DEFENCE DATA RESEARCH CENTRE

Attitudes to Data: Workshop Findings Vs Policy

Author: Dr Alex Hardy

Date: 26 September 2024

2024ESAE025

TABLE OF CONTENTS

TABLES AND FIGURES

ATTITUDES TO DATA: WORKSHOP FINDINGS VS POLICY

PREPARED FOR DSTL

ALEX HARDY, DDRC. 23 MAY 2024

ABSTRACT

This working paper contrasts the findings of a series of Attitudes to Data LEGO® workshops (Hardy, 2024; McClure, 2024a; 2024b; 2024c) conducted in late 2023 by the Defence Data Research Centre (DDRC) Attitudes to Data research team with the recent data-facing policies of the UK government. This paper analyses the latter approaches to data of the UK's Conservative government (2020-24, covering the Johnson, Truss, and Sunak administrations) and elucidates key themes from these documents. This analysis, combined and contrasted with the findings of our workshops, may be useful to policymakers and decision-makers seeking to understand and navigate the contemporary data challenges facing the UK.

INTRODUCTION

This research paper is borne out of our wider project to understand attitudes to data in the UK and the potential impact on the future of Defence that these attitudes may or may not have. This paper explores data from a series of interactive LEGO® workshops conducted in the second half of 2023 that were conducted to engage with various different sectors of workers across the British workforce regarding data use within their organisations. The paper contrasts and compares the findings of these workshops with a series of policy observations drawn from the proliferation of data-related policy documents in recent years from the UK government. While policy is usually written by civil servants and are typically strategies that set out the 'vision,' the aims, and the objectives of a government (Morley, 2022) this paper seeks to explore how accurately this vision resembles reality.

The paper seeks to address the following research question: Do the findings of our LEGO® data workshops coincide or contrast with the published data policy priorities of the UK Government in recent years?

To achieve this, the paper reviews the recent data-facing policies of the UK government and discusses in some detail some of the key ideas contained within these documents, highlighting quotations of note. The paper also establishes three common themes within and across those policies, based on analysis conducted using the qualitative software Atlas.ti[1]. These three themes are discussed and contrasted with the common ideas and co-occurrences of the LEGO® workshops, noting both similarities and differences between the key ideas raised in both. These, the paper argues, may form some of the strategic priorities of the new UK administration when it comes to tackling some of the issues surrounding data in UK organisations, such as access, ensuring the confidentiality and integrity of data, and secure data management (Hardy, 2024).

The UK's data, both public and private, as well as the personal data of its citizens, is closely linked to its national security (Hardy, 2024). How the UK treats that data is often very concerned with risk management by securing data and ensuring it cannot be used maliciously by malign actors (Morley, 2022). Data's centrality to effective national security lies not in its abundance but in its organisation, processing, and utilisation for decision-making (Babuta et al., 2020). Organisations, both public and private, harnessing their data is imperative for the UK's national security going forward (Roberts et al, 2023) and a significant challenge lies in harnessing that data for AI in the near future (Payne, 2024). This research has been funded by Dstl and takes specific direction from the UK's AI for Defence policy (2022) yet a myriad of other data-facing policy also exist. This paper seeks to explore some of that policy and understand whether it reflects the concerns of our workshop participants.

METHODS

Our study involved conducting 34 workshops across the UK. Our participants were sourced from England, Wales, and Scotland in multiple locations detailed in the Annex (A1). Participants were principally sourced via a mixture of snowballing research contacts and a recruitment email sent to prospective partners.

[1] ATLAS.ti is software that helps researchers qualitatively analyse data by coding and annotating features in unstructured data. It also offers visualisation functions to help researchers interpret their findings. Please see https://atlasti.com for further information.

The workshops themselves lasted for 90 minutes. The questions posed in the workshops are visible in the Annex (A2) and further detailed in Hardy (2024). These challenges were inspired by the UK Government's AI for Defence Strategy (2022) and the data priorities and were approved through dialogue with Dstl partners as being of use to better understanding UK citizens understanding of data. In the workshops, we recorded the explanations of participant's LEGO® models with a microphone and later transcribed these assisted by Otter AI. These transcriptions, once edited, were then uploaded to our chosen software, Atlas.ti. There, we inductively coded our transcriptions based on our ground-up interpretation of the data. This data has been analysed in several reports (Hardy, 2024; McClure 2024a; 2024b; 2024c) all of which have been concisely synthesised below. All research was undertaken within the parameters of good ethical conduct approved by both the MOD

Meanwhile, the policy analysis in this paper was undertaken in two ways. The documents were read and analysed by the researcher, and then discussed below drawing upon an interpretive policy analysis approach. While a traditional method of policy analysis, this has often been critiqued as being either disjointed from public impacts or being subject to the whims of the researcher (Yanow, 2007). To counter these weaknesses, the policy documents were also coded with the support of Atlas.ti's automated coding. This identified some key themes in these extensive documents and has been used to provide some visualisations in the 'Policy Overview: Coding' section of this report. Furthermore, the findings of this policy analysis are contrasted with our LEGO® workshop findings, which engage with the wider public on some of the urgent data issues of the day. By triangulating these approaches, this paper gives a broad overview of UK data policy and how it relates to the reality of data use in UK organisations.

WORKSHOP FINDINGS: DDRC REPORTS SO FAR

This section seeks to highlight some of the findings unearthed in our workshops and references the reports thus far based on varying different analyses of that data (See Hardy, 2024; McClure, 2024a, 2024b, & 2024c) . Below, Figure 1 shows the most common codes within our transcripts identified through qualitative transcription (Hardy, 2024a). The most discussed issue was processes/policies/practices within a given organisation.

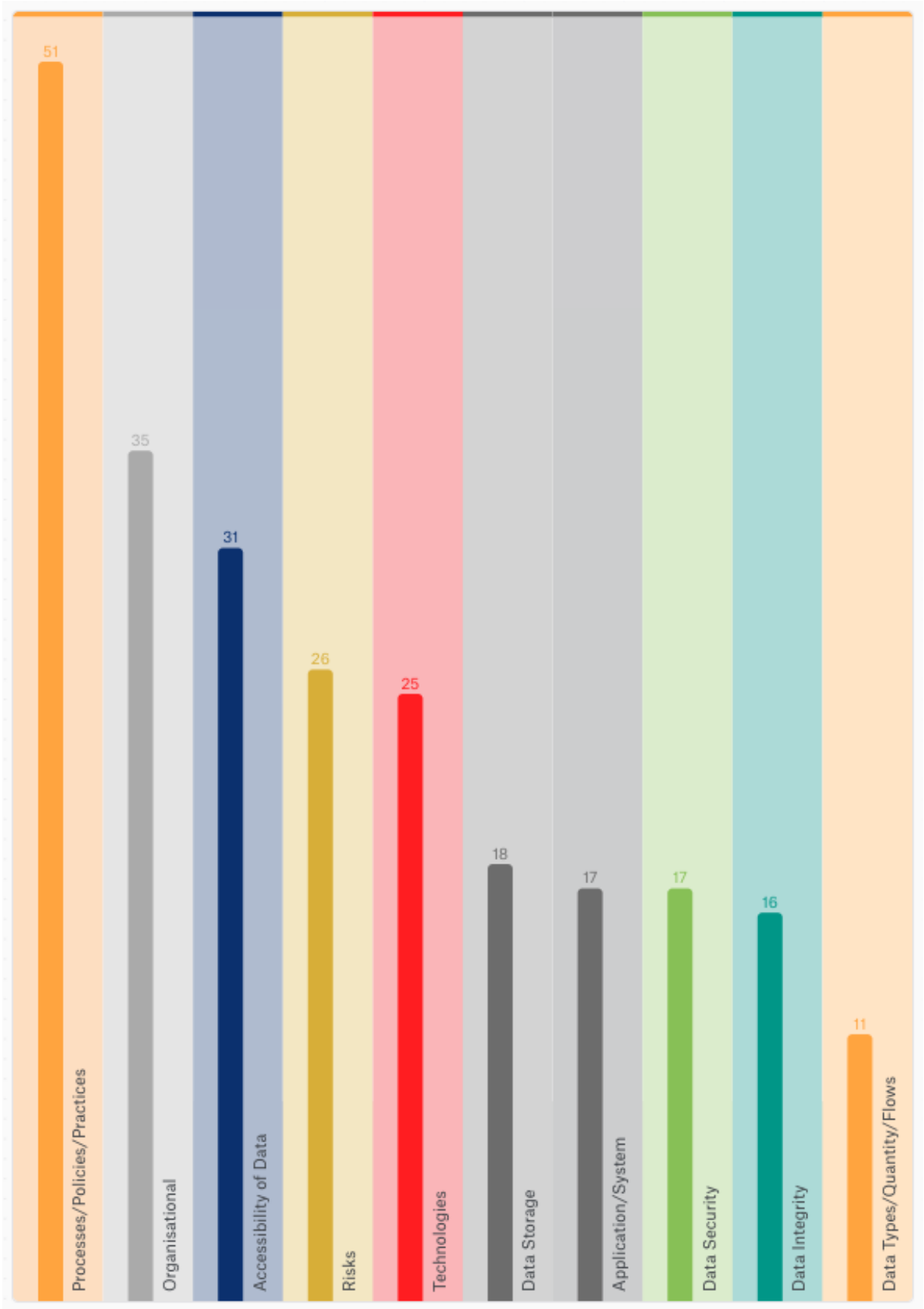

Figure 1: Top 10 Common Codes (Hardy, 2024)

We subsequently investigated the co-occurances between those top codes. These co-occurrences highlight links between commonly discussed issues.

This research then discussed the top four co-occurrences ([1]Organisational-Processes/Policies/Practices; [2] Accessibility-Security; [3] Accessibility-Processes/Policies/Practices; [4] Security-Risk) and interrogated the links between these themes identified by workshop participants (Hardy, 2024). This research revealed that data is complex and crucial for UK organisations. Our approach highlighted common issues across workshop participants including issues surrounding data access and policy frustrations, balanced by an understanding of security needs. Using creative methods like LEGO® workshops proved effective for engaging participants and generating detailed discussions and LEGO® visualisations. While many participants valued data security, concerns about data access were prevalent across sectors.

Additionally, McClure (2024a) utilised a computational linguistic approach to interpret stories from our LEGO® workshop participants, identifying key themes in the language used. A quantitative semantic analysis revealed three main emotive concerns: Anger, Discontent, and Worry. This was then analysed at a word and co-text level. The language patterns fell into four focus areas: data, technology, organisational processes, and employees. This report explores participants' language and emotions when talking about data in their workplace. (McClure, 2024a)

A following report (McClure, 2024b) using the same data, while also utilising a computational linguistic approach, identifies and interprets stories from DDRC workshop participants, revealing patterns not easily seen through close reading. Participants' language identified two main themes: Obligation or Necessity and Positive Evaluation. The report explores the link between participants' language and their concerns about the data environment, mapping common concerns across six different sectors of the economy to outline ideal conditions for their data, thus providing important information on potential improvements organisations in their respective sectors could make in the future (McClure, 2024:b) An additional report (McClure, 2024c) identified the differences among the different economic sectors our workshops engaged with (including education, services, public sector and more). It identified that certain sectors, such as the public sector, were more concerned with organisational issues

such as working processes and practices. Meanwhile, other sectors, such as non-profits, more highly valued data security, while the University sector was the least concerned by such issues. In sum, these reports identified considerable concerns around the accessibility of data and the working processes/policies/practices within organisations. These were tempered by some understanding of risk and security, but often generated emotion among employees. These emotions included worry, discontent, or even anger and these often related to the data itself, technology, organisational processes, and fellow employees. This reflects how data is discussed – in a positive, or negative fashion and reveals some of the key challenges that face the UK in terms of how to better understand and navigate data issues in the workplace (McClure, 2024c). This, we argue, (in line with UK policy) has wider implications for Defence, as we need to get the basics right on a larger societal scale, and ensure employees have the correct knowledge and skills to make the UK digitally resilient (Hardy, 2024; UK National Data Strategy, 2020).

"Individuals should be empowered to control how their data is used, and supported to have the necessary skills and confidence to take active decisions around the use of their data, in order to contribute to the wider societal benefit data can offer"

(UK National Data Strategy, 2020: 54)

POLICY OVERVIEW: CODING

The policy documents identified were analysed and coded using Atlas.ti's AI-enabled coding. These policy documents included:

Policy Document	Year of Release	Governmental Department
UK National Data Strategy	2020	DCMS
UK National AI Strategy	2022	DSIT
National Resilience Strategy	2021	Cabinet Office
Plan for Digital Regulation	2021	DCMS

UK Digital Strategy	2022	DCMS
'Build Back Better' Plan for Growth and Innovation	2021	HM Treasury
National Cyber Strategy	2022	Cabinet Office
UK Defence AI Strategy	2022	Ministry of Defence

Table 1: List of Policy Documents Analysed

Atlas.ti's automated coding has benefits in terms of the time consumed by the researcher but is traded off against direct human interpretation of the text. This was chosen as the policy documents are vast, being both numerous and long individually. Atlas.ti allows the researcher to instruct the automated analysis of how it should focus its coding. For this research, all documents were coded with the instruction 'Focus on the role of data in UK organisations'. This was instructed as considerable amounts of these policies were long and could be considered irrelevant to the task at hand. This, in turn, generated a focus on three significant codes (which also contained a number of sub-codes). These were identified across all eight policy documents. These three significant codes, identified due to the commonality of their presence within the policy documents accessed, were data utilisation, data challenges, and data impact. Within those areas, sub-codes also emerged. This is discussed further below and can be seen in Figures 3-5.

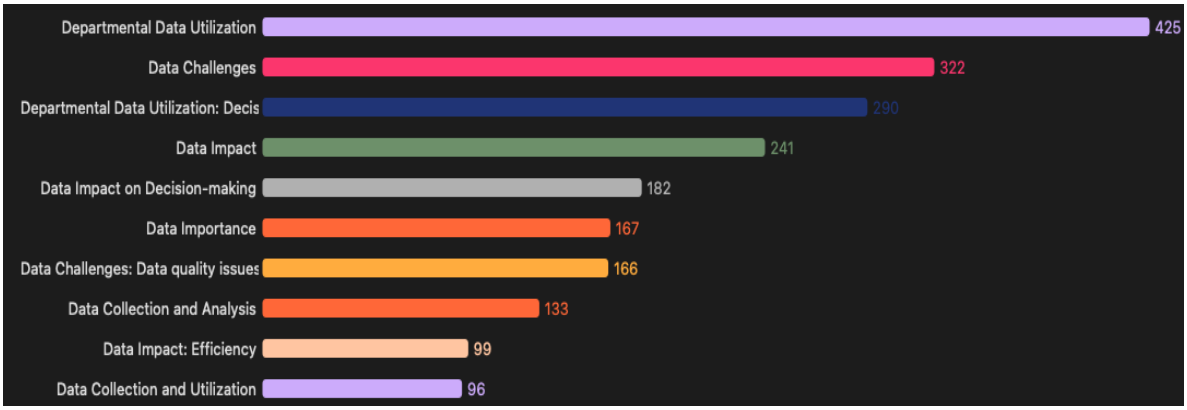

Figure 2: Most Commonly Coded Themes within UK Policy

As seen above in Figure 2, the AI-coding generated some dominant or 'parent' codes. These

included Data Utilisation (715 mentions across all documents noting concerns around wider utilisation or utilisation for decision-making), Challenges (322 mentions), and Impact (241 mentions). The most coded issue was how governmental departments could better use the data available to them. Subsequently, the policy documents focus heavily on the challenges of data and obstacles to success, followed by data utilisation issues, particularly around how data can be used to enhance decision-making and how to improve efficiency.

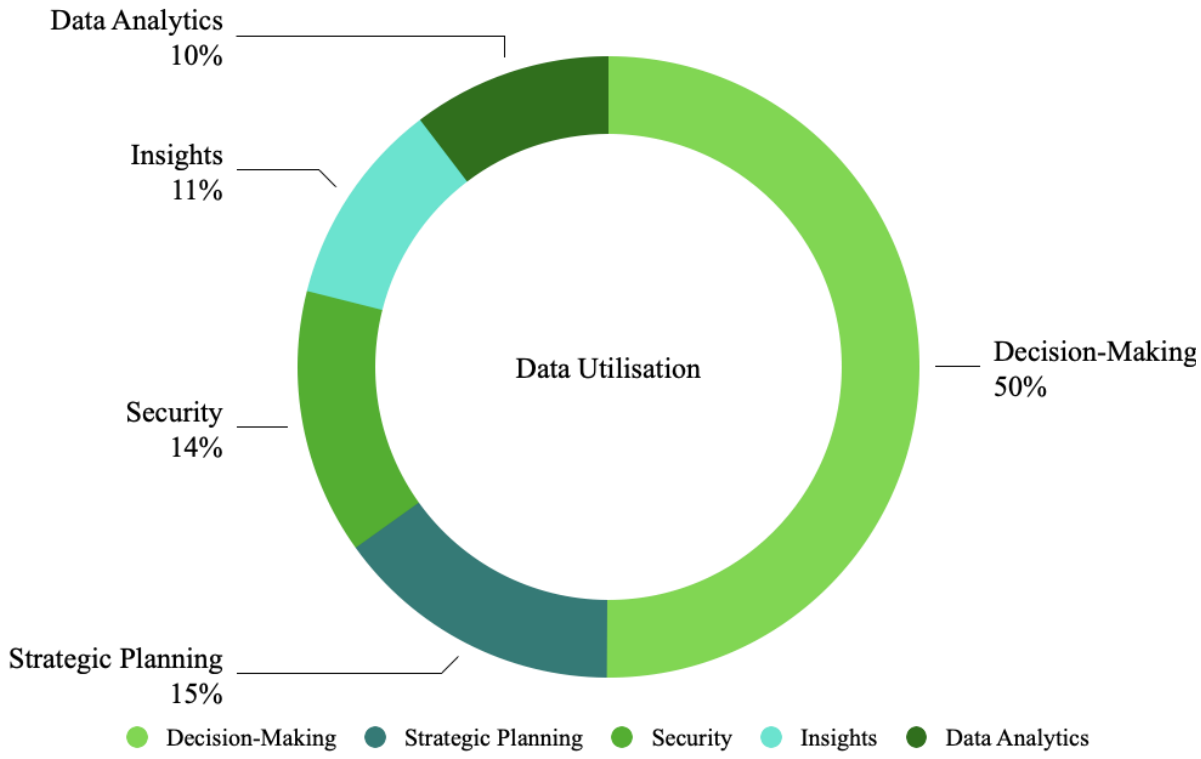

Figure 3: Key Aspects of Data Utilisation within UK Policy

When breaking down the Data Utilisation coding, a number of key sub-codes that constituted data utilisation issues emerged. Those are highlighted above in Figure 4, with issues surrounding secure data utilisation dominating this particular aspect of policy discourse. The other issues around data utilisation include decision-making, strategic planning, data for insights, and utilising data for analytics. It should be noted, however, that data for decision-making cuts across the categories of Data Utilisation and Data Impact.

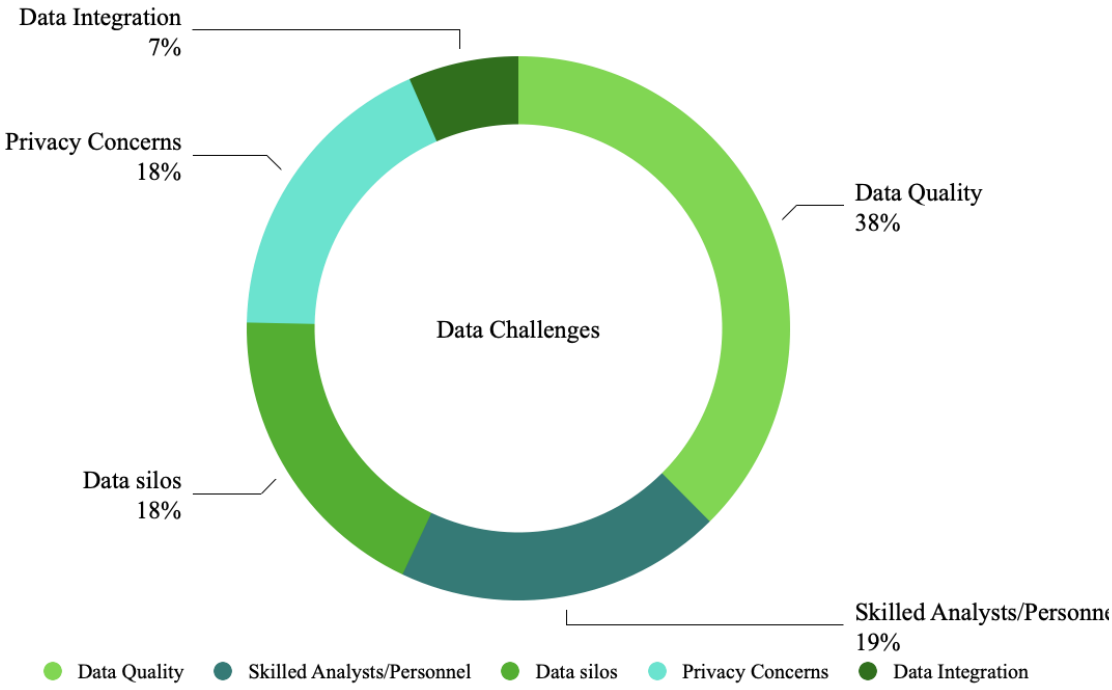

Figure 4: Key Aspects of Data Challenges within UK Policy

Figure 4 breaks down the sub-codes of the data challenges code identified within the policy documents. This is somewhat dominated by concerns around data quality, followed by concerns around a lack of skilled workers. Issues of privacy, data silos, and data integration follow.

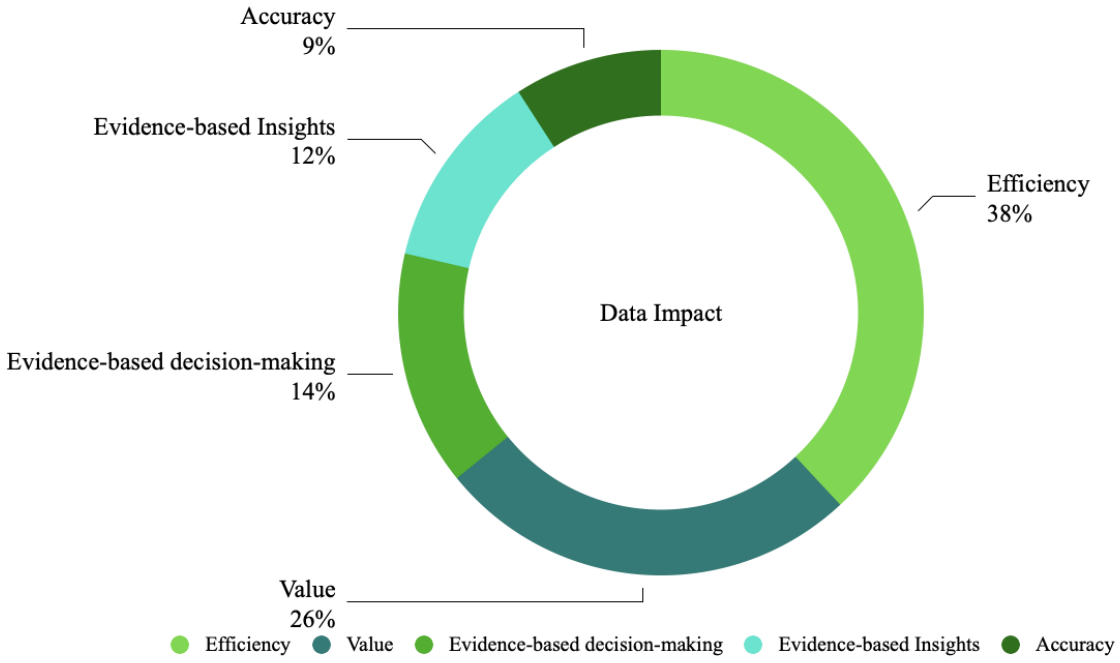

Figure 5: Key Data Impact Issues within UK Policy

Figure 5 illustrates a breakdown of the Data Impact code. This code is dominated by the efficiency sub-code. This is followed by accuracy and the ability to use data for impactful and evidence-based decision-making and insight.

POLICY OVERVIEW: ANALYSIS

In recent years, there has been a significant number of policies released in terms of strategies and visions for how data ought to be handled and managed and visions for Britain in the digital era. This analysis recognises this policy growth, as evidenced by the wide array of policies it engages with and seeks to highlight some of the patterns across these policies and assess how they measure up to the findings of our recent DDRC workshops.

UK policy pays particular attention to the importance of ordinary citizens and their interactions with that data. As highlighted later in this section, the UK is not a trendsetter in this regard and such approaches can be evidenced (to differing extents) in the policy of the UK's close allies such as the United States, fellow members of NATO, and members of the European Union. The UK government's 2020 National Data Strategy outlines a number of key goals for the UK in the coming years, including notably how they must become 'AI-

Ready':

"Data is a non-depletable resource in theory, but its use is limited by barriers to its access – such as when data is hoarded, when access rights are unclear or when organisations do not make good use of the data they already have. These barriers undermine the performance of public services and our economy, risking poorer outcomes for citizens."

(UK National Data Strategy, 2020)

Notable themes relating to the wider public include issues such as privacy, ethics, skills, and data availability. Namely, data-driven innovation must be sensitive to public trust and offer workable solutions; if the public does not believe that innovation is beneficial, secure, trustworthy, and practical, it is destined to fail.

This is further outlined in the National AI strategy (2022), highlighting the importance of people and data as vital to AI innovation. This strategy argues that access to people and data are 'key drivers of progress, discovery, and strategic advantage'. As an immediate priority, the strategy also outlines the need for investment in public outreach to create better data skills, better use of data across the economy, and investment in digital infrastructure. The AI strategy also calls for additional engagement with national security, defence, and leading researchers to understand what public sector actions can safely advance AI and mitigate 'catastrophic risks'.

It is worth noting the sheer amount of UK policy that addresses the issue of data in recent years, including the eight policies analysed in this report. While existing analysis has identified some common themes across these policies, with consensuses around upskilling the wider population, improving data access, and reducing vulnerabilities (Morley, 2022) it is also dubious that having policy spread across such a proliferation of different documents is helpful. The documents are extensive, sometimes repetitive, and as policy documents often do, set out wider aspirations. The latter years of the Conservative Government were marked by considerable upheaval, likely inflicted by changes in the Prime Minister, cabinet reshuffles, and changes to government departments. These changes include the recent decision to remove digital responsibilities from the Department of Culture, Media, and Sport (DCMS) and instead create the new Department of Science, Innovation, and Technology. Matters surrounding data are rightly of interest to multiple areas of government but the broad

scope of these policies and the rapid flurry of changes can appear confusing and overwhelming, making concise reporting and analysis important.

Across the policy analysed, data availability is widely seen as a potential driver for innovation and economic development. The UK Cyber Security Strategy's (2022) foreword pays explicit attention to the importance of data for the implementation of new AI-driven technologies and also the importance of securing personal data from cyber attacks such as ransomware. Meanwhile, the Cyber Strategy (2022) also outlines five pillars of the UK's approach to data security. Summarised for brevity, these included:

- Strengthening the 'cyber ecosystem' — Focus on people and skills
- Building Resilience — Reducing risks for businesses and citizens
- Leading in Tech Development — Building Industrial Capacity
- International Leadership — Emphasis on sharing best practices with allies
- Detect & Disrupt — Use creative approaches to deterring hostile actors

Due to the numerous overlapping policy areas covering matters of citizens' data, there are some common narratives throughout the different strategies. While ostensibly focused on economic growth, the 'Build Back Better' Plan for Growth and Innovation (2022), one of the Johnson government's headline initiatives, places emphasis on data for AI being developed so that it is secure and 'fair'. Similarly, data-wrangling is referred to as an opportunity to 'cut red tape' but also to improve the availability of data. Likewise, there is a commitment to developing international norms:

"We will support the development of global principles, norms and standards on those emerging areas that are not fully part of the existing international rulebook, at the frontier of the future global economy in areas such as services, digital and data."

(Build Back Better Plan for Growth and Innovation, 2022)

It should be stressed that these challenges are transnational as data easily traverses international borders. Further research and collaboration is needed to work with our international partners in NATO, the EU, and beyond to ensure that data is secure, its integrity is ensured, and it is accessible when needed. This is highlighted in the UK National Data

Strategy (2020):

"The importance of data to the daily lives of modern citizens has made it a geostrategic tool. The government is committed to supporting international data flows while ensuring that transfers of personal data from the UK uphold high data protection standards."

(UK National Data Strategy, 2020)

As recent research also concludes, the challenges of delivering data that is available, secure, and trusted are not challenges that the UK faces alone (Dwyer, 2022; Payne, 2024). There are significant lessons to be learned from our partners and allies, and potentially also our adversaries. The rapid development of and changes in policy represent a considerable challenge as well as the challenges identified in this policy analysis. It also risks an inconsistent and confused approach across government. For Defence, it is vital to keep abreast of these changes, addressing issues around access to data, the security of that data, and skills within organisations, as these represent key strategic priorities. The relationship between data, AI, and national security has become particularly exemplified in the war in Ukraine, where companies have developed a variety of AI solutions that are used on the battlefield, including uninhabited aerial and ground vehicles for reconnaissance, surveillance, fire adjustment and support, target ID, logistics, and evacuation. Furthermore, electronic warfare systems help shield cities from enemy drones and training and simulation systems support Ukrainian troops (Goncharuk, 2024). If the UK is to keep pace with these developments and integrate the wider use of AI into Defence, one of the key challenges is harnessing the data that drives AI capability, and this will require a broad societal approach.

"We must assess and mitigate AI system vulnerabilities and threats to both our capability and the data that drives it. We must harden AI systems against cyber-attack and other manipulations, addressing data, digital and IT vulnerabilities while developing and continuously evolving security methodologies for AI capability defence"

(Defence AI Strategy, 2022: 36)

CONCLUSIONS

To offer some conclusions, data is a key challenge for UK organisations operating within a

complex policy landscape. In turn, this has serious implications for national security and defence. Our workshops engaging with UK workers across various sectors of the UK economy identified a number of common patterns and issues that reflect the stated priorities of existing UK policy. This can be summarised into three findings.

What was prominent in workshops and across policy

Data Access – Discussion within our workshops consistently revolved around data access and availability, and frequently, how this could be improved.

Data quality issues – Discussion in workshops also touched upon data quality, with participants expressing concerns around issues like the poor quality of older data.

The importance of good security and the link to associated risks – Both the workshop discussion and policy extensively address the importance of secure data practices, and the risks posed by hostile or malicious actors.

What was slightly limited in our workshops but prominent in policy

Skill and training issues – these were touched upon in some workshops, particularly when some participants felt that management didn't really appreciate the value of data (see Hardy, 2024), however, they were not as prominent a concern articulated in policy.

What featured heavily in our workshops but was less prominent in policy

Internal working policies and procedures being problematic – frustrations with policies, processes, and practices were often aired in our workshops and this was often linked to access. We uncovered employee frustration, anger, and discontent, but also some positive solutions when participants discussed idealised scenarios (McClure, 2024b).

Our results somewhat diverged in terms of discussions around skill. As above, UK government policy places considerable emphasis on upskilling the population. While some workshop participants highlight this as an organisational issue (sometimes among senior staff), generally, it did not dominate our discussions as much as it features heavily in policy discussions. This may be attributed to the types of workers our workshops engaged with. These workers might be described as digital professionals, whose collective skills are higher than the UK average population, and upskilling is naturally less of a concern to them. Conversely, however, they also occupy a prime position to recognise the need to upskill others.

In an increasingly insecure world where Russian defence minister Andrey Belousov openly states that mastery of Artificial Intelligence is crucial to success in a confrontation with the West (TASS, 2024) the Defence case for improving our data could not be clearer. Given ongoing world events such as the conflict in Ukraine, where AI has growingly become part of the conflict, the need is urgent and time-critical (Goncharuk, 2024). This urgency is acknowledged by policy, and it is noteworthy that this stated urgency largely predated the full-scale invasion of Ukraine in 2022 – Only two of these policies make brief mention of the conflict (The Defence AI Strategy [2022] and the Digital Strategy [2022]). The increased use of AI for military purposes in that conflict further heightens the urgency and increases the risk of inaction. There is some degree of real-world alignment with UK government policy among the professionals we engaged with. However, there are also some challenges and room for improvement. Further research in this field, including research engaging with Defence personnel and those with fewer digital skills will be essential in the immediate future.

REFERENCES

Babuta, A., Oswald, M., & Janjeva, A. (2020). Artificial Intelligence and UK National Security: Policy Considerations (RUSI Occasional Paper, p. 57). Royal United Services Institute. Available at: https://rusi.org/sites/default/files/ai_national_security_final_web_version.pdf

Cabinet Office, 2022. National Cyber Strategy. Available online at: https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022

DCMS, 2020. National Data Strategy. Available online at: https://www.gov.uk/guidance/national-data-strategy

DCMS, 2021. Plan for Digital Regulation: Driving Growth and Unlocking Innovation, Available online at: https://www.gov.uk/government/publications/digital-regulation-driving-growth-and-unlocking-innovation

DCMS, 2022. UK Digital Strategy, Available online at: https://www.gov.uk/government/publications/uks-digital-strategy/uk-digital-strategy

Dwyer, A. 2022. A Foundry of Artificial Intelligence? The Case of UK National Security In Romaniuk, S. N., and Manjikian. M. (Eds). Routledge Companion to Artificial Intelligence and National Security Policy. Routledge.

Goncharuk, V. (2024) Russia's War in Ukraine: Artificial Intelligence in the Defence of Ukraine. *International Centre for Defence and Security*, Available at: https://icds.ee/en/russias-war-in-ukraine-artificial-intelligence-in-defence-of-ukraine/#:~:text=Ukrainian%20companies%20have%20developed%20a,and%20support%2C%20target%20identification%20and

Hardy, A. (2024) DDRC Workshop Report, Available at: https://ddrc.uk/wp-content/uploads/2024/06/DDRC-Workshop-Report-w-Front-Page-and-contents.pdf

HM Treasury, 2021. Build Back Better: Our plan for growth, Available online at: https://assets.publishing.service.gov.uk/media/6048fd05d3bf7f1d16e263fd/PfG_Final_Web_Accessible_Version.pdf

McClure, S. (2024a) DDRC Workshops: Emotive Concerns Surrounding Data, Available at: https://ddrc.uk/wp-content/uploads/2024/06/Public-DDRC-Workshops-Emotive-Concerns-Surrounding-Data.pdf

McClure, S. (2024b) DDRC Workshops: Idealised Data Surroundings, Available at: https://ddrc.uk/wp-content/uploads/2024/06/Public-DDRC-Workshops-Idealised-Data-Surroundings.pdf

McClure, S. (2024c) DDRC Workshops: Concerns by Sector, Available at: https://ddrc.uk/wp-content/uploads/2024/06/Public-DDRC-Workshops-Concerns-by-Sector.pdf

Morley, J. (2022) An Overview of UK Data Policy Developments, *Bennett Institute, University of Oxford*, Available at: https://www.bennett.ox.ac.uk/blog/2022/07/bennett-

insights-an-overview-of-uk-data-policy-developments/

Payne, K. (2024). Bright Prospects, Big Challenges: Defence AI in the United Kingdom. In *The Very Long Game: 25 Case Studies on the Global State of Defense AI* (pp. 85-105). Cham: Springer Nature Switzerland.

Roberts, H., Babuta, A., Morley, J., Thomas, C., Taddeo, M., & Floridi, L. (2023). Artificial intelligence regulation in the United Kingdom: a path to good governance and global leadership?. Internet Policy Review, 12(2), 1-31.

TASS. (2024) Top Russian Defence Official Lists Four Conditions for Success in Confrontation with the West, *TASS*, Available at: https://tass.com/defense/1827831

UK Cabinet Office, 2021. National Resilience Strategy, Available online at: https://assets.publishing.service.gov.uk/media/60ed4b288fa8f50c7ba9b46d/Resilience_Strategy_-_Call_for_Evidence.pdf

UK Department of Defence Science Innovational & Technology, 2022. National AI Strategy, Available online at: https://www.gov.uk/government/publications/national-ai-strategy

UK Ministry of Defence, 2022. Defence artificial intelligence strategy. Available online at: https://www.gov.uk/government/publications/defence-artificial-intelligence-strategy/defence-artificial-intelligence-strategy

Yanow, D. (2007). Interpretation in policy analysis: On methods and practice. *Critical policy analysis*, *1*(1), 110-122.

APPENDIX:

A1: List of workshops conducted.

Organisation	**Location**	**Date**
Government Office	Newcastle Upon Tyne	21/8/23
Civil Service	Newcastle Upon Tyne	27/9/23

Civil Service	Newcastle Upon Tyne	27/9/23
Civil Service	Newcastle Upon Tyne	27/9/23
Consultants	London	30/11/23
Consultants	Bristol	12/10/23
Consultants	Bristol	12/10/23
Consultants	Middlesbrough	16/11/23
Non-Profit	London	9/8/23
Non-Profit	London	4/10/23
Non-Profit	London	6/11/23
Civil Service	Edinburgh	9/10/23
Civil Service	Edinburgh	10/10/23
Data Study Group	Exeter	12/09/23
Data Study Group	Exeter	12/09/23
Data Study Group	Exeter	12/09/23
Manchester City Council	Manchester	11/08/23
Manchester City Council	Manchester	11/08/23
Naimuri	Manchester	23/08/23
OAP	North Wales	01/11/23
SME	Merseyside	01/10/23
SME	Exeter	04/09/23
University of Exeter	Exeter	13/09/23
University of Exeter	Exeter	13/09/23
University of Exeter	Exeter	13/09/23
University of Liverpool	Liverpool	16/08/23
Government Office	Portsdown West	10/08/23
Government Office	Portsdown West	10/08/23
Government Office	Portsdown West	21/08/23
Government Office	Portsdown West	21/08/23

Government Office	Porton Down	06/11/23
Government Office	Porton Down	06/11/23
Government Office	Porton Down	06/11/23

A2: Workshop tasks

Differentiated Shared Task Questions	**Consistent Framing Questions**
Working as a team, build a mode of data privacy concerns in your organisation.	Thinking about your day-to-day work activities that involve data, what is convenient and inconvenient? Can you visualise a time at work when you had difficulty accessing critical data you needed for your job? Has there been a time when your data has been compromised at work? Have you experienced concerns about who has access to your organisational data?
As a team, build what comes to mind when thinking about the value of data in achieving organisational success.	
As a team, build what comes to mind for improving digital technology management in your organisation(s).	
Working together, build what comes to mind for raising awareness of data risks in your organisation(s).	
As a team, build a model of how opportunities in data management can be pursued.	
Working together, build what comes to mind when you think of a data-driven organisational culture.	
Working together, build a model of possible barriers to accessing data needed for organisation success.	
Working together, build a model that expresses concern for the confidentiality and the integrity of organisational	

A3. Policy Documents Analysed

Policy Document	**Year of Release**	**Governmental Department**
UK National Data Strategy	2020	DCMS
UK National AI Strategy	2022	DSIT
National Resilience Strategy	2021	Cabinet Office
Plan for Digital Regulation	2021	DCMS

UK Digital Strategy	2022	DCMS
‘Build Back Better’ Plan for Growth and Innovation	2021	HM Treasury
National Cyber Strategy	2022	Cabinet Office
UK Defence AI Strategy	2022	Ministry of Defence

DDRC
DEFENCE DATA RESEARCH CENTRE

Contact Information:

Dr Alex Hardy, DDRC, University of Liverpool
Alex.Hardy@Liverpool.ac.uk

Disclaimer:

Acknowledgments:

Funding Information:

2024ESAE025