strand comprises:
    - **Capability Futures.** Development of an integrated x-HMG national security futures and horizon scanning programme aimed at identifying technologies that can contribute to the delivery of disruptive capabilities.
    - **Emerging Technology.** Development of an 'emerging technology' assessment capability in support of a x-HMG initiative spanning prosperity and national security.
    - **Global Technology Scouting.** Active global technology scouting capability and emerging technology reporting including reporting on global science and innovation programmes.
    - **Future Tradecraft**. Understanding future tech tradecraft and the changes consequent on the new digital environment.

36. The *Shape* strand comprises:
    - **Seed Venture Fund.** Seed investment and tech scouting, shaping the ecosystem. Extending the UK In-Q-Tel programme.
    - **Series A Venture Fund**. Growing the National Security Strategic Investment Fund (NSSIF), the successful Series A investment vehicle.
    - **Direct Investment**. Extending support through NSSIF to counter-FDI and to secure UK sovereign capabilities.
    - **Innovation Coordination**. Supporting NSTIx, a x-HMG strategic coordination and alignment function and 'front-door' for innovation programmes.
    - **Venture Builder.** Building start-ups to meet the national security 'problem set'.
    - **Accelerator Network**. Building a strategic network through systematic and proactive engagement with existing commercial and university accelerators.

37. The *Exploit* strand comprises:
    - **Interface Centre**. Supporting the development of open 'problem sets' and managing engagement with venture partners and portfolio companies with a view to pilots, trials and transfer to mission.
    - **Work Programmes.** Using the US In-Q-Tel approach. Funding for early use of 'HMG as a customer' to adapt, conduct pilots, trials and transfer to mission.
    - **Co-creation Centres.** Building co-creation centres that bring together HMG, SMEs, primes to work in partnership co-developing and sharing capabilities across classification levels.

IV NEXT STEPS

38. S&T has shifted from the periphery of national security strategy to the centre. This is broadly appreciated. The policy framework is in place and a substantial programme of work within the National Security Community is underway. Two further and important initiatives support this.

39. In order to achieve 'Strategic Advantage in S&T', the direction signalled in the Integrated Review, it will be necessary **to develop an end-to-end system that will provide much greater alignment between national security strategy and S&T policy** and **to strengthen the voice of S&T within the National Security Secretariat (NSS)**. The National Security Community strongly welcomes work on these important goals.

40. As the UK find its place in an uncertain international environment, with new issues and changed relationships to the fore, it will depend on its national security capabilities to deliver greater resilience domestically and a strategic edge overseas. It will require a wholly new integration with the prosperity mission of HMG.

41. **The UK is unusual amongst its allies in having no government-sponsored institution capable of driving the learning necessary to the formulation and execution of a modern national security doctrine.** The Integrated Review signals that the case for a UK College for National Security will be reviewed in preparation for the next Spending Review (SR).

42. **The broader national security community will require a significantly enhanced understanding of accelerating technological and societal developments so that it is well equipped with the skills necessary to address and exploit their potentially game- changing impact on our security and way of life.** Data (including large-scale qualitative open source materials), analytics, novel sensors, commercialised space, artificial intelligence (AI) and machine learning, behavioural sciences, bioengineering, global technologically mediated platforms, are all elements of this.

43. **A UK College for National Security (CfNS)** could play a key role in developing the synthesis of approaches necessary and equipping national security professionals for the changed environment. It would have the opportunity to: promote new curricula and new thinking, giving national security professionals the analytic skills and frameworks to adapt and develop; ensure the continuing role of UK as a leader in national security thought and practice; and act as a model of future professionalism. It could be a platform for innovative solutions to the toughest national security challenges. As a UK capability, the College could facilitate connectivity with allies and boost the UK's international reputation for innovative problem solving.

44. **The Integrated Review signals an important opportunity to place S&T (including data and behavioural sciences) alongside political analysis and international relations at the centre of national security recognising the transformative role they are playing and have the potential to play in the future.** It is difficult to envisage a well-formed response to such issues as 'debt trap diplomacy', 5G telecommunications, ubiquitous facial recognition, foreign direct investment, social media encryption, attempted theft of vaccine information, civil society concerns over corporate encroachment on personal information, and so on, without bringing together geopolitics and technology**. We are in a position to reinforce UK national security policy development and execution and build the UK's reputation as a global player capable of thriving in the 21st century.**

19 May 2021