Digital
Intelligence

BAE SYSTEMS

What's next for the cyber power ecosystem?

Considerations following recent discussions with government, industry and academia, at home and abroad

The last 12 months taught us many things about cyber power – while the concept isn't new, the cyber power landscape is constantly evolving, giving us new technical and geopolitical challenges to consider. And 2022 certainly threw new considerations into the ring.

While the conversation is clearly broader than covering just Europe, the changes witnessed on the continent have had an undeniable impact on the balance of cyber power across the globe – as attested by the National Cyber Power Index which ranked Russia third, just behind the US and China.

So what does the picture look like in 2023? What does that mean for the long-term view? And what can we do as an ecosystem to prepare for what's next?

Observations from engagements across the ecosystem

We've been fortunate to be able to discuss the topic in depth at a number of events in recent months, bringing together key players from across government, industry and academia from both the UK and internationally. There is much we can learn and collaborate on, and seeing the broad ecosystem come together in this way has been exciting as we work towards supporting a whole-of-alliance approach to cyber power.

This is what we've seen:

#1

There is a confidence and clarity across government in its cyber pursuits

We've had the pleasure of discussing cyber power with a number of government departments in recent months, and have seen a growing confidence across government cyber leads with respect to their own cyber pursuits.

While this is exactly what is needed, everyone recognises that cyber power is not a precise science, and there is a lot more thinking required around how to achieve the right impact and effect. So it's also promising to see the different departments listening to each other's views, learning from each other's experiences, and challenging each other in healthy debate.

#2

The ecosystem really can work together

We can all talk about collaboration eloquently but making it happen is sometimes another matter. However, our recent events have showcased the ecosystem working together on difficult strategic issues.

What has that looked like in practice? While government takes the lead on policy – setting strategic objectives and explaining its thinking and boundaries - industry players can play an active role in the debate and contribute their perspective and delivery experience. Meanwhile, academia can challenge the thinking of government - by providing academic rigour and evidence to difficult strategic policy questions such as 'what is responsible cyber power?' and 'does cyber deterrence work as a concept?' Furthermore, as mentioned in point one above, HMG departments can also benefit from asking each other challenging questions. Working like this, the whole ecosystem can support putting responsible cyber power into practice effectively.

#3

‘How can industry be incentivised?’ is a really common question

This is a challenge that has come up in several of our discussions. Certainly, as we work towards a whole-of-nation or whole-of-alliance approach to responsible cyber power, it is important for industry players to pull in the same direction.

Perhaps the key will be a combination of policy standards, industry-government communities and joint exercises, but this is something that will no doubt need to be considered further, particularly as we look to amplify government and industry impact overseas.

#4

There are unresolved issues

Our ecosystem is still challenged by several issues, as evidenced by some of our recent discussions with players across the board.

Those areas that we must explore further include:

- Cyber deterrence as an integrated set of capabilities which combine to deter adversaries or impose costs
- The vulnerabilities that remain in global supply chains and how resilience can be achieved in an interconnected world
- Influence over the way digital technology is developing and being adopted
- Proliferation of cyber capabilities in a way that reduces risk and projects responsible behaviour

These areas give us all an agenda to dig into over the coming months and years. They are issues that will not be solved fast, but provide further opportunities for government, industry and academia to come together.

#5

It's never been more important to share with and learn from allies

Hearing perspectives from the international community has been illuminating. We had an opportunity to discuss the topic with teams in the US recently, and learnt much about their different relationships with industry, and different approaches to deterring adversaries.

Sharing approaches with partners who have different views is useful for everyone – all nations have a different geopolitical landscape, capability toolkit and mindset, and a challenge like 'incentivising industry' is likely to be subtly different for each, so engaging on these specific topics with partners will help as we continue to shape our own position.

What have we shared about the BAE Systems view?

As evidenced by the above observations, cyber power is a topic that benefits from multi-stakeholder perspectives, and as research continues in both private and public domains, the diagram below sets out a functional model, which is used by BAE Systems to capture a single pane view of cyber power players within a nation.

We have shared this at recent events to discuss our view of the cyber power ecosystem.

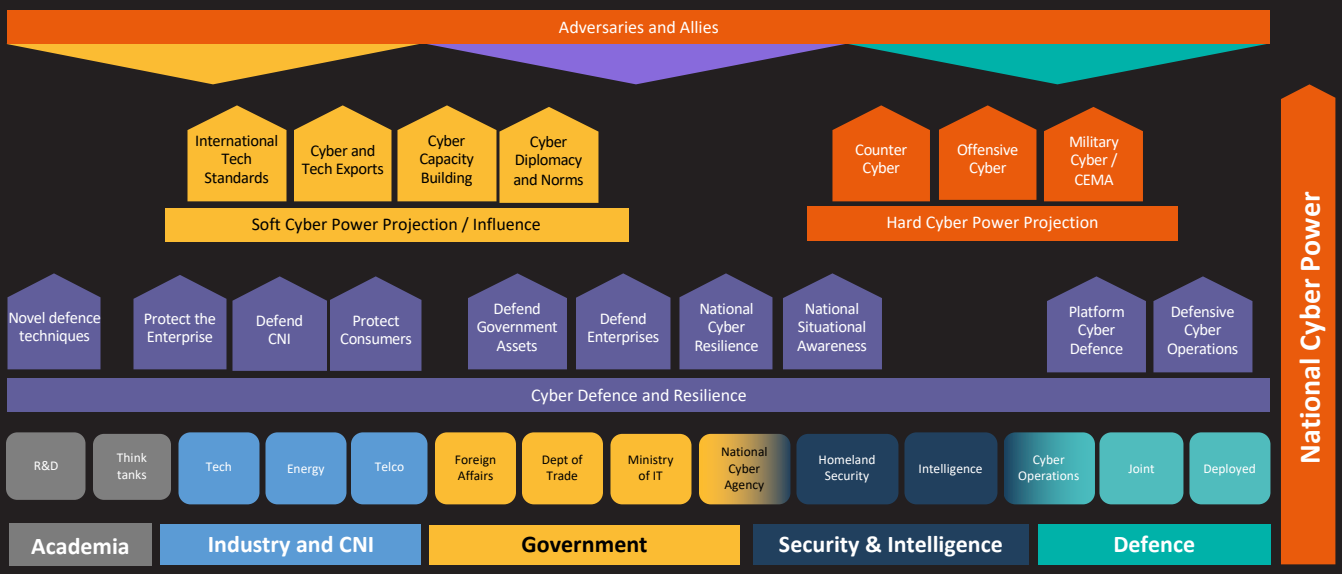

Figure 1: "The BAE Systems view of the National Cyber Power ecosystem."

At its core, cyber power is a national ecosystem that is capable of protecting itself. Both at an organisation level in terms of businesses and departments protecting their own assets and operations, and at the individual level, whereby societal resilience is achieved with citizens who are capable of maintaining their own cyber hygiene.

As well as the different parts of the ecosystem protecting themselves, national cyber defence requires a national coordinating centre, tech and policy leadership, deep situational awareness and protection of public and mid-space domains.

As the diagram shows, we must also consider capabilities that are more aligned to what we think of as 'hard power' – these are capabilities that are usually wielded by the state or on behalf of the state, often by security services and military. These capabilities produce cyber effects that are more adversarial, coercive, intrusive or potentially destructive.

But there is a whole emerging area of cyber power which we can think of as the softer power elements - international cyber capacity building, international trade, cyber diplomacy, influence over tech standards and global norms, all come into play here. As we can see, cyber power groups together some very different capabilities.

You could perhaps look at this ecosystem as a rugby team. Each player should be striving to hone their own skills in cyberspace – to master their craft, keep ahead of best practice and showcase that skill to the rest of the team, adversaries and peers. However, they must also be team players: thrive as part of set plays, understand and leverage the capabilities of teammates, and make sure to support each other.

What's next for the cyber power ecosystem?

We learned much from sharing our view of the cyber power ecosystem with other stakeholders over the course of 2022. But we are just one industry player, and it's the feedback and debate with others in the ecosystem that has been most valuable. As our five observations above indicate, there is much more to discuss in 2023, but having those open all-ecosystem conversations with both national and international players, is where we can make the most progress together.

BAE SYSTEMS

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

E: learn@baesystems.com | W: baesystems.com/threatintelligence