UK, US and Australia Cyber Strategies

A New Era of Collaborative Cyber Security

Digital Intelligence

BAE SYSTEMS

A New Era

of Collaborative Cyber Security

Since December 2021, the United Kingdom, United States and Australia have all set out new national approaches to cyber security. While not directly connected, this period has also seen the three nations sign the landmark AUKUS treaty, which itself has a cyber component and calls for close synergy between the three nations on cyber security.

There has been a close defence and national security partnership between the UK, Australia and the USA stretching back at least to the Second World War. It is enshrined, amongst other things, in those nations' membership of the 'Five Eyes' intelligence relationship, along with Canada and New Zealand.

More recently, the particular relationship between the three has been expressed in a new agreement – AUKUS. Announced in September 2021, AUKUS is centred around the nations collaborating to work with Australia on its **acquisition of nuclear powered submarines** (Pillar One).

Pillar Two of the treaty seeks to **strengthen trilateral capabilities in a range of technologies relevant to the military partnership, increase interoperability, and drive knowledge sharing and innovation.** An update in **December 2023** from an AUKUS defence ministers' meeting cited collaboration in various areas of technology including: quantum capabilities for positioning and navigation; AI to enhance force protection, precision targeting and intelligence, surveillance and reconnaissance (ISR); and advanced tooling to uplift cyber security in the naval supply chain.

The focus on cyber security is particularly important in the context of international collaboration in today's threat landscape. From sharing critical and sensitive defence technology to enabling interoperability, some degree of commonality in approach to cyber will be required.

Collaborating to drive processes and best practices for national cyber security

The Spotlight on Cyber

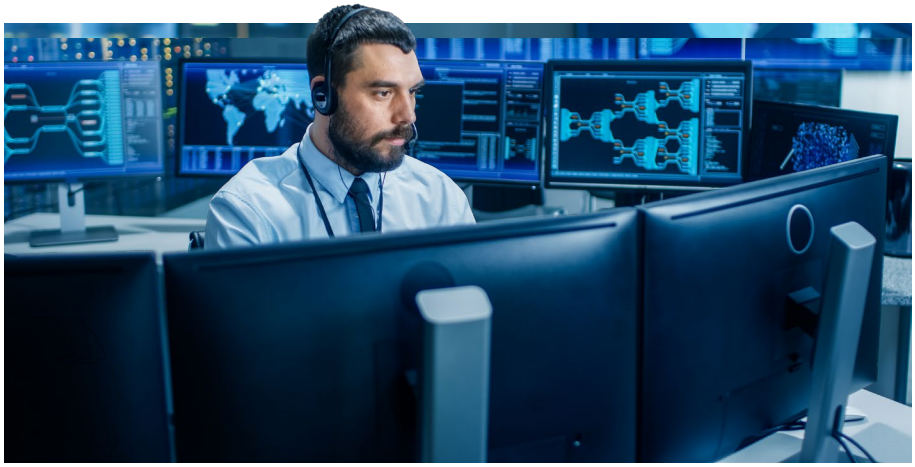
The UK's latest strategy was published in December 2021, shortly after the AUKUS announcement. The USA's followed in March 2023, and Australia's was issued in December 2023. This follows a series of high profile cyber-attacks in Australia, which seem to have led to a strong sense of momentum with regards to improving Australia's cyber security.

Given the important cyber dimension to the AUKUS treaty and the development of the new cyber strategies, it is worth comparing the latest thinking from each nation on cyber issues to **identify common themes and priorities,** along with **any areas of different emphasis** when it comes to addressing today's cyber challenges.

There are of course some fundamental differences inherent in the three nations which are, to some extent, reflected in the cyber strategies. For example, each nation operates within a distinctive constitutional framework, which affects the extent to which the national government can effect change.

In particular, the Federal Government in the USA needs Congressional support to achieve certain key changes, while individual states have considerable autonomy within the federal system. Australia and the UK have their own particular constitutional arrangements which affect the role of central government.

Each nation also must contend with the fact that central government only has a certain number of levers available to achieve change when so much of the critical national infrastructure, along with the technology underpinnings of the digital environment, are controlled by the private sector – often on an international basis.



Common Themes

Against that background, there are some common key themes in the Australia, UK and USA strategies. These include:

- A focus on national cyber resilience
- A need to strengthen regulation and incentives to help raise cyber security standards in critical infrastructure
- Partnership between government, private sector and civil society
- The intent to build further international partnerships and support for responsible behaviour in cyberspace
- A desire to shift the balance so that more responsibility for cyber security rests with the technology sector and less with the individual citizen

This coherence is reflected in the basic structures of the strategies. Each one has its own set of pillars, or what Australia refers to as 'shields', that provide structure. While the wording is slightly different in each case, they show a striking consistency of approach. To paraphrase the three strategies, each roughly structures itself across the following topics:

- Developing a cyber-resilient critical national infrastructure (CNI) and wider economy and society
- Detecting and disrupting threat actors
- Ensuring technology is inherently secure
- Building national cyber skills and a strong cyber industry
- Showing international leadership in cyber and building partnerships

The commonality in approach between the three nations in how they go about structuring their cyber strategies is a striking reflection of many years of thinking on cyber in each country. It forms an interesting blueprint for other nations in terms of updating their strategic approach.

Key Themes

Beyond these headings, each strategy focuses on some major themes, some of them highlighted as being new departures. Nevertheless, there is a high degree of commonality here also.

United Kingdom

The UK's latest cyber strategy emphasises four broad areas:

- Making the UK more **secure and resilient**
- Supporting an **innovative prosperous digital economy**
- Enabling a major increase in the UK's **science and tech capabilities,** especially in emerging technology
- Making the UK **more influential and valued globally,** supporting the agenda of responsible cyber behaviour

In doing so, it emphasises what it calls a 'whole of society approach' to delivering national cyber security. And it restates the UK's commitment to being a 'leading responsible and democratic cyber power'.

United States

The US strategy, while echoing the UK's themes, highlights two fundamental shifts in approach:

- **Rebalancing the responsibility for cyber security** away from end users and onto the technology companies and others that own and operate digital systems
- **Realigning incentives to favour long-term investments in cyber security,** shaping market forces and government programmes so they reward investment in security and resilience

Australia

The new Australian strategy is a focused and thoughtful document with a notable sense of urgency. Its 'shields' show a strong sense of coherence with the other AUKUS allies' thinking:

- **Creating strong citizens and businesses** who understand the cyber threat, understand the actions they can take to protect themselves, and have proper support in place should they become victims of an attack
- **Enabling safe technology** with cyber security built in through clear global standards
- **World class threat sharing between government and business,** along with the capability to block threats before they can cause harm
- **Improved cyber security for critical infrastructure,** including government
- **Building sovereign capability** including in skills and technolog
- **Building partnerships globally** and undertaking co-ordinated action

Resilience Enabled by Regulation and Incentives

It is no surprise that all three AUKUS countries are heavily focused on cyber resilience. Even after some years of cyber security investment, all nations face challenges in the cyber security of their CNI.

For the UK, this means both building a better understanding of the risk and improving its management. One element of improved risk management described in the UK strategy involves a wider rollout of 'Active Cyber Defence' capabilities. This is a suite of cyber services, drawing on private sector support, designed to remove certain high volume, low sophistication threats at scale. So far they have been largely limited to elements of the public sector, but it has long been an ambition to deploy them more widely.

More broadly, the UK is looking at how to more effectively hold CNI to account for delivering the right cyber security standards, including through a combination of regulation and incentives. For example, the UK has been increasing its emphasis on regulation and has discussed expanding the reach of the post-Brexit version of the NIS directive to include a wide range of businesses that provide products and services to CNI as part of a range of new measures.

The USA strategy calls for tailored regulatory frameworks (nodding to some of the risks with poorly developed regulation) and namechecks the work already done in sectors including oil and gas, aviation, rail and water. The intent is to fill remaining regulatory gaps across CNI. There is an action to review how to harmonise regulation, alongside an intent to use Federal procurement processes to demand stronger cyber security standards from suppliers and chase down those who fail to comply.

The Australian strategy sets out plans to review CNI cyber regulation to ensure its existing framework remains fit for purpose. There is a focus on the telecommunications and managed service provider sectors (reflecting close alignment with UK thinking). More broadly, Australia will look to ensure that CNI sectors are complying with their existing cyber obligations. Interestingly, Australia also highlights the need for more support for small and medium enterprises alongside the focus on larger CNI entities.

Driving knowledge sharing and innovation to strengthen trilateral capabilities in the new threat landscape

The flipside of regulations is incentives: the carrot to regulation's stick. The strategies talk about incentives to encourage CNI organisations to raise cyber standards, but some may feel the content here does not quite match the level of focus and detail on regulation.

The USA strategy talks in broad terms about reshaping the incentives landscape, including potentially looking at tax structures. The UK's recent regulation and incentives review discusses awareness raising, information sharing and helping to develop sectoral networks as ways of incentivising improved cyber security. There is a question as to whether this goes far enough. Meanwhile, the Australian strategy acknowledges the need for incentives, but this does not seem to figure particularly strongly as a theme.

Whole of Society Resonse

The complex inter-dependence between government, private sector and civil society in achieving national cyber security is at the heart of the latest cyber strategies. The UK has adopted the term 'whole of society' response to characterise the need for a collaborative and joined up approach to cyber.

Central to this concept is the premise that government cannot achieve success in cyber simply through its own actions, but nor can the private sector. The truth is that most of the key components of national cyber security are outside of government hands and rest in the private sector. But at the same time, there are certain things that only governments can do.

While the language may vary (the USA sometimes talks about a 'whole of nation' approach) the message is the same: a recognition of the need to have effective engagement, dialogue and influence across private sector, universities, civil society and citizens - at home and internationally. Government fundamentally depends on the private sector in multiple ways to achieve national cyber security, and vice versa.

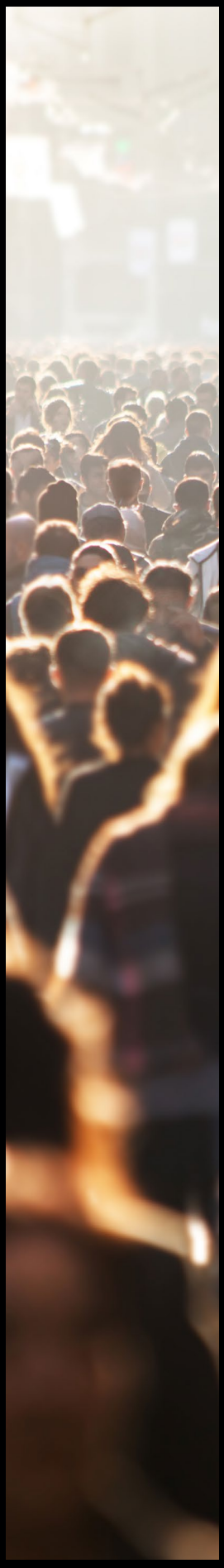
The UK strategy sets out the different roles and responsibilities of government, private sector and civil society. It also cites some practical measures including a new senior group to bring government and private sector together to engage on the most challenging cyber issues and steer the strategy.

The USA, meanwhile, emphasises measures including real time information sharing, bringing the private sector into taskforces including on ransomware and collaborative action to tackle cybercrime.

Australia also talks about enhanced public/private partnerships and states it will create a new Executive Cyber Council to bring together government and industry leaders to consult over the implementation of the strategy (albeit only convening twice a year). Australia also has a 'shield' dedicated to achieving significantly enhanced threat sharing between government and private sector.

The whole of society approach seems a logical solution, but there is plenty of room yet to flesh out what this means in practice and what more substantive actions may be needed to bring it to life. There is a major opportunity here for the private sector and civil society to lean in with their ideas and contributions.

Also tied to the 'whole of society' concept is finding a balance of responsibility for cyber security between the government, citizens and companies that deliver core communications and digital services. Initiatives like the UK's Active Cyber Defence illustrate a collaboration between public and private sector for the benefit of citizens, and Australia's strategy also talks about threat blocking at scale, working with the private sector. Whether governments are able to find the levers to achieve this transformational shift in the balance remains to be seen.



Responsible Cyber Behaviour Globally

Another core theme across all AUKUS nations is the need to have a strong global presence on cyber issues and to promote the principles of responsible cyber behaviour in the face of daily cyber threats from a range of hostile states. There is a high degree of consistency in the UK and USA approaches, while one of Australia's 'shields' is focused on global engagement and working to help create a cyber-resilient region across South East Asia and the Pacific.

A crucial element to this is shaping global internet governance to reinforce a free, open, peaceful and secure internet – in contrast to shaping it in a way that makes it about authoritarian state control. Each of the AUKUS nations are looking hard at how they can build coalitions of like-minded nations to maintain an internet that enshrines the value of freedom and is rooted in a multi-stakeholder approach.

Australia, the UK and the USA also are increasingly joining together with international partners to respond to breaches of the principles of responsible behaviour. This might include naming and shaming by public attribution of hostile attacks, or by co-ordinating on sanctions or other measures.

The strategies also seek to address the wider global issues around securing technology supply chains and building strength in emerging technologies that will be essential for future cyber security.

Countering Cyber Threats

While there is a high degree of commonality in the three cyber strategies, there are some differences in emphasis – perhaps most notably the focus the USA strategy gives to disrupting and dismantling cyber threat actors. The USA has been taking increasingly high-profile action against threat actors, particularly cybercrime groups, using various operational techniques to disrupt their operations, their technical infrastructure and even seek to regain money obtained from ransom payments.

This approach is reflected in the emphasis its strategy gives to this strand, with the aspiration being that disruption will be so sustained and targeted that criminal cyber activity is rendered unprofitable and hostile states no longer see it as an effective means to achieve their goals. This is a bold objective.

The UK strategy naturally has a fair bit to say about countering cyber threats, including using 'full spectrum' campaigns to deter threat actors. But the tone of the UK strategy overall suggests a main focus on cyber security measures as the means of defeating cyber threat actors.

Australia meanwhile has launched a new collaboration between the Federal Police and Australian Signals Directorate, seeing Australia adopt what its government describes as an aggressive approach to disrupting cyber-criminal activity. It remains to be seen how the UK and Australia will develop their approaches to more aggressively counter threat actors.

Conclusion

Overall, any nuances in approach are probably a matter of degree only and overall, the consistency between the three AUKUS nations' strategy approaches is striking. A major focus on national resilience, a commitment to a whole of society response, an emphasis on regulation and incentives, and a determination to promote responsible cyber behaviour through active international engagement appear fundamental to each nation's thinking.

This approach comes with some tough choices and challenges.

- Getting the balance right on regulation so it achieves the desired effect without stifling innovation and competitiveness
- Finding effective ways to make progress on ensuring secure by design principles are built into new technology, especially when so much of that is made overseas
- Putting a real dent into the criminal ransomware threat, which so far seems largely impervious to government intervention
- Successfully deterring and containing the continually evolving nation state cyber threat
- And having a genuinely collaborative approach with the private sector and civil society that truly embodies a 'whole of nation' vision, rather than simply paying lip service to it

It is perhaps inevitable that some of these issues are more fully addressed in the strategies than others, and some areas will prove more challenging to make progress on. But the new national approaches to cyber set out in the UK, USA and Australian strategies represent a coherent and highly active agenda for the future, where success will rest fundamentally on a collaborative approach between government, private sector and civil society – and between nations.

We are Digital Intelligence

BAE Systems Digital Intelligence is home to 4,800 digital, cyber and intelligence experts. We work collaboratively across 16 countries to collect, connect and understand complex data, so that governments, nation states, armed forces and commercial businesses can unlock digital advantage in the most demanding environments. Launched in 2022, Digital Intelligence is part of BAE Systems and has a rich heritage in helping to defend nations and businesses around the world from advanced threats.

For more insights, visit our Responsible Cyber Power page

BAE Systems Digital Intelligence
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom
T: +44 (0) 1483 816000

BAE Systems Digital Intelligence
Level 2
14 Childers St
Canberra
ACT 2601
Australia
T: +61 (0) 2 9053 9330

BAE Systems Digital Intelligence
Malta Office Park
ul. Abpa A. Baraniaka 88
Poznan
61-131
Poland
T: +44 (0) 330 158 3627

BAE Systems Digital Intelligence
Level 28, Menara Binjai
2 Jalan Binjai
Kuala Lumpur
50450
Malaysia
T: +60 327 309 390

E: learn@baesystems.com
W: baesystems.com/digital

linkedin.com/company/baesystemsdigital
@BAESystemsDigi

Digital Intelligence

BAE SYSTEMS