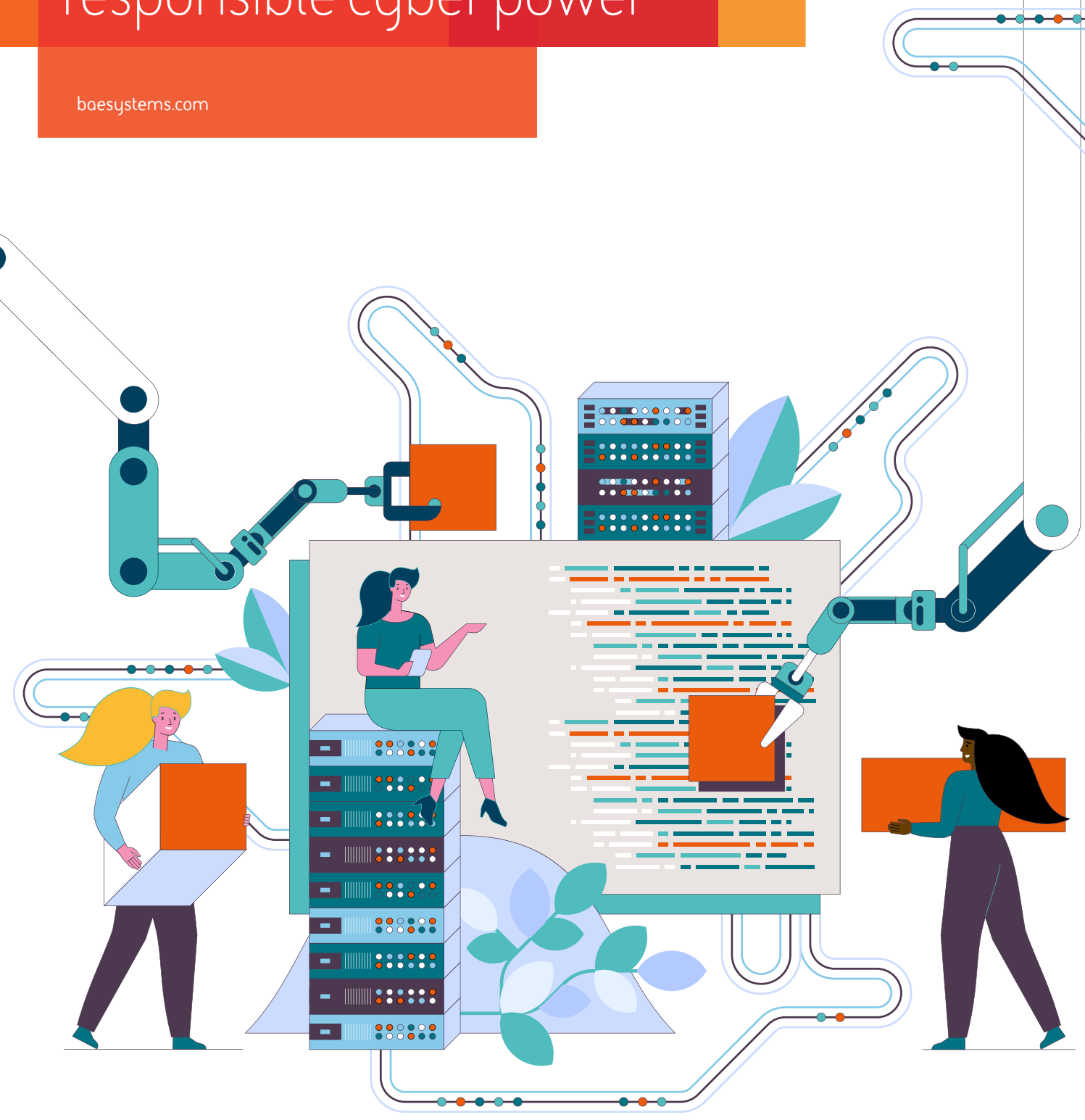
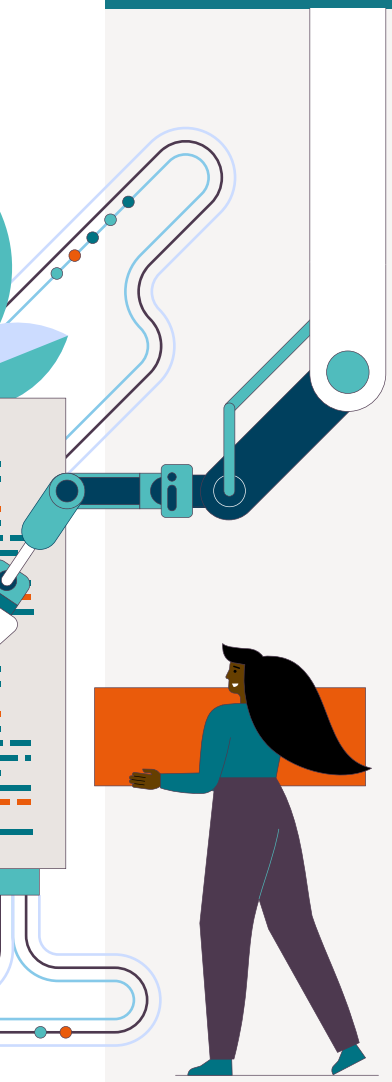
How the UK can be a responsible cyber power

baesystems.com



BAE SYSTEMS

The concept of a 'responsible cyber power' requires clearer definition and a broader, collective effort, says Mary Haigh



The UK's recent Integrated Review of security, defence, development and foreign policy mentions cyber power 22 times, and the foreword from the prime minister talks about the country being a "responsible cyber power". But what does a 'responsible cyber power' mean?

With many countries developing their own cyber power – as described by the Harvard's Belfer Center's National Cyber Power Index, for example – this is becoming an increasingly important question.

Language matters

There are many definitions of cyber power, and differing views as to its value as a concept. The term has a martial feel and it cannot become just another way of saying offensive cyber. If we take cyber power to mean being effective at all elements of cyber operations, and being influential internationally, then strong cyber defences must be the dominant aspect of it.

Without strong defences the UK's ability to wield offensive cyber capabilities is fundamentally weakened. The resilience of the UK's digital economy, its military capabilities, and the preservation of UK society's core values of democracy and free speech depend on having strong cyber defences.

Responsible cyber power must also mean that when the UK does employ offensive cyber capabilities, it does so in accordance with the law, and consistent with a strong ethical framework.

But some countries, such as China and Russia, for example, have very strong cyber capabilities and different thresholds as to what cyber power means.

Their competing narrative creates an imperative for democratic states including the Five Eyes powers to clarify what is meant by responsible cyber power, drawing out the multifaceted nature of it. By developing the UK's military doctrine, by exercising, by writing blueprints setting out the vision of the future, by creating and continually evolving cyber playbooks, the 'grey-zone picture' of the current concept will start to be coloured in, creating a definition of what 'responsible cyber power' means for the UK.

"The resilience of the UK's digital economy, its military capabilities, and the preservation of UK society's core values of democracy and free speech depend on having strong cyber defences"

The UK's **cyber economy is valuable,** generating an estimated **£4 billion** (gross value added), according to the 2021 UK Cyber Security Sectoral Analysis

A huge step forward was last year's creation of the National Cyber Force, uniting teams from the military and the intelligence services. Creating joint teams forces the collaboration so essential to producing an effective combination of hard and soft power. It brings together teams with very different backgrounds and organisational cultures, but with a shared, rare skill set. That diversity will create strength.

We often look at cyber in quite a negative light: emphasis is placed on investing in cyber to avoid expensive attacks, and having a zero-trust approach to ensure that sophisticated attackers are unable to breach one's defences. But it is important to remember that cyber also adds huge value to the UK's economy and its global influence.

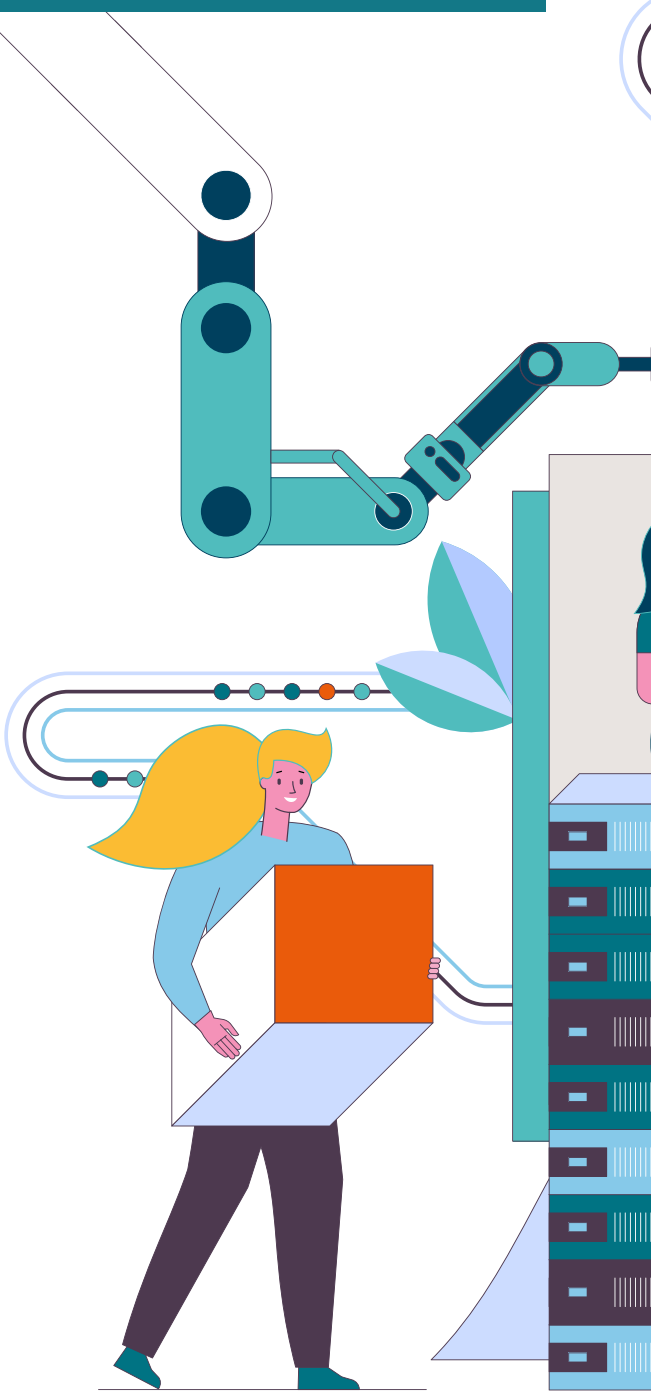
The UK's cyber economy is valuable, generating an estimated £4 billion (gross value added), according to the 2021 UK Cyber Security Sectoral Analysis. This world-leading position gives it great potential to leverage its expertise through cyber diplomacy, a key part of responsible cyber power

Helping others

Fundamental to cyber diplomacy is the sharing of the UK's cyber expertise, offering countries advice and sometimes helping UK allies build their digital infrastructure and cyber security capability. It is also about sharing a positive vision of the future shape of cyber.

Not only is cyber diplomacy invaluable in building relationships and influence overseas, but it also provides strong export possibilities – a perfect opportunity for UK industry and government to collaborate for mutual advantage. Through this cyber diplomacy the UK will be actively sharing its view of responsible cyber power by giving practical help to other countries in building their foundations of cyber power – their cyber strategies, infrastructure, tooling, skills, policies and procedures.

Responsible cyber power cannot be achieved by government alone; it will require the engagement of industry, universities, schools and society as a whole. The greater engagement we have already seen from government on the UK's cyber strategy as it is being written has been welcome. Being engaged in the strategy early on is invaluable to industry. It allows us to have a much deeper understanding of the intent behind the national strategy and to align our investments and strategy with it. Not only does this de-risk some of our investments and activities, but it also allows us to amplify government messages.



"Responsible cyber power cannot be achieved by government alone; it will require the engagement of industry, universities, schools and society as a whole"

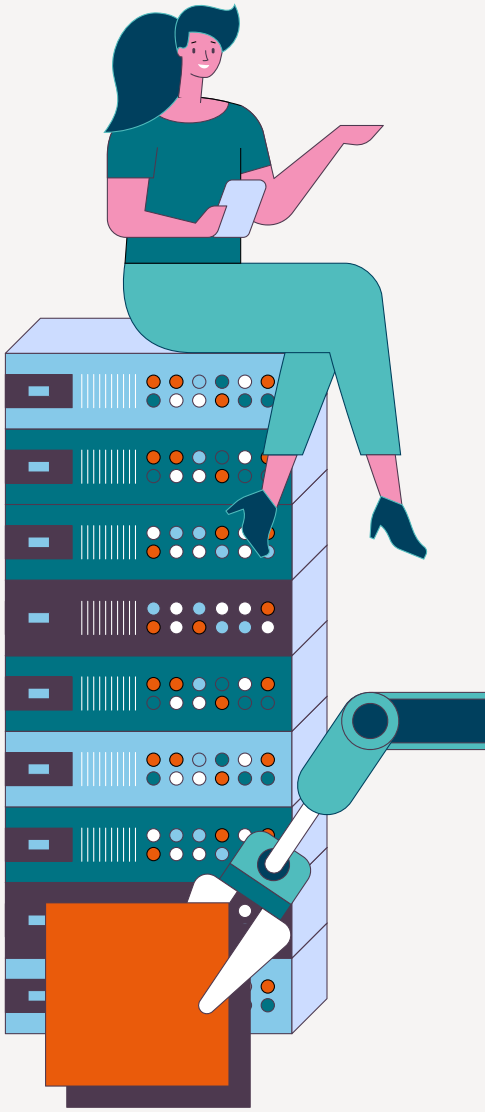
Clear priorities, working with government

When UK industry talks about cyber overseas it does not want to use contradictory or confusing language – it is far better to talk in the language of the UK government. It is also essential that we create not just formal interaction routes but also more one-to-one relationships between governments and industry at all levels.

This means quarterly conversations at the leadership levels, sharing strategies and roadmaps with each other and where activities are common between organisations, connecting up staff working on the detail to ensure best practise and ideas are shared. The more we can foster open conversations and strong relationships, the more leverage and amplification government can receive from industry.

Another key way in which industry can help build responsible cyber power is by working with government to provide scale, the most obvious example being capacity building overseas. The UK government may give advice to foreign allies, but it is limited in its ability to help deliver some of the required cyber transformation programmes.

A joint industry–government partnership will provide not just impartial high-quality advice, but also the support to deliver the changes needed. This is not just about large industry primes, but crucially must bind in smaller, innovative cyber companies as well. The UK government can work with large industry players to achieve reach across the whole of industry – large and small – and to build resilience in a scalable, achievable manner.



A collective, diverse cyber workforce

Responsible cyber power is a multifaceted concept and there are some highly challenging aspects to it. We therefore need to think very carefully about the collective cyber workforce. We need a skilled workforce, not just of software coders and computer scientists, but containing truly broad skillsets, from communications to marketing and from geopolitics to human behavioural scientists.

Moreover, our teams need to be strong teams: they should be able to challenge each other safely, and actively encourage creative thinking and collaboration. All the research shows that the strongest teams are diverse, in every sense of the word: diverse cognitively and culturally, and in terms of gender and sexuality. We cannot think about diversity as a separate topic which buys us 'brownie points'; we have to think about it as a core part of building a strong cyber workforce. The diversity conversation needs to become just a part of the everyday conversation.

One of the best aspects of the recent RUSI/BAE Systems Five Eyes panel discussion on responsible cyber power was that we pulled together an incredible panel of top cyber leaders across the Five Eyes who all just happened to be women.

"We need to pull together very different mindsets across many cultures to achieve any kind of global norms around responsible cyber power"

By having these women speak publicly about a topic in which they are world experts, we are shining a light on them as role models and starting to reset the balance of voices in the debate. Gender diversity is important, but so too is cultural diversity, especially given the global nature of the challenge.

We need to pull together very different mindsets across many cultures to achieve any kind of global norms around responsible cyber power. We need to actively seek out common ground and build out from there. If we achieve diversity in our teams, cyber diplomacy activities will be underpinned by a depth of understanding of perspectives across a range of cultures. We need to create debate, creative thinking and constructive challenge within our teams, and this is just not possible without real diversity.

Not a step, but a process

Achieving diversity is not done through one programme; if it were that easy, we would have already cracked the problem. It is achieved by many small actions, small changes and small initiatives, all of which act together to shift the dial in a meaningful way.

At BAE Systems we have created the RISE scheme for mentoring women in cyber, which is aimed at increasing the number of women in senior cyber positions by raising, inspiring, supporting and empowering (RISE) women. We realised early on that the strength of the scheme would be in opening it up not just to our employees but also to broader industry and government – not only in the UK but also in allied countries overseas.

This has a double-whammy effect: not only does it create a broader base of experienced mentors from a range of organisational and societal cultures, but it also helps to develop one-to-one relationships between industry partners and government organisations. This is a tangible example of the value of including the diversity conversation as part of the general conversation, as it can often lead to multiple, mutually advantageous outcomes.

The shaping of responsible cyber power presents a massive opportunity. We need to avoid groupthink, encourage creativity and foster debates, all of which relies upon a skilled and diverse cyber workforce. This is not just a government problem; industry, universities, schools and society all have to contribute. As many others have also said, cyber really is a team sport and we need the best possible team.

About the author

Dr Mary Haigh, Chief Information Security Officer at BAE Systems

mary.k.haigh@baesystems.com

We are

BAE SYSTEMS

At BAE Systems, we provide some of the world's most advanced technology defence, aerospace and security solutions.

We employ a skilled workforce of 82,500 people in over 40 countries. Working with customers and local partners, our products and services deliver military capability, protect people and national security, and keep critical information and infrastructure secure.

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

BAE Systems
8000 Towers Crescent Drive
13th Floor
Vienna, VA 22182
USA
T: +1 720 696 9830

BAE Systems
19, Boulevard Malesherbes
75008 Paris
France
T: +33 (0) 1 55 27 37 37

BAE Systems
Mainzer Landstrasse 50
60325 Frankfurt am Main
Germany
T: +49 (0) 69 244 330 040

BAE Systems, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK

E: learn@baesystems.com | W: baesystems.com/5G

linkedin.com/company/baesystemsai

twitter.com/baesystems_ai