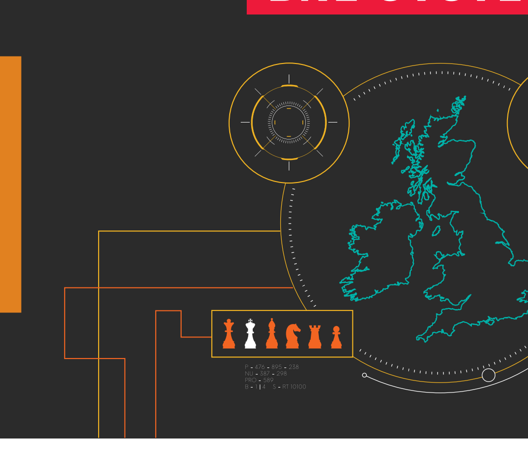
BAE SYSTEMS

UK National Cyber Strategy: BAE Systems Response



Executive Summary

The new **UK National Cyber Strategy**[1] has been released. Following on from the Integrated Review, and five years on from the 2016 National Cyber Security Strategy and its associated investment programme, the new strategy builds on experience and reflects on current context, charting a new course for UK national cyber defence.

In this paper we reflect on what has changed over the last five years, what we have learnt in that time about the challenges of cybersecurity and the UK's response, and how the new strategy aims to implement the UK's aspirations to be a global cyber power and a safer place to live and work online.

The backdrop for a new National Cyber Strategy

The previous National Cyber Strategy was issued in 2016. Much of the fundamental context that formed the backdrop of that strategy still holds true today. The cyber threat, though it has evolved and developed, continues to represent a real challenge for all parts of society. But there have also been some significant changes over the past five years, which are reflected in the new strategy.

One key evolution is the increased centrality of cyber in defence and security policymaking, as shown by its prominent role in the government's **Integrated Review**[2]. The new strategy is driven in many ways by the Integrated Review, and is intended to expand on its cyber and technology ambitions and outline how to operationalise them.

Five years ago, cyber was on the edge of policymaking; today, ministers now view cybersecurity as pivotal to the UK's future socio-economic prosperity and growth. As underlined by our collective experiences during the pandemic, the digital world underpins everything that we do.

At the same time, cybersecurity, cyber attacks and cyber espionage today feature much more prominently in the public discourse. Enabled by a combination of public awareness raising, media coverage and popular culture, the UK can now boast a much more cyber-aware population: five years ago its citizens were often unaware of cyber risks; today, **80 per cent**[3] say that cybersecurity is a high priority.

80%
in the UK say cybersecurity is now a high priority[3]

Meanwhile, a key change in the global context has been the return to prominence of great power competition as a critical challenge to security and prosperity. Today's top security priorities are no longer international terrorism or failing states like Afghanistan. The current issues are much more about the complex challenges posed by adversary nations.

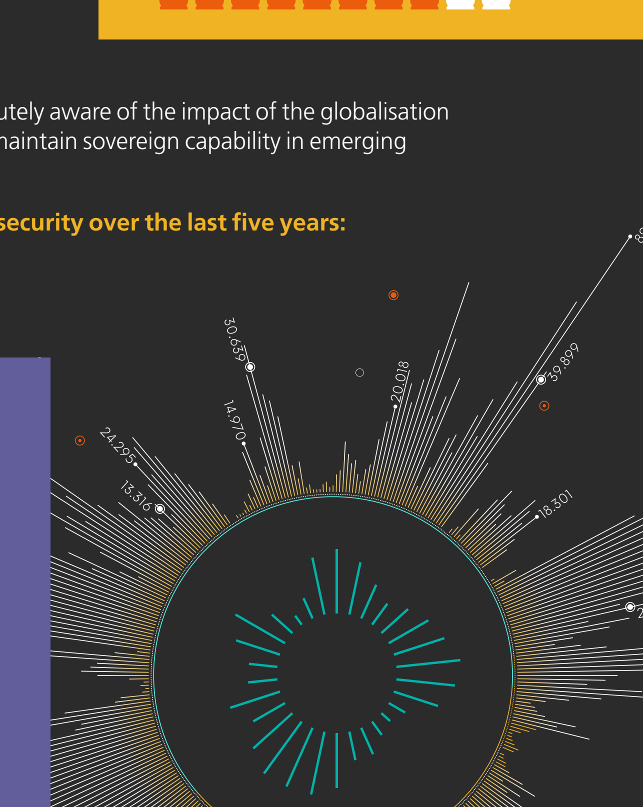
Cyber and technology are fundamental to these challenges and we have become acutely aware of the impact of the globalisation of technology, including on our critical supply chains and our ability to develop and maintain sovereign capability in emerging technologies. The controversy over Huawei is just one example of these issues.

Against that background, we have learned a number of lessons about cybersecurity over the last five years:

The NCSC is crucial, but it needs a cross government response

The creation of the National Cyber Security Centre (NCSC) was a cornerstone of the 2016 strategy. In just five years the NCSC has achieved a strong reputation for cybersecurity leadership. The case for having a coordinating centre for national cyber defence and the supporting ecosystem has been powerfully made. It is essential that this success is maintained and further developed, with the NCSC at the heart of the UK response to cyber.

But at the same time, we need cyber policymaking to be distributed across government. Every government department needs to be confident engaging on the cyber issues that relate to its own work, which will almost certainly overlap with the interests of other departments. Now is the time for mainstreaming cyber across the public sector.



International engagement and influence

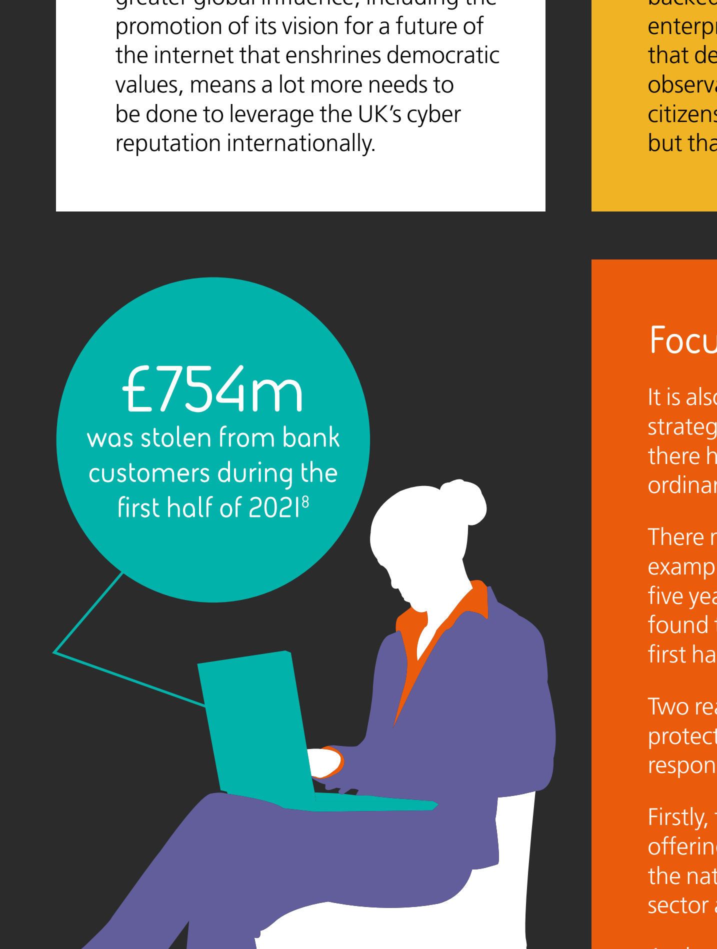
The NCSC has generated a strong, positive brand that is an asset for the UK, but the UK has not yet managed to fully capitalise on it internationally. Government has seemed to be struggling to resource the opportunities coming from having a strong international reputation in cybersecurity, particularly with regard to international engagement and partnerships.

But the UK's aspirations for much greater global influence, including the promotion of its vision for a future of the internet that enshrines democratic values, means a lot more needs to be done to leverage the UK's cyber reputation internationally.

Dealing with cyber threats

There have been other tough lessons learned since 2016. Tackling cyber-crime is hard – as attempts to address the ongoing ransomware epidemic have demonstrated. The **NCSC**[4] and **industry**[5] have provided some insights in addressing ransomware, but it is proving very difficult to achieve any impact against cyber criminals who are mostly located overseas, often in countries which will not co-operate with us effectively. Other nations, such as the US, have done more to address ransomware as a top threat to its **national security**[6], including presidential dialogue, an industry wide **taskforce**[7] and a **military cyber response**[8].

And we've learned that deterring hostile states from using cyber to do us harm is also really difficult; measures to deter such acts – including naming and shaming hostile states – seem to be having limited success if recent large scale cyber espionage operations are anything to go by. The state actors behind the high-profile SolarWinds supply chain attack are still actively conducting a range of sophisticated campaigns, and state-backed groups that have exploited vulnerabilities in MS Exchange and enterprise VPNs still pose a significant threat. Policymakers must accept that deterrence, like all security outcomes, is rarely a measurable or even observable: on the face of it, Western government, companies and citizens still get attacked despite having strong national cyber defences – but that shouldn't belittle the value of having them.



Focus on the citizen

It is also possible that with the emphasis from government on tackling strategic high end cyber threats, particularly from hostile nation states, there has been insufficient focus on what can be done to help the ordinary citizen.

There needs to be a refocus on safeguarding individual citizens. For example, although citizens are now far more aware of cybersecurity than five years ago, the UK's main banking industry body, UK Finance, has found that **£754 million**[9] was stolen from bank customers during the first half of this year – a 30 per cent rise on the same period in 2020.

Two real world events have underlined the need for greater citizen protection and the importance of government being agile enough to respond rapidly to such challenges: Covid-19 and ransomware.

Firstly, the pandemic has helped catalyse the government shift towards offering more advice to citizens about how to use home IT safely, and saw the national cybersecurity ecosystem lean in to support the healthcare sector as it struggled to provide care for citizens.

And secondly, ransomware has impacted organisations across all sectors, with impacts on citizens felt through loss of access to key services and disruption to supply chains. The rise of ransomware is not just affecting private businesses – the **London Borough of Hackney**[10] is a prime example of where critical services were rendered inaccessible by hackers.

We live in an unpredictable world, where crises can emerge very suddenly. Departmental policymakers engaging with the implementation of the National Cyber Strategy must recognise that cybercriminal activities and their responses to real world events (such as Covid-19 and ransomware) move at a different pace than geopolitical shifts. There is clearly a need for government responses to be agile enough to pivot to real world events and decide how it could most effectively provide its support across society, while not deviating from its strategic objectives.

Industry engagement

There have also been some lessons around how government and the private sector can best work together to improve national cybersecurity. The 2016 strategy marked a shift in approach by focusing on the role of government in tackling cyber issues in a much more interventionist way. This was a necessary change, but it may have led to a loss of focus on the role of other parts of society, including the private sector, and in particular those influential sectors that don't form part of the critical national infrastructure, and identify less clearly with national cybersecurity priorities.

There is a risk that, all too often, the private sector feel that the National Cyber Strategy is something done to them, not with them. That they are told what to do by government rather than involved in co-creating solutions to national challenges in which the private sector has an absolutely fundamental part to play. From government's point of view, there may be concern that the private sector is still not investing enough in cybersecurity, even where they form part of the country's critical national infrastructure. There is also frustration that, in practice, relatively few levers exist for government to drive up those cyber standards, beyond more regulation.

Industry engagement has always been a core mission of the national cybersecurity programme. But addressing the cyber challenges we face depends fundamentally on government and the private sector working together on a range of fronts, as part of a wider whole of society response. This has proved difficult to mobilise as effectively as it needs to be.

Globalisation of technology and the future of the internet

Globalisation of technology is a much broader question than cyber, but one that is closely related. The last few years have seen a growing prominence of big technology companies and the tensions over their accountability for security, privacy and disinformation issues, along with emerging national dilemmas about sovereign capabilities and sustained threats of espionage. These challenges have emphasised the need to find ways to manage the security risks inherent in a global technology supply chain where we have few direct ways of guaranteeing the security standards of technology that we rely on.

It is clear that countries can't simply receive and consume technology and still expect to control their digital destiny. Take cloud technologies, for example. These have been increasingly adopted to the extent that in ten years virtually everything will be in the cloud, but most countries are in the situation where they will have to accept an American or Chinese platform.

There have also been myriad initiatives, start-ups and accelerators for the cyber industry, as well as for other technologies considered to have a strategic impact, such as quantum, artificial intelligence, cryptography and the Internet of Things. But while allocating funding for technology innovation is a crucial first step, there is a risk that funding schemes will attract opportunistic applications from companies that will not have the right type of impact or the sustained growth that government seek.

Spotlighting the new National Cyber Strategy

So, what does the new National Cyber Strategy offer in response to these needs and the current era of systemic competition? The new approach sets cyber in a very broad strategic context, and sets out ambitious aspirations in some key areas. There are several significant aspects which appear particularly pertinent.

International dimension

The new strategy places significantly more emphasis on the international dimension, with a separate international pillar and a clear statement of the more activist leadership role the UK will take on internationally to promote its vision for the Internet. This builds on the ambitious statements made in the Integrated Review.

The prominence of cyber in the foreign policy agenda today compared to five years ago now sees the Foreign Commonwealth and Development Office taking a **vital leadership role**[11] including to promote a vision for the future of the internet and technology that embraces democratic principles and to encourage greater international collaboration on shared cyber challenges. Other departments including DIT, the Home Office and DCMS will each own international cyber objectives to support their own mandates, whether that be prosperity, homeland security or the digital economy.

The National Cyber Strategy needs to deliver a safe and prosperous digital world – an objective which combines both security and prosperity – and one that requires effective joined-up policymaking. There needs to be a complementary approach to delivering both security and prosperity; these days there is a greater understanding about the value of a successful digital society which combines both. Good cybersecurity is the foundation of a prosperous digital economy.

Ensuring that *all* these departments work well collectively, while preserving NCSC's work and reputation at the centre, is therefore crucial. And they will need to recognise the role of industry in innovating and influencing technology, and in exports as contributing to more than the national balance of payments, but as a strategic asset for international influence.

Truly whole of society

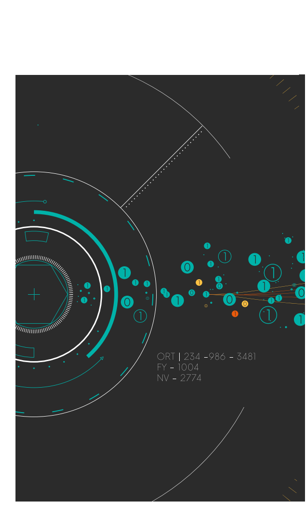
There is a strong emphasis on the "whole of society" approach to cyber. This emphasis on cyber as a team sport, depending not just on government but society as a whole, signals a welcome shift in approach.

While the NCSC clearly remains at the centre of our national effort, the strategy also acknowledges the need for all parts of government, and the wider public sector, to step up to the plate when it comes to working to address the cyber challenges to the nation.

The strategy sets out clear expectations around the responsibilities of both the citizen and the private sector to invest the necessary effort in protecting themselves against cyber attack. And it sets an aspiration for greater engagement with key stakeholders in a new 'national dialogue' on cyber, including through the new National Cyber Advisory Board, made up of senior leaders from the private and third sectors to challenge, support and influence the implementation of the new strategy. This is a welcome development as a means of engaging wider society in a collaborative way with government to help address our biggest cyber challenges. However, it must recognise the complex stakeholder landscape relevant to the national cyber ecosystem.

Industry is not one single type of entity. Different sectors have different structures, priorities and cybersecurity challenges, and companies need to be engaged on topics that are pertinent to them – whether that is because they have a particular role in national cyber resilience, or because it represents an industry that needs to grow, or because they represent another sector such as finance or venture capital.

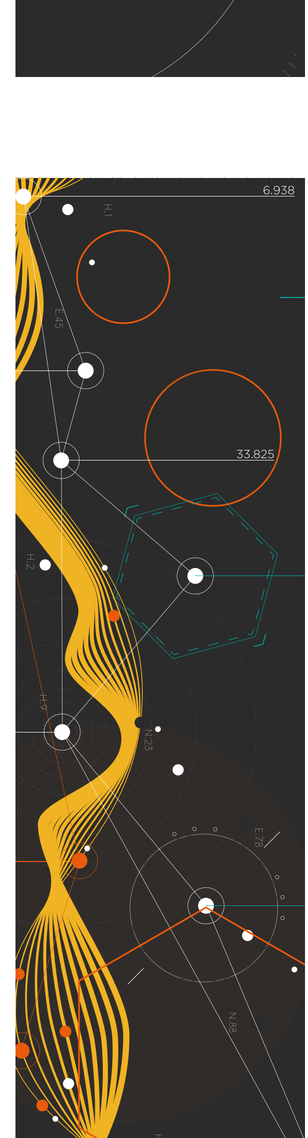
To get the best from industry engagement, we need a shift towards jointly identifying the challenges and priorities for the whole of society rather than just seeking industry support for government defined priorities. This will need a significant ramp up in the breadth and the effectiveness of mechanisms for engaging industry stakeholders.



Tackling the threat, including to the citizen

The strategy acknowledges that efforts to deter hostile threat actors from seeking to do us harm through cyber remain a challenge. As the threats evolve, the rewards increase and barriers to entry reduce. This candour is welcome. There is an emphasis on taking a more integrated and systematic campaign approach to deterring threat actors, drawing on all the levers available to government, including the National Cyber Force (NCF).

Based in Samlesbury, Lancashire, the NCF will have a vital role to play in disrupting threats from both state and non-state actors. As it further develops, it will be important for government to clearly and confidently make the case for responsible and democratic offensive cyber as part of the suite of capabilities that make up a legitimate cyber power.



Controlling the UK's digital destiny

The National Cyber Strategy sets out clear intents in two areas in particular: investment in the right R&D and having an influential and productive presence on international standards development organisations.

The strategy acknowledges a need to take more leadership in international standards development. The risk is that countries with a different view of how technology and the internet should be developed and secured prove more effective at influencing such bodies and the technology standards that emerge.

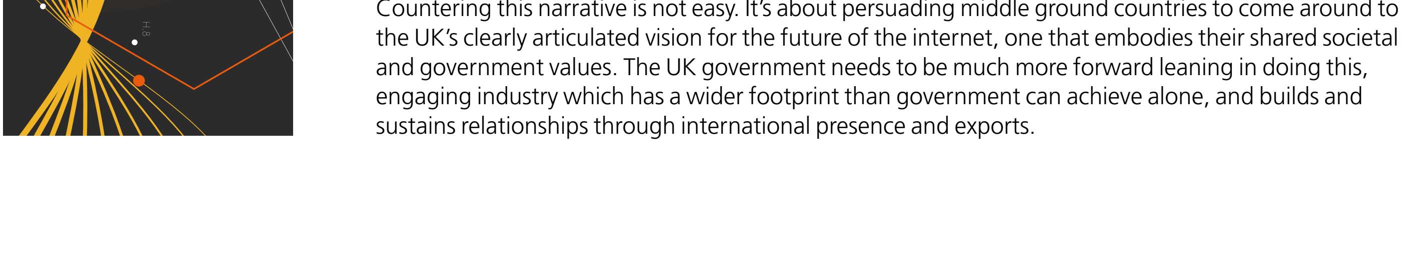
Putting this into practice will depend on sensible prioritisation of standards and technologies on which to focus, and close engagement with industry and academic champions with mutual interests. The UK needs to pick technologies that benefit society as a whole, and look very long term as it does so.

The strategy also elaborates ambitions around science and technology. Controlling your digital destiny is based on identifying technologies that will be influential and investing in their research and development. As an example, the UK government and industry has invested heavily in quantum technologies, resulting in strong research and development in this technology and its many applications.

Government has a critical role to play here in enabling the growth of industry which are fundamental to the nature of the UK economy and private sector. Funding investment is one aspect of this enablement, but it is much more about understanding the UK economy, its size and its reach, and the tech sector which is needed to deliver it and enable it to prosper, which may be a combination of technologies that need to remain sovereign, and technologies where the UK has a comparative advantage to offer the global market.

The UK and its allies believe in an internet that embraces the values of openness, democracy and privacy. But the fact is that there are assertive, aggressive and conflicting visions for the future of the internet coming from other nations. These see the internet as about state control, mass surveillance and repressing free speech.

Countering this narrative is not easy. It's about persuading middle ground countries to come around to the UK's clearly articulated vision for the future of the internet, one that embodies their shared societal and government values. The UK government needs to be much more forward leaning in doing this, engaging industry which has a wider footprint than government can achieve alone, and builds and sustains relationships through international presence and exports.



Conclusion

This National Cyber Strategy reflects a context of systemic competition. Given the lessons and evolved threat there is a transition from the mindset of 'fixing a problem' to that of 'staying ahead'. It underlines that cyber objectives are broader than the goal of securing the homeland and its digital economy, but are the foundation of prosperity and influence.

The strong international ambitions will require resourcing in a way that hasn't previously been possible. Dissemination of cyber policymaking across government to achieve the strategic objectives of the Integrated Review will require confident understanding and engagement on cyber issues and a greater degree of join-up to ensure that strategies and outcomes are tightly integrated, particularly with the agenda to gain greater control of the UK's digital destiny. A whole of society response also depends upon effective engagement, as well as the alignment of national and enterprise security objectives. Getting this right will catalyse the incentives that motivate industry, as well as extend cyber defence out to include the citizen.

We've all got a stake in ensuring that living and working online becomes safer and more secure. At BAE Systems Applied Intelligence we're looking forward to helping turn this vision into reality.

Visit our website: Responsible Cyber Power: Examining the Implications for Government, Industry and Society

For more information on the latest thinking and projects from the team at BAE Systems Applied Intelligence, subscribe to our **Government Insights**

1 National Cyber Strategy 2022, Pioneering a cyber future with the whole of the UK, HM Government December 2021
2 Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy, HM Government July 2021
3 New web tool to test your cyber risk as survey exposes 80% of British people fear online attacks, National Cyber Security Centre, March 2021
4 Ransomware: What board members should know and what they should be asking their technical experts, National Cyber Security Centre, June 2021
5 Ransomware: A Perfect Storm, BAE Systems Applied Intelligence, April 2001
6 White House Executive Order on Improving the Nation's Cybersecurity, May 2021
7 U.S. Department of Justice, Office of the Deputy Attorney General Memorandum for all Federal Prosecutors, June 2021
8 US military's hacking unit publicly acknowledges taking offensive action to disrupt ransomware operations, KTen News, December 2021
9 2021 Half Year Fraud Report, UK Finance, September 2021
10 Hackney still reeling from cyber attack six months on, Local Government Chronicle, April 2021
11 Client Conversation: Moving cyber into the diplomatic mainstream, BAE Systems Applied Intelligence, May 2021

BAE SYSTEMS

BAE Systems, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK
E: learn@baesystems.com | W: baesystems.com/governmentinginsights | T: +44 (0) 330 158 3627

Copyright © BAE Systems plc 2021. All rights reserved.
BAE SYSTEMS, the BAE SYSTEMS Logo and the product names referenced herein are trademarks of BAE Systems plc. BAE Systems Applied Intelligence Limited registered in England & Wales (No.1337451) with its registered office at Surrey Research Park, Guildford, England, GU2 7RQ. No part of this document may be copied, reproduced, adapted or redistributed in any form or by any means without the express prior written consent of BAE Systems Applied Intelligence.