CYBERSECURONOMICS

Cybersecurity and Labour's Modern Industrial Strategy

Progressive Britain Paper PB007

September 2023

PROGRESSIVE BRITAIN

FEPS FOUNDATION FOR EUROPEAN PROGRESSIVE STUDIES

LFP Labour Foreign Policy Group

AUTHORS AND PROJECT LEADS

ANDREW PAKES

Andrew Pakes is Deputy General Secretary and Research Director at Prospect Union where he co-ordinates the union's work on digital technology and the future of work with an interest in how economic change impacts workers.

FREDERICK HARRY PITTS

Frederick Harry Pitts is Senior Lecturer in Politics at the University of Exeter's Cornwall Campus in his hometown of Penryn. He is a Co-Investigator of the Economic & Social Research Council Centre for Sociodigital Futures.

This paper forms part of the Foundation for European Progressive Studies/ Progressive Britain project, 'Security at Work in an Uncertain World'.

CONTENTS

PROGRESSIVE BRITAIN

FEPS
FOUNDATION FOR EUROPEAN PROGRESSIVE STUDIES

Labour Foreign Policy Group

CYBERSECURONOMICS

CYBERSECURITY AND LABOUR'S MODERN INDUSTRIAL STRATEGY

1. Executive Summary

The digital transformation of our work and everyday life offers substantial benefits but entails great dangers. Every day we are better connected – to opportunities and to threats. The recent cyberattacks on the Electoral Commission and the Foreign Office – likely conducted in association with state adversaries – highlight just how dangerous these threats can be to the security of our society and political system..

Business and society have become more dependent on cloud computing, connected devices and digital monitoring to manage the post-pandemic reshaping of the places and spaces of work and commerce. So-called 'smart cities' and 'connected places' represent a further digital frontier being pushed at by central government and some local authorities.

At the same time, technology has become a battleground in the emergent cold war between the West and an authoritarian axis led by China and Russia – one that is increasingly comfortable operating in a grey zone of digital disruption, espionage and interference.

This generates new risks at multiple levels of everyday life, running the gamut from company networks and financial transactions to supply chains and critical national infrastructure. Cybersecurity is typically posed as the answer[1].

The importance of cybersecurity to the UK's defence and socio-economic resilience is reaffirmed in the government's 'refreshed' Integrated Review 2023.[2] Ensuring the safety of businesses, communities and infrastructure in the cyber domain is presented as one of the main priorities of UK defence and national security policy, and the UK's cyber power is presented as an existing source of strategic and competitive advantage.

But in a constantly escalating cyber arms race this strong position cannot be taken for granted. In the shadow of Russia's illegal invasion of Ukraine the review recognises the need to commit greater fiscal resources to defence and national security. This includes 'information operations and offensive cyber tools' that enable the UK to deter and ultimately defeat enemies in the cyber sphere as a distinct domain of conflict alongside conventional theatres like land, sea and air.

However, in terms of specific support for cybersecurity there is little in the Integrated Review refresh that goes beyond previous documents like the 2022 National Cyber Strategy.[3] This is particularly concerning as the UK recently dropped a place in the Harvard Cyberpower Index.[4] From opposition it is Labour's task to acknowledge where gains have been made and develop a plan to build upon them where more can be done to preserve and bolster the UK's cyber-status.

And there have been some considerable policy achievements by previous governments on this front – the creation of the National Cybersecurity Centre (NCSC) as a transparent mediator between the state and business being one of them. The NCSC is involved in a growing number of initiatives addressed to businesses at all levels, such as providing exercises that enable firms to experiment with their response to a cyberattack, as well as advising government on implementing new rules on 'secure by design' standards for tech products bought and sold in the UK, for instance.[5]

Labour's first step in this space, its 'new settlement for the digital age' – to be fleshed out further in a forthcoming green paper – promises to upskill workers and citizens in order to build a greater degree of 'cyber resilience and security against rogue states and actors'.[6]

The Party's Start-Up Review, meanwhile, shows the party is thinking about how to use government to create a positive regulatory, investment and procurement environment for innovative new businesses in the digital sector.[7]

Its Council of Skills Advisors' Report lays important groundwork for an all-encompassing skills policy that uses common national standards to codify quality training provision in crucial digital domains like cybersecurity.[8]

Knitting these policies together, recent speeches by the Shadow DCMS and Science, Research & Innovation teams speak of an ambition to use regulation to underpin greater trust in digital technologies as a platform to democratise access, generate innovation, and bolster the competitiveness and resilience of SMEs.[9]

The implied and explicit critique of Conservative initiatives is that they are insufficiently ambitious and lacking in commitment to the potential role that a positive, robust regulatory environment can play in stimulating and attracting business investment.[10]

Labour is seeking to go further than the government's AI white paper by requiring licensing for AI innovations rather than simply expecting individual entities and sectors to regulate themselves. This may imply the creation of a single AI regulatory body.[11] There is also talk of plans to reform government tech procurement to introduce greater consideration of sovereign capability and national resilience into how products and services are contracted.[12]

However, there is a danger that policy development in this area ends up being subsumed within the somewhat separate threat landscape of general purpose AI, or else within a generic offer on the digital economy. Whilst related to the dangerous acceleration of AI capability, we argue that cybersecurity should be treated as a distinctive focus of policymaking that bridges a number of domains of government – namely defence, foreign and industrial policy – associated with the period of manifold geopolitical and economic upheaval some have termed the 'polycrisis'.[13]

In response, this paper outlines how Labour, in opposition and in government, can bolster the UK's national capacity in cybersecurity in line with the framework set out in the 'securonomics' agenda the party is advancing, and in particular its 'modern industrial strategy'.[14]

Industries like cybersecurity fit within a major priority area of the modern industrial strategy, 'sovereign capabilities'. These provide the secure and stable access to digital networks and other utilities that underpin everyday life and guarantee safe conditions for business and investment in Britain.

These sovereign capabilities are particularly vital when it comes to the provision and protection of critical national infrastructure. But as many of the infrastructure and skills that represent our sovereign cyber security are in private hands, the modern industrial strategy suggests that the safety of the country and economy is threatened by the possibility of investment risk, market failures and foreign takeovers.

It is recommended that these industries cannot be left to the private sector alone, demanding that the state acts as a partner, using regulatory controls, strategic procurement and R&D spending to incentivise good decision making and firm behaviour among the owners and operators of critical infrastructure.

At its best, government investment and regulatory intervention in cybersecurity has the potential to help level up regional inequalities in accessing the skills, finance streams and markets associated with success in such sectors. Through this, we conclude that the cyber sector can help a future Labour government construct a positive relationship between economic security, national security, and better and more secure work, across the UK.

We conclude that, just as Labour's underpinning 'securonomics' agenda borrows from Bidenomics in the US, Labour can learn much from the Biden administration's own National Cybersecurity Strategy.[15] From the creation of a dedicated Minister for Cybersecurity, to greater financial support for domestic postgraduate degrees.

Some of the key recommendations we make are as follows (see main text for full references and sources):

Cybersecurity, innovation and industrial strategy

- Labour's 'Make, Buy and Sell More in Britain' agenda provides the opportunity to promote procurement of bespoke proprietary cyber products and services designed and delivered in collaboration with preferred British suppliers.

- Public procurement under a Labour government could also follow the example of some private sector pioneers in compelling contractors to conform to the Cyber Essentials standards set out by the NCSC, as a way of driving wider behaviour change.

- Labour's National Wealth Fund should provide a policy context for state backing in risky investments in the cyber sector, with the promise of a return to the taxpayer for successful ventures.

- UK governments can learn from the likes of France and the US, in developing strong policies to use state procurement procedures to privilege domestic cyber firms and provide venture capital where markets are not forthcoming.

- A Labour government should build upon the National Security and Investment Act and forthcoming Product Security and Telecommunications Infrastructure (Product Security) Regime, using them as a means to bolster constraints on the participation of foreign capital in national markets for cyber goods and services.

- Where there is a national security rationale, the UK should follow peer cyber powers in the EU and US in limiting the participation of domestic cyber firms in global markets. Greater clarity is needed as to how robust or successful the UK's Cyber Security Export Strategy has been in registering risks on the position of UK cyber companies and products in global supply chains.

- A narrowly protectionist approach could prevent the UK developing the flows of knowledge, labour and capital that stimulate growth in the cybersecurity sector and enable scaling up in cyber enterprises, and a system of independently competing national cybersecurity systems could create regulatory gaps allowing corporate arbitrage or manipulation by malign actors. Alongside the strengthening of sovereign capability, then, international trade and cooperation with trusted allies will continue to be indispensable to national security in this domain.

- Overseas provision of cybersecurity products and training is an emergent source of trade opportunities and soft power in the developing world and enables the UK to project values of openness and human rights in the cybersphere. Alongside the provision of conventional military means the UK-Ukraine Cyber Programme has made a unsung contribution to British solidarity against Russia's aggression, protecting governing institutions and critical infrastructure from cyberattack. The £100m spent on building cyber capacity in allied countries since 2021 should be seen as only a baseline for what can be achieved in this space.

- As part of the UK's cyber soft power on the world stage, the NCSC should be promoted overseas as a partner in international and industrial collaborations aimed at defending democracy against the threats posed by cyber interference, influence and misinformation.

- Fields like cryptography are specific areas where the UK must possess independent capacity, in a similar way that sovereign capability in steel production is central to the capacity to scale up defence manufacturing in the event of conflict.

- Labour should continue developing plans to support firms through processes of reshoring, insourcing and re-localisation of production, which can help safeguard against weak cybersecurity links in complex global supply chains.

- Greater support is also needed to ease firms through the transition to a safer digital economy where every company in the UK can draw upon appropriate local cybersecurity expertise. Tech UK's recent UK Tech Plan outlines relevant areas around skills, reform of the Apprenticeship Levy and future skills that complement Labour's existing thinking. This demands a broad and widely distributed skills base.

- The UK still invests far less in cybersecurity research than peers like the US, France and Germany, whose well-funded sectors subsequently attract the capital and talent the UK needs. Redressing this requires long-term funding of R&D based on state brokerage of more, better and stronger university-industry-government partnerships.

- In opposition Labour should monitor carefully how much of the new R&D spending announced in successive Integrated Reviews will be committed to cybersecurity.

Cybersecurity, corporate governance and critical infrastructure

- Thought should be given to how critical infrastructure is defined as geopolitical and technological trends increase the importance and mutual implication of diverse areas of social and economic life and supply chains become more and more complex. This redefinition should be used as the basis for universal expectations on cybersecurity enforced with regulation, to address the shortcomings in individual owner/operator responses.

- All new infrastructure and businesses over a certain size should be encouraged or compelled to have cybersecurity capability and capacity-building hardwired into their structure and constitution from day one, rather than having to play catch up when challenges arise.

- In revising the Network and Information Systems Regulations and elsewhere, it is important to strengthen the regulation not only of hardware but also of software – with the US and EU demonstrating possible approaches.

- Labour should argue that the UK, via the NCSC, should follow EU member states in seeking to ban products and services delivered by entities like Kaspersky, who have a relationship with the Russian state. A light-touch approach of asking that firms reflect on procurement choices is insufficient.

- There is the need for a review of whether specific regulatory institutions that oversee critical national infrastructure like energy, nuclear, telecoms, finance and transportation have sufficient power to impose cybersecurity requirements on their members.

- Too much of the UK strategy still rests upon placing limited 'expectations' on providers of the critical national infrastructure. Higher standards are needed. The content and consequences of incentives need to be made clearer, and backed up by regulatory force in order to prevent a 'race to the bottom' on cybersecurity as companies seek cheap and quick ways to avoid investing properly in the future.

- Too few firms seek cyber insurance and insurers are creating more restrictive policies. In government Labour should work with the NCSC, insurers and business to harness and extend insurance as a spur and incentive to cybersecurity. In this, they can learn from US initiatives to explore a federal backstop for cyber insurance.

- In government Labour should look carefully at recent recommendations to harness the UK's largely unregulated ecosystem of small IT contractors as a driver of better cyber hygiene. This could be done through the closer accreditation and regulation of IT companies, with compulsory certification via the NCSC Cyber Essentials scheme a condition of operating. Grants, modelled on similar schemes in Finland and Germany, could be offered to those companies that cannot meet the cost.

- Uptake of the Cyber Essentials scheme could be bolstered by partnering with professional and trade bodies to make certification a condition of membership.

- Consideration should be given to the constrained character of the revised NIS Directive as currently stated, which would only apply to companies over 50 employees and thus miss a vast majority of the firms operating in the IT sector, which tend to be micro or small businesses.

Cybersecurity jobs, skills and workforce development

- The lack of financial support available for Masters degrees make them unaffordable for domestic applicants, and many of our leading cybersecurity Masters serve international markets instead. Industry certifications are also expensive. Labour should consider greater government financial support to aid upskilling.

- Cybersecurity capacity should be increased from the ground up through early-career apprenticeships embedded in a specific industrial setting, or part-time sponsored Masters programmes for mid- and later-career professionals to upskill in cyber and bring their expertise back to their companies.

- The new government-funded Cyber Security Council should consider how to resolve these material barriers, with affordable provision of part-time postgraduate programmes a possible place to start. In particular, consideration must be given to offering ways for workers to transition into cybersecurity from diverse careers and industries, in order to ensure specific needs are met in areas like critical infrastructure.

- To effectively distribute cyber skills across the workforce rather than concentrate it solely in specialist roles, training should be improved for existing staff (including, where necessary, government support for third-party provision) and to give the future workforce a head start, cybersecurity awareness should be embedded in apprenticeships, degree apprenticeships and other professional qualifications.

- A Labour government should learn from comparator countries about how best to develop the cyber workforce, although the global character of the labour market and the shortages therein demand collaboration and cooperation with allies.

Cybersecurity and regional economic rebalancing

- Existing examples of successful public sector relocation should be emulated in schemes such as the National Cyber Force in Lancashire. More consideration should be given to how public sector relocation has helped grow regional skills and recruitment through apprenticeships and other means. The BBC's regional relocations could be one such case.

- New cyber clusters should be established in strategic locations and existing clusters strengthened. This needs to be beyond existing concentrations of cyber labour and capital, to grow regional capacity and improve access to local networks of knowledge and expertise.

- Rural businesses face particular challenges with accessing networks and clusters of cybersecurity skills and expertise to repel threats. Interlocking global crises are placing a new importance on foundational sectors like agriculture, space, maritime, renewables and critical metals/minerals. These key elements of critical national infrastructure are both increasingly digitally mediated and represent an increasingly strategically central part of the UK's global role, but often occupy rural and coastal areas with a lack of local cybersecurity capacity. Particular attention should be given to baking in cybersecurity as an underpinning principle of how new enterprises operate in these regional contexts.

- In developing a UK-wide strategy attuned to the specificities of its regions, Labour should learn from the Welsh Government's Cyber Action Plan, which sets out a plan for the devolved nation to expand cyber ecosystems, talent pipelines and resilience across the Welsh economy and public services, among other likeminded initiatives emerging from Wales.

Cybersecurity and political oversight

- There is a need to formalise and consolidate cybersecurity at the level of cabinet and government roles. A Labour government should give further thought to how relevant ministerial and National Security Advisor remits and roles can best be combined or distributed to effectively and democratically govern cybersecurity operations in the UK as a specific domain.

- Appoint a dedicated senior Minister. Labour could learn from its allies in the Albanese government in Australia, which has appointed a specific Minister for Cybersecurity. In the UK, cyber has fallen within the varied remit of ministers first in DCMS and now in the new Department of Science, Innovation & Technology. The latter move has produced more specific messaging and communication around cyber, but the minister responsible is a hereditary peer and thus much scrutiny occurs within the context of the Lords. Stronger definition and prioritisation of the role would help bolster oversight of a domain that straddles different departments beyond DCMS and DSIT.

- The government's recent Integrated Review refresh follows the latest cyber strategy in setting deadlines of 2025 to 'significantly harden' the state against cyberattacks and 2030 to render the public sector resilient against vulnerabilities. Considering the current threat landscape, Labour should push for greater haste in meeting these targets.

- Whilst the National Cyber Force has begun to bring clarity to the country's cyber operations, the current Conservative government has shown insufficient ambition and detail in defining the UK's role as a 'responsible cyberpower'. Labour should call on the current government to continue working internationally, as well as domestically, to build consensus about rules and norms of cyberwarfare in line with liberal democratic values and human rights.

- Labour should also have its own plans for government in order to bring transparency and clarity to the costs and consequences of offensive operations.

- Collaborative intelligence links with trusted partners and allies are central to the confident attribution of responsibility necessary to robustly punish transgressions and maintain deterrence.

- Rather than the threat of conflict confining cybersecurity spending and resourcing to conventional defence functions (e.g. in the Ministry of Defence), the kind of 'whole of society' approach model proposed for the Defending Democracy Taskforce in the Integrated Review refresh should be expanded under a Labour government to underpin as much as possible of the country's cybersecurity effort, spanning government, business, civil society and communities.

2. Introduction

As we have argued in a series of papers and reports for Progressive Britain and the Foundation for European Progressive Studies, the Labour Party's emergent policy agenda connects local, national and global challenges through the concept of security[16]. This cuts across economic security, national security and security at work.

Through a series of roundtables with social democrats and trade unionists in other European countries, we have also found that the concept resonates elsewhere within multiple public policy domains, especially in the context of what in Germany is labelled Zeitenwende – a historic shift in foreign affairs sparked by the illegal Russian reinvasion of Ukraine, with vast domestic implications.

Since then, the importance of security has been reaffirmed in a substantial paper by the Shadow Chancellor Rachel Reeves MP bringing together the various threads of the programme of economic stabilisation and renewal Labour has been outlining over the course of the past few years. 'Securonomics' is the term used to capture this vision.[17] [18]

The concept connects recent speeches from across the frontbench: the overarching vision of a future Labour government presented by Leader of the Opposition Keir Starmer KC MP, the strategic global reset put forward by the Shadow Foreign Secretary David Lammy MP, the commitment to sovereign defence manufacturing capacity set out by Shadow Defence Secretary John Healey MP, and the 'Modern Industrial Strategy' unveiled by Shadow Business Secretary Jonathan Reynolds MP.

The latter intervention is particularly important. Taking forward the party's 'Buy, Make and Sell More in Britain' policy, the modern industrial strategy sets out how Labour sees the UK economy surviving and thriving in a new age of geopolitical conflict and systemic competition over technology, resources and supply chains.[19]

In particular, the document articulates a new role for government based on addressing market failures through state intervention and brokering social partnerships between business and workers via new institutional frameworks. However, whilst the modern industrial strategy is clear-sighted in the need to adopt a defensive posture in protecting the economic foundations of our sovereign capabilities and critical infrastructure, a key aspect of these – cybersecurity – in which the UK already excels receives only a passing mention.

At the moment Labour's policy development in this area is in danger of being subsumed within the somewhat separate threat landscape of AI. Whilst related to the dangerous acceleration of AI capability, however, cybersecurity should be treated as a distinctive focus of policymaking.

Cybersecurity already forms a major priority area in the government's Integrated Review, recently refreshed for 2023. Subject to some important tweaks in light of the deteriorating geopolitical picture, insights and initiatives from the Integrated Review will likely continue resonating through government long after the current administration is gone, including in how a future Labour government approaches defence and national security. According to the refresh, cyber represents one of a number of overlapping 'strategic arenas' characterised by systemic competition taking place both 'above and below the threshold of armed conflict'. Across the piece, new technology shapes and in some cases defines these strategic arenas.

The new Integrated Review presents investment, export controls and data localisation as examples of how digital and information technologies are experiencing strategic realignment in a period where the global order is fragmenting in favour of protectionism, 'onshoring' and 'friendshoring'.

Cyberspace is listed as one of the domains where national interest will be prioritised against a difficult backdrop contoured by 'geography, the allocation of resources, regional and international architectures, rules and norms, and the relative balance of economic, military, diplomatic and cultural power'. However, on the specific implications of this for cybersecurity, scant further detail is offered additional to that presented in previous documents like the 2022 National Cyber Strategy and the National Security Bill being put forward to more closely regulate the country's interactions with potential systemic rivals. As the geopolitical stakes shift for the worse and outpace the capacity to act, this creates a gap for Labour to fill.

In this briefing we use cybersecurity as an industrial case study of where some of the main threads of Labour's modern industrial strategy meet, and, more broadly, how the different meanings of 'security' central to the party's emergent policy agenda combine in practice.

Cybersecurity shows how Labour's new agenda on economic and national security can provide a basis to hold government to account on those aspects of current strategy and policy that work well; and provide a better alternative where the government is incapable of brokering relationships and governing the economy.

Moreover, it is a sector that speaks to precisely the condition of 'weaponised interdependence' around digital technologies pivotal to the new foreign policy David Lammy outlined in his recent speech to Chatham House. In the current 'age of unpeace', as Mark Leonard puts it, connectivity itself becomes a source of conflict, with the contest for cyberpower a crucial part of what some see as a 'new cold war' that intertwines business, economy and working life with wider processes of geopolitical competition.[20] [21]

In this competition for global power, ideas and policies matter too, and not just material advantage. The internet and how it is used are intimately entwined with values and ideas of how society should be organised. Each model – from the libertarian laissez faire data market of the US's Silicon Valley; the surveillance and security architecture of China's closed cyberspace; what Leonard calls the 'bourgeois internet' the EU has attempted to establish, policing conduct through privacy laws; to the sphere of active disinformation and hybrid warfare propagated by Russia – reflects something about that society. Where the UK stands in this has been given some thought in the government's Integrated Review, which proposed to have liberal democratic norms and values running through the technological innovations produced by the UK's cyber industries.

Informed by these different moral and political worldviews, the ability to set rules and regulate new technology is a core area of advantage to players for global power in this age of unpeace. China is actively leading attempts to govern the implementation of new technologies like 5G and AI so as to grant its national state-capital competitive advantage worldwide, including in rival countries. As social media divides the internet into separate spheres around competing nationalisms, ideologies and versions of the truth, these tendencies all make cyberspace not simply a field of connections, but of conflict and fragmentation, shaping 'the flow of ideas, intellectual property and patents', as Leonard puts it.

Pivotal here is cybersecurity, where the two main global actors, leading their own sometimes loose blocs of other allied states and state-aligned groups, are the US National Security Agency and China's Ministry of Public Security. This defence and national security struggle reverberates through the corporate world as the West and China pit their own tech giants against one another in the market for hardware (e.g. chips and 5G) and software (AI, platforms, data, algorithms).

In the age of 'Global Britain' the actions of these major countries mean even the generally pro-competition UK government is belatedly recognising challenges around technology takeovers. NVIDIA (a US company) was effectively blocked by regulation from taking over ARM and Huawei has been explicitly, banned from a role in the 5G rollout.

From the perspective of those charged with protecting the UK's national security, the cyber risk this terrain entails poses a threat not only to privacy or intellectual property, but also to human life and the functioning of society and state. An example is the Russian cyberattack on UK businesses and public sector organisations in 2017, which disrupted NHS systems causing appointment cancellations, a forced return to analogue recordkeeping and ambulance diversions as hospitals struggled to accommodate emergency admissions amidst the chaos.

This is only a glimpse of what state or state-aligned hackers could achieve were they to target the National Grid, the Trident submarines or the UK banking system. The stakes of such a scenario were brought to greater public attention in the recent Channel 4 drama series The Undeclared War, where a Russian cyberattack on BT is augmented by a campaign of social media disinformation designed to erode public trust.[22]

The battle for cyberpower, characterised by the spiral of imitation and competition that characterises conflict in the era of connectivity, means that the West is increasingly compelled to create its own version of the 'big security' Xi Jinping espouses in China, whereby national security is recalibrated away from a narrow focus on conventional armed force to a focus on how enemy actors can manipulate interdependence in every aspect of society and everyday life, such as telecommunications, media, the financial system, industry and supply chains. One of the key outcomes of this will be to drive the regulation of cyber, 5G, AI, semiconductors and so on, in such a way as to ensure that Chinese state-backed firms fall afoul of guidelines on privacy and other issues, facing barriers to trade, competition and expansion beyond their immediate borders.

These risks, and the desire for a kind of 'big security' by way of response, are undoubtedly being registered by government. The Integrated Review 2023 emphasises the threat posed by the Chinese Communist Party to the UK's critical national infrastructure and other areas, with cybersecurity presented as a key part of defending against the risks of weaponised interdependence in these domains. But, we argue here, a Labour government can do much more.

Across these different but increasingly interconnected policy areas, we show that the case of cybersecurity is indicative of Labour's capacity to leverage two important narratives ahead of the next election. The first is that Labour are now strong on security and can today be trusted with the safety of the country and our partners overseas. The second is that Labour supports jobs, skills and industry guided by, if not necessarily beholden to, the principle 'buy, make, sell in Britain'.

Cybersecurity is at the core of Britain's future economic and national security. It sits across military, intelligence, infrastructure and business in ways that both suit and challenge the UK's strengths and pose challenges for government policy in the new era of global unrest since the Russian invasion of Ukraine. From the likely state-sponsored Russian cyberattack on organisations including the NHS, to the danger of investment by Huawei in digital infrastructure, to British business struggling to access digital skills and invest in security, and most recently concerns about the use of TikTok on government mobiles, the issue speaks to a diverse range of issues that are nevertheless related, and critical to get right in government.

The cybersecurity sector has the seeds of a positive national success story, representing a good test case for the kind of state-market collaboration Labour seeks to pioneer in government:

- UK fourth-placed cyber power in the world according to the Harvard Cyberpower Index 2022.[23]
- 14.1% growthin UK cybersecurity market in 2021, double that witnessed in 2020.[24]
- The sector comprises 1,979 firms employing 58,005 staff.[25]
- Added 5,300 new jobs in 2022, up 10% on 2021, increasing GVA per employee.[26]

- A concentrated industry, with the 8% of cybersecurity firms classed as 'large', including dedicated arms of companies like BAE and BT, making up 75%[27] of the total revenue of the sector.

- UK is the third-placed exporter of cyber security services and expertise worldwide, particularly to governments and leading corporates, although most sales of cybersecurity solutions are domestic.[28]

However, an unravelling geopolitical picture means the UK cannot rest on its laurels. From 2020 to 2022, the UK slipped a place from 3rd to 4th in the Harvard Cyberpower Index.[29] Tellingly, the rival state that overtook the UK was Russia. The UK needs to do much more to bolster cybersecurity as a foundation of national defence, resilience and prosperity in the more dangerous context produced by Russian aggression and the actions of other authoritarian states and groups. The capacity of the state to recruit business and civil society to the cause of cybersecurity is complicated by the conditions of inflation and economic uncertainty which, government evidence suggests, are seeing firms prioritise staying afloat over monitoring and reporting cyber breaches.[30] If the state and country as a whole are not secure, then the economy and society are not secure in turn. And if the economy and society are not secure, from the marketplace and the shopfloor upwards, then the state and the country as a whole are not secure either.

In this context, it is questionable whether the current government have the capacity to rise to the occasion. Ideologically, the Conservatives struggle to grasp the state-business collaboration that is needed to bolster cybersecurity, preferring command and control in the intelligence sphere while leaving infrastructure to the markets.

With government keen to signal spending cuts, an aversion to serious investment in defence and industrial capacity may even risk some of the recent gains from successive government strategies. There is a danger that the next year or so, prior to any election, sees the government embrace a less interventionist and strategic orientation towards industrial policy and a more hands-off attitude with reference to regulation.

This process may have already begun, with the abandonment of the Industrial Strategy and the stripping of its name from the government departmental structure in the most recent reshuffle. The policy reorientation concealed within the superficial shift in Conservative leadership could have unintended spillovers that harm our national security at a time of war.

3. Cybersecurity, innovation and industrial strategy

Articulated across the shadow frontbench, Labour's emergent agenda suggests that security[31] is the key building block for a prosperous economy, and a prosperous economy key to security in turn, underpinned by a new focus on defence in the context of European war. The fundamental role of cybersecurity within this means that the sector should not be seen as unprecedentedly novel, or outside the norms of industrial strategy, but as a key component of future growth, jobs and prosperity.

The current government having previously displayed a fleeting willingness to use state power to support the nation's strategic interests in certain industries, industrial strategy in general has been neglected under Prime Minister Rishi Sunak. What cybersecurity strategies have been issued under recent Conservative governments have each represented attempts to escape the constraints and weaknesses of their own reflexively market-based approach to state intervention and regulation, rather than a joined-up effort to bring public and private together for the sake of national security.

One partial success story comes from the flirtation with industrial strategy experienced under the first two Conservative premierships of the post-Brexit period. In 2016, the National Cyber Security Centre was created to mediate between the private and public sectors and help develop business cyersecurity capacity. It has a particular focus on SMEs, who constitute a majority of companies yet often lack the resources and expertise to protect themselves.[32] Its CyberEssentials scheme certifies SME cybersecurity capacity via a network of assessors.

The NCSC has been generally deemed a success in bringing a more strategic direction to state-industry relations in cyber, although a review is due into how successful other measures such as government incentives have been in driving behaviours.[33] The government's own evidence suggests an unsatisfactory level of uptake of the CyberEssentials standards, possibly because of the pervasive context of cost-cutting and an uncertain investment environment.[34] This reflects a broader underinvestment in cyber driven by rising costs, economic uncertainty and workforce shortages.[35]

Moreover, at present, the NCSC has only an advisory capacity and is not directly involved in developing or offering technological solutions.[36] It has also not yet been tested in the context of a major cyberattack. Despite progress in the UK cybersecurity sector, then, there is still evidence the Conservatives are not meeting the challenge.[37] The 2016 and 2022 national strategies suggest that government will step back when the sector meets expectations and achieves a state of self-sufficiency. But it is unclear, in a field where global competition and intelligence blend, that the private sector can ever become self-sufficient to the extent that the government can step back in such a way.

Despite its successes, the UK still contends with a widely perceived market failure of the private sector to adequately invest in protecting firms against cyber threats, and the labour market failure of insufficiently expanding the cyber workforce skills base in line with new demand for roles. As geopolitical tensions continue to ratchet up, government should level with businesses and voters that continued intervention and investment in cybersecurity will be necessary on the basis that the bar is set much higher, and the timeframe set much longer, for what represents adequate readiness and resilience.

For Labour, to target government and business achieving resilience together is both responsible and pragmatic. The government's approach still uses the power of the state to ultimately cede space to market incentives which do not always neatly align with cybersecurity needs. Despite steps in the right direction, both British security and British business are left in the lurch. Security and economy intertwine in this respect because domestic cybersecurity and cyber-resilience at the national level are the foundtion for the UK's cyberpower on the international stage, and vice versa.

Cyber Industrial Policy

The Integrated Review refresh cites cyber as one area where the current era of 'global volatility' impacts upon 'the daily lives of the British people', principally through the proliferation of threats, scams and attacks. In this context, domestic security and wellbeing is central to the country's global positioning, and vice versa. Hence the Integrated Review stresses the role played by cybersecurity in ensuring domestic resilience.

It states the UK should be 'developing the tools to deter, defend and compete in cyberspace, addressing both our domestic cyber vulnerabilities and supporting partners to build their own capabilities' - in other words, at home and abroad. If the UK's international leadership is the foundation of its national success, and vice versa, then both sides of this mutually reinforcing relationship depend upon a thriving industrial and innovation ecosystem in the UK.

Cybersecurity as a specific sector benefits from the UK's competitive strength in science and technology. But it also serves a wider economic purpose, producing the kinds of multiplier effects that some associate with UK defence spending. Investment in cybersecurity has the potential to create markets for goods and services that will help power industrial renewal in the UK – either directly or indirectly – and shore up trust in the technologies that many see as enabling a more productive and dynamic economy. As data has infused the world of work and industry, cyber risk has increased, but companies have not developed the infrastructure and skills necessary to anticipate and repel the threat generated by novel, untested and often underregulated new technologies.

Every nineteen seconds a firm or organisation faces an attempted hack.[38] 39% of UK businesses experienced a breach in 2021 (a hack being an intentional attack, and a breach an accidental information leak).[39] Crucially, this insecurity prevents companies investing and modernising to become more productive and competitive, and workers from feeling stable and protected from harms in the course of doing their jobs. Any revitalisation of manufacturing in the UK – specifically of the high-tech, high-value kind on which hopes of regional growth are based – will likely deploy new data-driven process technologies such as digital twins that will serve to exacerbate existing risks.

The Integrated Review refresh does not do enough to advance this agenda, with one its few new measures the announcement of a system of 'levers' to ringfence bulk data from being accessed and exploited by rival states and hostile actors. Discussions of strategic advantage, supply chain risk and 'own, collaborate, access' arrangements tend to refer to specific technological areas like AI, quantum, telecommunications and semiconductors rather than particular products and services associated with cybersecurity.

In this context, there are several areas in which government can do more to grow, and in some cases protect domestic cybersecurity capacity.

- Whilst public procurement of cyber products from UK suppliers is clearly increasing and has an important role in sustaining domestic markets, government can still do more to overcome what some in the past have observed to be a reliance on off-the-shelf commercial cybersecurity solutions rather than bespoke proprietary products and services designed and delivered in collaboration with preferred British suppliers.[40] The newly launched GovAssure scheme promises to hold departments to account for their compliance with cybersecurity standards, but the underpinning products and services should be within scope too.[41]

- Public procurement under a Labour government could also follow the example of some private sector pioneers in compelling contractors to conform to the Cyber Essentials standards set out by the NCSC, as a way of driving wider behaviour change.

- Moreover, many of the cutting-edge technologies that may give the UK competitive edge, such as quantum, still represent highly risky gambits for private investors and thus may require government support in the national interest. Labour's National Wealth Fund could provide the policy context for state backing in risky investments, with the promise of a return to the taxpayer for successful ventures.

- In granting such support the UK can learn from other countries, including the likes of France and the US, in developing strong policies to use state procurement procedures to privilege domestic cyber firms and provide venture capital where markets are not forthcoming. France's National Acceleration Strategy for Cyber Security is a good example, contributing a billion euros to the acceleration of cyber innovation and expansion and strengthening of the cyber ecosystem.[42]

- Some of the Conservative legislative agenda on cybersecurity may be left to a Labour government to take forward. At the time of writing, the Product Security and Telecommunications Infrastructure Act, for instance, has been passed but requires further regulation for its obligations on manufacturers, importers and distributors of 'smart' products to fully come into force.[43] Despite their limitations, a Labour government should build upon the Product Security and Telecommunications Infrastructure (Product Security) Regime and the National Security and Investment Act as a means to bolster constraints on the participation of rival states in national markets for cyber goods and services.

- Proximity to China means that counterparts like Australia and New Zealand have developed robust cybersecurity policies on international trade and supply chains which resonate with similar legislative steps the UK has taken in recent years. New Zealand in particular requires regulatory and compliance issues to be addressed at the point of contracting suppliers as opposed to playing catch up after the fact and demands a full security review prior to any change of ownership, mergers or major shareholding shifts – with the threat of exclusion, cancellation of contracts and return of assets and data should structures not meet security criteria.[44] With social democrats succeeding in government in these countries, Labour can look to them for lessons on how to render social democracy cybersecure.

- Where there is a national security rationale, the UK should follow peer cyber powers in the EU and US in limiting the participation of domestic cyber firms in global markets.[45] Greater clarity is needed as to how robust or successful the Cyber Security Export Strategy has been in registering risks on the position of UK companies and products in global supply chains.[46]

- However, a narrowly protectionist approach could prevent the UK developing the flows of knowledge, labour and capital that stimulate growth in the cybersecurity sector and enable scaling up in cyber enterprises.[47] Moreover, a system of independently competing national cybersecurity systems could create regulatory gaps allowing corporate arbitrage or manipulation by malign actors.[48] [49] Alongside the strengthening of sovereign capability, then, international trade and cooperation with trusted allies will continue to be indispensable to national security in this domain. As the US cyber strategy recognises, a level regulatory playing field prevents firms and countries seeking to undercut competitors by skimping on costs associated with cybersecurity.[50]

- Overseas provision of cybersecurity products and training is an emergent source of trade opportunities and soft power in the developing world and enables the UK to project values of openness and human rights in the cybersphere, on the basis that a safer world means a safer Britain and vice versa.[51] Alongside the provision of conventional military means the UK-Ukraine Cyber Programme has made a more unsung contribution to British solidarity against Russia's aggression, protecting government and critical infrastructure from cyberattack.[52] The £100m spent on building cyber capacity in allied countries since 2021 should be seen as only a baseline for what can be achieved in this space.[53]

- As part of the UK's cyber soft power on the world stage, the NCSC should be promoted overseas as a partner in international and industrial collaborations aimed at defending democracy against the threats posed by cyber interference, influence and misinformation.

- At the same time, it is necessary that the UK maintains the adaptability to bolster sovereign capability in the event of intensified tensions with Russia or other adversaries, further strained relationships with European allies or a renewed rightwards isolationist turn in the US. Fields like cryptography are specific areas where the UK must possess independent capacity, in a similar way that sovereign capability in steel production is central to the capacity to scale up defence manufacturing in the event of conflict.[54]

- Trends towards reshoring, insourcing and re-localisation of production enable firms to safeguard against weak links in complex global supply chains.[55] Labour should continue to call for government to help businesses make this transition and make plans to deliver improved support to firms in this transition when in power on the basis of the 'Make, Buy and Sell More in Britain' agenda.[56]

- Greater support is also needed to ease firms through the transition to a safer digital economy where every company in the UK can draw upon appropriate local cybersecurity expertise. If pent-up demand for investment in productivity-raising technologies is unleashed under a more strategic future government, the risks of connected working and trading will increase.

- Whilst generating a broad and widely-distributed skills base is one part of this requirement, another aspect of this is greater investment in R&D and collaboration with academia to develop national industrial capacity that can provide the products and services that offer firms and organisations peace of mind.

- As one example, the National Cyber Strategy proposes to build domestic industrial advantage by means of the production of 'secure by design' microprocessors and other technologies in conformity with cybersecurity standards (something taken forward in the National Semiconductor Strategy). However, despite the promises presented in the Integrated Review and other government strategy documents, the UK still invests far less in cybersecurity research than peers like the US, France and Germany. Rather than markets driving the development of the sector alone, the greater state support offered by these governments attracts the capital and talent the UK needs.[57]

- Whilst relationships with academia have improved in the decade or so since the first strategy, symbolised in the creation of a network of Centres of Excellence, in order to support a national industrial revival there is a need for long-term funding of R&D based on state brokerage of more, better and stronger university-industry-government partnerships.[58]

- It remains to be seen how much of the new R&D spending announced in the Integrated Review and its 2023 refresh will be committed to cybersecurity, and whether this will be commensurate with Britain's aspirations to be a major cyber power. The amount dedicated to cybersecurity will be an outcome of the settlement reached between the research councils and the government. Although precise sums are not offered, the new Integrated Review proposes greater spend on 'information operations and offensive cyber tools' against the backdrop of a more dangerous world. It is implied that much of this spend will be associated with digital transformation in the armed forces themselves, but elsewhere in the review domestic cyber-resilience is rightly associated with a need to expand capacity beyond the Ministry of Defence. Labour should monitor developments on spending carefully.

3. Cybersecurity, corporate governance and critical infrastructure

Critical national infrastructure is a key focus of cybersecurity policy. The integral role it plays in everyday life demands effective protection against cyber threats. Meanwhile, the tendency towards private ownership and complex global supply chains introduces new kinds of risk into our infrastructure. Many infrastructure owner-operators have struggled to keep up with the demands of cybersecurity in a more dangerous world, using off-the-shelf products even as risks multiply with the uptake of 'smart' technologies that are often dependent on supply chains entwined with the industrial capacity of rival states.[59]

Alongside addressing specific outside threats to the infrastructure, the government must also do more to counteract the inside threat posed by ownership and supply by enterprises linked to rival authoritarian states, most notably China. Unlike individual time-limited contracts for service provision or procurement of goods, foreign ownership is hard to undo once established. It can prevent domestic awareness of the full risk profile impacting areas of national infrastructure.

The UK's new approach to foreign takeovers, encoded in the 2021 National Security and Investment Act, suggests a longer notice period is required for potentially contentious foreign direct investment in the digital sphere and specifically in critical national infrastructure, as well as screening of all investment for national security concerns.[60] Steps are also being taken to diversify the supply of telecoms equipment and create domestic capacity to supply infrastructure providers.[61]

However, it is questionable whether the current regulatory frameworks and institutions governing parts of the critical infrastructure have sufficient power to impose cybersecurity requirements on private owners and operators. There is some evidence that company boards are taking a closer interest in rooting out Chinese or Russian hardware and software from their networks and infrastructures.[62] But there has been concern expressed at the highest level of the security establishment that business leaders are not taking cybersecurity seriously enough and must adopt a more 'hands-on' posture.[63] More must be done:

- Thought should be given to how critical infrastructure is defined, as geopolitical and technological trends increase the importance and mutual implication of diverse areas of social and economic life and supply chains become more and more complex. This redefinition should be used as the basis for universal expectations on cybersecurity enforced with regulation, to address the shortcomings in individual owner/operator responses. The US National Institute for Standards and Technology has expanded its cybersecurity framework beyond the typical consideration of critical national infrastructure. The EU has also begun to move away from narrow sectoral strategies with its Cyber Resilience Act, creating all-encompassing regulation that recognises the complexity of contemporary economies. The EU's revised NIS directive, too, imposes robust reporting and enforcement rules on a broader range of companies and industries, which the government should seek to emulate as it develops its own revision of the directive now transposed into UK law.

- In particular, all new infrastructure and businesses over a certain size should be encouraged or compelled to have cybersecurity capability and capacity-building hardwired into their structure and constitution from day one, rather than having to play catch up when challenges arise. This should start from the top down – the US Security and Exchange Commission has set outplans for a policy requiring board members of listed companies to state their cyber expertise.[64]

- There is the need for a review of whether specific regulatory institutions that oversee critical national infrastructure like energy, nuclear, telecoms, finance and transportation have sufficient power to impose cybersecurity requirements on their members. Legislation like the EU's Networks and Information Systems Directive and GDPR, both transposed into UK law, were considered means to incentivise

good practice in line with certain expectations, but have been rarely or toothlessly enforced on the cybersecurity terrain.[65] The Integrated Review refresh proposes to strengthen the 2018 Network and Information Systems Regulations, but in order to understand whether it will help address these issues a greater level of specificity is required.

- Government strategy and forthcoming legislative plans promise to ensure all connected consumer products sold in the UK, and all applications of 'smart' technologies and 'connected places' innovations in UK infrastructure, conform to minimum cybersecurity standards.[66] However, too much of the UK strategy still rests upon placing limited 'expectations' on providers of the critical national infrastructure. Higher standards are needed.

- It is not enough to only seek to regulate hardware – software needs a specific approach. The revised NIS Regulations seem unlikely to include software companies.[67] A more targeted response could be modelled on, or developed in conformity with, President Biden's executive order requiring that a 'Software Bill of Materials' accompany all products purchased in the US, although devolving responsibility for checking those materials to customers themselves.[68] The EU Cybersecurity Act also contains specific provisions on software certification.

- Where the National Cyber Strategy talks of 'incentives' for firms, their content and consequences need to be made clearer, and backed up by regulatory force in order to prevent a 'race to the bottom' on cybersecurity as companies seek cheap and quick ways to avoid investing properly in the future.

- The NCSC has not followed EU member states in planning for a ban on any products and services provided by the Russian regime-linked software security firm Kaspersky, merely recommending that firms reflect on the potential risk of using them.[69] This demonstrates the continuing legacy of a light-touch approach filtered down by successive governments who have failed to adjust to the untenability of the free market in a fragmenting geopolitical order. Labour should advocate for an outright ban.

- Insurance is emerging as a key concern in cybersecurity policymaking. Just as they fail to properly invest in other resilience measures, too few firms invest in specialist cyber insurance to cover breaches and attacks.[70] [71] Insurers, meanwhile, compound matters by writing 'cyberwar exclusion clauses' into policies limiting coverage for attacks by state actors, which as is the case with the adversaries like Russia and China, are often very difficult to directly attribute.[72] In government Labour should work with the NCSC, insurers and business to harness and extend insurance as a spur and incentive to cybersecurity. In this, they can learn from US initiatives to explore a federal backstop for cyber insurance.[73] [74] This would prepare a state response to a cyber catastrophe in advance rather than afterwards, creating a more stable and certain environment for insurers to insure and organisations to access insurance. The EU Cyber Solidarity Act also innovates in this space by laying the groundwork for an emergency response fund to deal with the fallout from a major cyber attack.[75]

Defragmenting security

A recent evaluation of the Cyber Essentials scheme suggests that much participation takes the form of reactive compliance rather than proactive adoption of the principles of cybersecurity.[76] Additionally, there is evidence that NCSC schemes like Cyber Aware and Cyber Essentials still struggle to connect with the UK's fragmented business community.[77]

One of the difficulties in ensuring private sector compliance with cybersecurity provisions is that firms take advice and guidance not from bodies like the NCSC but from the small IT companies they contract for a range of other digital services, products and networks. In particular, firms tend to use the NCSC schemes for general advice but for real-time updates and warnings consult IT contractors.

The IT sector itself faces challenges accessing the right support around cybersecurity – many companies are small or micro-businesses operating in a low-margin and largely unregulated context that addresses a highly local client base, and only a slender fraction of that IT market actively specialises in cybersecurity. Yet they have outsized power in influencing the cybersecurity behaviour of the firms that contract them. A Labour government could thus follow recent recommendations to harness the capacity of this commercial ecosystem to drive good cyber hygiene by improving standards and skills from the bottom up:[78]

- As with so much else in this domain, the capacity of the state to make and improve markets would be central to these efforts. This could be done through the closer accreditation and regulation of IT companies, with compulsory certification via the Cyber Essentials scheme a condition of operating.

- For firms who struggle to afford the cost of Cyber Essentials certification, the same recommendations suggest that financial support is made available to fund means-tested grants in exchange for compliance; this could be modelled on similar schemes found in Finland and Germany which aid small firms investing in cybersecurity. A future government could also further develop plans to bolster the role of NCSC schemes so that they offer not just general advice but specific responses to emergent risks and threats as they arise.

- The expansion of the capacity of the Cyber Essentials scheme to perform such a role could be aided by imposing the requirement to seek certification as a condition of membership of professional and trade bodies like the Chartered Associations and Institutes.

- In terms of small business, these steps would go further than the revised NIS legislation. Whilst the illustrative list of fields subject to the revised NIS includes various IT services, the new legislation is likely to apply regulations only to firms with fifty employees or more, missing the vast majority of enterprises from which many companies receive technical support and advice on cybersecurity.[79] This should be reconsidered.

- The US cyber strategy provides a possible template insofar as it recognises that securing the supply chain is as important as securing individual firms, and has set out plans to identify and address regulatory gaps that do not encourage best practice among third-party cloud and service providers.

All in all, there is a pervasive problem with how and why businesses and other organisations seek to conform to expectations around cybersecurity. The objective of national strategy should be to move beyond mere compliance to develop the UK's own sovereign readiness, responsiveness and resilience in the face of growing cyberthreats. This can only be achieved through partnership between government, the private sector and public sector bodies, such as around investment and skills. The bargain or contract here is that infrastructure providers align with the national interest in exchange for protection by the government, which takes responsibility for deterring and ultimately prosecuting cyberattack. One example of this is state funding for world-leading infrastructure testbed facilities at the University of Bristol, which conduct research and train graduates in anticipating, identifying and repelling cyberattacks.[80]

Such a social contract between state and industry can be the bare minimum the public expect, and proposals to strengthen it represent an opportunity for Labour to talk up the party's security credentials beyond specific debates about spending commitments on conventional military and defence measures. Cybersecurity, like other security considerations, impacts many areas of everyday life in such a way as to suspend some aspects of the cruel calculus of prioritisation that has set in as the fiscal resources at the state's disposal have steadily shrunk.

4. Cybersecurity jobs, skills and workforce development

Through its commitment to social partnership Labour has the potential to anchor cybersecurity as central to its wider vision for 'Securonomics' - meaning broad-based regional economic growth, productivity and skilled jobs.

Unlike in other areas of the economy this represents evolution, not revolution as the current National Cyber Strategy advocates a 'whole-of-society' approach to cybersecurity. The current government has already had some success with specific initiatives like the Defence Cyber Protection Partnership, which brings the state and industry together to render supply chains more secure.[81]

Other governments, like Australia, have sought to place responsibility with different social and economic actors for cybersecurity according to their role.[82] Governments have responsibility for protecting residents, businesses and infrastructure; businesses have responsibility for protecting customers; and communities and users must take necessary steps to protect themselves. One of the difficulties of this kind of responsibilisation for cybersecurity is that workers get left out both as potential subjects of cyber risk and as active participants in combatting it who should be rewarded and protected on this basis.

To realise a truly 'whole-of-society' approach, there is still a need to genuinely integrate other actors and voices such as employees and civil society into the national cybersecurity effort. A Labour government would be well placed to lead this. A posture of readiness, responsiveness and resilience to cyber threat goes hand-in-hand with a more secure economy that generates jobs, skills and growth. This requires social partnership spanning government, employers and, crucially, employees and employee organisations.

The Government's current approach is expressed in the creation of new institutions like the National Cyber Advisory Board, which met for the first time in November 2022.[83] The Integrated Review 2023 provides some further detail on the scheme, which will bring together academics, industry figures and third sector representatives to reflect a 'whole of society' approach to developing the cyber skills base and safeguarding digital supply chains.

However, there is no further light shed on the practical dimensions of the board's work, nor how it will meet the need for a broad partnership to ensure that the whole of the UK benefits from cyber skills and jobs. For example, the board includes private sector representation, but it is unclear whether it will feature involvement from the skills sector, workforce representatives or trade unions.

The UK will not be able to develop global leadership on cybersecurity without a 'whole-of-society' plan for skills and jobs in partnership with industry, universities and employee representatives.

Every organisation, across the economy, is today reliant on digital technologies. Many are dependent on outside contractors for support with cybersecurity. However, in future, in-house expertise will be essential to addressing the growing risk profile associated with cyberthreats. Tougher legislation – necessary and inevitable – will increase the demand for skilled cybersecurity labour across the economy as a whole, and for appropriate expertise across a range of different professional and occupational areas.[84]

Indeed, cybersecurity teams seem to have withstood some of the job losses associated with the tech sector in the current period of crisis, although there is the danger that as costs are cut further cyber capacity could be negatively impacted.[85]

In this context, there are many obstacles to the growth of cyber jobs and skills:

- Although the cybersecurity workforce has doubled in the past four years, 51% of all UK companies report a skills gap that impacts their ability to be more secure and stymies plans to scale up and grow.[86]

- Companies in the cybersecurity sector lose out in the race for talent to other nascent digital industries like big tech and fintech, who effectively corner the market for skilled graduates with the promise of lucrative pay, progression opportunities and less market risk. A particular issue is the 'brain drain' of UK talent to better funded and state protected corporate and research centres in Europe and the US.[87]

- Whilst the government is keen to celebrate the country's expertise in hardware production as a guarantor of cyberpower in domains like semiconductor production, equally important is a specific area where UK industry fails to retain its brightest and best: software security.[88] As an example of what this means in practice, leaking talent to big tech prevents UK industry developing indigenous software that meets the government's 'secure by design' standards, with security issues resolved only when breaches materialise.[89]

- Another area where there is shortage of employees with the right skills and qualifications is the construction of secure systems in critical infrastructure such as factories and powerplants. As new forms of infrastructure emerge – renewables, critical metals and minerals – there is a need to get ahead of adversaries who will seek to surveil and destabilise these industries.

Without generating sufficient new supply of trained staff across the length and breadth of the cybersecurity sector, solving the skills gap in these specific cases would simply displace the deficit to other occupations within the industry. The skills gap therefore requires careful policymaking and coordination addressed to specific situations. There is existing work ongoing to solve the skills gap in a systematic fashion:

- The Cyber Security Council, a government-funded professional body, has begun mapping career pathways in cyber.

- The National Cyber Security Centre accredits Masters programmes and other qualifications so that industry have certainty that applicants for jobs have the right skills

- A university-industry-government initiative, the Cybersecurity Body of Knowledge (CyBoK), brings together data and listings about available courses of education and skills certifications in the sector.

Current government support on training and education aims to direct or divert individuals into specialised career paths in cybersecurity. However, in order to address the specific needs of critical infrastructure for capacity in security analysis and systems-building, specialist undergraduate and postgraduate programmes alone are insufficient. The needs of infrastructure providers would be equally well satisfied by training routes that bring a cyber dimension to existing roles whilst retaining sector-specific knowledge:

- This could take the form of early-career apprenticeships embedded in a specific industrial setting (building on those already offered by the Institute for Apprenticeships and Technical Innovation) or part-time sponsored Masters programmes for mid- and later-career professionals to upskill in cyber and bring their expertise back to their companies.[90] The new UK-US Defence Cyber Academy provides a model for specialist postgraduate training underpinned by government support that could be extended to other fields and sectors.[91]

- One model for skills provision is the SANS Institute's Upskill in Cyber programme, which provides certified ten- or fourteen-week intensive training enabling participants to quickly move into cyber roles

from non-cyber backgrounds, with a focus on redressing regional gaps and inequalities.[92] This could also mimic, for individual employees, the three- or twelve-month intensive programmes the NCSC offers for start-up enterprises in a public-private partnership with Plexal.[93]

- Postgraduate education in particular is vital for the talent pipeline. However, the lack of financial support available for Masters degrees make them unaffordable for domestic applicants, and many of our leading cybersecurity Masters serve international markets instead. Industry certifications are also expensive. Labour should consider greater government financial support to aid upskilling.

- The new government-funded Cyber Security Council should consider how to resolve these material barriers, with affordable provision of part-time postgraduate programmes a possible place to start. Consideration must be given to offering ways for workers to transition into cybersecurity from diverse careers and industries, in order to ensure specific needs are met in areas like critical infrastructure.[94]

- One challenge confronting attempts to expand the cyber workforce through various kinds of learning and training is that the rapidly evolving threat landscape outpaces the capacity of awarding bodies to keep accreditation criteria and curricula up to date.[95] The requires careful thinking about how to institutionalise close and quick feedback loops between practice and the provision of education.

Opportunities to learn on or alongside the job have the potential to improve earning power, enrich job quality and create progression opportunities for workers from a range of backgrounds. To effectively distribute cyber skills across the workforce rather than concentrate it solely in specialist roles, training should be improved for existing staff (including government support for third-party provision) and to give the future workforce a head start, cybersecurity awareness should be embedded in apprenticeships, degree apprenticeships and other professional qualifications. TechUK has put forward useful ideas around digital skills in its recent UK Tech Plan which echo Labour's thinking around reform to the Apprenticeship Levy.

Providing a bottom-up response to the top-down difficulties faced by complex organisations in ensuring cybersecurity, this would distribute cyber expertise across sectors and enable all kinds of workers to acquire the skills needed for a more uncertain future of work. To push this agenda forwards, Labour should follow existing academic recommendations to call for, or implement in government, an audit of strategy for the cybersecurity workforce spanning the departments responsible.[96] There are several cyber workforce growth initiatives found among the UK's allies that a Labour government could take inspiration from:[97]

- Canada has a Cybersecurity Student Work Placement Programme facilitated by its employment and social development body.

- Australia meanwhile, has a large-scale Cybersecurity National Workforce Growth Program based on a range of different points of entry into the profession at all career levels and qualification routes: scholarships, apprenticeships, retraining and continuing professional development provision.

- The US cyber strategy is distinctive in seeking not only regional diversification but a greater representation of 'women, people of colour, first-generation professionals and immigrants, individuals with disabilities, and LGBTQI+ individuals' in the cyber workforce. This suggests that attempts to broaden and diversify the cyber workforce should not stop with just the regional dimension currently targeted by UK policy.

- Moreover, there is a need for cooperation with other countries in workforce development. Issues around workforce and skills development are not confined to the UK alone, but shared in common worldwide. In the context of a competition for talent that is often global in character, more collaboration on this theme could help address the widespread shortage in skilled labour.

5. Cybersecurity and regional economic rebalancing

Due to its strategic character, cybersecurity coverage will inevitably need to have a centralised, national-level dimension delivered through agglomerations of technical and administrative power. However, the fragmented structure of the UK economy, with a prevalence of SMEs and industries ill-equipped to anticipate the new risks they face, economic inequalities between places, and stark regional differentials in access to expertise and infrastructure require interventions at the local level to ensure that everyday support and guidance is evenly spread. Addressing the cyber skills gap and increasing industry's cybersecurity capacity is closely intertwined with the need to 'level up' cybersecurity and distribute opportunities and resources more equitably across the regions.

There are stark size, sectoral and regional differences in the propensity of firms to seek out advice and guidance in cybersecurity. Evidence suggests that, respectively, small businesses, food and hospitality industries and the Midlands are particular areas that need focus to ensure there are no weak links in an economy that is increasingly interconnected in ways that maximise the risk of even the smallest infringement.[98]

One potential response is the recently introduced regional Cyber Resilience Centres, which use partnerships with industry and academia to service the needs of specific geographical areas, enabling access and support for some of the harder-to-reach quarters of the economy. Likewise, 12 newly launched 'cyber clusters' will foster collaboration between various local stakeholders.[99]

The government's Cyber Security Sectoral Analysis also evidences stark regional differences in access to cybersecurity jobs. Although showing some improvement from the 91% recorded in the 2022 Sectoral Analysis, the 2023 figures show that London and the South East is still home to 75% of the investment in UK cybersecurity firms, with eight of the UK's regions registering less than 1% of the total.[100] Labour and the South East are also home to 75% of the country's cybersecurity workforce, marking little change on the previous year's figures. Whereas the mean advertised salary for cybersecurity roles in London is £71,000, it is only £52,200 in Wales.

The government's National Cyber Strategy commits to levelling up these disparities and diversifying the cyber workforce. However, one of its key recent initiatives demonstrate some of the potential challenges this strategy will face. The National Cyber Force will be based in Lancashire and will be home to 3000 personnel by 2030. Academics have raised questions as to the NCF's capacity to engage fully with the local area in terms of developing an adequate talent pipeline for the available roles, and at the same time the potential difficulty of attracting skilled labour to relocate from elsewhere in the UK.[101]

There are several policy measure a future government should consider to overcome these issues:

- Existing examples of successful public sector relocation should be emulated in the design of the National Cyber Force scheme. More consideration should be given to how public sector relocation has helped grow regional skills and recruitment through apprenticeships and other means. The BBC's regional relocations could be one such case.

- New cyber clusters should be established in strategic locations and existing clusters strengthened. One of the main means the state has used to create cybersecurity markets in the UK is industrial clusters that bring together large corporates, SMEs, start-ups, universities and local authorities with streams of skilled labour and investment or venture capital. By means of incubators and accelerators, innovation in the sector tends to see smaller microbusinesses either scale up or sell to larger market players who have the reach to retail cutting-edge products and services.[102]

- NCSC collaboration with 'innovation companies' like Plexal is a positive example of governmental support for this pipeline.[103] Co-locating firms or entrepreneurs in spaces tends to reproduce old or established ways of working without active facilitation in pursuit of defined missions. Plexal is seen as playing the role of 'orchestrating' connections within the context of co-located workspaces specialising in cyber, becoming part of the organising functions of the state in this domain by keeping collaborations on track to meet broader governmental goals.[104]

- However, where current cyber labour and capital agglomerates in clusters, it tends to be in those regions where the kind of economic opportunities the sector unlocks are already in evidence, such as the London-Oxford-Cambridge 'golden triangle' and the M4 corridor from Heathrow to Bristol.[105]

- Levelling up cybersecurity capacity through extending the coverage of clusters and funding new incubators and accelerators across the country would improve access to local networks of knowledge and expertise and help address the private sector's unsatisfactorily, although in some cases understandably, slow response to an era of rising cyber threat. This kind of intervention echoes what Progressive Britain heard from other high-tech industries as part of its 'Future Industries' programme.[106]

- There is a strong national security justification for 'levelling up' cybersecurity. The unequal concentration of cyber expertise and capacity in certain communities, industries and professions could compound existing digital inequalities and expose groups and individuals who are excluded from full access to, and knowledge of, digital technologies to greater danger.

- Rural businesses face particular challenges with accessing networks and clusters of cybersecurity skills and expertise to repel threats.[107] Interlocking global crises are placing a new importance on foundational sectors like agriculture, space, maritime, renewables and critical metals/minerals. These key elements of critical national infrastructure are both increasingly digitally mediated and represent an increasingly strategically central part of the UK's global role, but often occupy rural and coastal areas with a lack of local cybersecurity capacity. Whilst the NCSC is providing specialist support to companies in this bracket, particular attention should be given to baking in cybersecurity as an underpinning principle of how new enterprises operate in these regional contexts, rather than playing catch up after the fact.[108]

- In developing a UK-wide strategy attuned to the specificities of its regions, Labour should learn from the Welsh Government's Cyber Action Plan.[109] Drawing on academia-industry-government collaboration, this document sets out a plan for the devolved nation to expand cyber ecosystems, talent pipelines and resilience across the Welsh economy and public services.

- In taking a local approach to addressing regional inequalities in cyber skills and expertise, Labour can learn from other likeminded initiatives taking root in Wales, including the work of Nick Smith MP, who has helped establish a Cyber Hub in a college in his constituency of Blaenau Gwent.[110] In collaboration with private sector partners with a presence in the area, it has the explicit aim of encouraging young people to consider careers in the sector and meeting the demand of companies for staff with cybersecurity knowhow.[111] Importantly, it provides a non-graduate route into this kind of employment.

Indeed, the positive case study Wales provides in regional rebalancing of the cyber playing field is picked up in Labour's Commission on the UK's Future, which asks us to 'go to South Wales and see the new innovation hub which aims to create a global cyber security cluster - a 22nd century sector, never mind a 21st century one' and, moreover, to 'think of South Wales no longer as one of the world's biggest coal mining belts but now as the new location for the cyber security industry, with Cyber Wales a partnership involving not just Wales but also the South West of England, showing the benefits of cooperation between the nations of UK.'[112]

6. Cybersecurity and political oversight

UK cybersecurity policy is set with regular government National Cybersecurity Strategies, starting 2009. In line with the government's Integrated Review, increasingly these strategies see cyber not just as a problem of national security but a solution to so-called Global Britain's search for national power in a changing world.

The most recent UK strategy in 2022 saw a rebrand, 'security' being dropped in favour of the more general 'National Cyber Strategy'. This was distinguished by the embrace of 'cyber power' and 'cyber resilience' as key concepts. Whereas the former implies a more offensive posture in the use of cyber beyond Britain's border, the latter refers to the defensive capacity to resist or bounce back in the event of a successful cyber attack. The most recent strategy also professes a greater commitment to cybersecurity skills, jobs and industries as a part of 'Levelling Up' and extends the 'whole of society' approach introduced in the 2016 strategy.

The growing prominence and importance of cybersecurity raises issues for a Labour future government to consider in terms of its governance, funding and priority. These considerations include:

- There is a need for active leadership by government in order to combine the separate but increasingly intertwined goals of national and economic security. The Conservative Party's chaotic period of government has seen the National Audit Office note its failure to follow through on the requirement to regularly report progress against the targets of the National Cyber Strategy.[113]

- The deadlines set out in the National Cyber Strategy have been described as narrow considering the impending threat of a major cyberattack and the fiscal constraints facing government.[114] Labour must closely measure the implementation of the current strategy against its promises.

- There is a growing urgency to prioritise defence and security against the backdrop of a more dangerous world. The government's recent Integrated Review refresh follows the latest cyber strategy in setting deadlines of 2025 to 'significantly harden' the state against cyberattack and 2030 to render the public sector resilient against vulnerabilities. These deadlines seem somewhat relaxed considering the current threat landscape, which is already reshaping everyday life. Labour should push for greater haste in meeting these targets.

- There is a need for greater oversight and scrutiny. There is much in the current government strategy, and other documents like the Integrated Review, that aligns with Labour's 'Make, Buy and Sell More in Britain' agenda and the party's 'modern industrial strategy'.[115] But government action in this domain must be subject to constant scrutiny where opened to parliamentary oversight – including where the government is compelled to publicly report back on annual progress.

- There is a need to formalise and consolidate cybersecurity at the level of cabinet and government roles. Departmental responsibility for cybersecurity policy is currently being concentrated in the Cabinet Office but in effect distributed over multiple, sometimes competing, departments and ministerial briefs including now the new Department for Science, Innovation & Technology. There is insufficient clarity about the composition, frequency and remit of proposed committees dedicated to cybersecurity. Rather than its current fragmentary distribution over multiple briefs and departments, consolidated responsibility could protect cybersecurity from being spread too thinly across competing funding priorities.

- Cyber has fallen within the varied remit of ministers first in DCMS and now in the new Department of Science, Innovation & Technology. The latter move has produced more specific messaging and communication around cyber, but the minister responsible is a hereditary peer and thus much scrutiny occurs within the context of the Lords. Stronger definition and prioritisation of the role would help bolster oversight of a domain that straddles different departments beyond DCMS and DSIT and is thus at risk of falling through the cracks. A Labour government should give further thought to how relevant ministerial and National Security Advisor remits and roles can best be combined or distributed to effectively and democratically govern cybersecurity operations in the UK as a specific domain. Meeting the longstanding call for a dedicated senior ministerial position Labour could learn from its allies in the Albanese government in Australia. There, the Labor Party has appointed a specific Minister for Cybersecurity. [116, 117]

Global security, global markets

There is a continued need for international collaboration around cyber, even as the UK seeks to develop greater sovereign capability. In an era of 'systemic competition' the boundary between defensive and offensive cyber operations often blurs and, in the absence of established codes of conduct, there is a risk of escalation and miscalculation. In a continuation of the 2021 Integrated Review and the 2022 National Cyber Strategy, the Review refresh stresses the importance of 'engaging with technology companies and shaping responsible norms of behaviour with respect to cyberspace', as a means of heading off offensive threats from hackers and deterring or disciplining rival states.

The 2023 refresh contains clear commitments to transparency for the ethical guidelines followed by the National Cyber Force in its defensive and offensive operations, and cites efforts at the UN to promote collective codes of conduct. However, the continuation of such multilateral approaches will confront substantial barriers as global decision-making becomes more rancorous between conflicting blocs.

Maintaining its forerunner's sceptical stance vis-a-vis multilateralism, the review does not flesh out precisely how broader consensus around a set of norms will be achieved in practice. This has led some to comment that the current Conservative government has shown insufficient ambition and detail in defining the UK's role as a 'responsible cyberpower'.[118]

A recent National Cyber Force document has done much to flesh out the UK's approach to this area. But with the NCF straddling domains of government, questions remain about political oversight and accountability when this internal doctrine is put to the test on the international stage. [119, 120] In this context, Labour can push government to do more:

- Labour should call on the current government to continue working internationally, aswell as domestically, to build consensus about rules and norms of cyberwarfare in line with liberal democratic values and human rights. Labour should also have its own plans for government in order to bring transparency and clarity to the costs and consequences of offensive operations. This would more effectively establish deterrence in a dangerous world where cyberattacks are both a more common occurrence and more difficult to attribute to state and non-state actors. Collaborative intelligence links with trusted partners and allies are central to the confident attribution of responsibility necessary to robustly punish transgressions and maintain deterrence.[121]

- Even as the threat of direct conflict with adversaries intensifies, the multidimensional domestic and international character of contemporary conflict requires that cybersecurity spending and resourcing are not confined to conventional defence functions (e.g. in the Ministry of Defence) and a truly 'whole of society' approach is pursued. The new Defending Democracy

Taskforce announced in the Integrated Review refresh has a wider 'whole of society' remit than conventional cyber defence, but is narrowly focused on foreign interference in elections and the information space. The kind of model proposed for the Taskforce - 'bridging gaps between the national security establishment and non-traditional partners such as local councils, police forces and global tech companies' – should be expanded under a Labour government to underpin as much as possible of the country's cybersecurity effort, spanning government, business, civil society and communities.

Conclusion

We titled this paper 'Cybersecuronomics' partly because domains of practice like cybersecurity fit within a major priority area of Labour's modern industrial strategy, 'sovereign capabilities'. These provide the secure and stable access to digital networks and other utilities that underpin everyday life and guarantee safe conditions for business and investment in Britain. Particularly associated with the provision and protection of critical national infrastructure, this paper has suggested that their centrality to the safety of the country and economy is threatened by the possibility of nvestment risk, market failures and foreign takeovers.

As such, it is recommended that these industries cannot be left to the private sector alone and demand that the state acts as a partner, using regulatory controls, strategic procurement and R&D spending to incentivise decision making and good behaviour among the owners and operators of critical infrastructure.

Labour's industrial strategy is right to emphasise the importance of rebuilding and revitalising the UK's manufacturing capacity. But, as the Leader of the Opposition has argued in recent speeches this need not imply undoing the considerable strengths the UK has built up in knowledge-intensive sectors. Cybersecurity is one such example.[122]

The party's current plans promise to realise the potential for greater investment in R&D spending to foster regional clusters and collaborations between government, business and universities, aligning these sectors with new sources of strategic and competitive advantage in digital. The geopolitical context demands that this focus on the digital is extended to cutting-edge defence-adjacent domains like cybersecurity, whilst keeping in mind that the challenges the UK and its partners face undoubtedly require more conventional military means as well.

At its best, government investment and regulatory intervention in cybersecurity holds the potential to help level up regional inequalities in accessing the skills, finance streams and markets associated with success in such sectors. Through this, we conclude that the cyber sector can help a future Labour government construct a positive relationship between economic security, national security, and better and more secure work, across the UK – in other words, its vision of securonomics.

As widely noted, securonomics owes much to the modern supply-side 'Bidenomics' being pioneered across the pond. As this paper was being written, the Biden administration released its own National Cybersecurity Strategy informed by this broader economic rethink.[123] Labour should look closely at this document for signs of how 'securonomics' can translate in a specific domain of practice that cuts across industries and sectors. The US strategy presents in a coherent package many of the key distinctions Labour should seek to carve out with the Conservative programme in the UK. But it also speaks to a wider need for leadership in setting the cybersecurity agenda on the world stage.

The tendency in most cyber policymaking worldwide has been for greater regulatory harmonisation to prevent undercutting and avoid countries duplicating one another's efforts.[124] Where the UK may be tempted to trumpet an innovatory approach to regulating cyber, it is arguably more important to remain in line with what other likeminded states are doing. As many of the key cybersecurity issues concern international trade and supply chains in software and hardware, one of the main struggles is to align business and government around global norms and standards that apply across borders.

Moreover, differences in regulation fragment markets and enables competition based on arbitraging the rules in divergent national regimes. The complexity here becomes clear when one considers that a British

company doing business abroad will be protected from cyber threats only according to local jurisdiction, and national rules and regulations may even pose a threat in themselves, as for companies trading in China. This geopolitical context is what drives the transformation of technology procurement into a foreign policy issue and makes cybersecurity such a pressing governmental concern.[125]

However, the emerging cold war effectively rules out global bodies like the UN as a viable basis for the required alignment. It is more likely to be something organised within blocs of friendly countries – a trend picked up in Labour's recent thinking on 'securonomics' – and, under present leadership at least, the US is going to be the central actor in this.

In this respect, the US already wields considerable leadership in defining the terms of cybersecurity among its allies, and its National Cybersecurity Strategy concludes with what effectively represents a call for a US-led Western trading bloc around software and hardware supply chains. With allies in AUKUS and other pacts, the US projects soft power through building the capacity of partners in Africa and the Indo-Pacific to defend against cyber threats.[126] Its National Institute of Standards and Technology is looked to by many national governments for guidance with supply chains and other issues due to the compatibility of its recommendations with existing rules and regulations, with its advice readily accessible to global partners as a source of US soft power.[127]

Whilst the US role in the world remains uncertain due to potential political instability, the NIST is a well-placed source for a set of common principles and standards to be agreed upon by the international liberal democratic order. Under a Labour government, the UK should seek where possible to adhere to its codes and standards as alignment in this domain renders the West stronger against the threats it faces. This would continue the work of the Five Eyes alliance which collaboratively produced a statement on cybersecurity to help shape the agenda among the Western bloc.[128] However, the UK government has thus far not done enough to reach out and seek alignment with the EU Cybersecurity Act, overtaken by states like Singapore who have been eager to sign mutual recognition agreements, as well as the US whose bilateral agreements with the EU increasingly represent a key site of cyber policy. The Five Eyes framework, it is suggested, could provide a means for the UK and other allies establish third-country status on some of the bilateral bodies on which this US-EU nexus centres.[129]

At the time of putting the finishing touches to this paper, there are positive signs that Labour's trade team are already discussing with friendly Democrats the possibility of a deal with the US on digital products and services including cybersecurity.[130] As well as trading links, UK can also take cues from the Biden presidency on domestic cyber policy. A central priority of the US NCS is to 'rebalance the responsibility to defend cyberspace' and 'realign incentives to favor long-term investments' against a backdrop where markets and the private sector have failed to guarantee cybersecurity.[131]

Critical national infrastructure is a specific case where owners and operators have used the freedom afforded by a largely requirement-free landscape of incentives to play fast and loose with preventing, monitoring or reporting cyber breaches. Small businesses and individual users cannot be expected to take up the slack of the failures of a digital ecosystem propelled by the desire to rush minimal viable products to markets.[132] Rather, the US cyber strategy suggests government resources should be marshalled to the cause of cybersecurity in a much more interventionist and fundamental way – in particular by more robustly regulating expectations and standards around cybersecurity (especially as concerns critical infrastructure) and expanding the capacity of a capable class of cybersecurity experts to decentralise knowhow across economy and society.[133] This represents a substantial shift away from the free-market model of muddling through that characterised White House strategy in less dangerous times.[134]

That being said, the Biden cyber strategy symbolises how in the US, successive Democratic and Republican administrations have tended to build upon each others' cybersecurity policies rather than scrapping them and starting again.[135] Labour should approach cybersecurity policy in much the same spirit should they seize power from the Conservatives in the next election, recognising and taking forward the sub-

stantial gains and innovations achieved under previous governments. However, just as Biden's strategy has broken with previous administrations by stressing the need for government intervention and regulation as a response to free-market failure, so too should Labour be prepared to criticise and correct where previous policy has resulted in similar issues.

Compared to the robust challenge to market forces put forward in the US strategy, the UK's NCS still displays some timidity and naivety about just how far the private sector aligns with its vision of cybersecurity as a public good.[136] With the Conservative Party increasing fiscally averse to strategic intervention in industry and the economy, it will be left to Labour to pick up the pieces and follow in Biden's footsteps in taking a more assertive posture with reference to private sector cybersecurity.

Too much of the government's rhetoric about 'resilience', whilst well-meaning, covers for an underlying lack of courage to create tougher regulation to actively manage risk, especially in the context of our largely privately owned critical national infrastructure.[137] 'Resilience', here, effectively implies resignation to the risks translating into reality and being able to withstand it when they do. Total security against risk cannot be guaranteed – hence the popular use of the term 'resilience'. But the 'first political question' remains guaranteeing citizens security as a foundation for other social and economic goals. Labour should not lose sight of this imperative[138].

Endnotes

1 For examplary recent academic introductions to cybersecurity, see Stevens, T., (2023). What is Cybersecurity For? Bristol University Press, and Cornish, P. (ed.), (2021). The Oxford Handbook of Cybersecurity. Oxford University Press.

2 **Integrated Review Refresh 2023: Responding to a more contested and volatile world (2023).** Available at: https://www.gov.uk/government/publications/integrated-review-refresh-2023-responding-to-a-more-contested-and-volatile-world/integrated-review-refresh-2023-responding-to-a-more-contested-and-volatile-world.

3 National Cyber Strategy 2022: Pioneering a cyber future with the whole of the UK (2022). Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf

4 Voo, J. et al (2022) National Cyber Power Index 2022 | Belfer Center for Science and International Affairs. Available at: https://www.belfercenter.org/publication/national-cyber-power-index-2022.

5 Dawood, S. (2023) "Lindy Cameron: 'You can't retrofit security into AI – it needs to be built in at the start,'" New Statesman, 16 June. Available at: https://www.newstatesman.com/spotlight/cybersecurity/2023/06/lindy-cameron-interview-retrofit-security-ai.

6 Noone, G. (2023) "So what are Labour's tech policies, exactly?," Tech Monitor. Available at: https://techmonitor.ai/policy/digital-economy/so-what-are-labours-tech-policies-exactly.

7 START-UP, SCALE-UP: Making Britain the best place to start and grow a business (2022). Available at: https://labour.org.uk/wp-content/uploads/2022/12/WEB-17247_22-Start-up-review-v12-ALT-2.pdf

8 Learning and skills for economic recovery, social cohesion and a more equal Britain. COUNCIL OF SKILLS ADVISORS' REPORT (2022). Available at: https://labour.org.uk/wp-content/uploads/2022/10/WR-16813_22-Labour-Skills-Council-report-Edit-19-10-22.pdf

9 Brock, A. (2023) Chi Onwurah's speech at OPENUK's Honours Event June 2023 - OPENUK. Available at: https://openuk.uk/chi-onwurahs-speech-at-openuks-honours-event-june-2023/.

10 Afifi-Sabet, K. (2023) "Labour plans overhaul of government's 'anti-innovation' approach to tech regulation," ITPro, 7 February. Available at: https://www.itpro.com/business/policy-legislation/370024/labour-overhaul-government-anti-innovation-approach-tech-regulation.

11 Stacey, K. (2023) "AI should be licensed like medicines or nuclear power, Labour suggests," The Guardian, 5 June. Available at: https://www.theguardian.com/technology/2023/jun/05/ai-could-outwit-humans-in-two-years-says-uk-government-adviser.

12 Noone, G. (2023) "So what are Labour's tech policies, exactly?," Tech Monitor. Available at: https://techmonitor.ai/policy/digital-economy/so-what-are-labours-tech-policies-exactly.

13 Cybersecurity must be tightened up in this era of polycrisis (2023). Available at: https://www.weforum.org/agenda/2023/02/cybersecurity-in-an-era-of-polycrisis/.

14 The Labour Party (2022) Prosperity through Partnership: LABOUR'S INDUSTRIAL STRATEGY - The Labour Party. Available at: https://labour.org.uk/page/prosperity-through-partnership-labours-industrial-strategy/#:~:text=Labour%20is%20clear%20that%20all%20businesses%20and%20all,drive%20growth%20and%20build%20a%20more%20resilient%20economy.

15 NATIONAL CYBERSECURITY STRATEGY (2023). The White House. Available here: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

16 See: https://www.progressivebritain.org/author/harrypitts/.

17 A New Business Model for Britain: Building Economic Strength in an Age of Insecurity. (2023). Labour, Labour Together. Available at: https://labourtogether.uk/sites/default/files/2023-05/A%20NEW%20BUSINESS%20MODEL%20FOR%20BRITAIN_0.pdf

18 The Labour Party (2023) Rachel Reeves: "Securonomics" - The Labour Party. Available at: https://labour.org.uk/press/rachel-reeves-securonomics/.

19 The Labour Party (2021) Labour will make, buy and sell more in Britain - The Labour Party. Available at: https://labour.org.uk/press/labour-will-make-buy-and-sell-more-in-britain/.

20 Leonard, M. (2021) The Age of Unpeace: How Connectivity Causes Conflict. London: Bantam Press.

21 Lammy, D. (2023) ""We will reconnect Britain" – Lammy's foreign policy speech to Chatham House," LabourList | Latest UK Labour Party News, Analysis and Comment. Available at: https://labourlist.org/2023/01/we-will-reconnect-britain-lammys-foreign-policy-speech-to-chatham-house/.
22 Channel 4 (2022). The Undeclared War. Available at: https://www.channel4.com/programmes/the-undeclared-war
23 26 Voo, J. et al (2022) National Cyber Power Index 2022 | Belfer Center for Science and International Affairs. Available at: https://www.belfercenter.org/publication/national-cyber-power-index-2022.
24 Benson, V., Chinnaswamy, A. & Walton, N (2023) Future Growth Prospects for the UK Cyber Security Sector & the Role of Accelerators as Innovation Support Mechanisms. Available at: https://publications.aston.ac.uk/id/eprint/43859/1/Working_Paper_Doc_004_.pdf
25 DSIT cyber security newsletter - May 2023 (2023). Available at: https://www.gov.uk/government/publications/dsit-cyber-security-newsletter-may-2023/dsit-cyber-security-newsletter-may-2023.
26 DSIT cyber security newsletter - May 2023 (2023). Available at: https://www.gov.uk/government/publications/dsit-cyber-security-newsletter-may-2023/dsit-cyber-security-newsletter-may-2023.
27 Cyber security sectoral analysis 2022 (2022). Available at: https://www.gov.uk/government/publications/cyber-security-sectoral-analysis-2022/cyber-security-sectoral-analysis-2022.
28 The global city: The future of cyber insurance – next steps for the London Market (2021). Available at: https://www.theglobalcity.uk/cyber-security.
29 Voo, J. et al (2022) National Cyber Power Index 2022 | Belfer Center for Science and International Affairs. Available at: https://www.belfercenter.org/publication/national-cyber-power-index-2022.
30 Cyber security breaches survey 2023 (2023). Available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023#summary.
31 Pakes, F. Pitts, H. (2022) "Security at work in an uncertain world," Progressive Britain [Preprint]. Available at: https://www.progressivebritain.org/security-at-work-in-an-uncertain-world/.
32 Carr, M. and Tanczer, L.M. (2018) "UK cybersecurity industrial policy: an analysis of drivers, market failures and interventions," Journal of Cyber Policy, 3(3), pp. 430–444. Available at: https://doi.org/10.1080/23738871.2018.1550523.
33 Calcara, A. and Marchetti, R. (2021) "State-industry relations and cybersecurity governance in Europe," Review of International Political Economy, 29(4), pp. 1237–1262. Available at: https://doi.org/10.1080/09692290.2021.1913438.
34 Cyber security breaches survey 2023 (2023). Available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023#summary.
35 Aviva Risk Insights Report 2023 (2023). Available at: https://www.aviva.co.uk/risksolutions/aviva-risk-insights-report/.
36 Montasari, R. (2023). Cyber Threats and the Security Risks They Pose to National Security: An Assessment of Cybersecurity Policy in the United Kingdom. In: Countering Cyberterrorism. Advances in Information Security, vol 101. Springer, Cham. https://doi.org/10.1007/978-3-031-21920-7_2
37 Stevens, T. (2021). United Kingdom: Pragmatism and adaptability in the cyber realm. In Routledge Companion to Global Cyber-Security Strategy (pp. 191-200). Routledge. https://www.taylorfrancis.com/chapters/edit/10.4324/9780429399718-19/united-kingdom-tim-stevens
38 UK small businesses targeted with 65,000 attempted cyber attacks per day | Hiscox Group (no date). Available at: https://www.hiscoxgroup.com/news/press-releases/2018/18-10-18.
39 Cyber Security Breaches Survey 2022 (2022). Available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022.
40 Defence and Cyber-Security (2012). House of Commons Defence Committee. Sixth Report of Session 2012–13. https://publications.parliament.uk/pa/cm201213/cmselect/cmdfence/106/106.pdf
41 DSIT cyber security newsletter - May 2023 (2023). Available at: https://www.gov.uk/government/publications/dsit-cyber-security-newsletter-may-2023/dsit-cyber-security-newsletter-may-2023#government-launches-govassure-to-bolster-cyber-resilience.
42 Aggarwal, V.K. and Reddie, A.W. (2018) "Comparative industrial policy and cybersecurity: a framework for analysis," Journal of Cyber Policy, 3(3), pp. 291–305. Available at: https://doi.org/10.1080/23738871.2018.1553989.

43 Hüsch, P., and Sullivan, J. (2023). Global Approaches to Cyber Policy, Legislation and Regulation. RUSI. Available at https://rusi.org/explore-our-research/publications/special-resources/global-approaches-cyber-policy-legislation-and-regulation

44 Topping, C., Michalec, O., and Rashid, A., (2022). Contrasting global approaches for identifying and managing cybersecurity risks in supply chains." arXiv preprint arXiv:2208.02244. https://arxiv.org/abs/2208.02244

49 Calcara, A. and Marchetti, R. (2021) "State-industry relations and cybersecurity governance in Europe," Review of International Political Economy, 29(4), pp. 1237–1262. Available at: https://doi.org/10.1080/09692290.2021.1913438.

46 Department for Business and Trade (2018) "Cybersecurity export strategy," GOV.UK [Preprint]. Available at: https://www.gov.uk/government/publications/cyber-security-export-strategy.

47 Aggarwal, V.K. and Reddie, A.W. (2018) "Comparative industrial policy and cybersecurity: a framework for analysis," Journal of Cyber Policy, 3(3), pp. 291–305. Available at: https://doi.org/10.1080/23738871.2018.1553989.

48 Fidler, D., (2021). Cybersecurity, Global Commerce, and International Organizations', in Paul Cornish (ed.), The Oxford Handbook of Cyber Security, Oxford University Press, pp. 497-513. https://doi.org/10.1093/oxfordhb/9780198800682.013.31

49 Aggarwal, V.K. and Reddie, A.W. (2018) "Comparative industrial policy and cybersecurity: a framework for analysis," Journal of Cyber Policy, 3(3), pp. 291–305. Available at: https://doi.org/10.1080/23738871.2018.1553989.

50 NATIONAL CYBERSECURITY STRATEGY (2023). The White House. Available here: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

51 Steed, D. (2021). The Future National Cyber Security Strategy: Defending Values in Cyber. Centre on Cyber Security and Online Threats, Henry Jackson Society. https://henryjacksonsociety.org/wp-content/uploads/2021/06/HJS-The-Future-National-Cyber-Security-Strategy-Report-web.pdf

52 "UK boosts Ukraine's cyber defences with £6 million support package," GOV.UK, 1 November. Available at: https://www.gov.uk/government/news/uk-boosts-ukraines-cyber-defenc¬es-with-6-million-support-package.

53 Integrated Review Refresh 2023: Responding to a more contested and volatile world (2023b). Available at: https://www.gov.uk/government/publications/integrated-review-refresh-2023-responding-to-a-more-contested-and-volatile-world/integrated-review-refresh-2023-responding-to-a-more-contested-and-volatile-world.

54 Stevens, T. (2021). United Kingdom: Pragmatism and adaptability in the cyber realm. In Routledge Companion to Global Cyber-Security Strategy (pp. 191-200). Routledge. https://www.taylorfrancis.com/chapters/edit/10.4324/9780429399718-19/united-kingdom-tim-stevens

55 Topping, C., Dwyer, A., Michalec, A. Craggs, B., & Rashid, A. (2021). Beware suppliers bearing gifts!: Analysing coverage of supply chain cyber security in critical national infrastructure sectorial and cross-sectorial frameworks. Computers & Security 108: 102324. https://www.sciencedirect.com/science/article/abs/pii/S0167404821001486

56 Chappell, E. (2021) "Rachel Reeves sets out Labour plan to "make, sell and buy more in Britain"," LabourList | Latest UK Labour Party News, Analysis and Comment [Preprint]. Available at: https://labourlist.org/2021/07/rachel-reeves-sets-out-labour-plan-to-make-sell-and-buy-more-in-britain/.

57 Rashid, A., Hankin, C., & Schneider, S. (2020). The future of the UK's Cyber Security Research Position in the World. Report commissioned by National Cyber Security Centre. https://research-information.bris.ac.uk/ws/portalfiles/portal/247699752/The_Future_of_UK_Cyber_Security_Feb_2020.pdf

58 Academic centres of excellence in Cyber Security research (Published 2019, reviewed 2023). Available at: https://www.ncsc.gov.uk/information/academic-centres-excellence-cyber-security-research#:~:text=Academic%20Centres%20of%20Excellence%20in%20Cyber%20Security%20Research,Centres%20of%20Excellence%20in%20Cyber%20Security%20Research%20%28ACE-CSR%29.

59 Calcara, A. and Marchetti, R. (2021) "State-industry relations and cybersecurity governance in Europe," Review of International Political Economy, 29(4), pp. 1237–1262. Available at: https://doi.org/10.10

80/09692290.2021.1913438.
60 "National Security and Investment Act 2021," Available at: https://www.gov.uk/government/collections/national-security-and-investment-act.
61 National Cyber Strategy 2022: Pioneering a cyber future with the whole of the UK (2022). Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf.
62 Baines, V. (2023). UK Plc and Supply Chain Cyber Security: Where in the World is my Data?. British Foreign Policy Group. https://bfpg.wpenginepowered.com/wp-content/uploads/2023/04/BFPG-UK-plc-and-Supply-Chain-Cyber-Security-April-2023-2.pdf
63 Turner, B.C. (2023) "Business leaders need hands-on approach to stop cyber crime, says spy chief," The Telegraph, 28 January. Available at: https://www.telegraph.co.uk/news/2023/01/28/business-leaders-need-hands-on-approach-stop-cyber-crime-says/.
64 Hüsch, P., and Sullivan, J. (2023). Global Approaches to Cyber Policy, Legislation and Regulation. RUSI. https://rusi.org/explore-our-research/publications/special-resources/global-approaches-cyber-policy-legislation-and-regulation
65 Carr, M. and Tanczer, L.M. (2018) "UK cybersecurity industrial policy: an analysis of drivers, market failures and interventions," Journal of Cyber Policy, 3(3), pp. 430–444. Available at: https://doi.org/10.1080/23738871.2018.1550523.
66 Department for Science, Innovation and Technology (2023) "Secure by design," GOV.UK [Preprint]. Available at: https://www.gov.uk/government/collections/secure-by-design.
67 Hüsch, P., Sullivan, J. Global approaches to cyber policy, Legislation and Regulation (2023). Available at: https://rusi.org/explore-our-research/publications/special-resources/global-approaches-cyber-policy-legislation-and-regulation.
68 Baines, V. (2023). UK Plc and Supply Chain Cyber Security: Where in the World is my Data?. British Foreign Policy Group. https://bfpg.wpenginepowered.com/wp-content/uploads/2023/04/BFPG-UK-plc-and-Supply-Chain-Cyber-Security-April-2023-2.pdf
69 Baines, V. (2023). UK Plc and Supply Chain Cyber Security: Where in the World is my Data?. British Foreign Policy Group. https://bfpg.wpenginepowered.com/wp-content/uploads/2023/04/BFPG-UK-plc-and-Supply-Chain-Cyber-Security-April-2023-2.pdf
70 Dawood, S. (2023) "Lindy Cameron: 'You can't retrofit security into AI – it needs to be built in at the start,'" New Statesman, 16 June. Available at: https://www.newstatesman.com/spotlight/cybersecurity/2023/06/lindy-cameron-interview-retrofit-security-ai.
71 Thomas, H. (2023) "The UK will need more than words in this cyber war," Financial Times, 20 April. Available at: https://www.ft.com/content/a70d4af7-1006-409e-9e78-da0114c10a0a.
72 Glover, C. (2023) "Lloyd's of London cyber war exclusion rules come into effect today," Tech Monitor, 31 March. Available at: https://techmonitor.ai/technology/cybersecurity/lloyds-of-london-cyber-war-exemption-rules-effect-today.
73 The National Cybersecurity Strategy: Breaking a 50-Year losing streak (2023). Available at: https://www.lawfaremedia.org/article/the-national-cybersecurity-strategy-breaing-a-50-year-losing-streak.
74 NATIONAL CYBERSECURITY STRATEGY (2023). The White House. Available here: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
75 Hüsch, P., and Sullivan, J. (2023). Global Approaches to Cyber Policy, Legislation and Regulation. RUSI. https://rusi.org/explore-our-research/publications/special-resources/global-approaches-cyber-policy-legislation-and-regulation
76 Cyber Essentials scheme process evaluation (2023). Available at: https://www.gov.uk/government/publications/cyber-essentials-scheme-process-evaluation/cyber-essentials-scheme-process-evaluation.
77 Cartwright, A., Cartwright, E. and Edun, E. (2023) "Cascading information on best practice: Cyber security risk management in UK micro and small businesses and the role of IT companies," Computers & Security, 131, p. 103288. Available at: https://doi.org/10.1016/j.cose.2023.103288.
78 Cartwright, A., Cartwright, E. and Edun, E. (2023) "Cascading information on best practice: Cyber security risk management in UK micro and small businesses and the role of IT companies," Computers

& Security, 131, p. 103288. Available at: https://doi.org/10.1016/j.cose.2023.103288.
79 Cartwright, A., Cartwright, E. and Edun, E. (2023) "Cascading information on best practice: Cyber security risk management in UK micro and small businesses and the role of IT companies," Computers & Security, 131, p. 103288. Available at: https://doi.org/10.1016/j.cose.2023.103288.
80 Rashid, A., Hankin, C., & Schneider, S. (2020). The future of the UK's Cyber Security Research Position in the World. Report commissioned by National Cyber Security Centre. https://research-information.bris.ac.uk/ws/portalfiles/portal/247699752/The_Future_of_UK_Cyber_Security_Feb_2020.pdf
81 Stevens, T. (2021). United Kingdom: Pragmatism and adaptability in the cyber realm. In Routledge Companion to Global Cyber-Security Strategy (pp. 191-200). Routledge. https://www.taylorfrancis.com/chapters/edit/10.4324/9780429399718-19/united-kingdom-tim-stevens
82 AlDaajeh, S.H. et al. (2022) "The role of national cybersecurity strategies on the improvement of cybersecurity education," Computers & Security, 119, p. 102754. Available at: https://doi.org/10.1016/j.cose.2022.102754.
83 Scroxton, A. (2022) "UK's National Cyber Advisory Board convenes for first time," ComputerWeekly.com, 9 November. Available at: https://www.computerweekly.com/news/252527087/UKs-National-Cyber-Advisory-Board-convenes-for-first-time.
84 Hüsch, P., and Sullivan, J. (2023). Global Approaches to Cyber Policy, Legislation and Regulation. RUSI. https://rusi.org/explore-our-research/publications/special-resources/global-approaches-cyber-policy-legislation-and-regulation
85 Walsh, M. (2023) "Why cybersecurity teams escaped big tech's layoffs," Raconteur. Available at: https://www.raconteur.net/technology/why-big-techs-jobs-cull-left-cybersecurity-unscathed/.
86 Cyber security skills in the UK labour market 2022: Findings report. (2022). Zatterin, G., Atkins, G., Bollen, A., Shah, J.N., Donaldson, S. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1072767/Cyber_security_skills_in_the_UK_labour_market_2022_-_findings_report.pdf
87 Rashid, A., Hankin, C., & Schneider, S. (2020). The future of the UK's Cyber Security Research Position in the World. Report commissioned by National Cyber Security Centre. https://research-information.bris.ac.uk/ws/portalfiles/portal/247699752/The_Future_of_UK_Cyber_Security_Feb_2020.pdf
88 National semiconductor strategy (2023). Available at: https://www.gov.uk/government/publications/national-semiconductor-strategy/national-semiconductor-strategy.
89 Department for Science, Innovation and Technology (2023) "Secure by design," GOV.UK [Preprint]. Available at: https://www.gov.uk/government/collections/secure-by-design.
90 Benson, V., Chinnaswamy, A. & Walton, N (2023) Future Growth Prospects for the UK Cyber Security Sector & the Role of Accelerators as Innovation Support Mechanisms. Available here: https://publications.aston.ac.uk/id/eprint/43859/1/Working_Paper_Doc_004_.pdf
91 Ministry of Defence (2022) "New £50 million cyber academy to benefit influential UK-US relationship," GOV.UK, 28 September. Available at: https://www.gov.uk/government/news/new-50-million-cyber-academy-to-benefit-influential-uk-us-relationship.
92 Department for Science, Innovation and Technology (2023) "Record numbers looking to kickstart new careers in cyber," GOV.UK, 26 June. Available at: https://www.gov.uk/government/news/record-numbers-looking-to-kickstart-new-careers-in-cyber.
93 Thomson, F. (2023) "Public and private sector collaboration can deliver the UK innovation agenda," Open Access Government. Available at: https://www.openaccessgovernment.org/clos¬ing-gap-between-public-private-sectors-deliver-uk-innovation-agenda/154280/.
94 Benson, V., Chinnaswamy, A. & Walton, N (2023) Future Growth Prospects for the UK Cyber Security Sector & the Role of Accelerators as Innovation Support Mechanisms. https://publications.aston.ac.uk/id/eprint/43859/1/Working_Paper_Doc_004_.pdf
95 AlDaajeh, S.H. et al. (2022) "The role of national cybersecurity strategies on the improvement of cybersecurity education," Computers & Security, 119, p. 102754. Available at: https://doi.org/10.1016/j.cose.2022.102754.
96 Devanny, J., Stevens, T., Dwyer, A., & Ertan, A. (2021, Apr 21). The National Cyber Force that Britain Needs? The Policy Institute at King's. Available at: https://kclpure.kcl.ac.uk/portal/files/151198191/National

_Cyber_Force_report.pdf
97 AlDaajeh, S.H. et al. (2022) "The role of national cybersecurity strategies on the improvement of cybersecurity education," Computers & Security, 119, p. 102754. Available at: https://doi.org/10.1016/j.cose.2022.102754.
98 Cartwright, A., Cartwright, E. and Edun, E. (2023) "Cascading information on best practice: Cyber security risk management in UK micro and small businesses and the role of IT companies," Computers & Security, 131, p. 103288. Available at: https://doi.org/10.1016/j.cose.2023.103288.
99 Hüsch, P., and Sullivan, J. (2023). Global Approaches to Cyber Policy, Legislation and Regulation. RUSI. https://rusi.org/explore-our-research/publications/special-resources/global-approaches-cyber-policy-legislation-and-regulation
100 Donaldson, S. Crozier, D., Martorell, S., McLaren, I., Douglas, J., Coutinho, S. UK Cyber Security Sectoral Analysis 2023 (2023). Research report for the Department for Science, Innovation and Technology. Available here: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1149419/UK_Cyber_Sectoral_Analysis_2023.pdf
101 Devanny, J., Stevens, T., Dwyer, A., & Ertan, A. (2021, Apr 21). The National Cyber Force that Britain Needs? The Policy Institute at King's. Available here: https://kclpure.kcl.ac.uk/portal/files/151198191/National_Cyber_Force_report.pdf
102 Benson, V., Chinnaswamy, A. & Walton, N (2023) Future Growth Prospects for the UK Cyber Security Sector & the Role of Accelerators as Innovation Support Mechanisms. https://publications.aston.ac.uk/id/eprint/43859/1/Working_Paper_Doc_004_.pdf
103 Neville, M. (2023) "Interview: The 'innovation company' closing the gap between government, startups and industry," Bdaily Business News. Available at: https://bdaily.co.uk/articles/2023/02/16/interview-the-innovation-company-closing-the-gap-between-government-startups-and-industry.
104 Roughan, A. NCSC for Startups: an ecosystem-based approach to cyber security (2023). Available at: https://www.ncsc.gov.uk/blog-post/ncsc-for-startups-an-ecosystem-based-approach-to-cyber-security.
105 Cyber security sectoral analysis 2022 (2022). Available at: https://www.gov.uk/government/publications/cyber-security-sectoral-analysis-2022/cyber-security-sectoral-analysis-2022#regional-snapshots.
106 FUTURE INDUSTRIES: Technology Led Growth for Britain in the 2020s. (2022). Available at: https://www.progressivebritain.org/wp-content/uploads/2022/08/Future-industries-v1.3.pdf
107 Tiwasing, P., Clark, B., & Gkartzios, M. (2022). How can rural businesses thrive in the digital economy? A UK perspective. Heliyon, 8(10). https://www.cell.com/heliyon/pdf/S2405-8440(22)02033-3.pdf
108 Cyber Advisor (no date). Available at: https://www.ncsc.gov.uk/schemes/cyber-advisor.
109 Cyber action plan for Wales | GOV.WALES (2023). Available at: https://www.gov.wales/cyber-action-plan-wales.
110 UK Could Lead The World In Tackling Cyber Threats As Rapid Change Leaves "Huge Scale" Gaps (2023). Available at: https://www.politicshome.com/news/article/global-cybersecurity-workforce-shortage-uk-parliament-rusi-report.
111 Simister, G. (2022) "Welsh college opens cybersecurity hub," UKTN | UK Tech News. Available at: https://www.uktech.news/cybersecurity/welsh-college-cyber-hub-20220616.
112 A New Britain: Renewing our Democracy and Rebuilding our Economy. Report of the Commission on the UK's Future (no date). Available here: https://labour.org.uk/wp-content/uploads/2022/12/Commission-on-the-UKs-Future.pdf
113 Progress of the 2016-2021 National Cyber Security Programme - National Audit Office (NAO) press release (2022). Available at: https://www.nao.org.uk/press-releases/progress-of-the-2016-2021-national-cyber-security-programme/#:~:text=The%20National%20Cyber%20Security%20Strategy%202016%20%28the%20Strategy%29,just%20beyond%20the%20mid-point%20of%20the%20five-year%20Programme.
114 Montasari, R. (2023). Cyber Threats and the Security Risks They Pose to National Security: An Assessment of Cybersecurity Policy in the United Kingdom. In: Countering Cyberterrorism. Advances in Information Security, vol 101. Springer, Cham. https://doi.org/10.1007/978-3-031-21920-7_2
115 The Labour Party (2022) Prosperity through Partnership: LABOUR'S INDUSTRIAL STRATEGY - The

Labour Party. Available at: https://labour.org.uk/page/prosperity-through-partnership-labours-industrial-strategy/.
116 Theresa May urged to bring in new cybersecurity minister as committee blasts Britain's 'inadequate' defences (2020). Available at: https://www.politicshome.com/news/article/theresa-may-urged-to-bring-in-new-cybersecurity-minister-as-committee-blasts-britains-inadequate-defences.
117 Bongiovanni, I. (2022) Australia finally has a dedicated minister for cyber security. Here's why her job is so important. Available at: https://theconversation.com/australia-finally-has-a-dedicated-minister-for-cyber-security-heres-why-her-job-is-so-important-184322.
118 Dwyer, A., & Martin, C. (2022). A Frontier Without Direction? The UK's Latest Position on Responsible Cyber Power. Lawfare, 1st August. https://www.lawfaremedia.org/article/frontier-without-direction-uks-latest-position-responsible-cyber-power
119 Stevens, T., et al (2023). Evaluating the National Cyber Force's 'Responsible Cyber Power in Practice'. RUSI. 14th April. https://rusi.org/explore-our-research/publications/commentary/evaluating-national-cyber-forces-responsible-cyber-power-practice
120 The National Cyber Force: Responsible Cyber Power in Practice (2022) National Cyber Force, A Defense and Intelligence Partnership. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1148278/Responsible_Cyber_Power_in_Practice.pdf
121 Steed, D. (2021). The Future National Cyber Security Strategy: Defending Values in Cyber. Centre on Cyber Security and Online Threats, Henry Jackson Society. https://henryjacksonsociety.org/wp-content/uploads/2021/06/HJS-The-Future-National-Cyber-Security-Strategy-Report-web.pdf
122 The Labour Party (2022) Keir Starmer speech on Labour's mission for economic growth - The Labour Party. Available at: https://labour.org.uk/press/keir-starmer-speech-on-labours-mission-for-economic-growth/.
123 NATIONAL CYBERSECURITY STRATEGY (2023). The White House. Available here: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
124 Hüsch, P., and Sullivan, J. (2023). Global Approaches to Cyber Policy, Legislation and Regulation. RUSI. https://rusi.org/explore-our-research/publications/special-resources/global-approaches-cyber-policy-legislation-and-regulation
125 Baines, V. (2023). UK Plc and Supply Chain Cyber Security: Where in the World is my Data?. British Foreign Policy Group. https://bfpg.wpenginepowered.com/wp-content/uploads/2023/04/BFPG-UK-plc-and-Supply-Chain-Cyber-Security-April-2023-2.pdf
126 Hüsch, P., and Sullivan, J. (2023). Global Approaches to Cyber Policy, Legislation and Regulation. RUSI. https://rusi.org/explore-our-research/publications/special-resources/global-approaches-cyber-policy-legislation-and-regulation
127 Topping, C., Michalec, O., and Rashid, A., (2022). Contrasting global approaches for identifying and managing cybersecurity risks in supply chains." arXiv preprint arXiv:2208.02244. https://arxiv.org/abs/2208.02244
128 Protecting Against Cyber Threats to Managed Service Providers and their Customers | CISA (2022). Available at: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-131a.
129 Baines, V. (2023). UK Plc and Supply Chain Cyber Security: Where in the World is my Data?. British Foreign Policy Group. https://bfpg.wpenginepowered.com/wp-content/uploads/2023/04/BFPG-UK-plc-and-Supply-Chain-Cyber-Security-April-2023-2.pdf
130 Stacey, K. (2023) "Labour's shared values with Democrats will aid UK-US trade deals, says shadow minister," The Guardian, 7 August. Available at: https://www.theguardian.com/politics/2023/aug/07/labours-shared-values-with-democrats-will-aid-uk-us-trade-deals-says-shadow-minister.
131 Hamin, M., Herr, T., Loomis, W., Schroeder, E., Scott, S. (2023) "How will the US counter cyber threats? Our experts mark up the National Cybersecurity Strategy," Atlantic Council. Available at: https://www.atlanticcouncil.org/content-series/tech-at-the-leading-edge/the-us-national-cybersecurity-strategy-mark-up/.
132 The National Cybersecurity Strategy: Breaking a 50-Year losing streak (no date). Available at: https://www.lawfaremedia.org/article/the-national-cybersecurity-strategy-breaking-a-50-year-losing-streak.
133 Healey, J. Twenty-Five years of White House cyber policies (2023). Available at: https://www.

lawfaremedia.org/article/twenty-five-years-of-white-house-cyber-policies

134 Healey, J. Twenty-Five years of White House cyber policies (2023). Available at: https://www.lawfaremedia.org/article/twenty-five-years-of-white-house-cyber-policies

135 Healey, J. Twenty-Five years of White House cyber policies (2023). Available at: https://www.lawfaremedia.org/article/twenty-five-years-of-white-house-cyber-policies

136 Montasari, R. (2023). Cyber Threats and the Security Risks They Pose to National Security: An Assessment of Cybersecurity Policy in the United Kingdom. In: Countering Cyberterrorism. Advances in Information Security, vol 101. Springer, Cham. https://doi.org/10.1007/978-3-031-21920-7_2

137 The UK Government Resilience Framework (HTML) (2023). Available at: https://www.gov.uk/government/publications/the-uk-government-resilience-framework/the-uk-government-resilience-framework-html

138 See https://renewal.org.uk/bringing-securonomics-down-to-earth/