NATIONAL CYBER STRATEGY 2022: DEVELOPING AND HARNESSING UK CYBER POWER

On December 15th, the UK Government unveiled its National Cyber Strategy 2022. The 2022 Strategy is more open-ended than its predecessor, the landmark National Cyber Security Strategy 2016-21. In place of a five-year window for implementation, many of the stated objectives of the 2022 Strategy have been set a goal of 2030 for full implementation, aligning it neatly with the EU's 2030 Digital Compass roadmap. It also reflects the greater ambition of the 2022 Strategy. Whereas the focus of its 2016-21 counterpart was principally on ***security***, the 2022 Strategy adopts a more balanced approach, including complementary areas such as cyber skills development, diversification, digital transformation, and cyber resilience under its remit. This broader focus is matched by the promise of a significant expansion of public sector investment, with £2.6 billion earmarked over the next three years.

This marks an important and welcome shift in the Government's thinking. It reflects a growing awareness of the ever-increasing role transformative digital technologies will play in shaping our lives over the coming decade. It also demonstrates an understanding of the need for a robust strategic framework for managing the many challenges and opportunities the growing economic and political importance of cyberspace presents. The defining concept of this new framework is thus not cyber security, but ***cyber power***, defined as "the ability to protect and promote national interests in and through cyberspace".

The 2022 Strategy is designed as a programme for the cultivation of the UK's cyber power. It does so by outlining what it refers to as the "Five Pillars". Each pillar comprises three-four objectives which all fall under a unified theme.

FIVE PILLARS OF UK CYBER POWER

1 CYBER ECOSYSTEM
Improving the UK's cyber skills and knowledge networks

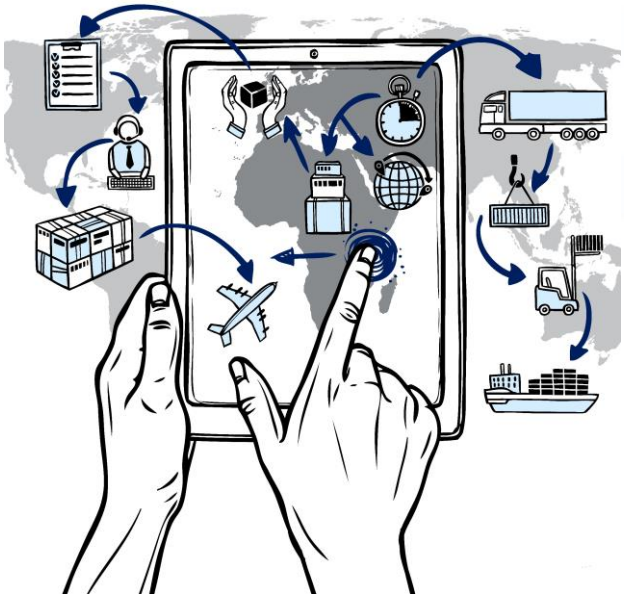
2 CYBER RESILIENCE
Improving the UK's overall cyber resilience

3 TECHNOLOGICAL ADVANTAGE
Advancing the UK's ability to influence the design, deployment, and securing of vital new digital technologies, such as AI, 5G/6G, and quantum computing

4 GLOBAL LEADERSHIP
Advancing the UK's global leadership of cyber security, resilience, and global governance

5 COUNTERING THREATS
Improving cyber security management, i.e., cybercrime, cyber espionage, and cyber warfare

The architectural analogy is apt. The five pillars are well chosen and represent the core areas on which the robustness of UK cyber power will depend. They are also mutually reinforcing. The UK's capacity to meet the objectives of each pillar is dependent on its striving to meet the others. The interconnectedness of the five pillars helps to illustrate just how substantial the challenges to advancing UK cyber power will be over the coming decade.



This occasionally jars with the 2022 Strategy's optimistic tone. Nowhere is this more apparent than on the thorny issue of digital supply chains. UK cyber resilience is contingent on the stability of the increasingly globalised and networked supply chains on which the UK's import-centric economy is deeply dependent. Many of these are heavily concentrated with a handful of suppliers and nations, where the UK has limited or no control over the supply chain. The 2022 Strategy's proposal that the UK develop robust alternative lines of sourcing in these cases in the short-to-near term is unfeasible for all but the most sensitive systems. A more realistic approach based on risk management will be required.

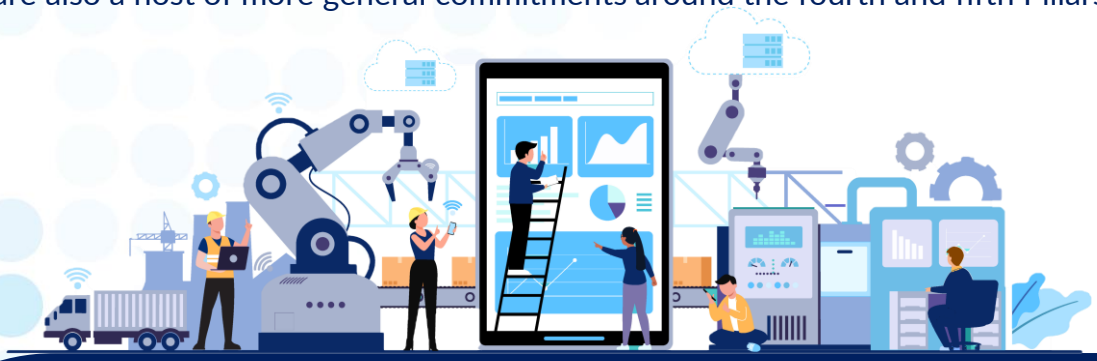
It is promising that the 2022 Strategy continues the recent trend of emphasising the importance of ***cyber resilience***. This focus makes it possible to settle otherwise thorny questions of responsibility and liability which cut across governments and private enterprises, especially those responsible for parts of critical national infrastructure. This need is felt all the more keenly in the context of the 2022 Strategy whose concern is not merely domestic cyber space, but that which we share with our global trading partners and geopolitical allies. More generally, adopting a resilience-based approach means embracing a more agile and pragmatic approach to cyber threats.

However, the 2022 Strategy has little to say about how greater cyber resilience will be achieved, or about how it should connect with the broader resilience agenda (a consultation is currently underway for a UK National Resilience Strategy). There are pledges to improve incident planning and exercising through the wider use of the NCSC accreditation scheme, the introduction of a similar scheme for exercising, and a promise to share new requirements for exercising of critical national infrastructure (CNI). But the remaining pledges concern risk mitigation rather than resilience.

Whilst the 2022 Strategy's focus on cyber resilience is welcome, there is relatively little said about how greater resilience will be achieved

The 2022 Strategy is much more explicit about its commitments to developing the UK's cyber ecosystem. A new National Cyber Advisory Board is promised to foster greater knowledge sharing between the public sector, industry, and academia. There are pledges to expand both cyber skills development programmes and investment in cyber startups. A Royal Charter has also been granted to the UK Cyber Security Council to make possible the establishment of a robust professional standards framework and the promised publication of a white paper to set out standards for cyber security technologies, products, and services

There are several other ambitious commitments found throughout the 2022 Strategy. Pledges are made to build a new NCSC applied research hub in Manchester and a national laboratory for operational technology security, both in support of the objectives of the third Pillar. There are also a host of more general commitments around the fourth and fifth Pillars.



CORE PLEDGES OF THE 2022 STRATEGY

1 CYBER ECOSYSTEM

- Establishment of National Cyber Advisory Board
- Post-16 cyber skills bootcamps
- Expansion of CyberFirst bursary scheme
- Chartered UK Cyber Security Council accreditation scheme
- Establishment of National Centre for Computing Education
- Investment in cyber start-ups via Cyber Runway and National Strategic Investment Fund

2 CYBER RESILIENCE

- Greater recording of Computer Misuse Act offenses
- Promotion of NCSC's Cyber Assessment Framework
- Expansion of Active Cyber Defence
- Publication of Government Cyber Security Strategy
- Review of the government's ability to hold CNI operators to account
- Introduction of a new cyber crime and fraud reporting service
- New requirements for exercising and incident planning for CNI operators

3 TECHNOLOGICAL ADVANTAGE

- Development of NCSC applied research hub in Manchester
- Development of national laboratory for OT security
- New standards for networked consumer products sold in UK
- New standards for digital service providers

4 GLOBAL LEADERSHIP

- Prioritising of cyber capacity building assistance in Eastern Europe, Africa and the Indo-Pacific
- Resolving of international debates on the application of rules, norms and principles in cyberspace

5 COUNTERING THREATS

- Amendment of the Proceeds of Crime Act
- Review of the Computer Misuse Act
- A scaling and development of the National Cyber Force

The boldness of the 2022 Strategy is clear. Much of it is backed up by ambitious commitments on implementation. It is a confident step forward into our increasingly unpredictable cyber future. However, some big questions remain about how some of these objectives will be realised. The UK's future prosperity as a digital economy and its capacity to continue to lead the advancement and regulation of cyberspace will depend on whether it can answer these questions, live up to the commitments of the 2022 Strategy, and – in some cases – be honest about the need for more realistic alternative approaches. It is on all of this that the UK's cyber power will depend.