ADS GROUP EVIDENCE ON THE NATIONAL SECURITY CAPABILITY REVIEW PART 1

About ADS

1.1 ADS is the national trade association advancing the UK’s Aerospace, Defence, Security and Space industries. ADS comprises over 1,000 member companies across all four sectors, with over 900 of these companies identified as Small and Medium Size Enterprises (SMEs).

1.2 The UK is a world leader in the supply of aerospace, defence, security and space products and services. From technology and exports, to apprenticeships and investment, our sectors are vital to the UK’s growth – generating £72bn a year for the UK economy, including £37bn in exports, and supporting around 900,000 jobs.

Overview

1.3 The UK Government has recognised that 2017 has seen a significant change in the UK security environment, including a number of terrorist attacks, further disrupted attacks and an increased pace of hostile cyber activity. In order to adapt to the challenges of this rapidly changing threat environment, the Government is seeking to review the plans in place to implement the National Security Strategy, which aims to ensure that the UK’s investment in national security capabilities is as joined-up, effective and efficient as possible.

1.4 ADS believes that the interdependency between government and industry with regards to delivering on national security requirements is only set to continue to increase, and in the context of the proliferation of threats we have seen over the last year, we see an urgent need for a step-change in public-private cooperation. Therefore, with industry and Government working in close cooperation, we can positively contribute to the delivery of national security objectives for the safety and prosperity of the UK and ensure that we are successfully adapting to challenges which were not necessarily foreseen at the time of the 2015 Strategic Defence and Security Review (SDSR).

Changing Threat Environment

1.5 Since the 2015 SDSR the threat environment has evolved rapidly and is continuing to do so. We have witnessed, in recent years, an increased frequency of terrorist attacks¹ in the West, including the UK. This increased tempo stems from three factors: (i) a shift in modus operandi, favouring low levels of sophistication which are far more challenging to pre-emptively detect and disrupt by security and intelligence services, (ii) new methods of communication between potential hostile actors and (iii) access to extremist materials

through increased use of social media and technological advances in areas such as encryption.

1.6 Additionally, cyber security threats present a growing, rapidly-evolving and potentially highly damaging challenge to UK national security. Both the wellbeing and economic prosperity of the UK depend on the effective functioning of Critical National Infrastructure (CNI) and the ability for industry to defend against hostile cyber actors. To this end, increased collaboration between CNI entities, relevant industry bodies and Government department and agencies, particularly the NCSC, is crucial. For further information, please see ADS’s recent submission to the Joint Committee on the National Security Strategy (JCNSS) on cyber security and protecting the UK’s CNI.

Response

1.7 To adapt to and overcome the issues presented by this evolving threat, new initiatives are required and several of these are currently being explored by Government. The Joint Security and Resilience Centre (JSaRC), based in the Home Office, is currently leading on a number of projects to deliver solutions in priority security areas, for example in protecting crowded places. This is now particularly relevant and key to establishing a robust, effective mechanism of defence against this evolving threat.

1.8 It is ADS’s view that increased collaboration between the public and private sector in security matters is crucial for the effective fulfilment of NS objectives. ADS believes that the following priorities will allow the Government to more effectively address the rapidly evolving threats and challenges in the current environment:

1.8.1 Close cooperation between industry and Government is fundamental to delivering the Government's national security aims, as well as promote the prosperity of the UK security sector. Working together with Government from an early stage will allow industry to play a leading role in the efficient and effective delivery of current and future national security requirements, improving both the safety and prosperity of the UK. In the non-military security area, given the step-change in threats highlighted above, it is of fundamental importance that proposals and projects are made a reality, through the implementation of programmes which meet the national security requirements of Government, such as those articulated in the 2015 National Security Strategy and SDSR. The security industry has a key role to play in delivering capability to state agencies as well as private sector operators, especially in an environment of rapid change and evolution of potential threats, and Government should harness capability and expertise from industry to meet national security requirements in the most efficient and effective way possible.

1.8.2 Additional capabilities are needed to tackle challenges presented by increasing levels of digitalisation, particularly in areas such as fraud and cyber. In order to counteract the rapidly growing problem of fraud, which the Office for National Statistics has found is now the country’s most common form of crime, it
is important for Government to recognise the key role that the security industry could play in countering this threat. It is recommended that a national programme is implemented with the goal of aligning industry suppliers with operational end-users in the fight against fraud. This would require appropriate resourcing levels and coordination across agencies and departments; however it would present an efficient and effective way of meeting Government’s commitment to tackling fraud and to making the UK the safest place to do business online. The NSCR presents an opportunity to improve public-private cooperation in the cyber security arena. For example, there should be an improved mechanism for companies to report cyber incidents and security breaches, building on existing initiatives such as the Cyber Security Information Sharing Partnership (CiSP) and the Action Fraud Business Reporting Tool for bulk reporting high volume low impact incidents to the Police. Additionally, benefits would arise from developing further cooperation with the security industry, through new mechanisms as appropriate, to explore the realms of the possible around how the private sector could support Government and Law Enforcement agencies to a greater extent in providing the capabilities that are needed to help mitigate all forms of cyber-crime.

1.8.3  In ADS’s view, the recent establishment of JSaRC is a hugely welcome development and is an enormous opportunity to deliver future private-public sector coordination and cooperation on national security requirements. Therefore, in the current environment, with the emergence of increasingly diverse and sophisticated national security threats, a proactive JSaRC will be vital to widen engagement with industry and to implement security capabilities across Government departments and agencies. ADS believes that, in order for Government to be on the front foot in drawing upon the private sector’s contributions to meet national security challenges, additional investment will be needed. Therefore, as we have promoted through the UK Security and Resilience Industry Suppliers’ Community (RISC) that we participate, JSaRC should be ‘scaled up’ in order to better meet the needs of significantly increased levels of interaction and coordination between Government and multiple industry stakeholders, with a proactive, forward-leaning approach. This will allow Government to proactively counter national security challenges, and ensure that appropriate levels of personnel and expertise are in place help to influence the posture of the wider private sector.

1.8.4  There should be transparency of both Government resource and future Research and Development (R&D) security requirements, particularly in those areas under review, in both the public and private sector. In order for industry to meet upcoming Government requirements, it is essential that there is a clear picture of available resource for individual programmes and projects, as well as a clear idea of the Government’s intended requirements. It is recommended that the Government takes the opportunity of the NSCR to formulate a programme of risk-driven R&D, with a view to developing an intelligent requirement pool. Subsequent engagement should then be characterised by transparency around resourcing levels, and there should be
interaction on a more proactive basis with industry in order to reflect Government’s requirements and budget at the earliest opportunity.

1.8.5 As ADS has proposed recently to the Department for International Trade’s Defence and Security Organisation (DIT DSO) in RISC’s preliminary submission we led on the refresh underway to the UK security export strategy, there is a requirement for a re-energised and action-orientated campaign on security exports. Industry recognises DIT DSO’s primacy on the promotion of UK security exports, but we also seek a more integrated, ‘whole of government’ approach in identifying export potential and industry has a lot to offer and must be fully engaged in HMG’s strategy and overseas engagements in order to maximise UK industry export potential. We understand that the scope of the NSCR involves some re-examination into how to align most effectively the UK’s national security and prosperity objectives, and it is in this context we believe the exercise represents an opportune moment to ensure that the country’s security export strategy is afforded appropriate attention across all relevant departments and agencies.

Conclusion

1.9 The UK is facing numerous threats and challenges in a rapidly evolving security environment. In order to address these challenges and respond effectively, innovative solutions are required. As UK industry has world-leading capability and expertise within the field of security, we recommend that that Government recognises this asset and increases levels of public-private sector collaboration in order to meet national security challenges in both an efficient and effective manner. In ADS’s view, harnessing the potential of the UK security industry, with increased transparency and openness, will significantly enhance the Government’s ability to defend the UK as a whole, by getting ahead of the curve and adapting rapidly to counteract potentially dangerous developments in both the physical world and cyberspace.