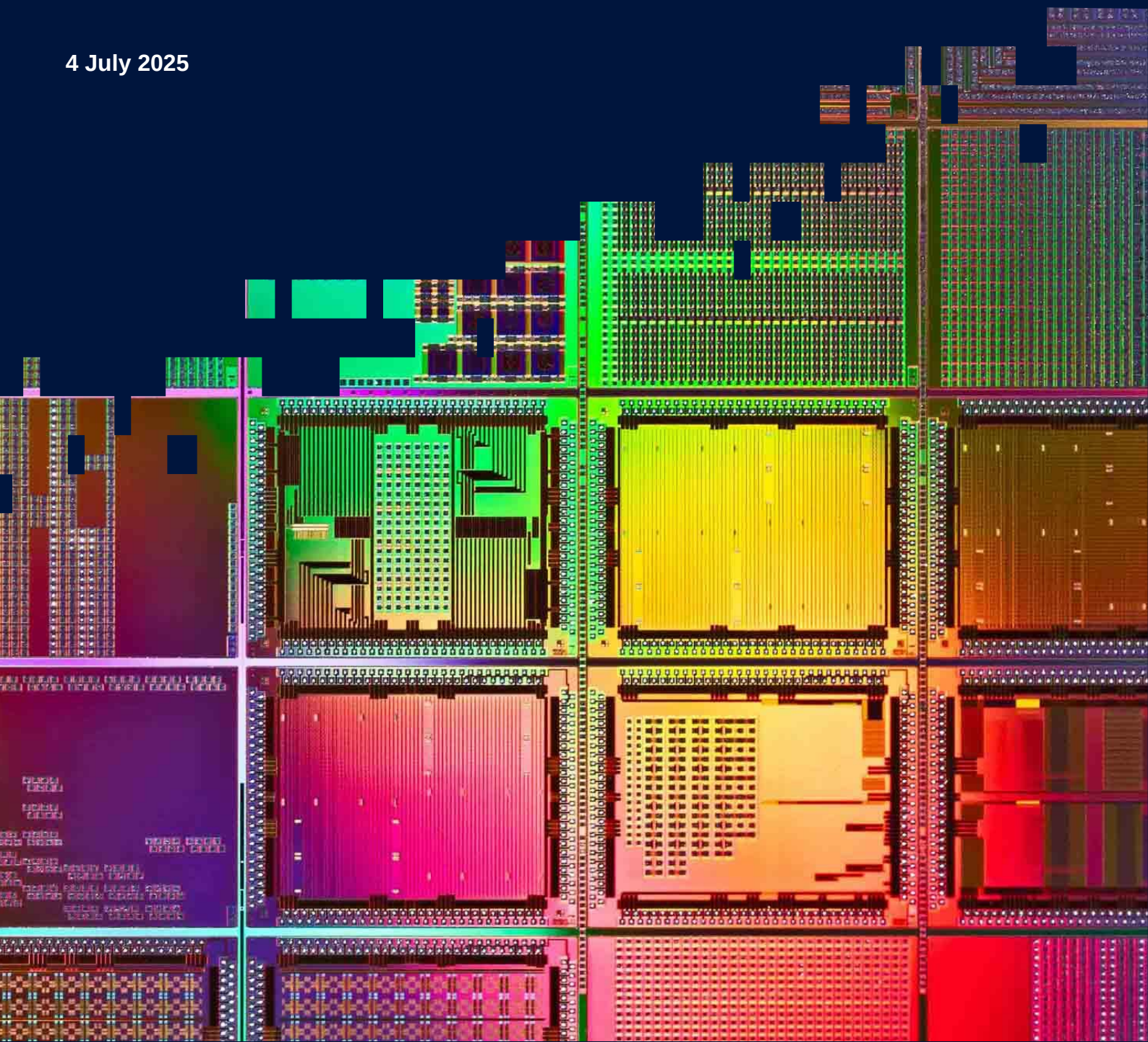
Final Impact Evaluation Report

Digital Security by Design Programme

4 July 2025



Executive summary

Introduction

This is the Final Impact Evaluation Report for the Digital Security by Design (DSbD) programme, an investment by the Industrial Strategy Challenge Fund (ISCF).

The DSbD programme launched in 2019 with £70 million funding from the UK Government and over £117 million matched investment expected from industry. The DSbD programme set out to transform the UK's digital infrastructure by addressing long-standing hardware security flaws. DSbD has aimed to tackle a critical market failure: the global reliance on inherently insecure microprocessor designs dating back to the 1970s. By fostering collaboration between academia and industry, DSbD has focused on developing a fundamentally secure hardware architecture.

The key takeaways and conclusions below are based on the evaluation questions agreed at the outset of the programme, and grouped into five sections, each of which is dealt with in detail in a chapter of this report. These findings are largely based on analysis of programme documentation, project reports, and interviews with people responsible for the delivery of the programme, those leading funded projects, and sector experts. The report also includes information from relevant secondary data sources, published reports, government strategy and policy documents, and media.

Key takeaways

Programme achievements and factors influencing outcomes

Following a nine-month delay agreed at the outset of the Covid-19 pandemic, the DSbD programme has progressed according to its revised schedule. All planned activities have been completed, with the exception of one academic proof project, 'AppControl: Enforcing Application Behaviour through Type-Based Constraints', which was granted an extension until May 2025.

The development of the technology platform prototype, known as the "Morello board," has been completed, verified, and delivered for use by funded projects and partners. The Morello board has been used to investigate the technology and its potential impact/benefits for new products and services.

The programme has adapted in response to market needs and availability of additional funding opportunities, resulting in several key adjustments outlined below.

- Amalgamating separate academic research strands into a single call, adopting a portfolio approach.
- Initial "De Minimis" calls for SMEs were followed by a larger-scale industrial research competition, aimed at upskilling potential SME participants in the latter.
- Running a joint IUK/EPSRC call to permit both academic- and industry-led bids.
- Increasing the number of industrial Demonstrators from five to six.
- Funding the development of RISC-V microcontroller based test boards (the "Sonata" and "Symphony" boards) to complement the Morello approach and using these instead of Morello for the final cohort of the Technology Access Programme (TAP).

The stream of work resulting in the RISC-V test board has been a catalyst for industrial investigation of the technology. This has led to the first commercially available CHERI products being announced using a RISC-V platform.

Any intervention which follows the DSbD programme to achieve further impact should aim to build on the activities and efforts of DSbD. Following information from DSbD participants and sector experts, it should

focus on: regulation, policy and standards; understanding of cyber threats and solutions; and skills to develop and integrate new solutions.

Impacts on R&D Capability and Capacity

DSbD programme has notably enhanced the R&D capability and capacity of researchers and businesses involved in developing new DSbD hardware and software. Most of the funded project stakeholders (17 out of 19) reported that DSbD projects facilitated the development of new skills and capacity for adopting emerging technologies.

Improvements in skills base of researchers and businesses

The DSbD programme has upskilled researchers and businesses involved in its funded projects, surpassing initial targets by facilitating 54 Master's and PhD degrees, compared to the goal of 30 PhD and MPhil degrees. Researchers have improved their skills through exposure to new security capabilities, career progression, and training sessions within funded projects. A number of early-career researchers have benefited from these opportunities.

Knowledge transfer through taking up new roles is identified as a key enabler of DSbD's success. Notably, DSbD technology has been integrated into taught academic programmes, engaging over 230 students. Additionally, five businesses have been established or influenced by DSbD, positively impacting industry innovation and development, and paving the way for DSbD technology's TRL progression and subsequent commercialisation efforts.

Further opportunities unlocked through the DSbD programme

Researchers and businesses have secured further opportunities through their involvement in the DSbD programme. Four primary investigators from academic proof projects and two organisations from De Minimis workstream were awarded funding in other DSbD workstreams.

Four DSbD projects have also received follow-on funding from EPSRC, NCSC, and DSTL, extending their CHERI work. Additionally, project partners from four academic proof projects, two software development ecosystem projects, and one demonstrator are currently submitting research funding proposals that further build upon their DSbD work.

The DSbD programme has facilitated broader opportunities, such as networking, identifying new partners for future collaborations, and invitations to events, workshops, and talks.

There is some evidence of further business opportunities unlocked through the DSbD programme. Business partners on a demonstrator project are exploring commercial opportunities that build on their DSbD work and expand their testing activities to potentially support early adopters of CHERI.

Impact on R&D Funding

R&D funding from other government sources

The DSbD programme has secured £30 million in additional funding from government sources other than UKRI and its Research Councils, significantly surpassing the initial target of £6 million.

The additional funding has supported the expansion of DSbD activities, such as

- increased investment in TAP;
- business-led demonstrator projects; and
- the production of Morello Boards.

This financial backing indicates greater confidence of UK government for DSbD technology and the programme's overall alignment with the UK research agenda and government's long-term strategy.

The government has also supported wider activities influenced by the DSbD programme. These include commissioned research into CHERI, providing follow-on funding for DSbD participants, and supporting the CHERI Alliance, which promotes the adoption and standardisation of CHERI technology.

Private investment related to the DSbD programme

To date, **the DSbD programme has secured over £238 million in co-investment from private organisations, surpassing its target** of £117 million of private co-investment by 2025.

The aligned private co-investment, amounting to nearly £132 million, was secured from 13 different sources, predominantly large industry players such as Google and Microsoft. As aligned co-investment is an indicator of investment in R&D beyond the parameters set by funded activities, this suggests a high level of confidence from private organisations in DSbD technologies and CHERI.

Additionally, an estimated £190 million in follow-on investment is expected in the coming years from four companies to further develop DSbD work with the intention of adopting and commercialising DSbD technology.

However, to achieve the long-term target of securing £800 million in private R&D investment by 2027 for delivery of DSbD enabled products and services, the DSbD technology must attract further aligned investment from large, influential companies. This target is likely to be attainable, provided that a CHERI-enabled chip becomes available for adoption in commercial products and services. It would also be beneficial to see contributions from a larger number of smaller companies that have been drawn into the developing ecosystem, as evidence of investment in product and service development.

Impacts on Collaboration

Business-academic engagement activities

The funded projects have effectively fostered business-academic collaboration, with 61% of the total projects being delivered through joint efforts between industry and academia. DSbD activities outside of the funded projects have also facilitated engagement between businesses and academic institutions, including:

- DSbD All Hands events – Included talks, demonstrations, poster sessions, and discussions. The All Hands events have supported networking activities and facilitated valuable industrial connections.
- CHERI Tech forum – Facilitated knowledge exchange between academia and industry through technical discussions.
- CHERI Alliance technical working groups – These provide a means of engagement between various stakeholder groups through technical working groups focused on addressing practical issues related to the adoption of the DSbD technology and reducing the associated costs of adoption. Run by CHERI Alliance, these will continue after the DSbD programme.

Level of collaboration between SMEs and large companies

The collaboration between SMEs and large companies has mainly occurred through the Technology Platform Prototype and Demonstrator workstreams, with 50% (3 out of 6) of demonstrators showcasing such partnerships.

However, only one out of twenty projects from the software ecosystem and De Minimis workstreams involved collaboration between SMEs and large companies. This highlights a missed opportunity; these projects aimed to enable the growth of the software ecosystem for adoption of DSbD technologies, and enhancing the capacity of SMEs to participate in further collaborations could have contributed to this.

While DSbD has facilitated some collaboration between SMEs and large companies, there remains potential to increase the level of collaboration, which would help SMEs develop key industrial connections and enhance their growth and capabilities for future projects.

Impact of multi- and interdisciplinary research and innovation (MIDRI)

Interdisciplinary research was more prevalent than multidisciplinary research in funded projects, indicating that these projects successfully integrated expertise from multiple disciplines fundamentally, rather than separating tasks.

- Academic Proof projects showed high levels of interdisciplinary collaboration, especially in computer science, cyber security, social sciences, law, and mathematics.
- Software Ecosystem projects, including De Minimis, had fewer multi- and interdisciplinary impacts, although academic-led projects contributed to such research.
- Demonstrator projects exhibited some interdisciplinary working, mainly through university-industry partnerships, with one project reporting multidisciplinary research.

To date, the DSbD funded projects have produced 209 publications, with 69% available as open access, thereby improving knowledge dissemination and research impact. The University of Essex, University of Manchester, and Imperial College London are leading contributors to DSbD-related publications, with the University of Manchester's collaboration with foreign institutions highlighting the global reach of DSbD research.

More broadly, **collaboration between hardware and software companies within the sector is improving but remains variable**, influenced by geography, sub-sector, and company size. The DSbD programme has positively impacted hardware-software collaboration, particularly in capability hardware and memory safety.

Impacts on Cyber/Digital Security

Understanding of needs of cyber security and raising awareness of cyber and digital security issues

The DSbD programme has actively contributed to raising understanding and awareness of cyber and digital security issues in multiple government departments, shaping government thinking. This has led to DSbD featuring in several government policy and strategy documents such as the Innovation Strategy 2021, National Cyber Strategy 2022, and Semiconductor Strategy 2023.

DSbD has also been successful in raising awareness among technical and cyber security experts, though there is still work to be done to engage senior decision-makers in large companies and demonstrate a strong business case with clear pathway to economic benefits.

The DSbD programme's impact on public awareness is minimal. However, the primary focus of DSbD has been to ensure that foundational security measures are integrated into products and services. This approach creates a more secure digital environment without relying on public understanding of technicalities behind cyber security measures.

Catalysing transformational change on cyber security

This has been achieved through:

- facilitating good progress in driving transformational change within the UK's cyber security landscape. government funding and support.
- influencing the commercialisation efforts of CHERI.

Internationally, the programme has notably influenced publications in the “memory safety” domain, particularly in the United States. CHERI technology has been referenced in official reports from the White House and Cybersecurity and Infrastructure Security Agency (CISA).

There is evidence that some companies are actively working towards commercialising DSbD technology. However, it is crucial that more firms join these efforts to integrate CHERI into their products and services, as this broader participation is essential to ‘shift the dial’ within the cyber security sector.

Moreover, additional intervention and follow-on funding are needed to further embed DSbD technology and CHERI into future products and services, thereby supporting widespread adoption.

Impact on cyber attacks

The DSbD programme's impact on reducing cyber attacks is yet to be realised, as there are no live DSbD-based products in the market currently.

However, it is expected that the successful implementation and adoption of DSbD technology can lead to a considerable reduction in cyber attacks, particularly benefitting medium and large businesses that face larger financial consequences from these attacks.

Awareness of new security capabilities

Evidence of interest and awareness in new security capabilities suggests a **slowly but steadily growing awareness of the DSbD technology** over the programme period. DSbD has attracted a global audience, with significant engagement from users in the UK and the US.

While traditional news posts reached approximately 31,000 individuals across 16 published articles, social media—despite a lower volume of posts—achieved significantly higher engagement, reaching around 95,000 users. Notably, the recent **DSbD Showcase emerged as a focal point of online engagement**.

Although DSbD led in terms of volume and reach within the Digital & Technologies category in February 2025, its overall visibility remained comparatively lower than that of other challenge areas, such as Net Zero. As the programme approaches its conclusion, there exists **a clear opportunity to extend its visibility and sustain the impact of its supported technologies beyond the formal end of its funding cycle**.

Impacts on Businesses

Creation of new products and services

Three physical products have been developed through the DSbD programme:

- The Morello Board (Arm).
- The Sonata Board (lowRISC/RISC-V).
- The Symphony Board (lowRISC/RISC-V).

While these products are prototypes for research and testing, they lay the groundwork for future commercial offerings.

The TAP has successfully introduced DSbD technology to UK businesses, particularly SMEs. Overall, TAP has received positive feedback across cohorts. Recommendations from cohorts highlight user-friendly documentation and support to ensure efficient onboarding and development on DSbD technologies.

Notably, 80% of DSbD survey respondents positively evaluated the Morello board for potential use in their future products and services. Despite this, the programme has not yet achieved its target of 200 companies positively evaluating the board.

DSbD-funded projects have developed over 31 software and tools, however, commercialisation of these developed tools remains a challenge, as a commercial product is not yet available. Stakeholder interviews revealed that the involvement of academic institutions has been crucial, but greater private sector engagement is needed to ensure the integration of DSbD technology into future products and services.

The independent use of DSbD technology by large companies such as Microsoft and Codasip strongly demonstrates its potential, opening pathways to achieve downstream adoption.

- In 2023, Codasip successfully demonstrated the first commercial implementation of the CHERI architecture within its X730 processor. Since then, the company has further integrated CHERI into another processor.

- Two companies – SCI Semiconductor, and Secqai – are expected to offer products with CHERI architecture in the near future. Market availability of CHERI-enabled products is projected as early as the end of this year or the beginning of 2026.

Impacts on organisational culture

The programme has influenced the organisational cultures of businesses and academic institutions by:

- Redirecting research efforts towards DSbD-related areas.
- Providing opportunities for the exploitation and commercialisation.
- Establishing the necessary infrastructure, supported by the government's long-term commitment to the DSbD programme.
- Influencing the strategic business models of private organisations.

Impacts on share of export market for businesses participating in the DSbD programme

At present, there is no fully commercialised product incorporating DSbD technology that could significantly influence export market share. However, there are a few examples suggesting that such developments may occur in the near future.

- Cyber Hive, funded by DSbD, has been pursuing international commercial traction through the CHERI USP in their existing product line, which has garnered demonstrable interest and excitement from companies.
- Codasip's implementation of CHERI was stimulated by a customer, indicating potential increases in export revenue through the commercialisation of DSbD technology.

Perceived contribution to UK productivity

Currently, there are no directly observable impacts on productivity as there is no fully commercialised product incorporating DSbD technology.

A DSbD survey conducted by Innovate UK revealed that all business respondents (6 out of 14) acknowledged the potential productivity advantages of adopting DSbD technology.

In 2024, 50% of UK businesses responding to the Cyber Breaches Survey reported experiencing cyber attacks, up from 39% in 2022. Through the funded projects, it has been demonstrated that DSbD technology can mitigate 70% of known memory safety vulnerabilities, thus reducing downtime from cyber attacks or memory-unsafe programming. The latter was responsible for the 2024 CrowdStrike outage reportedly leading to $5.4 billion in financial losses.

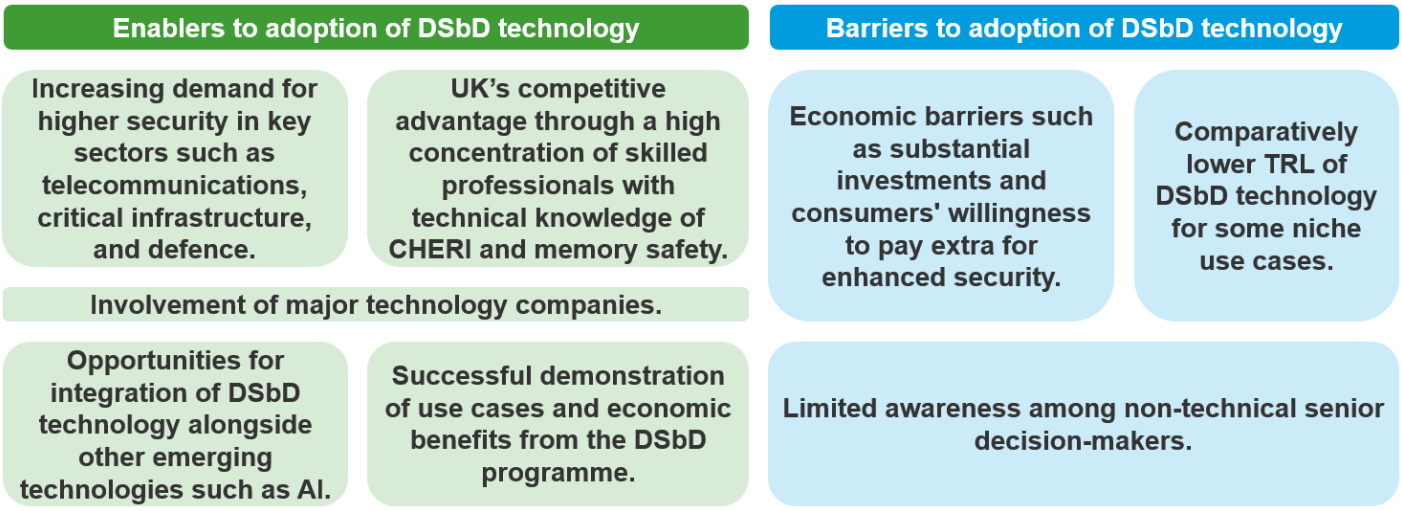
Additionally, the DSbD programme showed that adopting CHERI requires minimal code changes and enhances software verification, potentially reducing security review times and improving engineering productivity.

UK reputation in cyber security

The **DSbD programme has had a positive impact on the UK's standing in the field of cyber security**, primarily through substantial job creation and sectoral growth. To date, the DSbD has successfully facilitated the creation of 405 new jobs, far surpassing the initial target of 100 jobs by 2025. These new jobs are projected to contribute approximately £29.6 million in GVA to the UK economy.

Additionally, the DSbD programme has led government missions to the United States, Australia, India, and Japan. These missions have not only raised global awareness of DSbD technologies but have also facilitated the distribution of Morello Boards in the US and Australia.

Enablers and barriers to adoption of DSbD technology



Conclusions

The programme can be judged to be a success against its initial objectives for activities and outputs. In particular, the design, implementation, and formal verification of the Arm Morello platform is a significant milestone in secure computing, offering a solution in hardware to memory safety issues which at the outset of DSbD (and to this day) make up around 70% of reported vulnerabilities. The programme has also delivered six Demonstrator projects outlining specific use cases for industry (against an initial expectation of five projects in two tranches).

The original route to adoption, as set out in the business case, was for CHERI architecture to be adopted into an Arm reference design, at which point it could be used by the major mobile device operating systems and gain widespread adoption. This route is not likely in the medium term; even though the technology has been proven to be sound, the work required to update the codebase in the software ecosystems that might adopt it is prohibitive and would not be carried out without requisite demand from a major supplier of mobile devices and/or software.

In the near future, the route to market is in smaller microcontrollers for embedded computing and the Internet of Things. The programme has catalysed and part-funded research and development of a RISC-V based solution, culminating in funding of a design for a RISC-V test board. This provides the short-term route to adoption for CHERI, with three companies having announced CHERI processors scheduled for commercial availability in 2025.

The integration of DSbD technology into UK Government strategies and global policy documents referencing hardware and software solutions for "memory safety" provide an avenue for building awareness of the technology in future. The UK Government can also drive the market by laying down standards for memory safe computing and adopting CHERI into its new Secure by Design procurement framework as a method which meets required standards for security-critical products and services such as critical national infrastructure and defence.

According to DSbD participants and sector experts interviewed for this evaluation, the key external factors affecting successful delivery of cyber security projects are:

- **Regulation**, **policy**, and **standards** to guide companies in decision-making (whether suppliers or consumers of cyber security solutions).
- Lack of knowledge/understanding of cyber threats and technological solutions, cost pressures and risk aversion in the marketplace.
- **Skills** to develop new solutions (supply side) and to integrate them into existing systems (demand side).

Any future intervention to promote CHERI adoption and deployment could therefore focus on:

- Growing the UK cyber and digital security ecosystem, involving Government policy and procurement where possible.
- Building awareness of cyber security threats and the role that CHERI can play in addressing these, with particular reference to “memory safety” as an agreed set of problems and solutions.
- Developing capacity and capability to use CHERI technology when it becomes commercially available.

Contents

1. Introduction and Methodology

This is the final Impact Evaluation Report for the Digital Security by Design (DSbD) programme. RSM was commissioned to evaluate the DSbD programme in 2020 and we have produced the following reports:

- Evaluation framework (2020).
- Baseline report (2020).
- Process evaluation (2022) reports.
- Interim impact report (2023).

The principal research objectives of the impact evaluation are to answer a set of impact evaluation questions which were proposed by UKRI and developed and agreed at the evaluation framework stage. A table in this chapter sets these evaluation questions out, along with links to where they are addressed in this report.

This chapter introduces the programme, its activities and objectives, and the methods adopted for this evaluation.

1.1. About Digital Security by Design

1.1.1 Background and strategic context

The **Digital Security by Design (DSbD) Programme** (hereafter “the Programme” or just “DSbD”) was announced in January 2019 as a new programme to contribute to the objectives of the government's Industrial Strategy. It was to be awarded a total of £70 million of government investment from the Industrial Strategy Challenge Fund (ISCF) over the period April 2019 - March 2024 (with grant funding expected to be allocated by Q3 2021), matched by at least £117 million in expected funding from industry.

The DSbD programme aimed to overcome market failures and radically update the foundation of the insecure digital computing infrastructure that underpins the entire economy. Its objectives were to:

- Demonstrate a more secure hardware platform capable of protecting the integrity and resilience of software in response to significant market need for cyber security.
- Enable more secure platforms for services which make extensive use of secured, personal data and create investment in new scalable businesses, digital products and services.
- Accelerate the move towards digital transformation of industry, with the accompanying investment in productivity and improved reliability of digital services.

The market failure rationale for the intervention is that microprocessor designs are inherently insecure and have been since the progenitors of modern processors were designed in the 1970s, giving rise to security vulnerabilities. However, the global IT industry, and the skills of IT employees, are based on these designs, and any radical improvement in hardware design would require a step change in how IT companies go about their business. The market failure is based on both a coordination problem on the part of hardware and software engineers, and a lack of information in the target market:

- Hardware manufacturers will not design and build hardware for which software does not yet exist as there would be no market for it.
- Software developers will not write code for hardware that does not yet exist.
- Consumers have not been demanding more secure technology as they are largely unaware of the inherent risks.

The market has therefore not provided a solution to this historic vulnerability; instead, individual companies have attempted to write software that is not exploitable and have released patches to address vulnerabilities when they become aware of them, or when they are exploited. There is no commercial motivation for a single organisation to solve the problem. This is the context for funding DSbD to address this issue by a combination of government and industry innovation.

In this regard, DSbD directly contributes to the Industrial Strategy objective to increase R&D spending. It was designed to lever in significant additional R&D investment from industry, and also to unlock future investment in an area which is held back by market failure, but which could generate significant future private sector R&D investment, as companies adopt the new technology and develop products and services based on it.

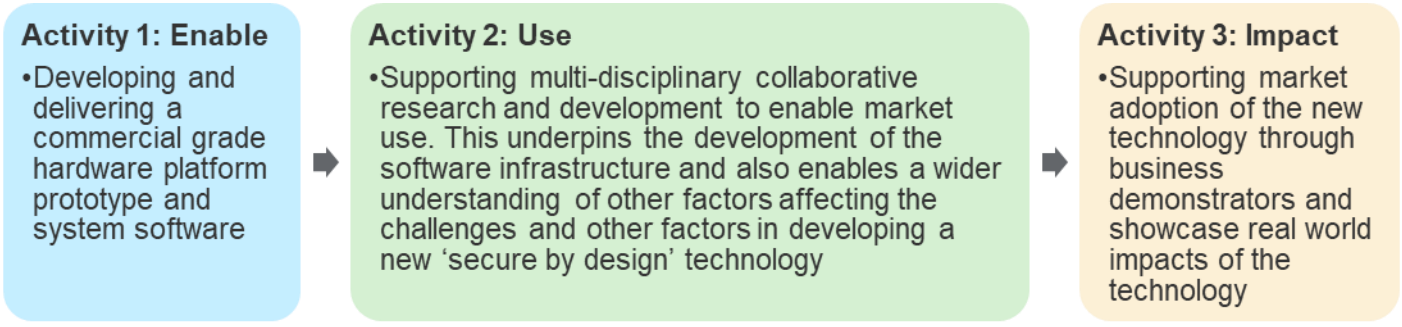
1.1.2 About DSbD

DSbD aimed to address the market failures set out above by funding the development of a microprocessor which does not suffer from the memory security problems common to current microprocessors and is therefore expected to be inherently more resistant to cyber threats. The changes involve replacing 'pointers' (references to locations in computer memory used in programming languages) with 'architectural capabilities'. This was expected to result in significantly improved memory safety, thereby allowing the creation of software that is inherently more robust against attacks. Computer hardware then current did not allow for this fine-grained level of memory control to be constructed in a performance-efficient way, meaning that hardware as well as software changes must be made.

This approach to modifying a microprocessor to protect the contents of its memory from poorly written software, and from others attempting to exploit this vulnerability, is based on the results of ten years of research led by the Computer Laboratory at the University of Cambridge through the Capability Hardware Enhanced RISC Instructions (CHERI) programme. CHERI and Arm have been collaborating since 2014, and the concepts developed by the CHERI project are being used by Arm to develop the prototype architecture.

The objectives for the programme – to demonstrate and enable a new technology platform and accelerate digital transformation through its adoption – were built into three groups of activities taking the technology from research to commercialisation. These were known as "Enable", "Use", and "Impact", and are set out in Figure 1 below.

Figure 1: DSbD activities



DSbD's contribution to the Industrial Strategy objective to increase R&D spending is built into the activities, as they were to be delivered by academic-industrial partnerships and would lever in significant additional R&D investment from industry in their delivery. The primary vehicle for this would be the Arm-led technology platform development project, which required significant co-investment and use of time and resources from Arm to be successful.

1.2. Overview of the methodology

Our methodology, set out below, is a theory-based evaluation methodology incorporating qualitative and quantitative evidence governed by a "Logic Model" for the programme, showing how the funded activities produce outputs and outcomes which in turn lead to eventual impacts.

Having developed a Logic Model, the evaluation framework needs to be able to test the validity of the causal links set out in the Logic Model (to show the extent to which the impacts can be attributed to DSbD) and assess the impacts against a **counterfactual** (what would have occurred in the absence of the intervention, taking into account other activities that may have been pursued). Following the initial inception meeting, RSM and UKRI jointly agreed that identifying such a counterfactual comparison group would not be feasible for the evaluation. This is due to the expected small number of funded projects under each activity strand, which systematically reduces the sample of comparable successful projects. This also rules out the use of other quasi-experimental approaches based on the econometric modelling of outcomes.

Furthermore, our familiarisation interviews highlighted the uniqueness of the DSbD programme and the fact that without it, the digital security sector would not organically produce a new hardware solution that can enable new secure software design/programming. This greatly limits the feasibility of constructing a credible counterfactual in this manner, as it is thus unlikely that unsuccessful applicants will be able to pursue similar activities in hardware-based digital security and at best would explore different areas of cyber and digital security not directly comparable with that of DSbD.

The evaluation is therefore based on a non-statistical, theory-based evaluation methodology. Our chosen approach is contribution analysis to assessing the extent to which the activities and inputs of the programme has contributed to the identified outcomes and impacts. This approach was selected because it is useful to understand how projects and businesses function in complex environments where sole attribution of impact is difficult.

The evaluation framework was developed at the interim evaluation stage and entailed refining the Logic Model and evaluation questions after completing interviews with staff responsible for programme delivery and some programme participants.

1.3. Evaluation questions

The evaluation questions, grouped into thematic chapters, are set out below.

In digital versions of this document, the chapter titles and section numbers are clickable[1] (underlined) links to the content which deals with them; clicking the Evaluation Question number (i.e. EQx) in an evidence chapter will return the reader to this table.

Table 1: Impact evaluation questions

Chapter	Impact Evaluation questions	Section
2. The DSbD Programme	How can DSbD activities be improved as the programme runs its course?	EQ1: 2.4
	What are the major factors influencing the achievement or non-achievements of DSbD outcomes?	EQ2: 2.5
3. Impacts on R&D Capability and Capacity	To what extent and how has DSbD improved R&D capability and capacity? To what extent has DSbD improved the UK skills base of researchers on new hardware? What further opportunities is DSbD opening up in the digital security innovation base?	EQ3: 3.3
4. Impacts on R&D Funding	To what extent and how has DSbD increased R&D funding from other government sources?	EQ4: 4.3

[1] Interactivity may vary by software; for example, in Microsoft Word for Windows, links must be Ctrl-clicked.

	Has DSbD increased private investment in UK digital R&D? And what are the profiles of investors?	EQ5: 4.4
5. Impacts on Collaboration	To what extent and how has DSbD increased business-academic engagement on innovation activities?	EQ6: 5.3
	To what extent and how has DSbD increased collaboration between younger, smaller companies and larger, more established companies up the value chain?	EQ7: 5.4
	To what extent and how has DSbD increased multi and interdisciplinary research?	EQ8: 5.5
6. Impacts on Cyber/Digital Security	To what extent has DSbD established the needs for cyber security? Has DSbD furthered the understanding of cyber security consumer needs?	EQ9: 6.3
	To what extent has DSbD helped raise awareness of the UK cyber and digital security issues? Has the DSbD programme provided a unified vision on how to remedy digital security issues? Is this vision shared by industries and policymakers?	EQ10: 6.3
	To what extent has DSbD catalysed or contributed to the cyber security transformational change? Why, why not?	EQ11: 6.4
	To what extent and how has the Challenge successfully enabled the potential reduction of the number of successful cyber attacks in the UK?	EQ12: 6.5
	To what extent and how has DSbD increased the awareness of new security capabilities?	EQ13: 6.6
7. Impacts on Businesses	To what extent and how has DSbD enabled the creation of new more secure products and services?	EQ14: 7.3
	To what extent has DSbD created the sustainable change in organisational cultures and structures in hardware/software development companies, and key industries which can ensure DSbD activities are sustainable beyond 2024? How far has this had an impact on the digital and cyber security industry?	EQ15: 7.4
	To what extent and how has DSbD increased the share of export market for those participating in the challenge?	EQ16: 7.5
	To what extent and how has DSbD contributed to productivity in the UK?	EQ17: 7.6
	Has DSbD improved the UK reputation in cyber security? Has this led to wider benefits such as new commercial ventures? How sustainable are they?	EQ18: 7.7
	What are the socioeconomic drivers leading to increased demand for digitally secured products and services? And what are the key barriers impeding the adoption of new DSbD technology?	EQ19: 7.8
8. Conclusions	What has been the principal value added of DSbD to date? To what extent have DSbD investments been value for money as a delivery mechanism for increasing UK digital security levels?	EQ20: 8.1
	To what extent has DSbD accelerated the adoption of the new hardware architecture? Is there any evidence of new products and services deployed as a result?	EQ21: 8.2
	What wider effects did DSbD investment had on funded projects?	EQ22: 8.3

1.4. Programme Logic Model

The Logic Model is a representation of the inputs to the programme, the planned activities, the outputs, outcomes (early/medium term results) and impacts (long term results corresponding to the key objectives of

the intervention). The time frames for these extend beyond the lifetime of the programme, with early and medium-term outcomes originally expected by 2022-24, and longer-term impacts expected beyond 2024 and well into the future, given the amount of time required to develop, commercialise, and scale up new technology.

The Logic Model is core to the evaluation as it provides the detail on the impacts expected at the outset from the investment made in DSbD. It has been used to evaluate if the programme has delivered the outcomes as intended, and if the intermediate steps toward the ultimate impacts can be observed, whether as direct results of the funded activities or arising from external developments.

The interim evaluation stage focused on the early-stage outcomes:

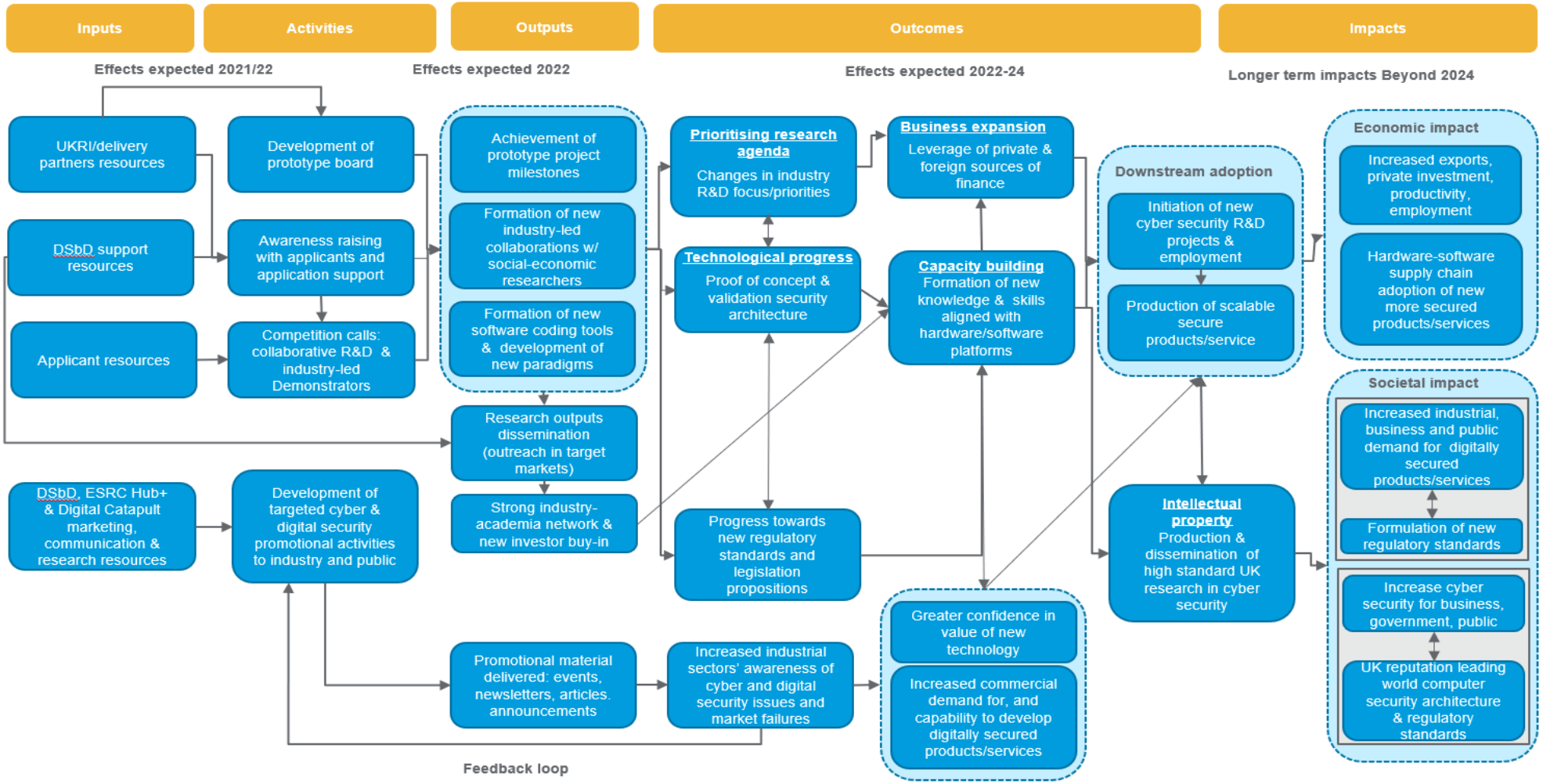
- Technological progress.
- Prioritising the research agenda.
- Business expansion.
- Capacity building.

This final evaluation report builds on this to provide detail on the programme's outcomes and achievements at the point of near-completion[2] and on the current state of CHERI technology, its market placement and potential future adoption and deployment.

The programme's Logic Model is shown in the diagram below.

[2] At the time of writing, all funded activities are complete except for one academic research project which has been extended to May 2025.

Figure 2: DSbD Logic Model



Assumptions

- Appropriate demonstrator projects are selected
- Prototype board tested and technology validated by academic & industry partners
- Development prototype boards are timely produced and delivered
- Government funding is match funded by industry
- Social and technological research professionals and industry collaboration

Assumptions

- Raised confidence in value of digitally secured products and services with private investors
- Agreement of targeted industries/companies & academic stakeholders of DSbD rationale and desired outcomes
- Demonstrators show potential to generate profitable returns, lower costs of digital security and replication
- Digital security industry has supply and access of skilled hardware-software engineers
- Targeted companies adopt DSbD new technology
- Public's awareness and motivations to adopt digital security requirements are elicited and considered in the design of products/services

1.4.1 Potential outcomes and impacts

A set of potential **outcomes** that were identified in the programme's Logic Model were as follows:

- Prioritising the research agenda and changing industry R&D priorities.
- Technological progress (proof of concept and validation security architecture.
- Progress towards new regulatory standards and legislation.
- Increased industrial sectors' awareness of cyber and digital security issues and market failures.
- Business expansion (leveraging private and foreign investment).
- Capacity building (formation of new knowledge and skills aligned with hardware/software platform).
- Greater confidence in the value of the new technology.
- Increased commercial demand for and capability to develop digitally secured products and services.
- Downstream adoption through:
  - Initiation of new cyber security R&D projects and employment
  - Production of scalable secure products and services
- Intellectual property (production and dissemination of high standard UK research in cyber security).

The **longer-term impacts** identified in the Logic Model are:

- Economics impacts:
  - Increased exports, private investment, productivity and employment
  - Hardware-software supply chain adoption of new more secure products and services
- Societal impacts:
  - Increased industrial, business and public demand for digitally secured products
  - Formulation of new regulatory standards
  - Increased cyber security for business, government and the public
  - UK reputation leading world computer security architecture and regulatory standards.

The table below sets out the evaluation questions, the Logic Model outcome and impact nodes they relate to and relevant data sources:

Evaluation Question	Logic Model Node	Data source
To what extent and how has DSbD improved R&D capacity and capability? To what extent has DSbD improved the UK skills base of researchers on new hardware architecture and software development? What further opportunities is DSbD opening up in the digital security innovation base?	Outcome: Capacity building: formation of new knowledge and skills aligned with hardware/software platforms	Researchfish; UKRI survey; interviews with funding recipients
To what extent has DSbD created the sustainable change in organisational cultures and structures in hardware/software development companies and key industries which come ensure DSbD activities are sustainable beyond 2024? How far has this had an impact on the digital and cyber security industry?	Impact: Increased industrial business and public demand for digitally secured products/services Outcome: Technological Progress: Proof of concept and validation security architecture Outcome: Progress towards new regulatory standards and legislation propositions	Interviews with funding recipients and Advisory Board

To what extent and how has DSbD increased multi and interdisciplinary research?	Outcome: Capacity building: formation of new knowledge and skills aligned with hardware/software platforms	Interviews with funding recipients; bibliometric analysis
To what extent and how has DSbD increased business-academic engagement on innovation activities?	Outcome: Prioritising research agenda: changes in industry R&D focus/priorities Outcome: Intellectual property: Production and dissemination of high standard UK research in cyber security.	Interviews with funding recipients, analysis of secondary data including Researchfish, TAP cohort reports.
To what extent and how has DSbD increased collaboration between younger, smaller companies and larger more established companies up the value chain?	Outcome: business expansion	Interviews with funding recipients
To what extent and how has DSbD increased R&D funding from other government sources?	Outcome: Prioritising research agenda: changes in industry R&D focus/priorities	interviews with funding recipients, analysis of secondary data
To what extent and how has DSbD increased the share of export market for those participating in the challenge?	Impact: increased exports, private investment, productivity, employment	Analysis of secondary data
Has DSbD increased private investment in UK digital R&D? What are the profiles of investors?	Impact: increased exports, private investment, productivity, employment	Analysis of secondary data
To what extent and how has DSbD contributed to productivity in the UK?	Impact: increased exports, private investment, productivity, employment	Analysis of secondary data, interviews
To what extent and how has DSbD established the needs for cyber security? Has DSbD further the understanding of cyber security consumer needs?	Outcome: increased commercial demand for and capability to develop digitally secured products/services.	Analysis of secondary data, interviews
To what extent has DSbD helped raise awareness of UK cyber and digital security issues? Has the DSbD programme provided a unified vision on how to remedy digital security issues? Is this vision shared by industries and policy makers?	Outcome: increased industrial sectors' awareness of cyber and digital security issues are market failures	Interviews
To what extent and how has DSbD enabled the creation of new and more secure products and services? What are the socio-economic drivers leading to increased demand for digitally secured products and services? What are the key barriers impeding the adoption of new DSPD technology?	Outcome: production of scalable secure products/services.	Analysis of secondary data, interviews
To what extent has DSbD accelerated the adoption of the new hardware architecture? Is there any evidence of new products and services deployed as a result?	Outcomes: All on Downstream adoption	Interviews with funding recipients and those outside of the programme

To what extent and how has the Challenge successfully enabled the potential reduction of the number of successful cyber attacks in the UK?	Impact: increased cyber security for business, government, public	Analysis of secondary data
How can the DSbD activities be improved as it runs its course?	All	Interviews with funding recipients and UKRI delivery team
What are the major factors influencing the achievement or non-achievement of DSbD outcomes?	All outcomes and impacts	Interviews with funding recipients and UKRI delivery team
Has DSbD improved the UK reputation in cyber security? Has this led to wider benefits such as new commercial ventures? How sustainable are they?	Impact: UK reputation leading world computer security architecture and regulatory standards	Analysis of secondary data
To what extent has DSbD catalysed or contributed to the cyber security transformational change?	Impact: increased industrial business and public demand for digitally secured products/services	Interviews, analysis of secondary data
To what extent and how has DSbD increased the awareness of new security capabilities?	Outcome: greater confidence in value of new technology	Analysis of secondary data
What has been the principal value added of DSbD to date? To what extent have DSbD investments being value for money as a delivery mechanism for increasing UK digital security levels?	All outcomes and impacts	Interviews, analysis of secondary data
What wider effects did DSbD investment have on funded projects?	All outcomes and impacts	Interviews with funding recipients.

This report is based on findings from a range of tasks completed by the study team over the course of the evaluation. An overview of these tasks is presented below.

1.4.2 Review of monitoring and management information

The report is based on management information collected by Innovate UK and the participating Research Councils, project completion reports and Researchfish impact submissions compiled by project teams. This has been supplemented by publicly available information such as research reports, government policy and strategy documents, and media.

1.4.3 Stakeholder consultations

For the evaluation we interviewed a range of stakeholders to develop and assess the contribution story for DSbD. The table below shows the numbers of people interviewed by type of stakeholder.

Table 2: Stakeholder Interviews Summary

Stakeholder groups	Evaluation Framework	Baseline	Process Evaluation	Interim Impact Evaluation	Final Evaluation
Board member*	0	0	4	1	0
Award recipient	3	14	11	22	21
Advisory group	10	3	3	2	1
Delivery group	4	8	10	1	1
Monitoring officer	0	0	1	0	0

Award panel	0	3	0	0	0
External expert**	1	2	0	0	2
Total	**18**	**30**	**29**	**26**	**25**

** Excludes Delivery Group members who attend the Board.*
*** External experts were asked contextual questions from the Advisory Group questionnaire.*

Interviews were conducted via Teams and notes/transcriptions added to an excel spreadsheet to analyse the results. Topic guides were prepared for different stakeholder groups to address the evaluation questions as shown in the table above and ensure consistency across /between stakeholder groups. Interviews were analysed thematically using a spreadsheet to collate responses. Responses were segmented by stakeholder group and topic guide question. Differences and similarities between and across groups were explored.

1.5. Limitations

It is difficult to test for many of the intended impacts within the life of the evaluation, as wider economic and societal impacts around improved security are unlikely to have occurred by the end of the funded programme activities, and are reliant on subsequent commercial research, deployment and adoption of the technology. However, the Logic Model approach allows us to trace whether the necessary intermediate steps have taken place or are planned.

While overall there has been a good level of stakeholder engagement (more than originally planned, in terms of engagement with people outside the DSbD funded activities), some stakeholders have not engaged so there is some missing information about particular projects.

At the time this evaluation report was completed, there were no commercial DSbD products available on the market. Consequently, it was not feasible to assess the impact of their adoption on cyber security within the scope of the evaluation (EQ12).

It was initially anticipated that DSbD technologies would be adopted within Arm chip architecture. However as the programme has progressed, It now seems likely that first adopters will be within RISC-V architecture and therefore we have consulted more with businesses in this space as the project has progressed.

2. The DSbD Programme

2.1. Introduction

This chapter addresses two evaluation questions that are crucial for understanding the programme:

- How can DSbD activities be improved as the programme runs its course?[3]
- What are the major factors influencing the achievement or non-achievements of DSbD outcomes?

2.2. Key findings

DSbD activities

- Following a nine-month delay agreed at the outset of the Covid-19 pandemic, DSbD has progressed to schedule. With the exception of one EPSRC-funded academic-led research project which has been extended to May 2025, all planned activities have now been completed.
- The technology platform prototype design has been completed, verified, and delivered in a physical implementation – the "**Morello Board**" – for use by projects and partners to investigate the technology and potential impact/benefits of this technology for new products and services.
- The programme has flexed in response to perceived market needs and availability of additional funding, amending planned workstreams and delivering new ones:
  - Amalgamating separate academic research strands into a single call with a portfolio approach
  - Arranging industrial research calls into an initial "de minimis" call for SMEs, followed by a larger-scale industrial research competition, to skill-up potential SME participants in the latter
  - Running a joint IUK/EPSRC call to permit both academic- and industry-led bids
  - Increasing the number of industrial Demonstrators from five to six
  - Funding development of RISC-V microcontroller based test boards (the "**Sonata Board**") to complement the Morello approach, and using these instead of Morello for the final cohort of the Technology Access Programme
- The last of these changes to the planned programme activities – the stream of work resulting in the RISC-V test board – has been a catalyst for industrial investigation of the technology and has led to the first commercially-available CHERI products being announced using a RISC-V platform.

Factors influencing achievement or non-achievement of DSbD outcomes

According to DSbD participants and sector experts interviewed for this evaluation, the key external factors affecting successful delivery of cyber security projects are:

- **Regulation**, **policy**, and **standards** to guide companies in decision-making (whether suppliers or consumers of cyber security solutions).
- **Lack of knowledge/understanding** of cyber threats and technological solutions, **cost pressures** and **risk aversion** in the **marketplace**.
- **Skills** to develop new solutions (supply side) and to integrate them into existing systems (demand side).

These factors suggest ways for any intervention which follows the DSbD programme to achieve impact.

[3] This research was carried out for the process evaluation in April 2022. The findings are repeated here, but it was agreed with Innovate UK that further research on this question between the process and impact evaluation was not necessary.

2.3. The DSbD programme and its progress to date

There was a nine-month overall delay agreed in the early days of the Covid-19 pandemic. Taking that into account, the programme broadly ran to schedule within the new timeframe, but there have been some changes in the details of the activities compared to the original design of the programme:

- In April 2020 Innovate UK commissioned Digital Catapult for an additional piece of work, the Technology Access Programme, which would offer UK companies the opportunity to have lab access to the DSbD technology being developed at an early stage. The overall vision for the Technology Access Programme was to accelerate the adoption of DSbD technologies by UK industries.
  - The Technology Access Programme has now delivered 6 cohorts of businesses using DSbD technology over the period to March 2025. The sixth and final cohort was based around the CHERIoT platform and lowRISC's Sonata Board, and as such was aimed at CHERI for embedded devices.
- In May 2020, Activities 1.2, 1.3b and 1.4 within the "Enable" activity were amalgamated into a single EPSRC call with three objectives aligned with the original separate activities and a portfolio of projects was selected targeting these.
- Also in May 2020, Activities 1.3a, 2.1 and 2.2, spanning a range of academic- and industrial-led software development activities in the "Enable" and "Use" phases, were grouped together into a single competition to meet the development needs of the programme. Then in August 2020, this was split into the SME software ecosystem competition and the main joint industrial and research competition. The SME component was intended to build SME capability and relationships with larger companies to facilitate diverse applicants to the main competition.
- In August 2020, Activity 2.3 was initiated with a £3.6 million investment from the ESRC to establish the DiScribe Hub—a dedicated social science research centre. The DiScribe Hub represents a collaborative effort among four academic institutions: the University of Bath, the University of Bristol, Royal Holloway, University of London, and Cardiff University. The Hub aims to advance social science-led research that supports the route to adoption of DSbD technologies. The Hub's research agenda is structured around four key thematic areas, designed to complement the efforts of the wider DSbD programme:
  - The barriers to and enablers of secure technology **adoption**.
  - The **readiness** of software engineers and developers to work with new secure hardware.
  - The role of **regulation and policy** in security product adoption.
  - Variances in barriers and readiness to adopt **across contexts** and cultures.
- In July 2021, the larger competitions (see Table 3 below) were combined into a joint IUK/EPSRC call to permit academic-led projects as well as industry-led projects with academic support.
- The programme originally planned to support up to five business-led technology Demonstrators. This was successful, with Demonstrators being funded in e-commerce, utilities, automotive, edge computing, and digital computing infrastructure. Subsequently, additional funding from DCMS was directed towards a new Demonstrator project and a direct award grant to a new project:
  - In March 2023, a second Demonstrator in the automotive sector was funded.
  - In August 2023, a grant was made to develop test boards for a RISC-V-based microcontroller implementation of CHERI, building on the CHERIoT[4] workstream funded earlier in the DSbD programme. The Sonata and Symphony test boards resulting from this work have been instrumental in catalysing further activity as they offer a second route to market to the Morello board, focusing on smaller, embedded processors for use in applications such as industrial control and the Internet of Things.

[4] CHERIoT is a small version of CHERI for IoT devices based on RISC-V architecture. Work to adapt CHERI to smaller embedded systems was led by Microsoft through their involvement in the DSbD programme.

The full list of work strands funded by the DSbD programme, their original and achieved dates of operation and final level of funding, are shown in Table 3 below.

Table 3: Programme strands

Original planned Work Strand	Original planned project dates	Final Work strands	Final agreed project dates	Funding
Activity 1.1: Technology Platform Prototype	October 2019 to June 2024	Activity 1.1 Technology Platform Prototype	October 2019 to October 2024	£37.5 million (IUK) – Sole awardee - Arm is industrial lead, academic leads are Cambridge and Edinburgh Universities.
▪ **Activity 1.2: Academic Proof** ▪ **Activity 1.3b: Systems Software (Academic Led)** ▪ **Activity 1.4: Impact Research**	June 2020 to April 2024	EPSRC Academic led research	July 2020 to May 2025	£9.6 million (EPSRC) Nine projects were awarded funding through this stream.
▪ **Activity 1.3a Systems Software (Industry Led)** ▪ **Activity 2.1 Developer Environment** ▪ **Activity 2.2 Language and Runtime**	▪ Activity 1.3a: June 2021 to April 2024 ▪ Activity 2.1 and 2.2: April 2021 to April 2024	Competitions to Develop Software Ecosystem	▪ SME Competition to Develop Software Ecosystem: 10 Projects ran between April 2021 and September 2021. ▪ Main Software Ecosystem Competition: 10 Projects starting April 2022 and finishing in December 2024.	£8.2 million (IUK & EPSRC).
Activity 2.3 Route to Adoption	June 2020 to April 2024	ESRC Hub +	September 2020 to August 2024	£3.6 million (ESRC) DiScribe Hub + awarded funding.
Activity 3.1 Business Led Demonstrators 1	October 2020 to April 2024	Business Led Demonstrators 1	January 2021 to January 2025	£5.8 million (IUK) – The Hut Group awarded funding for Soteria project.
Activity 3.2 Business Led Demonstrators 2	June 2021 to April 2024	Business Led Demonstrators 2	March 2022 to March 2025	£6 million (IUK). Five successful applicants.
N/A		Technology Access Programme	August 2021 to March 2025	£1.8 million (Digital Catapult).
N/A	September 2023 to December 2024	lowRISC Direct Award	September 2023 to December 2024	Funding provided by IUK for Sunburst Project (CHERIoT).

2.4. Improving DSbD activities over time

EQ1: How can DSbD activities be improved as the programme runs its course?

This question was included in the original impact evaluation design, but by agreement with the DSbD Delivery Team and Programme Board it was evaluated at process evaluation stage so that the findings

could contribute to the remainder of the programme and has not been revisited with additional evidence between the process and impact evaluations. The key findings are summarised here for context.

The process evaluation, finalised in April 2022, found that **the programme was generally being well-run** and was **making progress towards achieving its eventual objectives**. A strength of the programme was that it was able to **adapt to emerging challenges and opportunities** (for example, reconfiguring the planned competitions to better suit the state of the R&D ecosystem, and seeking alternative supply chains for required hardware).

The work did identify some potential improvements:

- The Programme Board would benefit from **additional written reports on technical matters, provided by the Delivery Group**. It would also be useful if leaders of the largest funded projects could make presentations on **progress and take questions from Board members.**
- **Themed breakout groups should be maintained and developed.** Advisory Board members have a useful role to play as ambassadors for the programme, and the ongoing training as part of the marketing and communications programme should be carefully managed.
- Information on project outcomes and impacts held in Researchfish has **been difficult to integrate** into regular programme monitoring reports; we suggested that this should be **investigated at Research Council level to see if the process could be improved.**
- **Monitoring has worked well,** particularly as it has coordinated the activities of Innovate UK and 2 other Research Councils. The level of monitoring is proportionate and not considered onerous.

A key element in the critical path for the programme has been **the delivery of the Morello prototype board** for use in projects and the Technology Access Programme. This was identified as a significant live risk at the time of the process evaluation. There have been serious concerns over the last 12-18 months that supply chain difficulties would have prevented delivery of boards in sufficient quantities to be useful, or even at all, but these have now been addressed.

A small number of participants in the interviews for this interim evaluation also offered comments on the programme design. The sequencing was thought to have been appropriate; one stakeholder suggested that in an ideal world, there would have been **more time to build academic engagement and the wider business ecosystem**, so that there would be a useful set of tools and an engaged marketplace at the point where the demonstrators were beginning to produce outputs. However, the duration available for the Challenge Fund meant that the whole programme had to be delivered within a set timeframe.

Key insights on improving and focusing DSbD activities: looking forward, the key steps in the Logic Model between achievement of the prototype project milestones and eventual adoption were seen to be:

- Prioritising the industrial R&D agenda.
- Making progress towards new regulatory standards and legislation proposals.
- Increasing industrial sectors' awareness of cyber and digital security issues and market failures.
- Capacity building: formation of new knowledge and skills to develop digitally secure products and services.
- Building confidence in the technology, and demand for the new products and services.

These depend upon **communication** as much as they do upon the successful delivery of the technology:

- With government.
- With the companies that could use DSbD technology to build new products and services.
- With the industrial marketplace for the new products, which will need awareness of the cyber security problems that DSbD solves and the skills to use new products and services.

- With the wider consumer marketplace that, while aware of cyber security as an issue, is still largely unaware of the specific nature of threats and the actions necessary to mitigate them.

The finding from the April 2022 process evaluation was that the programme would need to continue to respond to emerging challenges and opportunities in order to build the ecosystem.

2.5. Factors influencing achievement of DSbD outcomes

EQ2: What are the major factors influencing the achievement or non-achievements of DSbD outcomes?

2.5.1 Factors influencing cyber security projects in general

At the time of the interim evaluation (June 2023) the key external factors influencing cyber security projects were considered to be in the marketplace, such as:

- Reluctance to take risks with development and investment.
- Unproven commercial case for significant investment in digital and cyber security.
- Low awareness of digital security technology as a defence against cyber threats.
- Not wanting to be the first mover in a marketplace with low current demand for digital security.
- Skills issues which affect both developers and end users:
  - Shortage of skilled people in the UK for developers to recruit to work on new products and services.
  - Lack of skills within industrial customers to learn to use the new technology and integrate it into their existing systems and workflows.

According to consultations for this final evaluation, these issues have persisted to the present day. Interviewees from a range of project types (from academic proof to industrial demonstrators) brought up market-related issues related to:

- Business priorities: costs and benefits of investment in cyber security.
- Market pressure and competition.
- Reputational risks of ineffective cyber security.
- Costs of hardware solutions in the relatively small cyber security market (e.g. price of niche chips).

Interviewees were also more likely than at the interim evaluation stage to mention the **growing and evolving threat level**, and **the increasing importance of cyber security**, as factors influencing cyber security projects.

However, most notable of all in the final round of consultations was the emergence of governmental influence as the most commonly mentioned external factor on cyber security projects, whether through **regulation**, **standards**, or **policy goals.** A range of potential government and policy drivers were mentioned, including:

- Mandating “secure by design” systems through regulation or procurement requirements.
- Setting requirements for product testing.
- Championing particular technologies or frameworks. Interviewees were cautious about the ability of Government to mandate use of CHERI in procurement. However, if agreement could be reached on characteristics and standards for memory safe technology, then CHERI would likely emerge as a leading solution.

2.5.2 External influences on DSbD outcomes

A highly influential stream of activity, which has had a significant impact on the delivery of DSbD and the potential future of CHERI in the marketplace, was work begun by Microsoft on how to implement CHERI on

smaller, cheaper, more specialised processors, rather than fully featured multi-tasking application core processors like Morello:

- In September 2022, Microsoft published a blog post announcing that they had adapted CHERI to work on a microcontroller using the open source RISC-V architecture.
- DSbD then funded a project – Sunburst (CHERIoT) – which supported lowRISC to develop test boards implementing CHERI using Ibex, their 32-bit RISC-V processor core, and provide these to UKRI for distribution.
- The sixth cohort of the DSbD Technology Access Programme used these test boards instead of the Morello board to enable companies to develop embedded technology solutions using CHERI.

As a result, companies have started up, or changed their business models, to investigate commercial products based on CHERI – such as Codasip, SCI Semiconductor, and Secqai – on the RISC-V base. Codasip announced[5] the first commercial implementation of CHERI in October 2023; this is however not available for purchase at the time of writing.

2.6. Conclusions against evaluation questions

What are the major factors influencing the achievement, or non-achievement of DSbD outcomes?

According to the programme design and the Logic Model which describes it, the necessary steps between achievement of the prototype project milestones and eventual adoption are:

- Prioritising the industrial R&D agenda towards cyber security, and memory safety in particular.
- Making progress towards new regulatory standards and legislation proposals on cyber security and memory safety.
- Increasing industrial sectors' awareness of cyber and digital security issues and market failures, in order to stimulate development of secure products and services and build demand for these.
- Capacity building: formation of new knowledge and skills to develop digitally secure products and services.
- Building confidence in the technology, and demand for the new products and services.

The programme has made good progress in these areas:

- DSbD has good links with Government through the Advisory Group and continues to feature in Government strategy documents. Building CHERI and the concept of memory safety into policy and regulatory standards, and government procurement, helps build confidence in the value of the technology, stimulating demand and investment.
- DSbD has stimulated collaboration between academia and industry and built an ecosystem of developers and early adopters. For adoption, this would need to be expanded to a much wider potential industrial marketplace. The CHERI Alliance has emerged as a trade association to accelerate this.
- Deployment and adoption would benefit from the inclusion of large and small companies in the UK supply chain. If UK SMEs can provide services to large companies internationally, the UK can gain differential economic value via first mover advantage. Government procurement can also play a critical role here. The Technology Access Programme has opened up CHERI technology to UK SMEs to develop use cases.
- DSbD has brought in investment from government and the private sector; crucially, the Microsoft workstream investigating DSbD beyond the parameters of the funded activities has resulted in the RISC-

[5] Codasip delivers processor security to actively prevent cyberattacks (Codasip, 2023)

V based microcontrollers that are the first designs being used to take CHERI to market. Other private sector commitments are known of, but the commercial details are typically not publicly available.

According to DSbD participants and sector experts interviewed for this evaluation, the key external factors affecting successful delivery of cyber security projects are:

- **Regulation**, **policy**, and **standards** to guide companies in decision-making (whether suppliers or consumers of cyber security solutions).
- **Lack of knowledge/understanding** of cyber threats and technological solutions, **cost pressures** and **risk aversion** in the **marketplace**.
- **Skills** to develop new solutions (supply side) and to integrate them into existing systems (demand side).

These factors highlight the importance of any intervention which follows the DSbD programme in considering the following:

- Growing the UK cyber and digital security ecosystem, involving Government policy and procurement where possible.
- Building awareness of cyber security threats and the role that CHERI can play in addressing these, with particular reference to “memory safety” as an agreed set of problems and solutions.
- Developing capacity and capability to use CHERI technology when it becomes commercially available.

3. Impacts on R&D Capability and Capacity

3.1. Introduction

This chapter outlines the impact of the DSbD programme on the R&D capability and capacity of the researchers and businesses engaged in the funded projects and addresses the following evaluation questions:

- To what extent and how has DSbD improved R&D capability and capacity?
- To what extent has DSbD improved the UK skills base of researchers on new hardware architecture and software development?
- What further opportunities is DSbD opening up in the digital security innovation base?

The evaluation questions specifically address the R&D capacity and capability component of the first objective of the ISCF:

- Increase UK businesses' investment in R&D and **improve R&D capability and capacity** and technology adoption – through creating cross-sector collaborations which leverage significant industry co-investment, increase technical skills, and create additional highly skilled jobs while ensuring academic leadership.

For the DSbD programme, the pathways to impact on R&D capability and capacity are through advancements in the skills base of researchers and businesses engaged in developing new DSbD hardware and software and the further opportunities created by DSbD.

The business investment in R&D component of the objective is addressed in the subsequent chapter, specifically in Section 4.4 of this report.

3.2. Key findings

Improvement in R&D capability and capacity

- Most stakeholders (17 of 19) reported DSbD projects facilitated new skills and capacity for adopting new technologies.
- Five businesses have been established or influenced by DSbD, indicating enhanced R&D through industry innovation and their further development efforts.

Improvements in skills base of researchers and businesses

- 54 Master's and PhD degrees related to DSbD have been facilitated, surpassing the initial target of 30 PhD and MPhil degrees.
- 44% (4 of 9) of academic proof projects included training sessions and materials as part of project delivery.
- The Morello Board has been integrated into University of Glasgow's cyber security summer school and Aarhus Universitet's teaching programmes.
- The most significant impact on skills development was observed among junior staff and researchers, particularly postgraduate and PhD students.

Further opportunities unlocked through the DSbD programme

- Four primary investigators from academic proof projects and two organisations from De Minimis workstream were awarded funding in other DSbD workstreams.
- Four DSbD projects have received follow-on funding from EPSRC, NCSC, and DSTL, extending their CHERI work.

- Project partners from five academic proof projects, two demonstrator projects, and one software ecosystem development project reported identifying new partners through DSbD for future projects.

3.3. Extent to which DSbD has improved R&D capability and capacity

EQ3: To what extent and how has DSbD improved R&D capability and capacity? To what extent has DSbD improved the UK skills base of researchers on new hardware? What further opportunities is DSbD opening up in the digital security innovation base?

The assessment of R&D capability and capacity is based on evidence collected against the following quantitative Key Performance Indicators (KPIs):

- Number of academic PhD's/MPhil's related to DSbD.
- Number of training sessions delivered and extent of integration of DSbD technology with taught programmes.
- Number of DSbD funded projects involving early career researchers.
- Number of spin outs, start-ups, and joint ventures stemming from DSbD programme.
- Extent of further opportunities unlocked.

3.3.1 Impacts on improving research capabilities and capacity in academia

Table 4 below summarises the evidence for each quantitative KPI, outlining the specific ways in which DSbD has improved the skills base of researchers. The evidence base for these KPIs is informed through insights from stakeholder consultations, outcomes reported in Researchfish data, UKRI Benefits Profiles, and the DSbD survey conducted by Innovate UK.

Table 4: Quantitative indicators on skills base of researchers

Indicator	Evidence	Source
Academic PhD's/MPhil's related to DSbD	EPSRC-funded projects have facilitated 23 PhDs completed or in flight and 31 Master's either completed or in flight, which engaged with taught programmes employing DSbD.	UKRI Benefits Profiles
Training Sessions and integration of DSbD technology with taught programmes	▪ 4 of 9 (44%) Academic Proof projects incorporated training sessions and materials. ▪ A Morello Board recipient at the Aarhus Universitet in Denmark used the Morello Board as part of their teaching to 50 Master's students and 150 undergraduates. ▪ The University of Glasgow incorporated DSbD into School of Computing Science's cyber security summer school of 80 students. ▪ The University of Manchester are currently incorporating CHERI into the course for MSc.	UKRI Benefits Profiles, DSbD Survey
DSbD funded projects involving early career researchers	The following projects involved early career researchers: ▪ 4 of 9 (44%) Academic Proof projects. ▪ Two Software Ecosystem Development projects. ▪ Three Demonstrators. ▪ One De Minimis project.	Desk research, stakeholder consultations
Spin outs, start-ups and joint ventures	▪ CHERI Alliance and Capabilities Ltd were created as a direct result of the DSbD programme. ▪ SCI Semiconductor was established in Feb 2023 to commercialise the CHERIoT RISC-V microprocessor core, which was developed by Microsoft and lowRISC prior to involvement of SCI Semiconductor.	Stakeholder consultations, UKRI Benefits Profiles

	▪ Codasip developed the first commercial implementation of CHERI, incorporating it in their 700 processor series. ▪ Secqai created a new business model for CHERI-based System-on-Chips (SoCs).	

As shown in the table above, the **total number of Master's and PhD degrees related to DSbD has reached 54**, surpassing the initial target of 30 PhD and MPhil degrees. This engagement between PhD and Master's students and the new DSbD hardware indicates an improvement in the skill base of researchers, as greater exposure to DSbD has contributed to their academic progression. As these junior researchers have gained deeper insights into DSbD-related areas, including CHERI, this suggests that they are better equipped to contribute to advancements in these areas, thereby enhancing their R&D capability. Through hands-on experience with the Morello Board and CHERI, junior researchers have likely developed a robust understanding of memory safety concepts in general. This foundational competence positions them well to engage in research into secure computing and novel security capabilities.

The Morello Board has also been integrated into Master's and undergraduate courses in the UK and overseas, as highlighted in the table above. This suggests a wider dissemination of knowledge regarding DSbD, as it was used to teach at various educational levels (undergraduate, Master's, and summer school). Additionally, the University of Manchester is currently working on incorporating CHERI into an MSc course.

At least 10 DSbD-funded projects have actively engaged early career researchers. Two demonstrator projects reported upskilling of junior researchers involved in their project: one industry representative emphasised that their DSbD demonstrator project allowed them to get more technical sophistication within the company; and one academic representative reported co-funding a PhD studentship along with their industrial project partner. One academic proof project also funded a PhD student. Furthermore, one software ecosystem development project reported that the postgraduate student who contributed to their project has started their PhD, highlighting a direct link between involvement in DSbD and the upskilling and career progression of junior researchers. Stakeholder consultations revealed that **the most significant impact on skills development was observed among junior staff and researchers, particularly postgraduate and PhD students.**

Incorporating DSbD technologies into academic course materials also raises the profile of both the issues and market failures the programme seeks to address, and the specific technology developed which could support the adoption and diffusion of the technology among their employers.

Apart from integration of DSbD with taught programmes, academic-led ecosystem development projects have included DSbD-related training sessions and materials, such as workshops, tutorials, GitHub repositories[6] and online videos/podcast series to support the organisations and individuals who have received boards through the TAP. These training sessions foster a deep understanding of DSbD technology, enabling researchers to contribute to the DSbD projects more effectively.

3.3.2 Impacts on improving research capabilities and capacity in industry

DSbD programme has enhanced R&D capabilities and capacities for participating businesses, evidenced through the establishment of start-ups, spinouts, and joint ventures. These include:

- **Capabilities Ltd and CHERI Alliance**: Both were created as direct results of the DSbD programme. Capabilities Ltd brings together researchers from the University of Cambridge CHERI group and partners in industry such as Google to provide CHERI cyber security consultancy services. Although CHERI Alliance is not a product-led business, it serves as a trade association aimed at promoting the global adoption of CHERI. The establishment of the Alliance signifies improvements in R&D capability and capacity, as it unites researchers, industry experts, and public sector organisations highly skilled in DSbD

[6] The DSbD website currently lists 11 GitHub repositories related to funded projects, but the overall number is known to be much higher – for example a search for repositories using the term "CHERIoT" yields 23 results, and there is likely to be some overlap with the 11 listed on the DSbD website and at least 3 which do not appear to be related to DSbD technologies at all.

areas. Their technical working group focuses on advancing R&D efforts in various domains, including CHERI in SoC and CHERI Virtual Machines. Additionally, the involvement of many CHERI Alliance members in the DSbD programme highlights the ongoing efforts to furthering the R&D work initiated by DSbD.

- **SCI Semiconductor**: This company was founded to address a market gap stemming from the lack of commercial products with CHERI embedded, to take the advantage of substantial investment through the DSbD programme. SCI Semiconductor aims to commercialise the CHERIoT RISC-V microprocessor core, developed in collaboration between Microsoft and lowRISC as part of the DSbD programme. This demonstrates enhanced R&D capability through the creation of potentially commercially viable products and improved R&D capacity, as the planned commercial implementation highlights efforts by businesses to exploit this opportunity, clearly indicating the pathway for Technology Readiness Level (TRL) progression.
- **Codasip**: Although Codasip was not established as a result of the DSbD programme, they were the first company to commercially implement CHERI, integrating it into their 700 processor series. Their collaboration with the University of Cambridge to develop a stable and industry-ready specification culminated in the formation of the RISC-V CHERI standardisation team. This collaboration not only signifies an enhancement in R&D capacity and capability but highlights valuable exposure gained by academic researchers for research translation.
- **Secqai**: The company has created a new business model based on CHERI. Although Secqai has not been directly involved with or funded by the DSbD programme[7], their intention to adopt CHERI further illustrates industry innovation.

3.3.3 Further digital security research opportunities opened up through DSbD programme

This section assesses the further opportunities for project partners that have emerged through their involvement with the DSbD programme. These opportunities highlight pathways for improvement in R&D capabilities and capacities, particularly for academic institutions, by enabling them to advance the research work conducted under DSbD and continue their efforts in this domain. Furthermore, leveraging these new funding opportunities using their DSbD project as a foundation clearly demonstrates an improved position for securing additional funding.

The further opportunities unlocked through the DSbD programme are evidenced below:

- **Further funding opportunities within the DSbD programme itself:**
  - Four primary investigators who were awarded funding for the academic proof projects have subsequently been awarded funding in other DSbD workstreams.
  - Two organisations involved in the De Minimis projects also progressed to undertake additional projects with the Software Ecosystem Development workstream.
- **Follow-on funding and R&D grants received or in progress outside DSbD:**
  - Three academic proof projects and one software ecosystem project received follow-on funding from EPSRC, NCSC, and DSTL, extending and advancing their work done on CHERI and DSbD.
  - Notably, one representative from an academic proof project has obtained funding for three additional projects.
  - An academic-led ecosystem project has attracted interest from various academic and industry groups, including Google, which is considering funding further development of this work.
  - Interviewees from four academic proof projects, two software development ecosystem projects, and one demonstrator have reported that they are in the process of submitting research funding proposals

[7] However, Secqai was a TAP board recipient.

that further build upon their DSbD work. The funding bodies involved include Horizon Europe, EPSRC, the European Research Council, and other UK government entities.

- **Other further opportunities currently in pipeline:**
  - Stakeholder consultations revealed that the DSbD programme has facilitated additional opportunities, such as networking, identifying new partners for future collaborations, and invitations to events, workshops, and talks.
  - Representatives from five academic proof projects, two demonstrator projects, and one software ecosystem development project reported identifying new partners for future projects, primarily through All Hands events and engagement with the DSbD ecosystem. However, only representatives from two academic proof projects and one demonstrator project have begun collaborating with these new partners.
  - A representative from an academic proof project noted that, while they did not identify new partners, they discovered additional expertise at existing academic partners, leading to further discussions and knowledge sharing.
- **Further business opportunities unlocked through DSbD programme:**
  - Business partners, in collaboration with academics on a demonstrator project, are exploring further commercial opportunities that build on their DSbD work. One business partner reported being in a position to expand their testing activities and expressed interest in supporting any early adopters.
  - One software ecosystem development project indicated that their DSbD project work has positioned them to potentially collaborate on silicon projects in future.

3.4. Conclusions against evaluation questions

The previous chapter identified that skills gaps in R&D—whether in companies developing new products and services or in the industrial target marketplace needing skills to integrate them—were a major factor influencing the achievement of DSbD outcomes. Consequently, building R&D capability and capacity is crucial for the programme's success. In the programme's Logic Model, capacity building is essential for downstream adoption and intellectual property generation.

Evidence indicates that the **DSbD programme has notably enhanced the R&D capability and capacity of researchers and businesses involved in developing new DSbD hardware and software.** 54 DSbD-related PhD and Master's degrees have been facilitated through EPSRC funded projects. Additionally, there has been a direct improvement in the researcher's skill base through exposure to new security capabilities, career progression (Master's students pursuing PhDs), involvement of early career researchers, and leading training sessions and materials.

Knowledge transfer through taking up new roles is identified as a key enabler of DSbD's success. A particularly encouraging aspect of the academic-led work has been the integration of DSbD technology into taught programmes, engaging over 230 students across various education levels. These participants have requisite knowledge to potentially pursue future research in DSbD technology or apply their knowledge in industrial positions.

Evidence also suggests that DSbD has impacted the R&D capability and capacity of businesses, either through their establishment or by influencing their business strategy. These businesses have advanced R&D efforts in several domains such as RISC-V implementation of CHERI and standardisation and adoption efforts, highlighting industry innovation stemming from the DSbD programme. This improvement in R&D capability and capacity in businesses can pave the way for DSbD technology's TRL progression.

Researchers and businesses have also secured further opportunities through their involvement in the DSbD programme, including additional opportunities within the DSbD programme, follow-on funding, and broader opportunities from networking and knowledge transfer.

Overall, the results on building R&D capacity and capability are positive, indicating increased R&D capability and capacity within the UK. However, **the level of further opportunities unlocked through the DSbD programme needs to increase further.** Although some researchers and businesses have secured these opportunities, they need to be more widespread to benefit a larger proportion of DSbD participants, ensuring continued development efforts in the DSbD area, thereby addressing long-term skills barriers.

4. Impacts on R&D Funding

4.1. Introduction

This chapter details the tangible impacts of the DSbD programme on R&D funding in the UK within the cyber and digital security landscape. The chapter assesses financial contributions secured from governmental sources (excluding UKRI) as well as private investments from both domestic and international companies into the DSbD funded projects and further independent R&D activities related to DSbD. The chapter addresses the following evaluation questions:

- To what extent and how has DSbD increased R&D funding from other government sources?
- Has DSbD increased private investment in UK digital R&D? And what are the profiles of investors?

The definitions used for the different types of co-investment, as classified by UKRI's co-investment recognition strategy document[8], are as follows:

- **Pledged** – This includes investment (in terms of eligible costs) a grant recipient declares it (and collaborators) plan to make on R&D activity part-funded through an ISCF Challenge programme, in line with ISCF business cases/project plans. Declaration of this pledge is made by signing the Grant Offer Letter (GOL).
- **Accompanying** – This includes extra public (but non-UKRI) and non-public investments in ISCF-funded R&D activity over and above those which are considered eligible costs as part of the grant subsidy. This may include further costs outlined in the business cases/project plans for that activity but made in order to achieve the agreed output or outcome.
- **Aligned** – This includes investment in a technology/research area thematically aligned to, and catalysed by, ISCF-funded R&D activities. This could be driven by increased confidence in the area created by the focus of the ISCF Challenge. Equally, an organisation could start a second, related research project with no grant from the ISCF inspired by the original activity.
- **Follow-on** – This includes investment to take to market, or exploit, outcomes from ISCF-funded R&D activity.

4.2. Key findings

R&D funding from other government sources

- A total of £30 million in additional funding has been allocated by other government sources to the DSbD programme and its associated technologies, far exceeding the initially set target of £6 million by 2025.
- Key contributors of additional government R&D funding include DSIT and DSTL.
- The government R&D funding figures do not account for additional investments made to support activities influenced by the DSbD programme, such as commissioned research and follow-on funding secured by DSbD participants. These efforts highlight the government's broader commitment to advancing DSbD technologies beyond the core programme.

Private investment related to the DSbD programme

- To date, just over £238 million of co-investment has been secured specifically from private organisations, surpassing the set target of £117 million in private co-investments by 2025.

[8] Co-investment Recognition Strategy (UKRI)

- Nearly £132 million has been secured through aligned co-investments from large industry players; £102 million has been secured through accompanying co-investments, primarily sourced through Arm for the Morello Board; and £4.4 million has been secured through pledged project co-investments.
- Estimated forecast follow-on co-investment currently amounts to £190 million from four companies, indicating strong commitment to the continued development and commercialisation of DSbD technology.

4.3. Impact of DSbD on R&D funding secured from other government sources

EQ4: To what extent and how has DSbD increased R&D funding from other government sources?

This section assesses the impact of the DSbD programme on activity funded by government departments and aligned bodies (except Innovate UK / Research Council funds committed through DSbD) to promote CHERI and DSbD technologies, including adoption and commercialisation efforts. The initial target for securing R&D funding from other government sources was set at £6 million by 2025.

The evidence for this KPI includes R&D funding secured from other government sources, specifically related to:

- The DSbD funded projects.
- Other core DSbD activities (excluding funded projects).
- The CHERI technology.

Since the outset of the DSbD programme, **other government sources have contributed £30 million in additional R&D funding** to the DSbD programme's activities. The funding secured exceeds the initially set target of £6 million from other government sources, indicating a significant level of confidence and support from government for the tools and technologies developed under the DSbD programme.

Table 5 presents a breakdown of investment from other government organisations stemming from the DSbD programme. This includes investments from DCMS (now part of the Department for Science, Innovation and Technology (DSIT)) between 2020 and 2023 and investments from Defence Science and Technology Laboratory (DSTL) between 2022 and 2023.

Table 5: Value of R&D grants from other government sources

Government department	Amount of co-investment	Form of co-investment
DSIT / DCMS[9]	£12.96m	Aligned
DSTL Industrial Business Partners	£15.00m	Aligned
Defence and Security Accelerator (DASA) competition	£1.50m	Aligned
Ministry of Defence MoU	£0.50m	Aligned
Total	**£29.96m**	**Aligned**

Source: UKRI Benefits Profiles and Co-investment data

As seen in the table above, DSIT and DSTL were the largest contributors of providing R&D funding related to the DSbD programme, providing £12.96 million and £15 million, respectively. Between 2020 and 2023, DSIT allocated £11.16 million to support various DSbD activities. These funds were instrumental in advancing academic-led proof of platform/architecture projects, projects aimed at broadening system software and approaches enabled by the Morello platform and conducting research into the long-term

[9] Due to the governmental restructuring in February 2023, the 'digital' component of DCMS was moved to DSIT, at which point DSIT became the department most closely aligned with DSbD. However, the team from DCMS that has been engaging with the DSbD programme remains the same.

impacts and consequences of these changes. Additionally, the funding supported the DiScribe Hub, with focus on social and economic research, business-led demonstrators, and the TAP.

Further investment by DSIT, amounting to £1.8 million between October 2024 and March 2025, was directed towards addressing the need for more secure and resilient technologies based on the DSbD programme's CHERI secure-by-design semiconductor capability. This investment facilitated the production of a hardware with CHERI extension to RISC-V, the management of a cohort within the Technology Access Programme, and the delivery of the Tested by Morello activity along with the subsequent test data.

All investment secured from other government sources was classified as 'Aligned', indicating that the DSbD programme has successfully demonstrated the importance of cyber and digital security. This suggests an increase in the government's confidence in the technological and research advancements fostered by the DSbD programme, as the additional R&D funding from other sources exceeded the expected amount by almost 500%.

Additionally, the United States Defense Advanced Research Projects Agency (DARPA) has maintained a long-standing relationship with the Cambridge University team responsible for developing CHERI. DARPA has been supporting this technology since 2010. However, this investment predates the DSbD programme and, consequently, has not been included in the table above.

The government R&D funding figures shown in Table 5 above only include the investments related to the DSbD programme and its associated technologies such as CHERI. However, the government has also provided additional support and funded other related activities that are influenced by the DSbD programme. These additional investments and support have not been accounted in the R&D funding estimates because they are not officially part of the DSbD programme itself. These include:

- **Follow-on funding for three academic proof projects and one software ecosystem project, extending their work done on CHERI and DSbD**. Notably, one representative from academic proof workstream has obtained funding for three additional projects. Additionally, interviewees from four academic proof projects, two software development ecosystem projects, and one demonstrator have reported that they are in the process of submitting research funding proposals that further build upon their DSbD work. The funding bodies involved include Horizon Europe, EPSRC, the European Research Council, and other UK government entities.
- **Research on Adoption and Diffusion of CHERI**[10], commissioned by DSIT in early 2024. This commissioned research was aimed at identifying key sectors, barriers, enablers for adoption, and anticipated pathways for CHERI's implementation. This indicates DSIT's and other government entities' strong awareness of the tools and technologies developed under the DSbD programme. Moreover, it highlights their commitment to providing additional support and funding, independent of DSbD's core activities, to further explore commercialisation and adoption opportunities.
- Contract work released by DSIT in May 2025, commissions new research work for the **Adoption and Managed Deployment of CHERI technology**. The corresponding ITT highlights that the DSbD programme has demonstrated the efficacy of CHERI in securing systems at the silicon level. This new work emphasises on implementing a TRL 8 CHERI deployment in use cases within sectors of national importance, i.e., critical national infrastructure.[11]
- Funding and support provided by DSIT to the **CHERI Alliance**, which was formally launched in November 2024. The specific details regarding the value of funding allocated to the CHERI Alliance are not publicly available. The CHERI Alliance aims to build on top of the DSbD ecosystem to extend this work and advance efforts beyond initial adoption and secure industry endorsement.[12] NCSC is a member

[10] CHERI Adoption and Diffusion Research (DSIT, 2024)
[11] ITT - Adoption of CHERI Technology II (DSIT, 2025)
[12] CHERI Alliance

of the CHERI Alliance, and is providing in-kind support through networking, connecting with the target audience, and advocacy of CHERI technology.

Additionally, various bids have been submitted by UKRI as part of the Spending Review process, focusing on managed deployment, ecosystem development, skills enhancement, and policy standards around CHERI.

4.4. Impact of DSbD on private investment in UK digital R&D

EQ5: Has DSbD increased private investment in UK digital R&D? And what are the profiles of investors?

This section provides an assessment of the realised co-investment into the DSbD programme from private organisations as of 2024/25, based on the following KPIs:

- R&D spend associated with delivery of DSbD enabled products and services (co-investment as part of funded projects).
- Level of private co-investment.
- Investor confidence in cyber security sector.

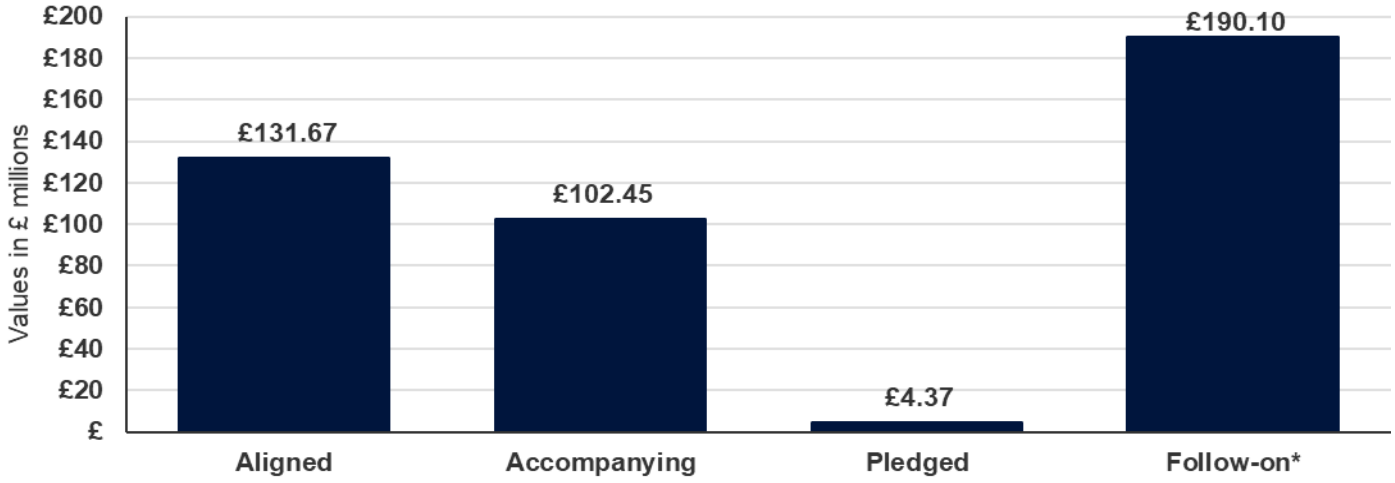
We have analysed all investments generated through DSbD projects and through the specific tools and technologies developed as part of the DSbD programme. The initial target for securing private co-investments from industry was set at £117 million by 2025.[13]

Figure 3 presents total leveraged private finance by different types of co-investments. The **total value of private co-investment currently amounts to just over £238 million**, which is more than double the set target of £117 million of total private co-investments.

The long-term target for R&D investments from private organisations associated with delivery of DSbD enabled products and services is set at £800 million by 2027. Should the follow-on investment forecasts of £190 million be realised within the next 1-2 years, the total private co-investment would amount to approximately £429 million, which remains below the long-term goal. To successfully achieve the £800 million target, it is essential that a CHERI-enabled chip becomes commercially available for integration into products and services. Additionally, a broader base of companies, including SMEs, must actively invest in the adoption and commercialisation of CHERI-enabled commercial chip and DSbD technologies.

As of drafting this report, the total value of private co-investment is considered as a conservative estimate. This is due to several companies, known to have made significant investments in DSbD, are either not disclosing the amounts invested or have not provided an update on their investment figures.

Figure 3: Level of leveraged private finance by type of co-investment (in £ million)



[13] Global businesses – including Google and Microsoft – back UK to block cyber threats with new tech (GOV.UK, 2019)

*Source: UKRI co-investments data | *Follow-on co-investment represents a forecast, and an indication of the amount companies are planning to invest in DSbD over the next few years. This information has been gathered by UKRI through direct engagement with companies to obtain their future investment forecasts.*

Aligned co-investments have garnered the highest amount, totalling £132 million, with contributions from 13 different sources including companies such as Google, Microsoft, and Amazon. For example, Microsoft's investments were targeted towards developing the Capability Hardware Extension to RISC-V for IoT (CHERIoT) platform. The substantial investment amounts and the large number of contributors for aligned co-investments reflect a greater level of confidence from investors and private organisations in the DSbD technologies and CHERI. Representatives from three private sector companies, known to have significantly invested in DSbD, have expressed strong confidence in CHERI, citing that the DSbD programme has proved CHERI's significant resolution capabilities. This trend indicates that the DSbD programme has demonstrated potential of CHERI technology and the programme has generated momentum within the cyber and digital security sectors, thereby creating a ripple effect that has encouraged private organisations to invest in DSbD-related areas.

Accompanying co-investments have emerged as the second highest contributing form of co-investment, securing £102 million. However, this substantial amount is sourced primarily from Arm, with additional support from Linaro, to develop the Morello Board via the Technology Platform Prototype workstream.

The forecasted follow-on co-investment amounting to £190 million indicates that some companies are committed to continuing their investment in DSbD technologies even after the programme's conclusion. This forecasted follow-on funding has not been accounted for in the estimated value of leveraged private co-investment, as these funds have not yet been realised. As the follow-on investments are focused on commercialisation activities, this suggests that some companies are looking to further exploit and leverage the outcomes achieved from the DSbD programme.

The pledged co-investment constitutes just 1.9% (£4.4 million) of the realised private co-investment, encompassing contributions from businesses engaged in R&D activities partially funded through the DSbD programme. Notable contributors to the pledged co-investment include The Hut Group (THG) and lowRISC which provided co-investment as part of their funded DSbD project. In other instances of pledged co-investment, specific data regarding the investing organisations is unclear; however, the workstreams in which private co-investments were made are identifiable. These include SME investments in System Software, private investments in the Software Development ecosystem, and private investments in Demonstrator Tranche 2.

Table 6 provides a breakdown of the sources of private DSbD co-investments, detailing the amount contributed by each source, the form of co-investment, and additional details related to the investment.

Table 6: Private co-investment breakdown by type of co-investment (as of FY 2024/25)

Source	Co-investment amount	Details
Businesses - Aligned[14]	£129.97m	Includes companies such as Microsoft, Google, Amazon, HP, Ericsson, Codasip, CHERI Alliance, Secqai, SCI Semiconductor, and Rolls Royce.
Businesses - Accompanying	£102.45m	Includes companies such as Arm, Linaro, and Thales.
Businesses - Pledged	£1.33m	Includes companies such as THG and lowRISC.
Workstreams[15]		
SME System Software	£0.71m	Project co - investment

[14] A portion of this includes co-investments from international recipients of the Morello board. It is important to note that the total amount does not solely represent co-investments from private enterprises but also includes other co-investments. As the specific details are not publicly disclosed, these have been presumed to be part of private co-investments.
[15] While we know that these are project co-investment, it is not clear which private organisations have invested this amount.

Software Development	£0.68m	Project co - investment
Demonstrator Tranche 2	£1.66m	Project co - investment
Morello Board Recipient[16]	£1.70m - £2.81m	Project co - investment
Total	**£238.5m - £239.6m**	Total co-investment from private organisations

Source: UKRI co-investments data

Table 7 illustrates the anticipated follow-on investments from companies into DSbD. Presently, five companies have indicated their intention to continue investing in DSbD. Majority of follow-on co-investment is currently expected to come from UK businesses. Notably, some of these companies' follow-on investments are expected to be primarily directed towards the commercialisation and adoption of CHERI into chips and hardware.

However, the table does not account for other companies actively engaged with CHERI, such as the CHERI Alliance. These companies are likely to invest in DSbD and CHERI in the forthcoming years, as evidenced by Codasip's commercial implementation of CHERI and CHERI Alliance's strategic focus on using the DSbD ecosystem as a foundation and progressing commercialisation and standardisations efforts for CHERI.

Table 7: Future forecast for follow-on co-investments

Source	Estimated amount
Businesses headquartered in UK	£185.10m
Businesses with international headquarters	£5.00m

Source: UKRI co-investments data

4.5. Conclusions against evaluation questions

R&D funding from other government sources

Since the outset of the DSbD programme, it has received £30 million in additional funding from other government sources. This substantial financial support is crucial, as the programme's Logic Model indicates that achieving its objectives of downstream adoption and generating economic and societal impacts necessitates contributions to the UK research agenda, the establishment of new regulatory standards, and the demonstration of the value of DSbD technology.

The additional funding has enabled the expansion of ongoing DSbD activities, including increased investment in the TAP cohorts, business-led demonstrator projects, and the production of Morello Boards. This significant financial backing and support from government sources suggest that the DSbD programme is well-aligned with the UK research agenda and priorities, as well as government's long-term strategy.

Further evidence of this alignment is seen in the investments and support provided by other government sources to wider activities influenced by the DSbD programme. These include commissioned research into CHERI, follow-on funding for DSbD participants, and support for the CHERI Alliance, a trade association promoting the adoption and standardisation of CHERI.

Private investment related to the DSbD programme

To date, the DSbD programme has secured over £238 million in co-investment from private organisations, surpassing the target of £117 million by 2025. This achievement is a positive indicator, as the programme's Logic Model suggests that increased private investment is directly linked to downstream adoption.

Aligned co-investment serves as a useful leading indicator of future development and adoption, demonstrating investment in R&D beyond the parameters set by funded activities. Aligned co-investments have attracted the highest amount of private co-investment, totalling nearly £132 million, with contributions

[16] Calculated by UKRI as follows: (Average monthly salary for a software developer, based on Glassdoor estimates of £2,666.67–£4,416.67 + Employer's National Insurance contributions at 15% + Statutory minimum employer pension contribution of 3%) × 540 staff months.

from 13 different sources, predominantly large industry players. These substantial co-investment amounts indicate a high level of confidence from private organisations in DSbD technologies and CHERI.

Additionally, an estimated £190 million in follow-on investment is expected to be made in the coming years by four companies to further develop DSbD work with the aim of adopting and commercialising DSbD technology.

To meet the long-term target of £800 million in private R&D investment by 2027, the programme is likely to need to attract further aligned investment from large, influential companies. It would also be beneficial to see contributions from a larger number of smaller companies that have been drawn into the developing ecosystem, as evidence of investment in product and service development.

5. Impacts on Collaboration

5.1. Introduction

This chapters details the collaborative and engagement activities between industry and academia, addressing the following evaluation questions:

- To what extent and how has DSbD increased business-academic engagement on innovation activities?
- To what extent and how has DSbD increased collaboration between younger, smaller companies and larger, more established companies up the value chain?
- To what extent and how has DSbD increased multi and interdisciplinary research?

DSbD is funded by the Industrial Strategy Challenge Fund and was designed to align with **five of the Fund level objectives**. Four of these either explicitly require collaboration or were to be delivered by DSbD using a collaborative approach – they are as follows:

1. **Increase UK businesses' investment in R&D and improve R&D capability and capacity and technology adoption –** through creating cross-sector collaborations which leverage significant industry co-investment, increase technical skills, and create additional highly skilled jobs while ensuring academic leadership. The ESRC awarded grant (the DiScribe Hub+) was to review various questions to enable adoption across industry.
2. **Increase business-academic engagement on innovation activities** – by facilitating a mix of business and academic collaborative projects and start up creation, supported with committed business co-investment and economic drivers. All activities within the programme were to form collaborations between business and academics. Academic grant winners are required to engage with industry throughout the programme.
3. **Increase multi and interdisciplinary research** – to be achieved through the design of DSbD competition to create holistic collaboration across hardware, software, social science and ICT in general. The ESRC and EPSRC strands were to contribute by engaging not only the digital academic community but also the social and economic community in digital security.
4. **Increase collaboration between younger, smaller companies and larger, more established companies up the value chain** – through activities across the market chain that consists of all such companies. Competitions across the activities run by Innovate UK were to achieve this objective.

The first of these objectives has already been addressed in previous chapters (in Section 3.3 for the impact on R&D capability, and Section 4.4 for business investment in R&D). The remaining three objectives (2 - 4) are covered below.

5.2. Key findings

Business-academic engagement activities

- 61% of funded projects featured active collaboration between industry and academic institutions. In contrast, only 10% of the funded projects were carried out exclusively by academic institutions.
- Business-academic engagement has extended beyond funded projects, also taking place though DSbD All Hands events, CHERI tech forums, and participation in CHERI Alliance's technical workshops.

Level of collaboration between SMEs and large companies

- The Technology Platform Prototype, and three of the six demonstrators, did include SME partnerships; however, only one of the 20 software ecosystem projects did, representing a missed opportunity.

- The De Minimis competition aimed to develop collaboration opportunities for SMEs to be involved in the software ecosystem workstream. However, only two undertook additional projects within the Software Ecosystem Development workstream, one of which was a large company collaboration.
- Informal avenues for SME / large company collaboration included the software development calls, Technology Access Programme, and DSbD events, which have engaged the large companies who are core delivery partners with SMEs. For example, EPSRC software projects run by SMEs featured letters of support, funding, or contribution in kind from partners including Arm, Microsoft, Google and Amazon.

Impact of multi- and interdisciplinary research and innovation (MIDRI)

- Interdisciplinary research was a much more common outcome of funded projects than multidisciplinary research, suggesting that it was built into projects at a fundamental collaborative level. In particular, eight out of nine Academic Proof projects had carried out interdisciplinary working.
- Multi- and inter-disciplinary working was much less common in software ecosystem and demonstrator projects, although two demonstrators have reported MIDRI publications in academic journals, and one in a joint industry/academic journal.
- Barriers between hardware and software specialists were reported as a key barrier to MIDRI; however six interviewees reported that their DSbD project had had a positive impact on this.

5.3. Impact on business-academic engagement activities

EQ6: To what extent and how has DSbD increased business-academic engagement on innovation activities?

This section details the extent of business-academic collaborations and engagements activities undertaken as part of the DSbD programme. The assessment of business-academia engagement is based on evidence collected against the KPIs:

- Proportion of beneficiaries who agree DSbD has led to greater businesses or academia engagement on digital security R&D projects.
- Number of industry-led collaborations.
- Number of academic-led collaboration.
- Number & nature of joint publications.
- Mix of partner types within each project Consortium engaged in the programme.

Many of the DSbD programme's funded project workstreams have included both academic and industrial partners:

- The Technology Platform Prototype workstream.
- All (six) funded Demonstrators.
- The ESRC Hub+.
- Seven out of nine EPSRC Academic Proof projects.
- Six out of ten of the full Software Ecosystem development projects.
- Two out of ten De Minimis software ecosystem development projects.

Considering all the different funded projects, relatively few were academic-only, while the remainder were roughly an even split of industry-led, academic-led, or industry-only. Table 8 below provides a summary breakdown.

Table 8: Summary of project types and leads

Project consortium type	Number of projects
Industry Led	11 (29%)
Academic Led	12 (32%)
Academic Only	4 (10%)
Industry Only	11 (29%)
Total	**38**

The detailed list of collaborators involved in the funded projects is detailed in Table 9 below, with project leads distinctly highlighted in **bold**. Out of the 38 projects that received funding, a significant 23 (61%) have been delivered collaboratively. This encompasses all six Demonstrator projects, the Technology Platform Prototype, and the ESRC Hub+.

Notably, the largest share of these collaborative projects originates from EPSRC Academic Proof and Software Ecosystem Development workstreams. Specifically, seven projects under the Academic Proof category and six projects focused on Software Ecosystem Development have been co-delivered through joint efforts between industry and academia. As part of stakeholder consultations, eleven interviewees from funded projects reported that they had developed strong relationships with their consortium partners through collaboration efforts during the project. Additionally, they are seeking further collaboration opportunities with their project partners and expect to continue engaging with them in future work including follow-up proposals and funding initiatives. Three interviewees from two demonstrator projects further highlighted the importance of sustained industry engagement beyond the DSbD funding period, deeming it essential for the adoption and acceptance of the technology, which are the next steps for CHERI technology.

The De Minimis competition aimed to enable the growth of the software ecosystem, recognising that this development of SMEs collaboration is essential for the successful adoption of DSbD technologies. While two SMEs from the De Minimis workstream have progressed to undertake additional projects within the Software Ecosystem Development workstream, they are not involved in any business-academic collaborations for these additional projects.

Table 9: List of collaborators in DSbD funded projects (project leads highlighted as bold)

Project	Academic Partners	Industry Partners
Technology Platform Prototype		
Morello Board	▪ University of Cambridge ▪ University of Edinburgh	▪ **Arm** ▪ Linaro
EPSRC Academic Proof		
SCorCH	▪ **University of Manchester** ▪ **University of Oxford**	▪ Amazon ▪ Arm
CHaOS	▪ **University of Cambridge**	▪ Google ▪ HP ▪ Arm ▪ Microsoft ▪ SRI International
CapableVMs	▪ **University of Glasgow** ▪ **Kings College London**	▪ Shopify ▪ Arm
CAPcelerate	▪ **University of Cambridge**	None

Project	Academic Partners	Industry Partners
CAP-TEE	▪ **University of Birmingham** ▪ University of Surrey ▪ Loughborough University	▪ Samsung ▪ Horiba Mira Automotive ▪ Thales UK ▪ HP ▪ Siemens AG ▪ Toyota ▪ Qinetiq
AppControl	▪ **University of Glasgow** ▪ University of Essex ▪ Imperial College London	▪ UltraSoc ▪ NASA JPL
CapC	**University of Kent**	None
HD-Sec	**University of Southampton**	▪ Atomic Weapons Establishment ▪ AdaCore ▪ Galois Inc. ▪ Altran ▪ Thales ▪ Airbus ▪ Arm ▪ L3 Harris ▪ Northrup Grumman
CloudCAP	**Imperial College London**	Microsoft
Number of collaborative projects		**7**
De Minimis Competition (all SME-led)		
Data Path Development Kit	Queen's University Belfast	**Pytilia Ltd**
Porting Edge AI Workflows	None	**Oxon.Tech**
Multi Compartment Computation Protocol	None	**MindHug Ltd**
CHERI Stone	None	**Drisq Ltd**
SecurIOT	University of Sheffield	**IOETEC Ltd**
TEE-aware compartmentalisation framework	None	**Verifoxx Ltd**
A feasibility study of a data security software product adopting Digital Security by Design (DSbD) technology	None	**Anzen Technology Systems**
Trusted Ring Security for Morello Devices	None	▪ **Metrarc Ltd** ▪ BT
Quantum Resistant DSbD Security Leveraging Micro Tokenisation	None	**Valid Datum Ltd**

Project	Academic Partners	Industry Partners
Assessing the Viability of an Open Source DSbD Desktop Software Ecosystem	None	**Capabilities Ltd**
Number of collaborative projects		**2**
Software Ecosystem Development (EPSRC / Innovate UK joint delivery)		
SNbD	University of Oxford	▪ **Nquiringminds** ▪ Techworkshub
Developing and Evaluating an Open-Source Desktop for Arm Morello	None	**Capabilities Ltd**
CAMB	**University of Cambridge**	TODAQ Holdings Ltd
FlexCap	**University of Manchester**	NEC Europe
MOJO	University of Manchester University of Oxford	**THG**
CHERI WebAssembly Micro Runtime	None	**Verifoxx Ltd**
Morello-HAT	▪ **University of Glasgow** ▪ Imperial College London	None
Chrompartments	**King's College London**	Arm
Capabilities for Coders	**University of Glasgow**	Arm
Complementing capabilities	**University of Kent**	None
Number of collaborative projects		**6**
Demonstrators		
Soteria	▪ University of Manchester ▪ University of Oxford	**THG**
High security communications infrastructure using peer-to-peer Mesh VPN	University of Oxford	**100 Percent IT Ltd**
DEFGRID	University of Strathclyde	▪ **Southern Gas Networks** ▪ Deltaflare
MoatE	University of Manchester	**Iceotope Technologies**
AutoCHERI	▪ University of Exeter ▪ University of Swansea ▪ Coventry University	▪ **Beam Connectivity** ▪ Compound Semiconductor Catapult ▪ Idiada Automotive Technology
RESAuto	University of Warwick	▪ **Thales UK** ▪ Beam Connectivity ▪ AESIN
Number of collaborative projects		**6**

Project	Academic Partners	Industry Partners
ESRC Hub+		
DiScribe Hub+	▪ **University of Bath** ▪ University of Bristol ▪ Royal Holloway University ▪ Cardiff University	▪ HP ▪ Microsoft ▪ Thales ▪ Roke ▪ Qualcomm ▪ Airbus ▪ HSBC ▪ RSA Security
lowRISC Direct Award		
Sunburst project	▪ None	▪ **lowRISC CIC** ▪ NewAE Technology (wholly owned subsidiary of lowRISC)

Source: DSbD programme documentation

The DSbD programme's activities, other than funded projects, have also facilitated business-academic engagement. These activities encompass awareness-raising efforts, events, workshops, and broader undertakings outside the funding workstreams.

The DSbD All Hands event unites funded project partners and stakeholders from diverse sectors to exchange ideas and knowledge on developed tools and technologies. This event typically features talks, demonstrations, poster sessions, and discussions. Overall, insights from stakeholder consultations reveal that the DSbD All Hands event has been pivotal in establishing valuable industrial connections and raising awareness of what other organisations are working on. Additionally, representatives from four academic proof projects and one software ecosystem development project indicated their intention to pursue collaborations stemming from connections established during the All Hands events.

Established in 2022 by a funded project, the CHERITech forum aims to provide a platform for technical discussions on various aspects of CHERI infrastructure, including hardware, software, and verification. According to interviewees from two academic proof projects, the CHERITech forum has significantly facilitated knowledge exchange between academia and industry, while also showcasing their work.

The DSbD programme has also hosted several other events, such as the DSbD Technology Access Programme Showcase and the Automotive Security by Design Summit (AutoCHERI demonstrator). These events, although primarily focused on showcasing and demonstrating developed technologies, have also offered networking opportunities and engagement with stakeholders across the UK's cyber security landscape.

The CHERI Alliance builds on the DSbD ecosystem. It includes companies that participated in DSbD, such as Google, lowRISC, and Capabilities Ltd, as well as companies independently investing in CHERI research, including Codasip and SCI Semiconductor. The Alliance's membership also extends to academic institutions like the University of Cambridge and the University of Birmingham, and government departments that have engaged with DSbD, such as DSTL and NCSC. The Alliance has had the following impacts on collaboration:

- Facilitating engagement between various stakeholder groups, including industry and academia, through its technical working groups. To date, these groups have focused on addressing practical issues related to the adoption of the technology and reducing the associated costs of adoption.

- CHERI Alliance is organising the CHERI Blossoms Conference 2025, scheduled for April 2025. This event aims to bring together researchers, technologists, industry leaders, and business strategists to further the advancement of DSbD tools and technologies.

The Alliance's efforts indicate **continuation of engagement of DSbD participants and new stakeholders with CHERI and DSbD ecosystem**, even after the completion of DSbD-funded projects.

Additionally, a funded project interviewee emphasised that Innovate UK has actively encouraged project partners to disseminate information about the DSbD programme and the Morello boards within their networks. The interviewee found this approach highly effective for fostering connections and has engaged with individuals from UK organisations, as well as those in Australia and Sweden.

5.4. Collaboration between younger, smaller companies and larger, more established companies

EQ7: To what extent and how has DSbD increased collaboration between younger, smaller companies and larger, more established companies up the value chain?

The DSbD programme, as part of the ISCF initiatives, aims **to increase collaboration between younger, smaller companies and more established, larger companies up the value chain.** This section is based on evidence collected against the following KPIs:

- Number of SME collaborations with larger companies.
- Proportion of beneficiaries who agree DSbD led to more collaborations across the cyber security industry and companies.
- Mix of company types that are engaged with the programme.

Evidence suggests that this objective is being realised through collaborations formed to bid for funded projects with Innovate UK.

- The Technology Platform Prototype workstream highlights this collaboration, featuring Arm, a prominent firm listed on the NASDAQ 100 with over 7,000 employees, and Linaro, a medium-sized company with a turnover of £27.3 million in 2023.
- Additionally, three of the six demonstrators illustrate such partnerships:
  - **DEFGRID**: Led by Southern Gas Networks Plc, supported by the smaller company Deltaflare Technologies.
  - **AutoCHERI**: Links Beam Connectivity, an SME, with Idiada Automotive Technology, a multinational employing over 2,200 people worldwide.
  - **RESAuto**: Connects Thales UK, a multinational company with a 2023 turnover of £1.1 billion and over 7,000 employees in the UK, with Beam Connectivity.

However, only one of the 20 software ecosystem development projects meets the criterion for collaboration between different scales of business, involving Metrarc Ltd and BT. Given that these projects aim at Ecosystem Development and the De Minimis projects were partially intended to upskill SMEs to enable them to join collaborations, **this represents a missed opportunity**.

Formal project collaborations are not the sole avenue for developing supply chain links. The software development competitions and Technology Access Programme has offered **opportunities for informal collaboration with core delivery partners**. For example, many of the EPSRC software development projects received letters of support, funding or contribution in kind from partners including Arm, Microsoft, Google and Amazon. In some instances, academic funding awardees have moved across to work in industry in the companies that they partnered with. These links are crucial, as the programme's Logic Model suggests that:

- Increased industrial sector awareness of issues and market failures, and DSbD as a response, leads to confidence in technology, and increased demand for solutions.
- Growing the ecosystem and building skills, collaborations and supply chain linkages increases UK capacity and capability to develop digitally secured products and services.

Other activities, such as DSbD events, have also provided opportunities for developing links between smaller companies and larger, more established companies. Stakeholder participation in DSbD events has been diverse, including representatives from industry, academia, and government departments. Industry stakeholders have included large companies such as Arm, and Thales UK, alongside smaller companies like Deltaflare and Beam Connectivity, thereby **offering a platform for networking, connecting, and developing links between businesses of varying scales.**

As mentioned above, the CHERI Alliance members include large corporations as well as SMEs, spanning over five countries and aims to collaborate across the entire value chain—from university research to commercial deployment. Although not directly part of DSbD, the CHERI Alliance's impact on developing supply chain links between smaller and larger companies, both nationally and internationally, can be attributed to the DSbD programme, as the Alliance likely would not have formed without it.

5.5. Impact on multi and interdisciplinary research

EQ8: To what extent and how has DSbD increased multi and interdisciplinary research?

This section sets out the impacts perceived from multi and interdisciplinary research, based on evidence collected against the following KPIs:

- Number of research projects cutting across academic disciplines (inter).
- Number of research projects involving experts within academic disciplines (multi).
- Level of collaboration between hardware, software, social science and ICT.
- Publication of academic papers on multi / interdisciplinary research areas.

Our consultations at the interim stage showed that **funded projects were much more likely to report interdisciplinary working than multidisciplinary**, suggesting that if any collaboration was required in projects it was built into them at a fundamental level to work jointly on difficult problems, rather than split projects into tasks which were addressed separately by experts from different disciplines.

It was agreed at the evaluation framework drafting stage that inter- and multi-disciplinary research are not always well defined or universally understood. From our research at the baselining stage, we have arrived at a common working definition:

- **Interdisciplinary research** involves experts from multiple disciplines collaborating on solutions together.
- **Multidisciplinary research** similarly involves experts from multiple disciplines, but these can be working separately on different aspects of a problem without necessarily collaborating directly and sharing knowledge.

The Multi- and Inter-disciplinary Research and Innovation (MIDRI) impacts to date are summarised by workstream in Table 10 below. It shows a high level of interdisciplinary working in the academic proof projects, and a rather lower incidence of MIDRI working practices in the Demonstrators and software ecosystem projects (particularly the de minimis workstream), although there is some evidence of MIDRI publications produced by the full ecosystem projects and Demonstrators.

Table 10: Multi- and inter-disciplinary research summary

Multi and interdisciplinary research	Academic Proof	Software Ecosystem (de minimis)	Software Ecosystem (full)	Demonstrators
Research projects employing interdisciplinary working	8	2	2	1
Research projects employing multidisciplinary working	3	0	1	0
Projects publishing MIDRI papers in academic journals	2	0	2	3
Projects publishing in joint industry/academic journals	3	0	2	1
Total projects in workstream	**9**	**10**	**10**	**6**

Some details of the MIDRI impacts by workstream are explored below.

Academic Proof workstream

- Eight out of the nine Academic Proof projects reported that **they had carried out interdisciplinary working as part of their projects**. The other project said that their research did not generate much human-computer interaction, and so they had approached it as standalone research.
- The interdisciplinary work carried out by the Academic Proof projects had differing levels of engagement with other disciplines:
  - Two of the projects carried out interdisciplinary work, but mostly within computer science and cyber security disciplines.
  - Four more worked cross-department, including social sciences, law, and mathematics
  - Two more worked cross-department and also included partners from industry.
- Two of the projects reported that they have explicitly published MIDRI research in academic journals. Additionally, three of the projects indicated that they have either published or are in the process of publishing MIDRI research through other academic routes, such as conference papers.
- Four projects reported that they have published research in joint academic/industrial journals and one project reported that they have published their work with a private research firm independently.

Software ecosystem – de minimis and main competitions

Multi- and interdisciplinary research impacts were less common in the software ecosystem projects.

- Among the two “de minimis” software ecosystem projects reporting interdisciplinary working, one had attracted the backing of DSTL for computer security research, and other reported an informal partnership with a university professor.
- The main software ecosystem workstream, originally to support industry-led projects, was redesigned as a joint Innovate UK / EPSRC project which could attract either industry- or academic-led bids, in order to involve more research institutions in the developing ecosystem.
  - The two main software ecosystem projects that reported formal interdisciplinary working were both academic led; one project worked with the PETRAS national centre of excellence in cyber security research on the Internet of Things, and the other project collaborated with experts in financial services.
  - Two projects published MIDRI papers in academic journals, while a third project reported that they mostly published their work as part of a single domain but had collaborated with some departmental colleagues in other research domains.

- Two projects published papers in joint academic/industry journals, while one more had unacknowledged support from industry for one of their publications.

- All of the impacts reported above in the main software ecosystem projects were generated by four projects, of which three were academic led.

Demonstrators

- One demonstrator project reported that it had carried out interdisciplinary work based on the partnership between the Universities of Manchester and University of Oxford. A few different people on the team have published MIDRI research in academic journals.
  - The overall approach of the project is more industrial than academic, however there is some overlap which has led to some multidisciplinary work through use of consultants with ties to academia and participation at conferences.

- Two demonstrators have reported MIDRI publications in academic journals and one has published in joint industry/academic journals through their university partner.

5.5.1 Analysis of DSbD related publications

Publications from DSbD-funded projects serve as valuable indicator for assessing the research impact generated through the aforementioned multi- and interdisciplinary working practices. To evaluate this impact, we have employed bibliometric analysis to measure various aspects of DSbD-related publications, thereby gaining insights into their research influence and identifying emerging key trends.

The data for the DSbD publications was sourced from Researchfish and provided to us by UKRI. This dataset includes the study titles and/or Digital Object Identifiers (DOIs) for publications released by funded projects under the DSbD initiative. However, it is important to note that the dataset used for this evaluation is not exhaustive as many projects concluded in late 2024 and early 2025, and stakeholder consultations revealed that additional publications were released near the project completion dates. Some publications were still in the pipeline at the time of the interviews, indicating that the dataset may not capture all relevant publications.

To ensure comprehensive coverage, the data for identified publications was sourced from OpenAlex. OpenAlex is an open-access, comprehensive catalogue of the global research system. OpenAlex aggregates data from multiple sources, such as CrossRef, PubMed, and institutional repositories, providing a broad and detailed view of scholarly works across different disciplines and regions.

To analyse DSbD related publications, the following data was collected from OpenAlex for each publication:

- Publication title
- Year published
- Type of publication
- Authors
- Institution of authors
- Citation count
- Topics related to the publication
- Keywords related to the publication
- Whether the publication is open access.

The DSbD programme has seen a significant output of research studies, with a total of 209 publications to date. 69% of these, amounting to 144 publications, are available as open access, making the research widely accessible. Additionally, DSbD-related publications have collectively garnered 3,849 citations. Table 11 and Table 12 provide descriptive statistics of DSbD-related publications by year published and publication type, respectively.

Table 11: Descriptive statistics by year published

Year Published	Number of publications	Number of publications that are available Open Access	Citation Count
2020	13	10	880
2021	34	20	1,511
2022	54	39	345
2023	61	48	1,058
2024	38	22	55
2025	9	5	0
Total	**209**	**144**	**3,849**

Table 12: Descriptive statistics by publication type

Publication Type	Number of publications	Number of publications that are available Open Access	Citation Count
Article	147	109	2,631
Book	4	0	52
Book-chapter	30	7	1,004
Preprint	25	25	74
Review	3	3	88
Total	**209**	**144**	**3,849**

There is a clear upward trend in both the number of publications and the availability of open access research.[17] Notably, 2023 and 2024 each saw a substantial number of publications, at 54 and 61 publications released, respectively. Despite having fewer publications in 2021, the year recorded the highest number of citations at 1511, suggesting that the research produced during that period had a higher impact.

Articles are the predominant type of publication within the DSbD programme, comprising 70% (147) of the total. These articles also account for 68% of the total citations, signalling their significance and reach. In addition to articles, the programme's output includes 30 book chapters, which comprise only 14% of the total publication. However, the research impact of the book-chapters is high, contributing to 26% of the total citations

Figure 4 illustrates the top institutions with the highest contributions to DSbD-related publications. The data encompasses multiple institutions based on the number of authors for each publication. In instances where publications were associated with multiple institutions, the weighting was distributed proportionally among them. For example, if a publication was associated with two institutions, each institution received a 50% weight; if associated with four institutions, each received a 25% weight. This methodology ensured that the distribution of each institution was proportionally represented according to its frequency. Subsequently, we calculated the weighted count of institutions for all publications by estimating the weighted occurrences.

As depicted in the figure below, the University of Essex exhibited the highest research output for DSbD, contributing to and co-authoring 12.5% of the total publications. Comparatively, DSbD-related publications from the University of Cambridge are lower at 1.9%, likely from a combination of factors. This could be due to University of Essex's stronger focus on publication-driven funded project outputs and DSbD research collaborations with foreign institutes. In contrast, Cambridge's work on CHERI predates the DSbD programme and publications released pre-DSbD fall outside the evaluation scope. There is also a possibility

[17] This trend is not observable in 2025, as the latest DSbD-related publications may not be covered by the Researchfish data.

that some publications from the University of Cambridge (or other institutions) may not have been fully captured by Researchfish and OpenAlex.

Following Essex, the University of Manchester and Imperial College London contributed to and co-authored 9.46% and 7.6% of DSbD-related publications, respectively. Universidade Federal do Amazonas and Technische Universität Wien (TU Wien) are the only foreign academic institutions to feature in the list, contributing to 1.7% and 1.2% of the total publications, respectively. This is likely due to these two institutions collaboration with the University of Manchester on several DSbD-related publications.

Figure 4: Top institutions that contributed to DSbD related publications

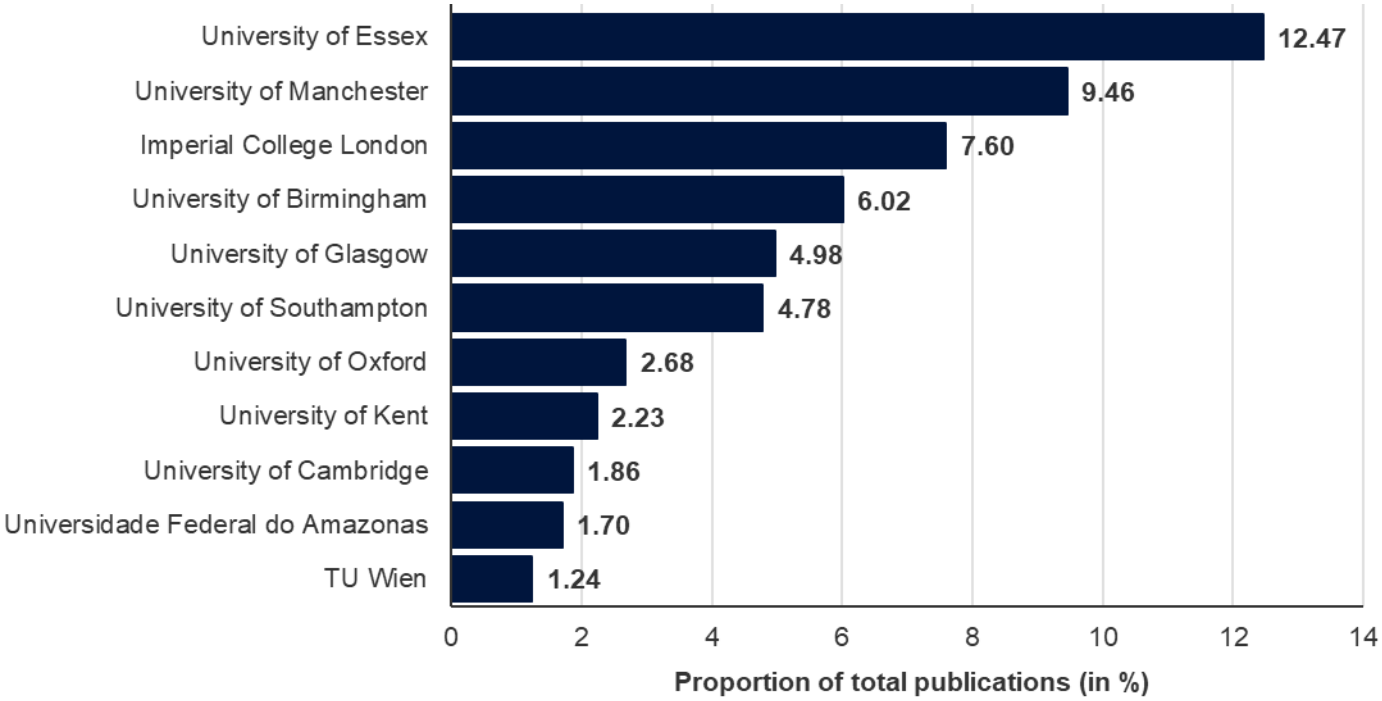
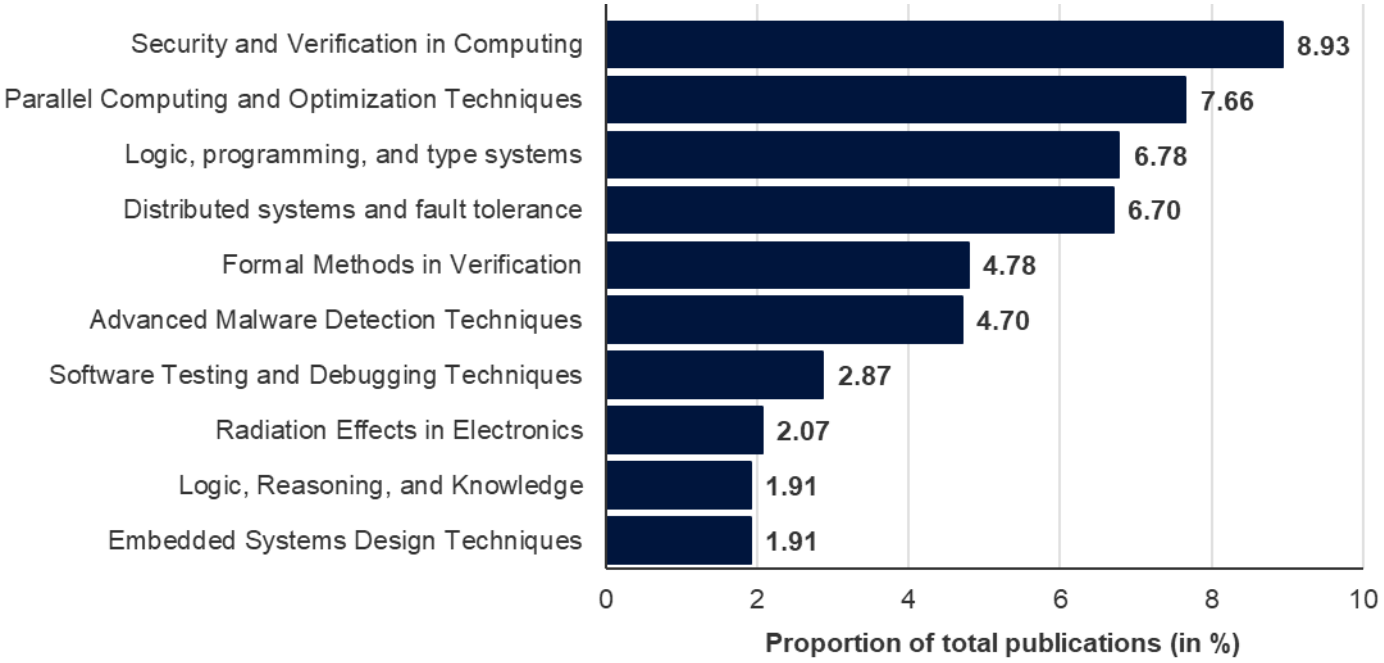


Figure 5 presents the top ten topics of DSbD-related publications, delineating the domain of these publications. The identical weighted count approach has been employed to estimate the proportion of publications within each topic, as was applied for institutions.

DSbD-related publications encompass a broad spectrum of topics. Notably, there is a significant emphasis on 'Security and Verification in Computing,' which constitutes 8.93% of all publications. 'Parallel Computing and Optimisation Techniques', 'Logic, Programming, and Type Systems', and 'Distributed Systems and Fault Tolerance' represent 7.7%, 6.8%, and 6.7% of the total publications, respectively. These topics are well-aligned with the overarching objectives of DSbD technology, focusing on addressing various challenges in computing and security, with a pronounced emphasis on system reliability and protection against cyber threats.

Figure 5: Topic 10 topics of the DSbD-related publications



5.5.2 Perspectives on collaboration between hardware, software, social science, and ICT

Multi- and interdisciplinary research requires expertise and collaboration across various domains. Specifically, in areas related to DSbD, it is essential to foster collaboration among hardware, software, social sciences, and ICT companies. Such collaboration ensures that complex research problems are addressed from multiple angles. Furthermore, the degree of collaboration between these fields serves as an indicator of the efficiency of the hardware and software teams working together, particularly in the context of interdisciplinary research.

Interviewees had a diverse range of opinions regarding the collaboration between hardware and software companies within the broader digital and cyber security sector. During the final interview phase, seven out of fourteen respondents expressed a cautiously optimistic view, noting that while collaboration levels are improving, there remain opportunities for further enhancement and sustainability. Three interviewees indicated that the desired level of collaboration is still lacking between the two parties. The remaining four respondents provided neutral or mixed feedback, highlighting variability in collaboration depending on the sub-sector or discipline, or acknowledging that collaboration does occur in some areas but is not sufficiently widespread.

The insights presented below integrate thematic analyses from stakeholder consultations at both the interim and final stages. The perspectives across these stages are well-aligned, with the final stage interviews placing greater emphasis on the impact of DSbD on level of collaboration between hardware and software companies.

- Some individuals reported that, because it is **uncommon for a company to have specialisms in both hardware and software**, collaboration serves as a valuable problem-solving tool. However, companies often operate in silos and do not collaborate extensively.
    - The size of the company makes a difference: larger companies are more likely to work in both hardware and software. An interview provided an example, indicating that large companies involved in cloud computing or mobile technology, such as Intel and Microsoft, exhibit tight collaboration.

  - The level of collaboration also varies based on sub-sector or product type. Insights from stakeholder consultations highlighted significant lapses in the security of smart home devices, with hardware and software security often being overlooked.
  - Regional and geographical factors also contribute to the variability in the level of collaboration.
- Two interviewees noted that collaboration between hardware and software can be challenging due to the specialised nature of academic work. One researcher elaborated that Research Councils encourage MIDRI proposals, but reviewing them objectively is difficult as they are primarily reviewed by single-subject specialists.
  - Historically, the UK has focused more on theoretical computer science, formal methods, and related fields. However, this has changed recently, with a larger proportion of PhD students shifting from pure hardware or software specialisms towards hardware-software co-design.
- Collaborations between IT and social sciences were viewed as rare, although some respondents expressed interest in developing such collaborations in their sector. In cyber security service provision, there is an opportunity for this. One researcher noted that it was challenging to secure funding for such projects before DSbD, as there were few sufficiently focused MIDRI calls.
- Collaboration in the ICT sector, in general, was seen as beneficial but not as common as it should be. Some reasons given were:
  - The sector is dominated by large players who want to retain control over their IP.
  - Problems in cyber security are large and complex, making them hard to grasp or build large teams for.
  - Collaboration is more feasible in certain sectors, such as telecoms and cloud computing.

There is considerable evidence from stakeholder consultations indicating that **DSbD has made a difference**. Overall, six interviewees explicitly stated that the DSbD programme has positively impacted hardware-software collaboration. One interviewee emphasised that DSbD has created opportunities for cross-disciplinary interaction, more so than other programmes they have encountered. Three interviewees reported that their hardware-software collaborative experiences within their DSbD-funded projects have highlighted greater opportunities and benefits of this type of collaboration. It was further explained that DSbD has helped strengthen this collaboration, particularly within capability hardware and memory safety. Three projects explained that the scope of CHERI and the DSbD programme has enhanced hardware-software co-design, as it required determining what works in hardware and what works in software.

Although no one had strongly negative comments about DSbD's efforts to build collaboration, one interviewee noted that there have not been changes in computer architecture within the scope of CHERI and Morello in decades. However, software evolves with hardware and vice versa, highlighting this collaboration as natural.

5.6. Conclusions against evaluation questions

Business-academic engagement activities

The DSbD projects have proven to be **effective in fostering business-academic collaboration**, with 61% of the total projects being delivered through joint efforts between industry and academia. Furthermore, various DSbD events, such as the All Hands meetings and the CHERI tech forum, have significantly contributed to business-academic engagement activities, facilitating networking opportunities and knowledge sharing.

These collaborations are crucial for reinforcing several links in the programme's Logic Model, which connects programme activities to their eventual impacts:

- Building a strong industry-academia network leads to capacity building and eventually to creation of new products and services, provided that investment becomes available.

- Increased industrial sector awareness of issues and market failures, and DSbD as a response, leads to confidence in tech, and increased demand for solutions. Growing the ecosystem while building collaborations and supply chain linkages increases UK capacity and capability to develop digitally secured products and services.
- Both the above contribute to downstream adoption, which is the key to eventual economic and societal impact.

Level of collaboration between SMEs and large companies

The evidence indicates that **collaboration between SMEs and large companies has primarily been realised through the Technology Platform Prototype workstream and the Demonstrator workstream**, with 50% (3 out of 6) of demonstrators showcasing such partnerships.

However, only one of twenty software ecosystem development projects, including the De Minimis workstream, can be classified as a collaboration between SMEs and large companies. **This suggests a missed opportunity, as these projects were intended to enhance the capacity of participating companies to engage in further collaborations.**

While DSbD has facilitated collaboration between SMEs and large companies to some extent, there remains significant potential to increase the level of collaboration. Facilitating these partnerships further would enable SMEs to develop key industrial connections, thereby supporting their growth and improving their capability and capacity to contribute effectively to future work on new security capabilities.

Impact of multi- and inter-disciplinary research

Interdisciplinary research was much more common than multidisciplinary research in funded projects. This indicates that projects requiring collaboration are designed to integrate expertise from multiple disciplines at a fundamental level, rather than separating tasks.

Academic Proof projects demonstrate a high level of interdisciplinary collaboration, particularly within the fields of computer science, cyber security, social sciences, law, and mathematics. In contrast, Software Ecosystem projects (both De Minimis and main competitions) exhibited fewer multi- and interdisciplinary impacts, although academic-led projects made significant contributions to multi- and interdisciplinary research. Demonstrator projects showed some interdisciplinary work, primarily through partnerships between universities and industry, with one project reporting multidisciplinary research.

The DSbD programme has produced a substantial number of publications, totalling 209, with 69% available as open access. This broad accessibility enhances the dissemination of knowledge and amplifies the research's impact.

The University of Essex, University of Manchester, and Imperial College London are leading contributors to DSbD-related publications, indicating higher research outputs from these institutions. The University of Manchester's collaboration with foreign institutions on publications underscores the global reach of DSbD research.

Collaboration between hardware and software companies within the sector is improving but remains variable, influenced by geographical factors, sub-sector, and company size. **The DSbD programme has positively impacted hardware-software collaboration, particularly in the areas of capability hardware and memory safety.**

6. Impacts on Cyber/Digital Security

6.1. Introduction

This chapter outlines the impacts of the DSbD programme on the wider cyber and digital security landscape and addresses the following set of evaluation questions:

- To what extent has DSbD established the needs for UK cyber security? Has DSbD furthered the understanding of cyber security consumer needs? (Covered in Section 6.3)
- To what extent has DSbD helped raise awareness of the UK cyber and digital security issues? Has the DSbD programme provided a unified vision on how to remedy digital security issues? Is this vision shared by industries and policymakers? (Covered in Section 6.3)
- To what extent has DSbD catalysed or contributed to the cyber security transformational change? Why, why not? (Covered in Section 6.4)
- To what extent and how has the Challenge successfully enabled the potential reduction of the number of successful cyber attacks in the UK? (Covered in Section 6.5)
- To what extent and how has DSbD increased the awareness of new security capabilities? (Covered in Section 6.6)

DSbD impacts on the wider cyber and digital security landscape are identified in the programme's Logic Model as intermediate outcomes such as:

- Changing priorities in the research agenda.
- Progress towards new regulatory standards and legislation propositions.
- Increased industrial awareness of cyber and digital security issues and market failures, leading to:
  - greater confidence in the value of new technology.
  - increased commercial demand for, and capability to develop, digitally secured products and services.

6.2. Key findings

Understanding of needs of cyber security and raising awareness of cyber and digital security issues

- DSbD has actively contributed to raising understanding and awareness of cyber and digital security issues in multiple government departments, shaping government thinking and leading to references to DSbD featuring in government policy and strategy documents.
- The programme has raised awareness among technical and cyber security experts in industry, though there is still work to be done to engage senior decision makers in large companies.
- Public awareness of cyber security needs and risks remains basic, and DSbD's impact here is seen as minimal.

Catalysing transformational change on cyber security

- The DSbD programme has made good progress through the government awareness raising and support mentioned above, which has in turn led to additional funding contributions to the programme from Government.
- A significant global development has been the emergence of "memory safety" as an internationally understood term for the cyber security issues that CHERI was designed to fix. CHERI appears as a hardware solution for memory safety issues in papers produced by Google, the White House, and the UK

Government. DSbD participants have contributed to a paper, “It is time to standardize principles and practices for software memory safety”, which surveys the field and notes that procurement cannot proceed without a common language for describing cyber security problems.

Impact on cyber attacks

- The DSbD programme's impact on reducing cyber attacks is yet to be realised, as there are currently no live DSbD-based products. It is expected that the successful implementation and adoption of DSbD technology can lead to a significant reduction in cyber attacks.

Awareness of new security capabilities

- Evidence of interest in new security capabilities, measured through social media engagement of DSbD handles, suggests a slowly growing awareness of the DSbD technology.
- Traditional news posts reached approximately 31,000 individuals across 16 published articles in February 2025. Social media—despite a lower volume of posts—achieved significantly higher engagement, reaching around 95,000 users. Notably, the DSbD Showcase emerged as a focal point of online discourse.

6.3. Understanding of needs of cyber security landscape and raising awareness of cyber and digital security issues

EQ9: To what extent has DSbD established the needs for cyber security? Has DSbD furthered the understanding of cyber security consumer needs?

EQ10: To what extent has DSbD helped raise awareness of the UK cyber and digital security issues? Has the DSbD programme provided a unified vision on how to remedy digital security issues? Is this vision shared by industries and policymakers?

This section sets out the extent to which DSbD has established the need for cyber security, furthered the understanding of cyber security consumer needs, and helped raise awareness of UK cyber and digital security issues within the industry and the government. Additionally, it examines whether DSbD has provided a unified vision on how to remedy digital security issues and if this vision is shared by industries and policymakers.

This section is based on evidence collected against the following KPIs:

- Perceived improvements in industries and general public’s awareness of cyber security problems and challenges.
- Level of acceptance by industries and general public of the need for more digitally secured products and services.
- Perceived ability by industries and businesses of DSbD to present cyber and digital security concepts in a unified way.
- Agreement on cyber security issues depicted within key sectors, and solutions proposed by DSbD.
- Perceived mandate of UKRI/DSbD programme to provide a cyber and digital security research agenda, and platform for regulatory discussions.

6.3.1 Government awareness

Government awareness of DSbD technology is crucial for addressing cyber security issues at national level. Engagement from the government ensures that they stay informed about developments, thereby enhancing visibility and enabling effective investment in areas with strong potential, national alignment, and higher return on investment. Additionally, government involvement in regulatory changes and standardisation efforts ensures regulations keep pace with technological advancements.

The **DSbD programme has successfully engaged various government departments**, indicating a high level of governmental awareness and support. The DSbD Programme Board and the Advisory Board includes representatives from DSIT, DSTL, NCSC, and DESNZ, highlighting the visibility of DSbD activities across government departments within the UK. In 2024, DSIT commissioned work to explore barriers and enablers to CHERI adoption and diffusion[18], evidencing the perceived value of DSbD outputs and the government's commitment to promoting these technologies as solutions to cyber security challenges.

DSbD's success in securing funding from BEIS under the Industrial Strategy Challenge Fund emphasises its alignment with national strategic objectives. The successor to the Industrial Strategy – the Innovation Strategy[19] of July 2021 – explicitly mentions the DSbD programme under the technological pillar, recognising the societal benefits and cost savings associated with digital secure technology. Additionally, the Integrated Review Refresh 2023[20], a refresh to IR2021's[21] five-year strategic framework on national security and international policy, focuses on cyber security to address vulnerabilities though greater resilience and proactively supporting the capabilities, supply chains and technologies that are of strategic importance to the UK.

The National Cyber Strategy 2022 features DSbD under its objective of fostering and sustaining an advantage in the security of technologies critical to cyberspace. This includes a case study on the Soteria demonstrator led by the THG Group, showcasing practical applications of DSbD technologies. Additionally, the 2023 Semiconductor Strategy references DSbD and has pledged continued support to the DSbD programme (See Section 6.4 for more details).

Although the Government Cyber Security Strategy 2022-2030[22] does not explicitly mention DSbD, its central aim aligns with DSbD's objectives, emphasising secure technologies and cyber security procedures. The strategy's goal for government critical functions to be significantly hardened to cyber attacks by 2025, and for all government organisations to be resilient to known vulnerabilities by 2030, aligns with DSbD's timeframe and objectives.

Given that the DSbD has been referenced in key policy and strategy frameworks, and its objectives are well-aligned with other relevant national policies, this opportunity presents a pathway for DSbD technologies to be further integrated into national and cyber security frameworks. This will only be feasible with the availability of a commercialised product incorporating CHERI.

The UKRI DSbD team has also actively engaged at CyberUK, the UK government's flagship cyber security event hosted by NCSC.[23] CyberUK attracts over 2,000 cyber security leaders from the UK and internationally, including government delegates, industry experts, and academia. The CyberUK 2023 focused on newly launched joint framework and guide for 'Secure by Design' and included two plenary sessions for the DSbD programme, showcased in the main auditorium with Microsoft and Google demonstrating their support.[24] At CyberUK 2024, DSbD showcased their work through an exhibition stand, featuring contributions from five demonstrator projects.

Ollie Whitehouse, Chief Technology Officer (CTO) at NCSC, remarked during CyberUK 2024, *"We know how to build cyber resilient technology. If you look at CHERI, there's a mechanism for addressing memory safety."* Moreover, the theme for CyberUK 2025 will focus on creating incentives for adoption. This signifies that DSbD has effectively highlighted the needs of the cyber security sector, successfully raising awareness among government stakeholders.

[18] CHERI Adoption and Diffusion Research (DSIT, 2024)
[19] UK Innovation Strategy: leading the future by creating it (GOV.UK, 2021)
[20] Integrated Review Refresh 2023: Responding to a more contested and volatile world (Cabinet Office, 2023)
[21] The Integrated Review 2021 (Cabinet Office, 2021)
[22] Government Cyber Security Strategy: 2022 to 2030 (Cabinet Office, 2022)
[23] CyberUK 2025 (NCSC, 2025)
[24] CyberUK 2023: Part 2 (IoTSF, 2023)

6.3.2 Industrial awareness

Increasing the industrial awareness of cyber security issues and market failures is a necessary step to building confidence in the value of the new technology, increasing commercial demand for secure products, and ultimately to downstream adoption of the technology. The DSbD campaign, launched in November 2021, has played a key role in raising awareness of the cyber security issues and the role of DSbD in addressing them.

The Logic Model suggests that this awareness will arise from marketing and communications efforts by the DSbD communications team, the ESRC Hub+, and the Digital Catapult.

According to DSbD funded project stakeholders:

- Funded projects have an increased awareness of the DSbD technology and cyber security issues, stemming from easy access to DSbD technologies such as the Morello Board, to experiment with use cases specific to their businesses and develop skills in using memory safe technologies.
- DSbD's engagement activities, as discussed in Section 5.3, have **successfully built a tight ecosystem around the tools and technologies developed** as part of the funded projects. The DSbD Advisory Group noted that the **ecosystem's strength lies in its diversity**, encompassing not only the varied sizes and types of companies but also a diverse range of domains involved. The DSbD ecosystem includes contributions from small startups to global corporations, as well as numerous academic institutions. Furthermore, the DSbD ecosystem has made contributions across a wide array of domains, addressing not only technical aspects but also social science and economic dimensions.
- Despite the reported high level of awareness among technical and cyber security experts regarding DSbD technology and its role in addressing cyber security issues, **there is still significant work to be done to raise awareness among senior decision-makers at large companies**.
- To date, marketing and communication materials aimed at raising awareness of CHERI and DSbD have primarily focused on technical aspects. **Moving forward, engaging with the non-technical senior decision makers would require more focus on the business case for adoption**.
- **Efforts to raise market awareness should be concentrated on sectors likely to be early adopters of CHERI**, such as IoT/embedded devices, defence, critical infrastructure, autonomous vehicles, and telecommunications.

Evidence from Researchfish data indicates that organisations involved in the DSbD programme are presenting the cyber and digital security concepts of their funded projects in a unified manner:

- **CAP-TEE:** The project has resulted in identification of Common Vulnerabilities and Exposures (CVE), the CVE-2022-43309, and a security patch issued by Supermicro, contributing to better securing the crucial server ecosystem. Their open-source work around compartmentalisation and TEEs using CHERI has resulted in attention from industry, which will likely feed into further collaboration, possibly through a Knowledge Transfer Partnership (KTP), with a multinational semiconductor IP company.
- **CloudCAP:** The ideas developed by this academic proof project and the associated source code releases have influenced and shaped a number of commercial efforts of capability-based technologies in the DSbD ecosystem.
- **CHaOS:** In 2023, the primary investigator of this project reported that their compartmentalisation models are the de facto standard compartmentalisation implementations used on Arm's prototype Morello Board, and will be used by dozens of companies and universities in the UK and internationally as part of the DSbD programme.
- **Capabilities for Coders:** The learning resources and developer documentation generated by this project have contributed to the growing DSbD ecosystem, enabling faster on-boarding and good awareness raising about CHERI and Morello systems.

Additionally, recent publications from Google on memory safety reference CHERI, and Microsoft Research's publications and GitHub repositories on their work with CHERIoT further highlight increased industrial awareness.

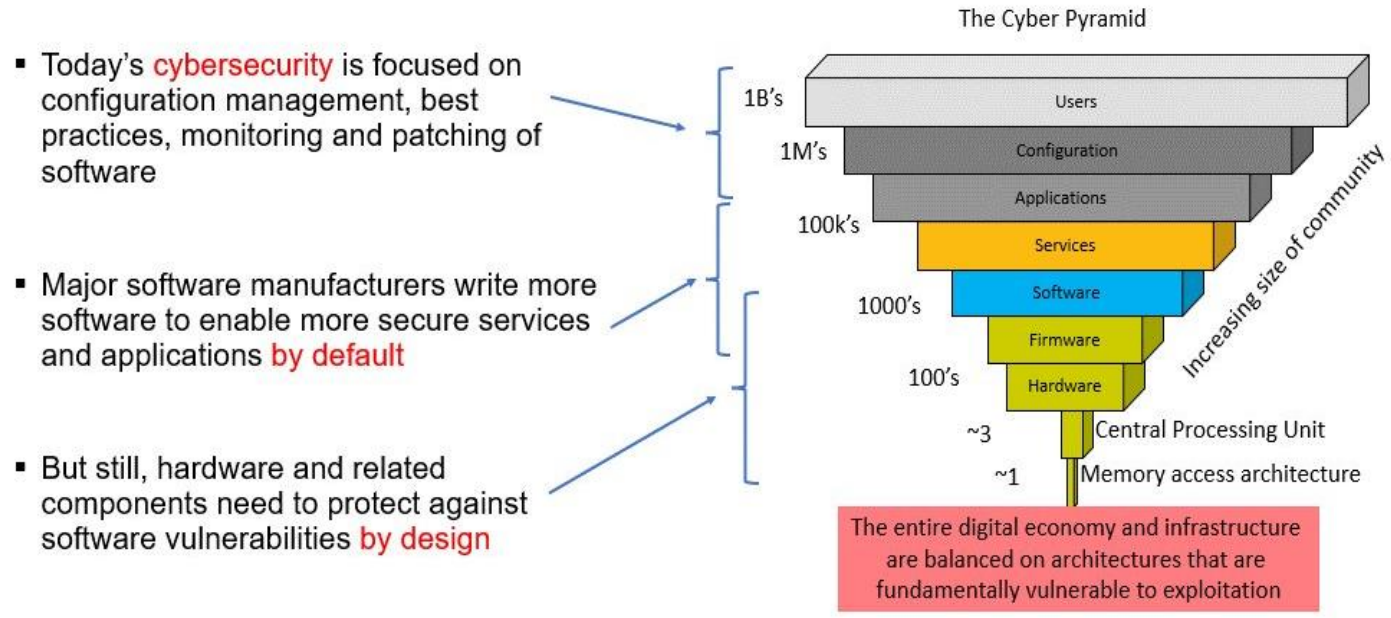
Consultations with industrial stakeholders held as part of the DSIT CHERI Adoption and Diffusion research[25] reveal greater industry awareness of cyber security. Insights from these consultations indicate that while security is becoming increasingly important, it should not compromise performance. Additionally, stakeholders reported that **emerging technologies such as AI also have security implications and are currently a more significant area of interest** for companies determining research priorities.

6.3.3 Public awareness

Stakeholder consultations reveal that while the **general public has a basic awareness of cyber security needs and risks**, there is a generational gap, with younger people being more informed. This gap in understanding is compounded by the expectation that manufacturers should provide standard security measures without additional costs. This is consistent with findings from a report by the Ada Lovelace Institute, which reported that only 26% of the public report knowing a fair amount about digital regulation, and few express confidence in existing protections around digital technologies.[26]

Public awareness of DSbD itself continues to remain minimal, as highlighted in the interim impact evaluation. Within the cyber security landscape , the UK's Secure by Design framework and the DSbD programme work well, even without the public knowledge of the technical aspects of the cyber security issues. Figure 6 illustrates the cyber pyramid which highlights the need to fix the foundations.

Figure 6: The cyber pyramid - Fix the foundations



Source: DSbD programme documentation

For example, the DSbD programme has successfully demonstrated the potential of the CHERI architecture, which can mitigate 70% of vulnerabilities and significantly enhance memory safety at the hardware level. These vulnerabilities have adversely affected the IT sector since the early days of computing and connectivity. Therefore, if organisations address foundational issues and integrate security measures into hardware using the Secure by Design framework or the DSbD technology, the success of these new security capabilities should not be contingent upon public awareness.

[25] CHERI Adoption and Diffusion Research (DSIT, 2024)
[26] Who cares what the public think? (Ada Lovelace Institute, 2022)

6.4. Catalysing transformational change on cyber security

EQ11: To what extent has DSbD catalysed or contributed to the cyber security transformational change? Why, why not?

Transformational change in the UK cyber security environment is likely to require all the changes set out in the previous section – in the policy and research environment, in industrial and public awareness of cyber security risks, and the capability to exploit the technology.

Additional R&D funding from the government to support DSbD-related areas shows a clear commitment to addressing cyber security challenges (see Section 4.3 for more details). For example, DASA ran a CHERI for Defence competition in 2022/23, funding ten projects that explored the implementation of the Morello Board and CHERI in mission-critical and defence settings. However, some interviewees reported the need for active intervention and follow-on funding to catalyse a transformational change for long-standing issue of memory safety and progress to next steps of adoption, standardisation, and regulation for CHERI.

The MoD has specified a Secure by Design procurement framework, which was developed in collaboration by the Central Digital and Data Office, Government Security Group and the NCSC. This framework changes the security emphasis from accreditation and demonstration of security at or near the end of a project, to the explicit requirement that security is addressed throughout the life of a project, from design onwards. **The success of the DSbD programme contributed to the thinking behind the development of Secure by Design.**

Additionally, the 2023 Semiconductor Strategy pledged continued support to the DSbD programme including:

- Expanding international outreach on the global challenge in delivering semiconductor chips that embed digital security.
- Working with other governments and international businesses to promote the widest possible take up of the CHERI technology.

On the industry front, commercialisation efforts within the UK have also facilitated transformational change to some extent (see Section 3.3.2 for more details). Multinational firms such as Arm, Microsoft, and Google engaged with the DSbD programme board and have invested in the programme. These companies have published papers on memory safety, a key security issue that the programme aims to address, referencing technologies and techniques developed within the DSbD programme. Codasip's commercial implementation of CHERI has demonstrated the capability of companies operating in the UK to exploit the technology for commercial purposes. Additionally, SCI Semiconductor is currently working on a commercial implementation of the CHERIoT RISC-V microprocessor core. The potential for transformational change through commercialisation remains constrained, as Codasip is currently the sole company to have integrated CHERI into their processors. Furthermore, stakeholder consultations have indicated that Arm is not actively advancing the commercialisation of CHERI, with reports suggesting a postponement of CHERI implementation in their roadmap. This delay may have impacted the confidence of other stakeholders.

Further opportunities unlocked through the DSbD programme have primarily supported transformational change for academic institutions and researchers (see Section 3.3.1 for more details). By enabling them to advance their research and build on their DSbD work in the cyber security landscape, the programme has significantly improved their R&D capabilities.

At the international level, DSbD has potentially driven transformative changes in addressing memory safety. The White House has published a report titled "Back to the Building Blocks: A Path Toward Secure and Measurable Software[27]," which underscores the urgent need to eliminate memory safety vulnerabilities. This report highlights the importance of adopting memory-safe programming languages and

[27] Back to the Building Blocks: A Path Toward Secure and Measurable Software (The White House, 2024)

acknowledges CHERI as a memory-safe technology, thereby demonstrating the international impact and significance of DSbD's efforts in raising awareness about memory safety issues, not just CHERI.

Furthermore, the US Cyber Security and Infrastructure Security Agency (CISA) released an article in 2023 titled "The Urgent Need for Memory Safety in Software Products[28]," which emphasises the "Secure by Design"[29] best practice guidance and identifies CHERI as a potential solution to memory safety concerns.

The Secure by Design guidance launched in 2023, formally titled "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software[30]," is a collaborative effort by CISA and 17 US and international partners, including cyber security agencies from the UK, Canada, and Australia, among others. This guidance provides best practices and principles for developing products that are secure by design, with a strong emphasis on addressing memory safety.

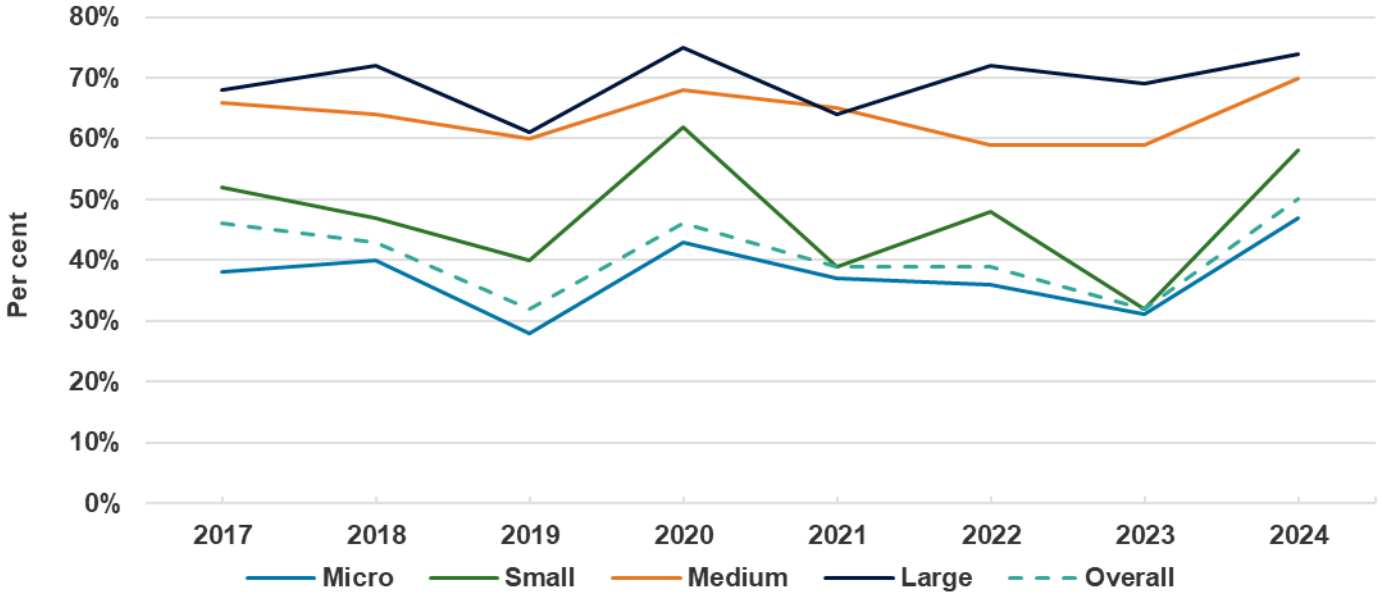
6.5. Impact on cyber attacks

EQ12: To what extent and how has the Challenge successfully enabled the potential reduction of the number of successful cyber attacks in the UK?

As per the interim report, there are currently no live DSbD-based products, and therefore any impact on cyber attacks lies in the future. The aim of the figure presented below is to provide an expanded picture of the impacts on cyber attacks since the interim report in 2022.

The rationale for the programme is grounded in the ongoing threat posed by cyber security breaches to companies, individuals, and the public sector. As outlined in the interim report, evidence from the Government's annual Cyber Security Breaches Survey shows that the proportion of firms reporting cyber security breaches remained relatively stable between 2017 and 2022, with some fluctuations. However, the latest data from 2023 and 2024 indicates a sharp increase in breaches across firms of all sizes after a decrease in 2023. It is also possible that improved cyber security practices have led to greater detection and reporting of incidents, suggesting that less cyber-mature organisations may still be underreporting breaches. Statistics by size of firm are set out below in Figure 7.

Figure 7: Proportion of firms reporting cyber security breaches from 2017 to 2024



Source: RSM recreation from Cyber Security Breaches Surveys (2017 to 2024)
N = 1000+ UK businesses each year; 640+ Micro; 260+ Small; 140+ Medium; 130+ Large

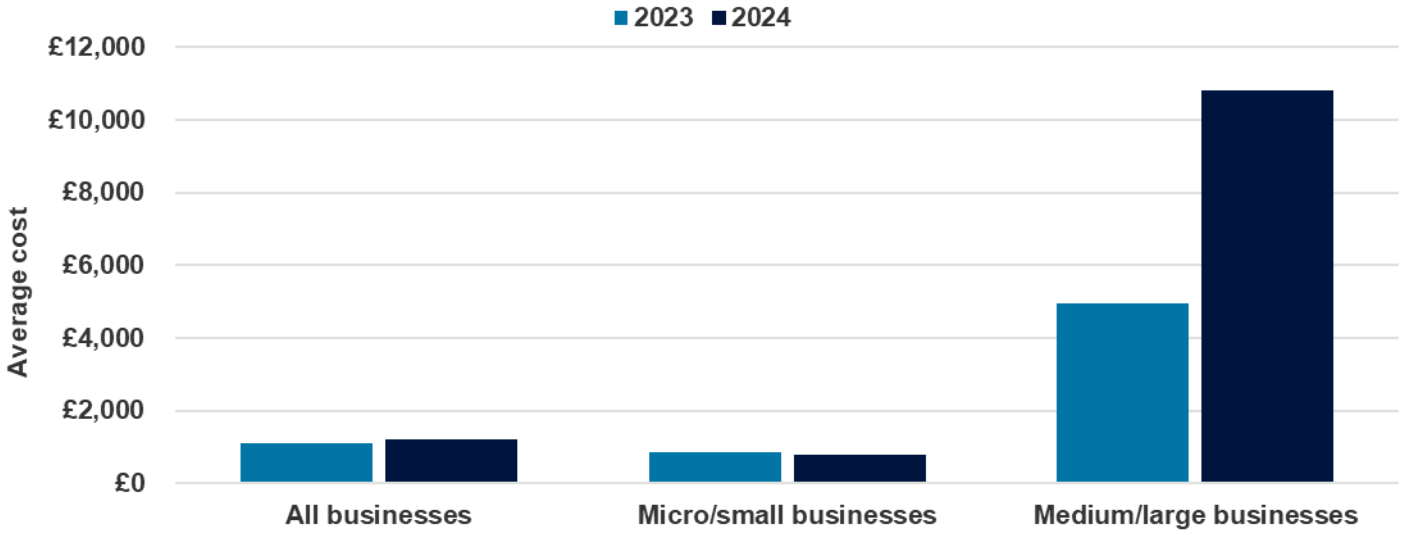
[28] The Urgent Need for Memory Safety in Software Products (CISA, 2023)
[29] Secure by Design (CISA, 2023)
[30] Secure by Design (CISA, 2023)

The average cost of all breaches reported in the 2022 survey was £1,200 (as noted in the interim report), which is broadly in line with Figure 8 for the 2023 and 2024 data. However, due to a change in the data collection methodology in 2022, the 2023 and 2024 statistics are not directly comparable with the earlier years presented in the interim report. Specifically, the 2023 and 2024 figures reflect the average total cost of the most disruptive breach or attack over time, whereas previous surveys reported the average cost of all breaches across all businesses.

Despite this change, the statistics presented in this report are a useful addition for understanding how this phenomenon is increasingly affecting medium and large businesses in particular. Notably, the average cost of major breaches for medium/large businesses more than doubled between 2023 and 2024 in the UK. This could indicate that:

- **Attacks are becoming more severe or sophisticated**, especially those targeting larger organisations.
- **Medium and large firms are becoming more reliant on digital infrastructure**, thereby increasing potential damages when breaches occur.
- **There is better detection and reporting among larger firms**, revealing the true scale and cost of high-impact attacks.
- **Cyber criminals may be strategically targeting larger firms,** expecting higher payoffs.

Figure 8: Average total cost of the most disruptive breach or attack – 2023 and 2024

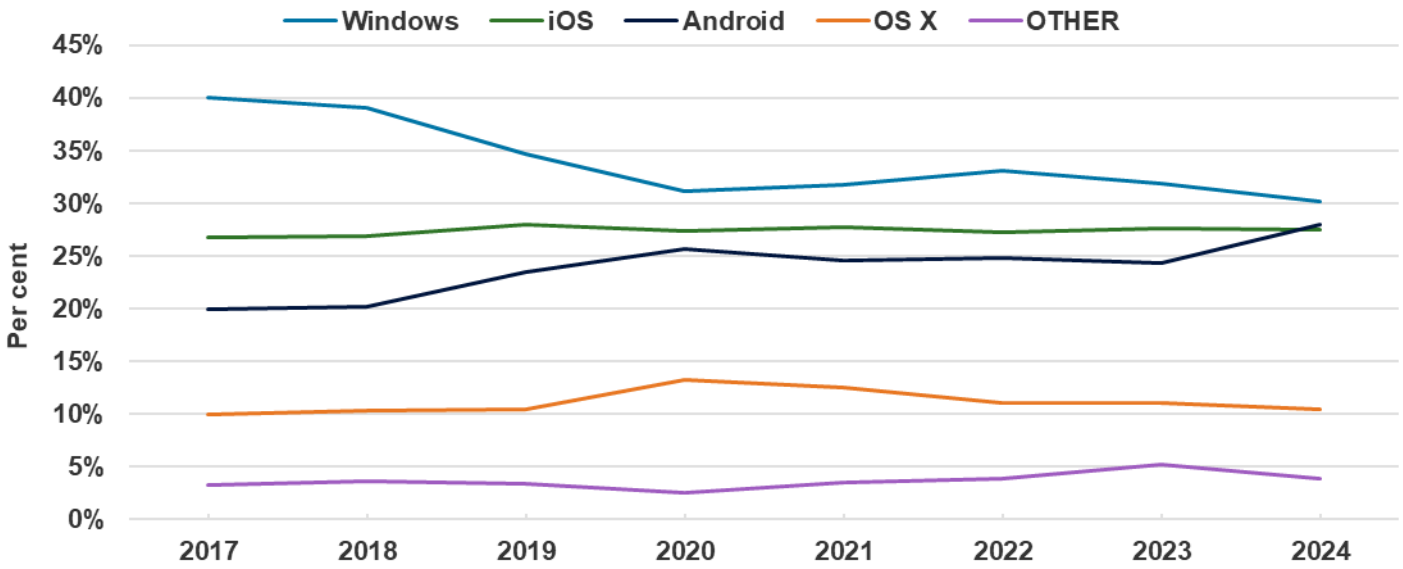


Source: RSM recreation from Cyber Security Breaches Surveys (2023 and 2024)

Finally, as introduced in the interim report, a key indicator of the programme's eventual success will be the market share of operating systems that support the new technology—through a combination of CHERI-embedded processor and an operating system that enables its use. Since the number of operating systems with significant market penetration is small, and Arm holds a dominant position as the designer of processors for mobile devices in particular, the actual number of companies that would need to adopt the technology to build market share is relatively low. Figure 9 below shows the evolving market share from 2017 to 2024.

The major operating systems in the market have remained relatively constant since 2017; however, there is a slight decline in Windows' market share and a convergence trend emerging within the Android operating system landscape in 2024.

Figure 9: Market share of operating systems: yearly average from 2017 to 2024



Source: RSM recreation of data from Statcounter[31]

6.6. Increasing awareness of new security capabilities

EQ13: To what extent and how has DSbD increased the awareness of new security capabilities?

This section outlines the perceived awareness of new security capabilities catalysed through the DSbD programme. This section is based on evidence collected against the following KPIs:

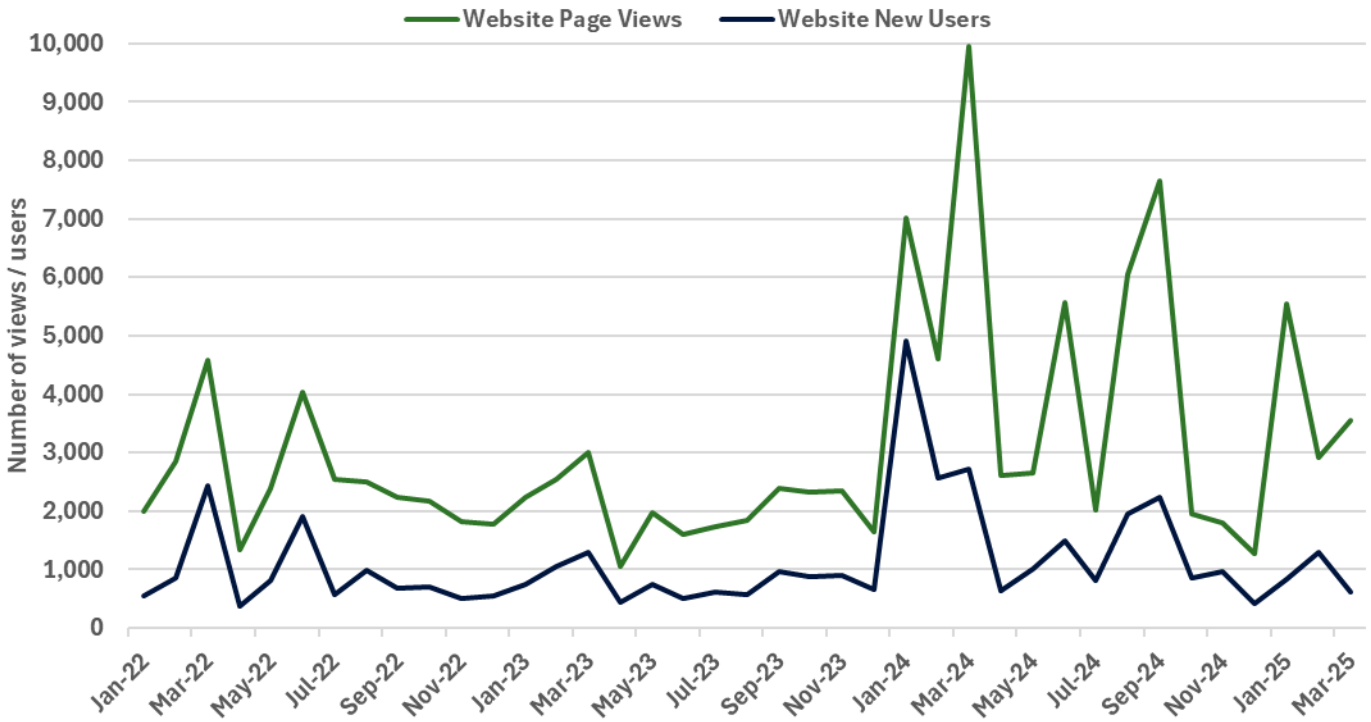
- Count of mentions of DSbD and its associated technologies.
- Increase in count of viewers and impressions on DSbD's social media handles.

Figure 10 illustrates the active users[32] and webpage views of the DSbD website from January 2022 to March 2025. There is a noticeable upward trend in both active users and webpage views, albeit with fluctuations, indicating slow but steady growth in user engagement with the DSbD website. This trend may be attributed to the increased resources available through the website over the course of the programme, including competition details, publications, and other technical resources. Notably, there are significant fluctuations with upward spikes in the first quarter of each year. This could be explained as the beginning of 2022 was busy in terms of publicity for the project – the first press releases announcing the Morello Board, the launch of the TAP and the four nations roadshows all occurred in the first three months of 2022. Moreover, the DSbD All Hands could also be a contributor to the sharp increase in active users as the event typically occurs around March and April.

The most significant surge in webpage views and active users occurred during the first quarter of 2024, with metrics peaking at almost 10,000 webpage views and 5,000 active users. This notable increase is likely attributable to a combination of key initiatives and events during that period. These included the open call for TAP Cohort 5, the DSbD All Hands event, public availability of Sonata boards, strong promotional efforts for the CHERI Remote Access Labs, and the dissemination of research updates from the Discribe Hub, particularly those addressing regulatory and policy implications as well as challenges related to industry adoption. A secondary spike in engagement was observed in August and September 2024. This uptick may be linked to SCI Semiconductor's public announcement regarding their development of a commercial CHERI-enabled chip, alongside the open call for TAP Cohort 6.

[31] Operating System Market Share United Kingdom (Statcounter, 2024)
[32] Active users refers to the number of unique visitors who have interacted with the DSbD website.

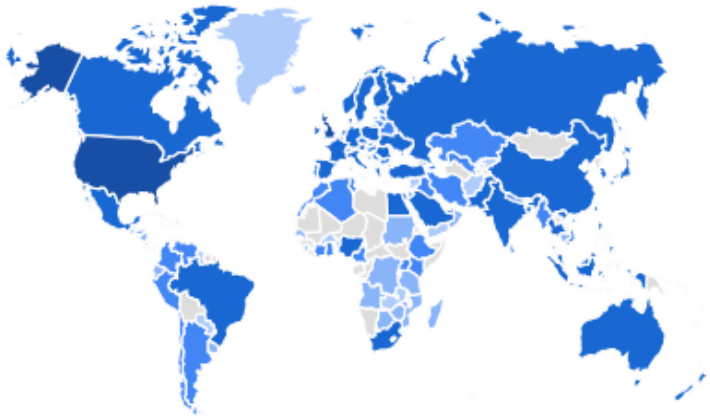
Figure 10: Active users and page views of DSbD Website (From January 2022 – March 2025)



Source: UKRI data

Figure 11 reveals that the DSbD website has received visitors from across the globe. However, the majority of the website users are concentrated in the UK, with 21,000 active users, followed by the US with 8,100 active users. This concentration is expected, given that a considerable number of awareness-raising activities have been focused within the UK and the US. India has the fourth largest active user base for DSbD website, which is unexpected as awareness-raising activities have not been specifically targeted there. This could likely be an indirect result of the CHERI Alliance, which includes members from India.

Figure 11: Active users of DSbD website (by region)



COUNTRY	ACTIVE USERS
United Kingdom	21K
United States	8.1K
Poland	1K
India	969
Netherlands	834
Finland	782
France	734

Source: UKRI Benefits Profiles

The February 2025 edition of the UKRI Challenge Fund Media Analysis Report[33] provides an overview of news coverage and social media engagement related to the DSbD programme. During this period, a total of 16 news articles and posts referencing DSbD were published, reaching an estimated audience of 31,000 individuals. Notably, Business Manchester featured a piece announcing that EdgeSynergies will unveil and present their DSbD-funded project at the upcoming DSbD Showcase event. The article also included explicit support for the DSbD programme from EdgeSynergies.

While the volume of social media activity was comparatively lower, with 10 posts recorded, these achieved a significantly broader reach, collectively engaging 95,000 users. The DSbD Showcase emerged as the dominant theme across social platforms. For instance, lowRISC highlighted the CHERIoT-Ibex core—described as “the processor at the heart of the UKRI-funded Sonata platform”—in a post on X (formerly Twitter).

According to the February 2025 Media Analysis Report, the DSbD programme led in both volume and reach within the Digital & Technologies category of the UKRI Challenge Fund. This strong performance is likely attributable to a higher volume of communications during the month, which may vary over time depending on the timing and intensity of awareness-raising and marketing activities across programmes within the same challenge area. However, when viewed in the broader context of the UKRI Challenge Fund, DSbD-related content demonstrated comparatively lower volume and reach than initiatives in other challenge areas, such as Net Zero.

This trend may reflect a natural tapering of outreach momentum following the marketing and engagement efforts during the interim phase of the DSbD programme (2022–2023), particularly as the programme approaches its conclusion. This presents an opportunity to consider how best the visibility and engagement of the DSbD programme—and the innovative technologies it has supported—can be effectively sustained beyond the formal conclusion of DSbD.

6.7. Conclusions against evaluation questions

Understanding of needs of cyber security and raising awareness of cyber and digital security issues

The DSbD programme has **actively contributed to understanding and raising awareness of cyber security needs** within the following groups:

- **Government awareness:** The programme has engaged multiple government departments, securing high levels of awareness and support. This engagement has facilitated DSbD technologies being referenced into national strategies and policies, **contributing to the importance of cyber security at a national level**. According to the stakeholder interviews, the impact at the level of government strategy is seen to be significant. Sustaining the current level of support from government can positively drive future regulatory changes and standardisation efforts, ensuring that technological advancements are matched by appropriate regulations.
- **Industrial awareness:** DSbD was also successful in raising awareness among technical and cyber security experts, though **there is still work to be done to engage senior decision-makers in large companies** and **demonstrate a strong business case with clear pathway to economic benefits**. Increasing awareness and understanding among non-technical senior stakeholders can facilitate more informed decision-making and support the adoption of DSbD technology.

The **DSbD programme's impact on public awareness is minimal.** While public awareness is important, the primary focus of DSbD has been to ensure that foundational security measures are integrated into products and services. This approach **creates a more secure digital environment without relying on public understanding of technicalities behind cyber security measures**.

[33] Data and report provided by UKRI.

Catalysing transformational change on cyber security

The DSbD programme has made **good progress in driving transformational change within the UK's cyber security landscape.** This has been achieved through securing additional government funding and support, as well as influencing the commercialisation efforts of CHERI technology by both UK-based and multinational firms.

The programme has notably advanced the memory safety domain, both nationally and internationally, particularly in the United States. CHERI technology has been referenced in official reports from the White House and CISA.

While there is evidence that some companies are actively working towards commercialising DSbD technology, it is imperative that more firms join these efforts to integrate CHERI into their products and services. This broader participation is essential to 'shift the dial' within the cyber security sector. Furthermore, additional intervention and follow-on funding are needed to further embed DSbD technology and CHERI into future products and services, thereby supporting widespread adoption.

Impact on cyber attacks

The DSbD programme's impact on reducing cyber attacks is yet to be realised, as there are currently no live DSbD-based products. However, the programme's rationale is grounded in addressing the ongoing threat of cyber security breaches.

It is expected that the successful implementation and adoption of DSbD technology can lead to a significant reduction in cyber attacks, particularly benefitting medium and large businesses that face larger financial consequences from these attacks.

Awareness of new security capabilities

Evidence of interest in new security capabilities, measured through social media engagement of DSbD handles, suggests a slowly growing awareness of the DSbD technology. DSbD has attracted a global audience, with significant engagement from users in the UK and the US.

An assessment of media coverage and social media engagement referencing DSbD indicates that, while traditional media reached approximately 31,000 individuals across 16 published articles in February 2025, social media—despite a lower volume of posts—achieved significantly higher engagement, reaching around 95,000 users. Notably, the DSbD Showcase emerged as a focal point of online discourse.

Although DSbD led in terms of volume and reach within the Digital & Technologies category in February 2025, its overall visibility remained comparatively lower than that of other challenge areas, such as Net Zero. As the programme approaches its conclusion, there exists a **clear opportunity to extend its visibility and sustain the impact of its supported technologies beyond the formal end of its funding cycle**.

7. Impacts on Businesses

7.1. Introduction

This chapter focuses on the observable impacts to businesses and the economy, addressing the following set of evaluation questions:

- To what extent and how has DSbD enabled the creation of new more secure products and services?
- To what extent has DSbD created the sustainable change in organisational cultures and structures in hardware/software development companies, and key industries which can ensure DSbD activities are sustainable beyond 2024? How far has this had an impact on the digital and cyber security industry?
- To what extent and how has DSbD increased the share of export market for those participating in the challenge?
- To what extent and how has DSbD contributed to productivity in the UK?
- Has DSbD improved the UK reputation in cyber security? Has this led to wider benefits such as new commercial ventures? How sustainable are they?
- What are the socioeconomic drivers leading to increased demand for digitally secured products and services? And what are the key barriers impeding the adoption of new DSbD technology?

DSbD impacts on businesses and the economy are identified in the programme's Logic Model as longer-term impacts, expected to materialise after the end of the programme, such as:

- Hardware-software supply chain adoption of new, more secured products/services.
- Increased exports, productivity, and employment.
- UK reputation in leading computer security architecture and regulatory and standards.

These longer-term impacts require the DSbD programme to have been successful in building the technology, tools, ecosystem, and market awareness as described in the previous chapters.

7.2. Key findings

Creation of new products and services

- Three physical products have been developed through the DSbD programme: the Morello Board (Arm), and the Symphony and Sonata boards (lowRISC/RISC-V). While these products are prototypes for research and testing, they lay the groundwork for future commercial offerings.
- **80% of DSbD survey respondents positively evaluated the Morello board for potential use in their future products and services.** Despite this, the programme has not yet achieved its target of 200 companies positively evaluating the board.
- DSbD-funded projects have also shown significant progress in developing software and tools over the programme period. However, commercialisation of these developed tools remains a challenge, as a commercial product is not yet available.
- Independent use of CHERI by companies demonstrates its potential beyond the DSbD programme. Microsoft and lowRISC's work on CHERI for RISC-V microcontrollers is a key driver here, with three companies – Codasip, SCI Semiconductor, and Secqai – expected to offer products with CHERI architecture at the microcontroller scale in the near future.

Impacts on organisational culture

- Representatives from four academic proof projects, one demonstrator, and one software ecosystem development project reported notable cultural changes due to the DSbD programme.
- These representatives indicated their intentions to continue advancing their DSbD work. They noted that DSbD has influenced their research directions, established essential infrastructure, promoted the expansion of testing activities, and fostered a personal interest in CHERI.
- Few companies, such as Verifoxx and Secqai, have strategically changed their business models in response to the DSbD programme and the associated technologies developed.
- Three new businesses have explicitly been created as a response to the DSbD technology, further signifying the organisational impacts of the DSbD programme. These include Capabilities Ltd, SCI Semiconductor, and the CHERI Alliance.

Impacts on share of export market for businesses participating in the DSbD programme

- Impacts on export market share of businesses cannot be estimated currently as the DSbD technology has not yet been adopted by businesses and there is no fully commercialised product with CHERI embedded.
- Cyber Hive, funded by DSbD, has been pursuing international commercial traction through the CHERI USP in their existing product line, which has garnered demonstrable interest and excitement from companies.

Perceived contribution to UK productivity

- Currently, no commercial products or services based on DSbD technology have been adopted, and thus, there are no directly observable or reportable impacts on productivity.
- A survey conducted by Innovate UK in 2022 and 2023 revealed that all business respondents (6 out of 14) acknowledged the potential productivity advantages of adopting DSbD technology.
- In 2024, 50% of UK businesses responding to the Cyber Breaches Survey reported experiencing cyber attacks, an increase from 39% reported at the interim stage (in 2022). The core productivity benefit of DSbD technology lies in reducing the number of working days lost to cyber attacks. DSbD technology has the potential to enhance organisational productivity by minimising downtime, as evidenced by its capability to mitigate 100% of historically reported memory safety vulnerabilities.
- The DSbD programme has demonstrated that adopting CHERI requires simple recompilation of code with minimal modifications. The benefits of CHERI can often be realised in existing development languages. Additionally, the programme has shown that CHERI provides formal software verification tools with enhanced semantics, potentially reducing the time required for security reviews and compliance checks if DSbD technology is adopted.

UK reputation in cyber security

- The DSbD programme aimed to create 100 jobs by 2024 but has already resulted in 405 new jobs, surpassing the target by fourfold. This figure likely underestimates the total number of jobs created, as it does not account for companies independently implementing the CHERI architecture currently.
- The GVA per employee in the cyber security sector in 2025 ranges from £73,118 for micro businesses to £123,896 for large businesses. The direct expected contribution in GVA by the 405 new jobs created through the DSbD programme is approximately £29.6 million.

- The DSbD delivery team has explored international markets through government-led missions to key countries like the US, India, Japan, and Australia. The relationship with the US and Australia is significant due to the Five Eyes global security partnership, with Morello boards distributed to these two countries.
- Programme stakeholders regard the UK highly for its cyber strategies, publicly funded programmes, regulatory approaches, and research and development.
- Fifteen stakeholders reported significant progression of the DSbD ecosystem. Eleven stakeholders expressed optimism about the ecosystem's sustainability, although some anticipated a reduction in its size post-programme.
- Stakeholders highlighted the need for government funding, continued industrial interest and advocacy, and addressing market-related mechanisms to ensure sustainability. Few stakeholders expressed scepticism regarding the ecosystem's sustainability, noting the need for active engagement and commercialisation efforts from larger industry players.

Enablers and barriers to adoption of DSbD technology

- Enablers to adoption of DSbD technology include: Increasing demand for higher security in key sectors such as telecommunications, critical infrastructure, and defence; involvement of major technology companies; UK's competitive advantage through a high concentration of skilled professionals with technical knowledge of CHERI and memory safety; successful demonstration of use cases and economic benefits from the DSbD programme; and opportunities for integration of DSbD technology alongside other emerging technologies such as AI.
- Barriers to adoption of DSbD technology include: Economic barriers such as substantial investments and consumers' willingness to pay extra for enhanced security; comparatively lower TRL of DSbD technology for some niche use cases; and limited awareness among non-technical senior decision-makers.

7.3. Creation of new secure products

EQ14: To what extent and how has DSbD enabled the creation of new more secure products and services?

This section outlines the ways in which DSbD has enabled creation of new, more secure products and services. To date, three physical "products" have been developed through the DSbD programme, in collaboration with private businesses such as Arm, Linaro, and lowRISC:

- **Morello Board:** The Technology Prototype Platform of the DSbD programme, implementing CHERI architecture to explore new security features.
- **Symphony Board:** A feature-rich evaluation platform allowing for full analysis of CHERI enhancements in a wider system.
- **Sonata Board:** Developed as part of the Sunburst project, Sonata board is a low-cost development board, based on the CHERIoT-Ibex hardware design, for investigating CHERI security enhancements in embedded systems.

These products are essential element of the critical path to development of products in the marketplace as it permits the demonstrators and industrial projects to create working physical prototypes and for SMEs to experiment with the technology through the Technology Access Programme (TAP).

7.3.1 Insights from Technology Access Programme

The TAP projects aim at accelerating the adoption of DSbD technologies by UK businesses, providing them with the opportunity to integrate DSbD technology into their operations. The programme has seen six cohorts, involving a total of 51 businesses across the UK. The first five cohorts, comprising 42 participants, were provided with the Morello Board and asked to use it alongside the CHERI software environment to develop and demonstrate use cases as part of the DSbD programme. The latest cohort, Cohort 6, were supplied with the CHERIoT-based Sonata board.

Feedback from the cohorts who used the Morello (Cohort 1 – 5) was generally positive, with several suggestions for improvement, including:

- Sending the Morello board to participants already set up: The participants were required to set up the Morello board with help from Digital Catapult and the associated documentation they were given. This included a user guide to the board and its key capabilities, as well as directions to reference libraries available.
- Offering more hands-on and/or in-person workshops to cover OS installations, booting CheriBSD, porting, and other technical processes.
- Creating instructional videos to demonstrate the step-by-step compilation process.
- Establishing a central programme hub for all materials, presentations, and recordings.
- Facilitating connections between current and past cohort members to share experiences and knowledge for smoother onboarding.

Feedback from the Cohort 6, who used the Sonata board was positive to a large extent, acknowledging the level of improvements made on the developer experience throughout the programme, particularly for creating and managing compartments. However, there were some minor initial difficulties with finding and navigating the various documentation and repos, but this has been greatly improved since then.

Participants were categorised into Tier 1 (SMEs) and Tier 2 companies, with Tier 1 members receiving project funding, while Tier 2 members did not. The following table provides a detailed breakdown of all TAP cohorts:

Cohort	Number of Tier 1 companies	Number of Tier 2 companies
Cohort 1	9	1
Cohort 2	10	4
Cohort 3	4	0
Cohort 4	8	0
Cohort 5	8	0
Cohort 6	7	0
Total	**46**	**5**

Source: DSbD programme documentation

The TAP summary reports for the first five cohorts provide valuable insights into the perspectives of their participants regarding various aspects of DSbD outputs, specifically Morello and CHERI.

Documentation: Members of Cohorts 1 and 2 found the setup documentation for Morello and CHERI challenging to locate and utilise. In contrast, participants in Cohort 3 generally found Morello and CheriBSD easier to use than anticipated, while Cohort 4 participants reported an effortless and swift onboarding process. However, some members of Cohort 5 reported that the set up documentation of Morello and CHERI was slightly unclear, with one company suggesting a ‘master document’ with all information centralised.

Members of the first three cohorts were asked to rank the ease of use on a scale from 1 to 10, with 10 being very easy to use and 1 being very difficult.[34] **The data indicates that Cohorts 2 and 3, with higher average scores, found the documentation relatively easier to use compared to Cohort 1. Cohort 4's feedback of effortless onboarding suggests that usability concerns have been significantly**

[34] The recommendations from Cohort 3 emphasised the improvement of feedback collection methodologies from cohort members. Additionally, it was proposed that 1-10 scales in reporting should be removed, which Digital Catapult has acknowledged as 'to be actioned'. Consequently, this likely explains the absence of the ranking system in the Cohort 4 report.

addressed. However, it can be refined further as the feedback from Cohort 5 shows some challenges with set up documentation.

Table 13: TAP - Ease of finding/using documentation

Cohort	Cohort 1 (average score; N = 10)	Cohort 2 (average score; N = 14)	Cohort 3 (average score; N = 4)
Ease of using Morello documents	5.9 / 10	7.5 / 10	8 / 10
Ease of using CHERI documents	6.1 / 10	7.6 / 10	7.5 / 10
Ease of using Linux/Android documents	4.6 / 10	5.6 / 10	5.5 / 10

Source: Summary of interim TAP reports

Usability of CHERI on Morello: The usability of the Morello Board was evaluated by members of Cohorts 1 and 2, with scores ranging between 5 and 9. Most members of Cohort 1 indicated that the **technology met their expectations, although they acknowledged that significant progress is needed for commercialisation**. In Cohort 2, six out of fourteen members noted that **certain aspects of the technology were less developed than anticipated.** However, the existing CHERI features were praised for their functionality and the protection they offered.

A notable improvement was observed in Cohort 3, with an average usability score of 8.2. This suggests that the **TRL of the Morello Board aligned well with their expectations**. This improvement is likely attributed to Digital Catapult's implementation of a more rigorous judging process and enhanced support during onboarding. Cohort 3 members particularly appreciated the flexible representation of memory access permissions and the ease of development.

Most members of Cohort 4 and Cohort 5 found **CHERI/Morello to be user-friendly, describing it as a strong research platform with mature tools and documentation.**

Table 14: TAP ease of using CHERI on Morello

Cohort	Average score	Min	Max
Cohort 1 (N = 10)	6.9	3	9
Cohort 2 (N = 14)	7.3	5	10
Cohort 3 (N = 4)	8.2	No data	No data

Source: Summary of interim TAP reports

The initial five cohorts have enhanced the exposure of UK businesses to CHERI and the Morello Board, enabling them to explore use cases relevant to their operations. These five TAP cohorts have developed a variety of tangible open-source software products, fuzzing and debugging tools, and partial or complete ports of various components. These contributions have potentially enriched the broader DSbD ecosystem.

Findings from Cohort 6 shows that, unlike previous cohorts that worked with Morello, Cohorts 6 have gained valuable exposure to CHERIoT, significantly enhancing their expertise in this area. All members of Cohort 6 have all indicated ideas for how they will continue to work with Sonata/CHERIoT beyond the programme, both in conducting further testing of their projects, but also in new business opportunities.

However, the **outputs from TAP are not yet at a stage suitable for commercialisation, as these cohorts are short-term projects often constrained by limited resources, which affects the stability and support capabilities of the products/tools developed**. Additionally, the Morello Board provided to TAP cohorts 1-5 is a prototype rather than a finished product. However, findings from Cohort 6 have indicated interest in CHERIoT and Sonata Board as they are looking to continue working with the technology.

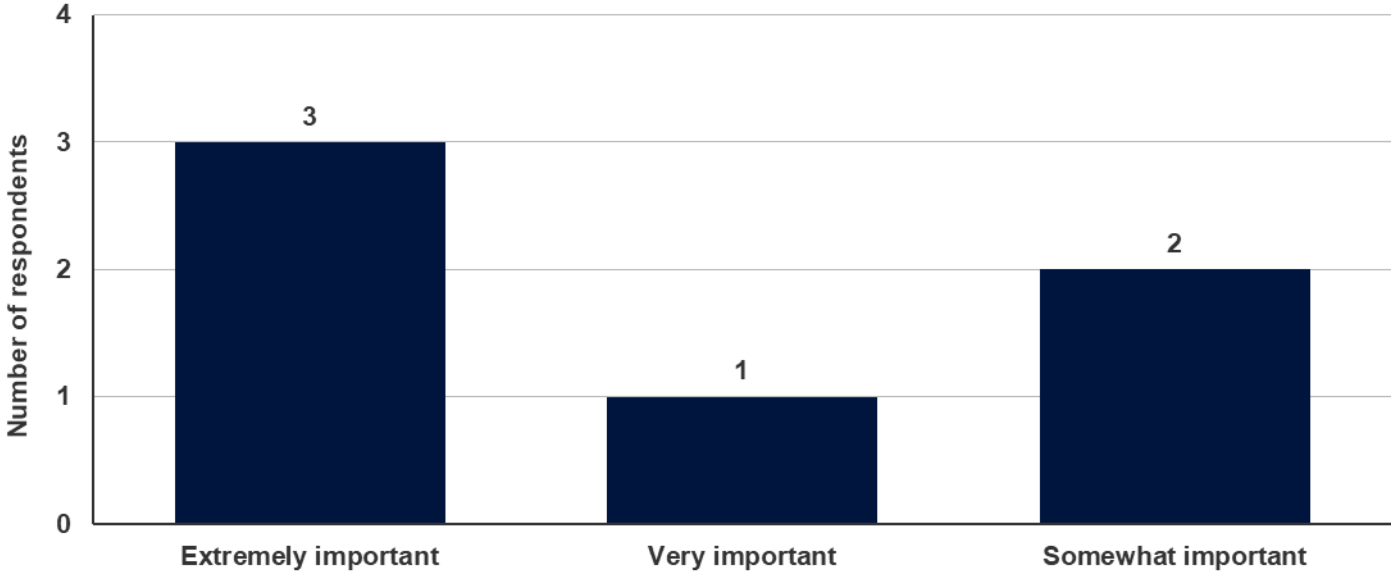
Overall, the Technology Access Programme serves as a pathway to introduce companies to DSbD technology and stimulate interest in developing products and services based on it. Notably, the third and fourth cohorts reported a more favourable impression of the documentation and ease of use of the Morello Board package, indicating improvements over time.

7.3.2 Insights from DSbD funded projects

Insights from DSbD funded projects indicate that successful testing and internal use, particularly within the academic community, have been achieved for 31 software, including two web tool applications. Despite these achievements, the software has not yet been commercialised. Moreover, these projects are predominantly led by academic institutions, as tracked by Researchfish, and the extent of private business involvement in the development of these software remains unclear.

Additionally, the DSbD Survey conducted by Innovate UK in 2022 and 2023 asked stakeholders to rank the importance of DSbD technology for future products and services, especially in terms of enhancing security. Out of the fourteen respondents, six were businesses, including two from demonstrators, two from de minimis projects, and two from software ecosystem development projects. Figure 12 provides a breakdown of their responses. All six business respondents acknowledged the importance of DSbD technology for future products and services, with three rating it as 'Extremely important,' two as 'Very important,' and one as 'Somewhat important.'

Figure 12: Business perception of the importance of DSbD technology to future products and services



Source: UKRI DSbD Survey, Dec 2022-Jan 2023

The DSbD programme initially set a target of having 200 companies positively evaluate the boards by 2025. This target serves as a useful indicator for assessing the anticipated level of adoption of DSbD technology within products and services in the near future. DSbD survey responses from 2022 and 2023 indicate that **80% of respondents positively evaluated the Morello board for potential use in their future products and services.** This positive feedback suggests that businesses involved in the DSbD programme are likely to adopt and implement DSbD technology in their future offerings, provided that the commercialised chip or hardware becomes available.

However, it appears that **the programme has not achieved its target of 200 companies positively evaluating the board, as the total number of businesses involved in the programme is lower than the set target.** While there are companies not included in the survey who have indirectly interacted with the Morello board and may have a positive evaluation of the DSbD technology, it remains unlikely that the DSbD programme has met its target of 200 companies positively evaluating the board.

7.3.3 DSbD technology usage outside of DSbD funded activities

The Morello Board prototype and the Arm microprocessor are engineered with the requisite power and complexity to operate phones, computers, and servers. Arm's Morello processors are targeted at high-value, high-power electronics.

However, in September 2022, Microsoft announced the development of **CHERIoT, an adaptation of the CHERI architecture into a microcontroller.** Microcontrollers have considerably less processing power and memory than the processors used in laptops and phones, which have to have extensive general purpose capabilities to run apps and connect with peripheral devices.

Microsoft's work on CHERIoT is significant for several reasons:

- It demonstrates a major IT player's commitment to exploring CHERI technology without DSbD funding, thereby co-investing in the R&D for CHERI.
- It opens a pathway to market that does not rely on the Arm Morello technology platform, thereby widening the potential impact of DSbD on product and service creation.
- It mitigates the risk that the Arm technology route might not succeed or be adopted by Arm within their roadmap post-programme completion.
- The use of microcontrollers broadens the application of CHERI, making it available in systems that do not require a powerful general-purpose CPU but do need high levels of security, such as embedded control systems, remote sensors for vehicles, advanced manufacturing or construction facilities, and medical devices.
- It could also enhance security in mass-market IoT devices that tend to use relatively inexpensive microcontrollers.

Microsoft's CHERIoT work has also directly influenced the DSbD programme through the establishment of the Sunburst project. Led by lowRISC, the Sunburst project developed two boards based on the CHERIoT-Ibex hardware design – Symphony Board and Sonata Board. The development of **Sonata and Symphony boards allows for exploring use cases previously unfeasible with the server-grade Morello board.** The lower cost of the Sonata board facilitates wider distribution, which was previously not feasible with the Morello Board due to remarkably high costs. Additionally, the Sonata board is available for general public purchase at around £340 per unit.

SCI Semiconductor is actively working on a commercial implementation of the CHERIoT RISC-V microprocessor core, expected to reach the market by the end of this year. This indicates that DSbD technology is being incorporated into upcoming products and services of UK businesses.

Codasip, having developed the first commercial implementation of the CHERI architecture in their X730 processor in 2023 without DSbD funding, has since integrated CHERI into another processor. This demonstrates that companies outside of DSbD are positively evaluating and implementing CHERI technology in their product lines.

Secqai, a quantum hardware company, has shown interest in the DSbD programme and CHERI architecture, reportedly creating a new strategic business model based on CHERI. Secqai is expected to introduce CHERI in their products and services in the near future.

7.4. DSbD impacts on organisational culture

EQ15: To what extent has DSbD created the sustainable change in organisational cultures and structures in hardware/software development companies, and key industries which can ensure DSbD activities are sustainable beyond 2024? How far has this had an impact on the digital and cyber security industry?

This section outlines the changes fostered by the DSbD programme within organisational cultures and structures of companies and academic institutions. The resultant impact pathway from these cultural shifts is

expected to ensure the sustainability of markets and ecosystems based on DSbD technology post-programme closure.

Representatives from four academic proof projects, one demonstrator, and one software ecosystem development project have reported notable changes in organisational cultures attributed to the DSbD programme.

Academic representatives from two academic proof projects, one demonstrator, and one software ecosystem development project have acknowledged that their engagement with the DSbD programme has significantly influenced their research direction.

- One representative from the demonstrator project has developed a personal interest in the adoption of CHERI and its economic implications.
- Another representative from a software ecosystem development project has shifted their research focus from performance and power consumption to security, allowing them to secure additional funding.
- One academic proof project representative noted their plans to continue developing their work despite the end of DSbD funding, elaborating that they have preliminary plans to pursue commercial directions that build on their DSbD worth.

Two interviewees, one from a demonstrator project and the other from an academic proof project, have indicated that the DSbD programme has facilitated the establishment of essential infrastructure.

- The industry representative from the demonstrator project reported being in a position to expand testing activities and expressed interest in supporting early adopters of CHERI.
- The academic proof representative mentioned their involvement with the CHERI Alliance.

A representative from CAPcelerate, an academic proof project, reported that their subsequent DSbD project, Chromepartments, which is part of the software ecosystem development workstream, came about from their involvement with CAPcelerate.

More broadly, the academic representatives emphasised the need for additional funding to sustain their current level of involvement and retain key personnel. A few academic representatives noted that their future work on CHERI is contingent upon commercial interest from the industry.

On the industry front, the organisational impacts of the DSbD programme are evident through two pathways: the transformation of existing business strategies and models of companies due to DSbD technology, and the establishment of entirely new companies to exploit this technology. As the DSbD technology has not yet achieved widespread adoption, it is still early to observe large-scale organisational impacts across the cyber and digital security sector. However, there is evidence to suggest that organisational change is happening as a result of the DSbD programme.

Several companies have strategically changed their business models in response to the DSbD programme. For instance, Verifoxx, an SME specialising in identity management, received funding through the De Minimis competition. Following this project, Verifoxx reportedly shifted its business model to focus on DSbD technology.[35] The company was subsequently awarded additional funding in the software ecosystem development workstream.

Although not directly part of the DSbD programme, Secqai has transitioned its business model from quantum encryption to CHERI-based System-on-Chips (SoCs). This shift is directly attributable to the awareness of CHERI and DSbD technology raised through the DSbD programme. This serves as a positive indication of DSbD's impact on the business strategies and organisational culture of companies within the cyber and digital security sector, even those not formally involved in the DSbD programme. Similarly, Codasip, despite not receiving DSbD funding, has commercially implemented CHERI into their 700

[35] It should be noted that this information was obtained through secondary sources. We have not been able to confirm this with Verifoxx.

processor series and founded the CHERI Alliance, highlighting their strategic decision to invest in CHERI and its significance within their strategic roadmap.

Furthermore, independent development work by Microsoft on a microcontroller implementation of CHERI, via the CHERIoT platform, provides an encouraging sign that a major player in the IT sector is exploring ways in which DSbD could be integrated into its company strategy.

For the second pathway of organisational impact, three new businesses have been explicitly created through the DSbD programme. SCI Semiconductor was established to directly exploit DSbD technology by commercialising the CHERIoT RISC-V microprocessor core, indicating that the company's culture and structure are fundamentally based on DSbD technology. Additionally, Capabilities Ltd, which has received funding for two DSbD projects, is a spin-out from Cambridge University involving the Computer Laboratory CHERI team.

Although not a product-led company, CHERI Alliance CIC's organisational culture is entirely based on CHERI and DSbD technology. As of the writing of this report, the Alliance comprises 23 member organisations, and its board of directors includes representatives from the University of Cambridge, Codasip, LowRISC, and Emerging Tech Radar. This composition further indicates a potential shift in organisational cultures within the member organisations, as their active engagement with the Alliance suggests an increased importance of DSbD technology and cyber security in general to these member organisations.

7.5. Share of export market for businesses participating in DSbD

EQ16: To what extent and how has DSbD increased the share of export market for those participating in the challenge?

This section outlines the observed share of the export market for businesses involved in the DSbD programme. The share of the export market serves as a useful indicator of the global reach of the technology. The competitive advantage for businesses participating in the DSbD programme is reflected in the export revenue generated from the sale of commercialised DSbD products and services.

In line with findings in the interim impact evaluation report, the technology has not yet been adopted by businesses currently, and there is no fully commercialised product with CHERI embedded that could have a measurable impact on the share of the export market. Respondents to the 2022 and 2023 DSbD surveys conducted by Innovate UK were unable to quantify perceived increases in exports.

However, it was reported that **Cyber Hive, funded by DSbD, has been pursuing international commercial traction through the CHERI USP in their existing product line**, which has garnered demonstrable interest and excitement from companies. Additionally, **Codasip's implementation of CHERI was stimulated by a customer**, indicating potential increases in export revenue through the commercialisation of DSbD technology.

We also investigated available secondary data from business finance databases such as FAME and Beauhurst to determine if it would be possible to analyse the financial data to measure these impacts on the ecosystem and the businesses involved. These databases include detailed financial information for companies that submit full accounts, including revenue derived from exports. However, there was limited to no information on DSbD participants, primarily because SMEs are not mandated to submit full accounts. In contrast, large multinational corporations like Google and Microsoft have extensive financial data available. Nonetheless, attributing any increase in export market share to DSbD remains challenging due to the vast product and service lines they offer and the global nature of these companies.

7.6. Perceived contribution to UK productivity

EQ17: To what extent and how has DSbD contributed to productivity in the UK?

This section outlines the perceived contribution of DSbD to UK productivity, addressing several types of productivity within the programme:

- **Organisational productivity:**
  - Less scheduled and reactive patching.
  - Less downtime from cyber attacks.
- **Engineering productivity:**
  - Reductions in time for security reviews & compliance checks.
  - More efficient ways of writing code.

Currently, no commercial products or services based on DSbD technology have been developed, and thus, there are no significant impacts on organisational productivity that can be observed or reported. However, we have investigated the rationale for expecting an economy-wide productivity boost from DSbD due to increased security. This encompasses existing evidence on the scale of the problem and insights from surveys and interviews with project delivery partners regarding perceived productivity improvements in their environments.

7.6.1 Organisational productivity

The core productivity benefit of DSbD, as stated in the business case, is to reduce the number of working days lost to cyber attacks, i.e., less downtime from cyber attacks. This would have a significant impact, as the proportion of UK businesses identifying cyber attacks was at 50% in 2024, a sizeable increase from the 39% reported in 2022 (at interim evaluation stage).[36]

According to the 2024 Cyber Security Breaches Survey[37], 32% of businesses reported experiencing cyber breaches at least once a week, and 53% reported breaches once a month. Among those that identified any breaches or attacks, 32% of large businesses experienced some negative outcome (vs. 13% of businesses overall). Among these large businesses, 9% reported compromised accounts or systems used for illicit purposes, and 5% reported loss or theft of assets, trade secrets, or intellectual property. Most businesses were able to recover from their most serious attack within 24 hours. For organisations reporting a material outcome, such as loss of money or data, the average estimated cost of all cyber attacks in the last 12 months was £3,270. For medium and large businesses, this figure rises to £17,970.

The DiScribe WP1 studied the determinants of firms' secure hardware adoption decisions. Findings show that adopting secure hardware reduces the probability of successful cyber attacks, thereby reducing liability costs for firms and minimising working days lost due to cyber attacks.[38]

To measure progress against the DSbD target to increase the productivity of future products and services by 5%, UKRI conducted a survey between December 2022 and January 2023. Respondents were asked whether they perceived a productivity advantage in adopting DSbD technology (such as Morello and CHERI). Six of the 14 respondents were businesses, and all affirmed the productivity advantage. However, apart from two estimates of 50% and 10%, most respondents stated that measuring productivity gain at this stage was challenging, with one business noting it was a research problem DSbD was trying to solve.

UKRI published DSbD programme outcomes report[39], providing evidential claims for the CHERI technology. It is estimated that businesses currently spend $1.4 million on preventing, detecting, and remediating vulnerabilities. Claim #1 states that CHERI enables high-performance compartmentalisation of code, mitigating 100% of historically reported memory safety vulnerabilities. By mitigating vulnerabilities, CHERI would reduce spending on reactive security measures such as patch development, with expected benefits of 7% in developer productivity. This aligns with DSbD survey findings, where respondents highlighted

[36] Cyber security breaches survey 2024 (DSIT and Home Office, 2024)
[37] Cyber security breaches survey 2024 (DSIT and Home Office, 2024)
[38] Drivers and barriers for secure hardware adoption across ecosystem stakeholders (Andrew Tomlinson, Simon Park, and Siraj Shaikh, 2022)
[39] DSbD programme outcomes report (UKRI, 2025)

improved security and robustness of applications running on CHERI-enabled hardware, supporting arguments for increased organisational productivity and reduced time required to identify and rectify bugs.

An interesting example of the potential impact of secure hardware design on organisational productivity can be drawn from the global technology outage of 2024. This incident was triggered by a faulty software update issued by a Fortune 500 cyber security firm. The update inadvertently introduced a vulnerability that led to widespread system failures across multiple sectors, resulting in an estimated $5.4 billion in financial losses due to operational downtime and disrupted trading activities.[40]

It is claimed that the implementation of CHERI could have significantly mitigated, if not entirely prevented, the downtime from this vulnerability.[41] CHERI's fine-grained memory protection and compartmentalisation capabilities are designed to contain faults and limit the propagation of security breaches.

Another economic benefit consistently identified in DiScribe Hub's work is the link between digital security and opportunities for digital transformation among firms. A follow-up study[42] using Eurobarometer survey data of 3,180 manufacturing sector SMEs noted that SMEs are adopting digital technologies to increase productivity or meet supply chain requirements. IT security issues positively affect this digitalisation, and digital transformation poses new security challenges that firms must address to fully exploit the opportunities offered through digital transformation.

7.6.2 Engineering productivity

The DSbD impacts on engineering productivity can be evidenced through the outputs and key achievements of the DSbD projects. The following CHERI claims[43] in the DSbD programme outcomes report[44] provide an early indication of improved engineering productivity through DSbD technologies:

- **Claim #4**: Adopting CHERI can be as simple as recompilation with minimal modification.
  - As part of DSbD funded projects, significant efforts towards porting application software stacks across various devices have demonstrated that less than 0.1% software change is required while delivering memory safety capabilities. This minimal change suggests that CHERI can be incorporated into existing projects without significant disruption or cost.
- **Claim #7**: The benefits of CHERI can be realised in existing development languages, enabling memory safety for legacy and unsafe code.
  - The DSbD programme has shown that CHERI benefits a variety of both legacy and memory-safe development languages, including C/C++, Java, Rust, and Python. This broad level of support allows developers to utilise CHERI without learning a new language or extensively rewriting existing code, thereby enhancing efficiency in code writing.
  - A representative from one demonstrator project reported that CHERI reduces the need for continuous cyber security efforts, providing more stability and reducing the need for constant updates and changes.
- **Claim #9**: CHERI-based architectures provide formal software verification tools with additional semantics to accelerate and improve the accuracy of software verification.
  - Currently, software verification tools operate without a well-defined understanding of memory manipulation by software, requiring significant time and complexity to deduce memory operations. However, the implementation of CHERI provides extra information about memory manipulation to software verification tools, leading to faster and more accurate verification.

[40] CrowdStrike global outage to cost US Fortune 500 companies $5.4bn (The Guardian, 2024)
[41] UKRI Benefits Profiles
[42] The effect of IT security issues on the implementation of industry 4.0 in SMEs: Barriers and challenges (Marta F. Arroyabe, Carlos F.A. Arranz, Ignacio Fernandez de Arroyabe, and Juan Carlos Fernandez de Arroyabe, 2024)
[43] All the claims have been extracted from the corpus of project outputs generated during the DSbD programme 2019-2025.
[44] DSbD programme outcomes report (UKRI, 2025)

- Representatives from two demonstrator projects highlighted that CHERI was able to detect previously unnoticed memory errors. One representative elaborated that this capability has allowed for more effective automatic code generation and facilitated the rapid scaling of teams by catching errors made by less experienced developers. Another representative explained that they have had instances where errors would have been challenging to debug on non-Morello hardware, but CHERI provided immediate results that clarified the issues.
- Conversely, a stakeholder from another demonstrator project reported that their project revealed an unexpected output, where existing engineering processes and standards were not compatible with the new technology, leading to challenges in integrating it effectively.

Additionally, the Soteria project has been actively working to quantify potential productivity increases and identifying specific use cases where CHERI can provide significant benefits. The UKRI DSbD team has also informed us that future research will focus on measuring productivity gains more precisely.

7.7. Impact on UK reputation in cyber security

EQ18: Has DSbD improved the UK reputation in cyber security? Has this led to wider benefits such as new commercial ventures? How sustainable are they?

This section sets out the impact of the DSbD programme on UK's reputation in cyber security through the following impact pathways:

- Job creation.
- Gross Value Added (GVA) of the cyber security sector.
- Perceived DSbD contributions in increasing UK's status as a reference for cyber and digital security.
- Perceived extent to which outcomes achieved by DSbD, and specific projects, will be sustained beyond the DSbD investment lifetime.
  - Consideration of key factors influencing the achievement or non-achievement of sustainability digital security outcomes.

7.7.1 Creation of new jobs

The creation of jobs in the UK's cyber security sector is a useful indicator of its growing reputation. This trend reflects the increasing demand for cyber security professionals, positioning the UK as a recognised hub for cyber expertise. Furthermore, these job opportunities contribute to economic growth and reinforce the UK's status as a leader in the sector.

The DSbD programme delivery team initially set a target of creating 100 jobs by 2024. **To date, the programme has resulted in the creation of 405 new jobs, surpassing the target by fourfold**.[45] It is important to note that this figure likely underestimates the total number of jobs created, as it does not account for companies independently implementing the CHERI architecture, such as Secqai, SCI Semiconductor, and Codasip.

According to the most recent cyber security sectoral analysis[46] published by DSIT in 2025, the Gross Value Added (GVA) per employee in the cyber security sector ranged from £73,118 for micro businesses to £123,896 for large businesses. While the GVA per employee for micro businesses has decreased by 12.7% since the interim evaluation using 2022 estimates, the GVA per employee for large businesses has increased by 11.4%.

Overall, the GVA from the UK's cyber security sector was £7.5 billion for a total of 2,165 firms, reflecting a 21% increase from the previous year and a 41.5% increase compared to 2022 estimates. This steady

[45] UKRI Benefits Profiles
[46] Cyber security sectoral analysis 2025 (DSIT, 2025)

growth in GVA signals the sector's improved ability to generate value through its products and services, indicating robust growth and innovation.

Based on this data, **the direct expected contribution in GVA by the 405 new jobs created through the DSbD programme would be approximately £29.6 million.**[47] It could be assumed that any new jobs created in the future would exhibit similar levels of productivity, although the extent to which these jobs are entirely additional remains unclear, especially given the UK's generally high levels of employment.

7.7.2 DSbD contributions in improving UK's reputation for cyber security

The United Kingdom consistently performs well in international cyber security rankings. Notably, in the 2024 Global Cybersecurity Index[48], the UK secured a position in the top five.

The UKRI DSbD delivery team has explored international markets through government-led missions to key countries:

- The United States, for instance, has a long-standing relationship with the Cambridge University team that developed CHERI, supported by DARPA since 2010. The US is a significant target market due to its recent efforts in the memory safety domain, to which the DSbD programme has contributed through awareness-raising activities. Additionally, a substantial proportion of multinationals involved in the funded projects, and co-investing in the programme, have their headquarters in the US.
- These missions have also extended to India, Japan, and Australia. The relationship with Australia is particularly significant due to the Five Eyes global security partnership, which unites five nations in various security efforts, including cyber warfare. Moreover, some of the Morello boards have been delivered to Australia and have the potential to be integrated into the supply chain for Five Eyes security initiatives.

Interviews with stakeholders indicate that the UK is highly regarded for its cyber strategies, publicly funded programmes and their accompanying evaluations and surveys, regulatory approaches and codes of practice, and research and development.

The programme stakeholders also commented on the **sustainability of outcomes achieved by DSbD, particularly the DSbD ecosystem**, beyond the DSbD investment's lifetime.

Fifteen stakeholders from four demonstrators, three software ecosystem development projects, and six academic proof projects **reported significant evolution of the DSbD ecosystem over the programme's course**. They emphasised its essential role in fostering collaboration between hardware and software and demonstrating CHERI's capabilities and integration. However, some stakeholders questioned the ecosystem's importance without broader industrial engagement.

Eleven stakeholders from two demonstrators, one software ecosystem development project, and five academic proof projects **expressed optimism about the ecosystem's sustainability**, although some anticipated a reduction in its size post-programme.

- Representatives from three academic proof projects highlighted the need for government funding to ensure sustainability.
- Three stakeholders from two demonstrators noted that sustainability would depend on continued industrial interest and advocacy. They elaborated that while larger organisations like Arm and Microsoft have significantly contributed, the ecosystem's future relies on broader industry engagement and adoption.
- A stakeholder from a demonstrator emphasised the need to address market-related mechanisms such as policy and procurement, rather than relying solely on additional funding.

[47] Due to the lack of turnover and employee data for businesses participating in the DSbD programme in secondary data sources such as FAME and Beauhurst, we have utilised the GVA for micro businesses as a conservative estimate in our calculations.
[48] Global Cybersecurity Index 2024 (ITU, 2024)

Conversely, three stakeholders from one demonstrator, one software development ecosystem project, and one academic proof project each **expressed scepticism regarding the ecosystem's sustainability**.

- Two stakeholders noted that sustainability would only be achievable with active engagement and commercialisation efforts from larger industry players.
- Another stakeholder pointed out that the some of the software developed is often challenging for others to use due to limited resources for ensuring stability and providing support.

7.8. Enablers and barriers to adoption of DSbD technology

EQ19: What are the socioeconomic drivers leading to increased demand for digitally secured products and services? And what are the key barriers impeding the adoption of new DSbD technology?

This section details the enablers and barriers to the adoption of DSbD technology and CHERI. Investigating these factors is crucial as it enables focused efforts by identifying strengths and drivers. Understanding the barriers to adoption is equally important, as it highlights potential challenges and provides opportunities to address these obstacles and market mechanisms that hinder the adoption pathway. These enablers and barriers have been identified through stakeholder interviews, DSbD programme outputs, and research conducted for DSIT's CHERI Adoption and Diffusion report[49].

Enablers to adoption of DSbD technology:

1. **Increasing demand for higher security, resilience, and integrity in key sectors:** The growing need for robust security measures in sectors like telecommunications, critical infrastructure, autonomous vehicles, and defence presents a unique opportunity for the adoption of digitally secure products like CHERI. These sectors are critical to national infrastructure and require a robust system for regulations and standards, thereby making enhanced security and resilience paramount.
2. **Involvement of major industry players:** The participation of leading companies such as Microsoft, Google, and Arm in the development and demonstration of DSbD technology is a major enabler for its adoption. These industry giants bring substantial resources, expertise, and influence. Thus, their active involvement can accelerate the integration of CHERI as their engagement signals credibility and confidence within the sector. Also, involvement of companies like Microsoft, Google, and lowRISC has the potential to significantly influence open platforms and cloud offerings.
3. **UK's competitive advantage:** The UK has a significant advantage in the adoption of DSbD technology and CHERI due to its concentration of skilled professionals with expertise in this area. The presence of leading research institutions like the University of Cambridge and companies actively working on DSbD projects provides a strong foundation for further innovation and development. This skilled workforce can drive the adoption and diffusion of CHERI technology, making the UK a hub for secure computing solutions.
4. **Integration with other emerging technologies:** The CHERI Adoption and Diffusion report highlights the necessity of modifying legacy code to accommodate emerging technologies like quantum computing and AI. As organisations undertake code reviews and modifications to integrate these trending and innovative technologies, they can simultaneously recompile their code for DSbD technology. This approach allows for a seamless integration of enhanced security features with updates for other purposes, making the adoption of CHERI more practical and efficient.
5. **Demonstrating use cases of CHERI and its economic benefits:** The developed DSbD ecosystem has proven to be important, successfully validating the technology, facilitating knowledge exchange, and enabling hardware-software co-design. It has also demonstrated the use cases of CHERI across various sectors. However, further efforts to explore and showcase the economic benefits and implications of adopting CHERI can potentially enhance the adoption levels of CHERI. Additional R&D competitions or

[49] CHERI Adoption and Diffusion Research (DSIT, 2024)

technology demonstrators, specifically targeted at key sectors, could effectively highlight the productivity gains and economic advantages associated with CHERI. This is particularly the case for CHERI's compartmentalisation features, which could generate performance gains and cost savings if appropriately used, which would militate against any perception of CHERI as a security feature which would have costs in terms of resources and system performance.

Barriers to adoption of DSbD technology:

1. **Economic Barriers**: One of the primary challenges to adoption of DSbD technology is the economic cost. Implementing CHERI requires significant investment in developing and deploying new commercial processors before it can be adapted with existing hardware and software ecosystems. Organisations have to weigh the enhanced security benefits against these costs to determine if the investment is justified. The economic feasibility of adopting DSbD technology is a critical factor that influences decision-making processes. Additionally, the adoption of DSbD technology also depends on whether the customers value the enhanced security enough to justify additional costs, as this some of the cost is likely to pass along the supply chain to the end users. Recent reports[50] indicate that a large proportion of consumers are concerned about cyber security, however, only a small percentage are willing to pay for extra for additional security.
2. **Improving the TRL of the technology:** Interviewees have highlighted that for some use cases, CHERI is still in the experimental and research phase, with a low to mid TRL. This means that it is not yet ready for widespread commercial deployment. For these use cases, further research and development are needed to explore the benefits of compartmentalisation and improve compatibility with existing tools and codebases. The experimental nature of CHERI poses a barrier to its immediate adoption in some areas, as organisations may be hesitant to invest in technology that is not fully mature.
3. **Limited awareness among non-technical stakeholders:** Awareness of DSbD technology is predominantly limited to technical, research, and cyber security experts. Marketing professionals and senior decision-makers in large companies are less familiar with the technology, which can hinder its adoption. Further marketing efforts focused on these stakeholders regarding the economic benefits of DSbD technology are essential to overcoming this barrier. Increasing awareness and understanding among non-technical stakeholders can facilitate more informed decision-making and support the broader adoption of DSbD technology.

7.9. Conclusions against evaluation questions

Creation of new products and services

Three physical products have been developed through the DSbD programme: the Morello Board, Symphony, and Sonata boards. While these products are prototypes for research and testing, they lay the groundwork for future commercial offerings.

The TAP has been instrumental in introducing DSbD technology to UK businesses, particularly SMEs. TAP has received positive feedback across cohorts, however recommendations from members highlight the **importance of user-friendly documentation and support to ensure efficient onboarding and development on DSbD technologies.**

Notably, **80% of DSbD survey respondents positively evaluated the Morello board for potential use in their future products and services.** Despite this, the programme has not yet achieved its target of 200 companies positively evaluating the board, as the total number of businesses involved in the programme is lower than the set target. DSbD-funded projects have also shown significant progress in developing software and tools over the programme period. However, **commercialisation of these developed tools remains a challenge, as a commercial product is not yet available.** Stakeholder interviews revealed that

[50] Consumer Trust & Behavior After Recent Cybersecurity Lapses (Civic Science, 2024)

the involvement of academic institutions has been crucial, but greater private sector engagement is needed to ensure the integration of DSbD technology into future products and services.

The **independent use of DSbD technology by large companies such as Microsoft and Codasip demonstrates its potential beyond the programme.** This external interest validates the technology's potential and opens pathways to achieve downstream adoption. Additionally, three companies – Codasip, SCI Semiconductor, and Secqai – are expected to offer products with CHERI architecture in the near future.

Impacts on organisational culture

The DSbD programme has influenced the organisational cultures of businesses and academic institutions by:

- Redirecting research efforts towards DSbD-related areas, including CHERI, memory safety, and compartmentalisation.
- Providing opportunities for the exploitation and commercialisation of developed DSbD technologies.
- Establishing the necessary infrastructure, supported by the government's long-term commitment to the DSbD programme.
- Influencing the strategic business models of private organisations.

Impacts on share of export market for businesses participating in the DSbD programme

As the DSbD technology has not yet been adopted by businesses, **there is no fully commercialised product with CHERI embedded that could have a measurable impact on the share of the export market.** DSbD survey respondents were also unable to quantify perceived increases in exports.

However, **Cyber Hive, funded by DSbD, has been pursuing international commercial traction through the CHERI USP in their existing product line**, which has garnered demonstrable interest and excitement from companies. Additionally, **Codasip's implementation of CHERI was stimulated by a customer**, indicating potential increases in export revenue through the commercialisation of DSbD technology.

Perceived contribution to UK productivity

From the DSbD business case, the main route to increased UK productivity in future would be to **reduce the working days lost to cyberattacks**. Data on continuing levels of cybercrime in the UK, and the performance of the CHERI technology in addressing vulnerabilities, suggest that this rationale is still valid.

The DSbD programme has the **potential to enhance UK productivity by mitigating downtime caused by cyber attacks and improving engineering efficiency**. Theoretical models and funded projects have demonstrated that DSbD technology contributes to productivity gains in both organisational and engineering contexts. However, the **direct impacts of these productivity gains are yet to be observed**.

UK reputation in cyber security

The DSbD programme has had a positive impact on the UK's standing in the field of cyber security, primarily through substantial job creation and sectoral growth. To date, the DSbD has **successfully facilitated the creation of 405 new jobs**, far surpassing the initial target of 100 jobs by 2025. These **new jobs are projected to contribute approximately £29.6 million in GVA**.

Additionally, the DSbD programme has led government missions to the United States, Australia, India, and Japan. These missions have not only raised global awareness of DSbD technologies but have also facilitated the distribution of Morello Boards in the US and Australia.

Enablers and barriers to adoption of DSbD technology

Key enablers to adoption of DSbD technology include:

- The need for robust security measures in critical sectors like telecommunications and defence provides the opportunity to drive adoption of digitally secure products like CHERI in this area.
- Involvement of major industry players such as Microsoft, Google, and Arm brings resources, expertise, and credibility to the DSbD ecosystem
- UK's competitive advantage lies in the skilled professionals and leading research institutions with extensive knowledge of DSbD technology and CHERI.
- Modifying legacy code for other innovative technologies like quantum computing and AI allows for seamless integration of DSbD technology alongside it.
- Validating the technology and showcasing its economic advantages can enhance adoption levels, particularly through targeted R&D competitions.

Key barriers to adoption of DSbD technology include:

- Significant investment is required to develop and deploy new processors, and the cost may be passed along the supply chain to end users, who may not be willing to pay extra for enhanced security.
- CHERI is still in the experimental phase for some use cases, requiring further research and development for commercial deployment in some areas.
- Awareness of DSbD technology is predominantly limited to technical experts, necessitating marketing efforts to inform senior decision-makers and non-technical stakeholders about the economic benefits of DSbD technology.

8. Conclusions

8.1. Principal added value by DSbD to date

EQ20: What has been the principal value added by DSbD to date? To what extent have DSbD investments been value for money as a delivery mechanism for increasing UK digital security levels?

The DSbD programme has succeeded in its primary aim of a **technology platform prototype** – the Morello board – which can be used to investigate the benefits of a new secure processor design based on CHERI. It has accomplished this in the face of significant external headwinds such as Covid-19 and global semiconductor supply chain issues. The technology is genuinely novel, and the evidence is that it provides a solution to memory safety issues that are endemic in processors, but which have not been resolved by market forces. This was the market failure rationale for the programme.

The programme has also commissioned academic research to investigate and verify the properties and behaviour of the technology, social science research to investigate perceptions of cyber security and barriers to adoption, a set of industry-led technology Demonstrators, and smaller grants for business-led projects to investigate specific use cases.

The programme has proved flexible in response to challenges and opportunities, and has attracted additional funding from Government (DCMS/DSIT and DSTL) which has been directed towards specific use cases and potential user groups. These have helped support two significant new directions for potential adoption of CHERI technology:

- UK defence technology, supported by DSTL funding.
- The Technology Access Programme, which supported five cohorts of businesses to investigate the Morello board, and a sixth cohort employing the RISC-V Sonata board to investigate embedded computing applications. The final cohort is of particular significance as RISC-V microcontrollers currently provide the most likely path to market for CHERI and are currently being developed by at least three companies with the intention to release commercial products in 2025.

The DiScribe Hub has made key contributions to the DSbD programme through a combination of interdisciplinary research, stakeholder engagement, and policy influence. DiScribe's work has illuminated the human, technical, and societal dimensions of digital security innovation, structured across four core work packages:

- WP1 (led by the University of Bath): Examined the adoption and integration of emerging technologies.
- WP2 (led by the University of Bristol): Investigated software engineers' readiness to develop for the CHERI architecture.
- WP3 (led by Royal Holloway, University of London): Explored the regulatory and policy implications of digital security innovations.
- WP4 (led by Cardiff University): Analysed societal and sectoral perceptions of Digital Security by Design.

To date, DiScribe has supported 57 researchers, collaborated with over 19 universities and 16 industry partners, and contributed to the academic community with more than 34 peer-reviewed publications in journals and conference proceedings.

In addition to its research contributions, DiScribe has actively fostered stakeholder engagement through a variety of events and creative outreach initiatives under its Futures programme. It has also informed national policy by submitting evidence to the McPartland Review, participating in government and industry working groups, and presenting at key conferences. These efforts have highlighted the economic and societal cases of embedding security into the design of digital technologies.

8.2. Extent to which DSbD has accelerated adoption

EQ21: To what extent has DSbD accelerated the adoption of the new hardware architecture? Is there any evidence of new products and services deployed as a result?

8.2.1 Routes to adoption accelerated by DSbD

The primary route to market envisaged at the outset of the programme was for CHERI to become a standard feature of a mass-market processor, with the most likely route being a reference design from Arm. If this design were then to be adopted by at least one of the four major operating systems for mobile devices – Windows, iOS, Android, or OS X – it would give access to a huge, mature global market.

At this final evaluation stage, it appears that the barriers to this route to market are viewed as too great for the time being. These barriers consist of the amount of code that would need to be rewritten in the existing ecosystems and the resource investment accompanying it, opportunity costs for the chip designers and competition for physical space on the processor with other features requested by customers. Arm however have stated that they remain interested in the CHERI technology, and their own compartmentalisation technology is being designed to a fully compatible approach with CHERI's.

The alternative route to market is through microcontrollers and embedded computing. The research and development necessary to permit this emerged during the programme:

- Microsoft's investigation of how to scale CHERI down to small cores on the cheapest microcontrollers (published September 2022).
- The CHERIoT project to specify a RISC-V-based microcontroller design and tools, part-funded by DSbD and involving Microsoft Research and the academic partners in the CHERI research group.
- The CHERIoT Ibex core, an open source reference implementation of CHERIoT developed by Microsoft based on lowRISC's Ibex core design.
- The Sunburst project, funded through DSbD for lowRISC to produce two classes of test board (Sonata and Symphony) using CHERIoT-Ibex.
- The 6th cohort of the DSbD Technology Access Programme, which funded businesses to develop use cases with Sonata boards, just as the previous 5 cohorts had with Morello.

As a result of this R&D work, at least three companies (Codasip, SCI Semiconductor, Secqai) have started up or adopted new business models in order to produce commercial CHERI processors at the microcontroller scale based on RISC-V. These are currently expected to release commercially available products in 2025, although none were available at the time of completion of this evaluation report.

8.2.2 Wider effects of funded projects

The funding commitments and letters of support from the private sector set out in "Chapter **Error! R eference source not found.**: **Error! Reference source not found.**" demonstrate that CHERI is being investigated by a range of companies including Google, Microsoft, and Amazon. While little of this work has been made public, and no commercial CHERI solutions are currently available, there are indications of the direction of travel. Principally, the CHERIoT workstream, begun by Microsoft as additional research not directly funded by DSbD but incorporated into the funded programme once it was made public, is having a significant impact as it offers the most immediate route to market for CHERI, and was the catalyst for the commercial solutions which have been announced and are expected in 2025.

Another impact has been the creation of the CHERI Alliance as a trade association aimed at promoting the global adoption of CHERI. The CHERI Alliance was not directly funded by DSbD but has been formed to represent and promote CHERI technology through its membership and technical working group including researchers, industry experts, and public sector organisations. It has run conferences on Cybersecurity by Design in November 2024 and Cultivating a Safer Digital Future in April 2025.

DSbD and CHERI have been mentioned in a sequence of Government policy documents, as set out in Section 6.3.1. These have included the Innovation Strategy, Integrated Review Refresh, and Semiconductor Strategy, and there is clear alignment between the Cyber Security Strategy 2022-2030 and DSbD's objectives to develop secure technologies.

CHERI has also been mentioned as part of increasing global recognition of "memory safety" as a set of solutions to cyber security problems, for example in the White House's February 2024 report titled "Back to the Building Blocks: A Path Toward Secure and Measurable Software[51].

8.3. External factors for future adoption of CHERI, and potential interventions

EQ22: What wider effects did DSbD investment had on funded projects?

According to the programme design and the Logic Model which describes it, the necessary steps between achievement of the prototype project milestones and eventual adoption are:

- Prioritising the industrial R&D agenda.
- Making progress towards new regulatory standards and legislation proposals.
- Increasing industrial sectors' awareness of cyber and digital security issues and market failures.
- Capacity building: formation of new knowledge and skills to develop digitally secure products and services.
- Building confidence in the technology, and demand for the new products and services.

The programme has made good progress in these areas:

- DSbD has **good links** with Government through the Advisory Group and continues to feature in Government strategy documents. Building CHERI and the concept of memory safety into policy and regulatory standards, and government procurement, helps build confidence in the value of the technology, stimulating demand and investment.
- DSbD has stimulated collaboration between academia and industry and built an ecosystem of developers and early adopters. For adoption, this would need to be expanded to a much wider potential industrial marketplace. The CHERI Alliance has emerged as a trade association to accelerate this.
- Deployment and adoption would benefit from the inclusion of large and small companies in the UK supply chain. If UK SMEs can provide services to large companies internationally, the UK can gain differential economic value via first mover advantage. Government procurement can also play a critical role here. The Technology Access Programme has opened up CHERI technology to UK SMEs to develop use cases.
- DSbD has brought in investment from government and the private sector; crucially, the Microsoft workstream investigating DSbD beyond the parameters of the funded activities has resulted in the RISC-V based microcontrollers that are the first designs being used to take CHERI to market. Other private sector commitments are known of, but the commercial details are typically not publicly available.

According to DSbD participants and sector experts interviewed for this evaluation, the key external factors affecting successful delivery of cyber security projects are:

- **Regulation**, **policy**, and **standards** to guide companies in decision-making (whether suppliers or consumers of cyber security solutions).
- **Lack of knowledge/understanding** of cyber threats and technological solutions, **cost pressures** and **risk aversion** in the **marketplace**.

[51] Back to the Building Blocks: A Path Toward Secure and Measurable Software (The White House, 2024)

- **Skills** to develop new solutions (supply side) and to integrate them into existing systems (demand side).

The focus on Government among the people consulted for this evaluation – and how it can act through legislation, policy, and promotion of standards – is a new development since the interim evaluation two years ago. This perhaps reflects the growing maturity of the technology and a changing focus on what is required to achieve its adoption and deployment. It may also have been influenced by DSbD/CHERI being mentioned in UK Government strategies, and recent developments such as the UK Product Security and Telecommunications Infrastructure Act 2022, the EU Cyber Resilience Act, the UK Government Secure by Design procurement standards, and international policy and technical papers on “memory safety”.

These factors highlight the importance of any intervention which follows the DSbD programme in considering the following:

- Growing the UK cyber and digital security ecosystem, involving Government policy and procurement where possible.
- Building awareness, among non-technical stakeholders, of cyber security threats and the role that CHERI can play in addressing these, with particular reference to “memory safety” as an agreed set of problems and solutions.
- Developing capacity and capability to use CHERI technology when it becomes commercially available.

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM UK Consulting LLP
25 Farringdon Street
London
EC4A 4AB
United Kingdom
T +44 (0)20 3201 8000
rsmuk.com