baesystems.com/theintelligencenetwork

The Human, Economic and Global Risks of Emerging Technology

The six key issues society faces in the new technological landscape

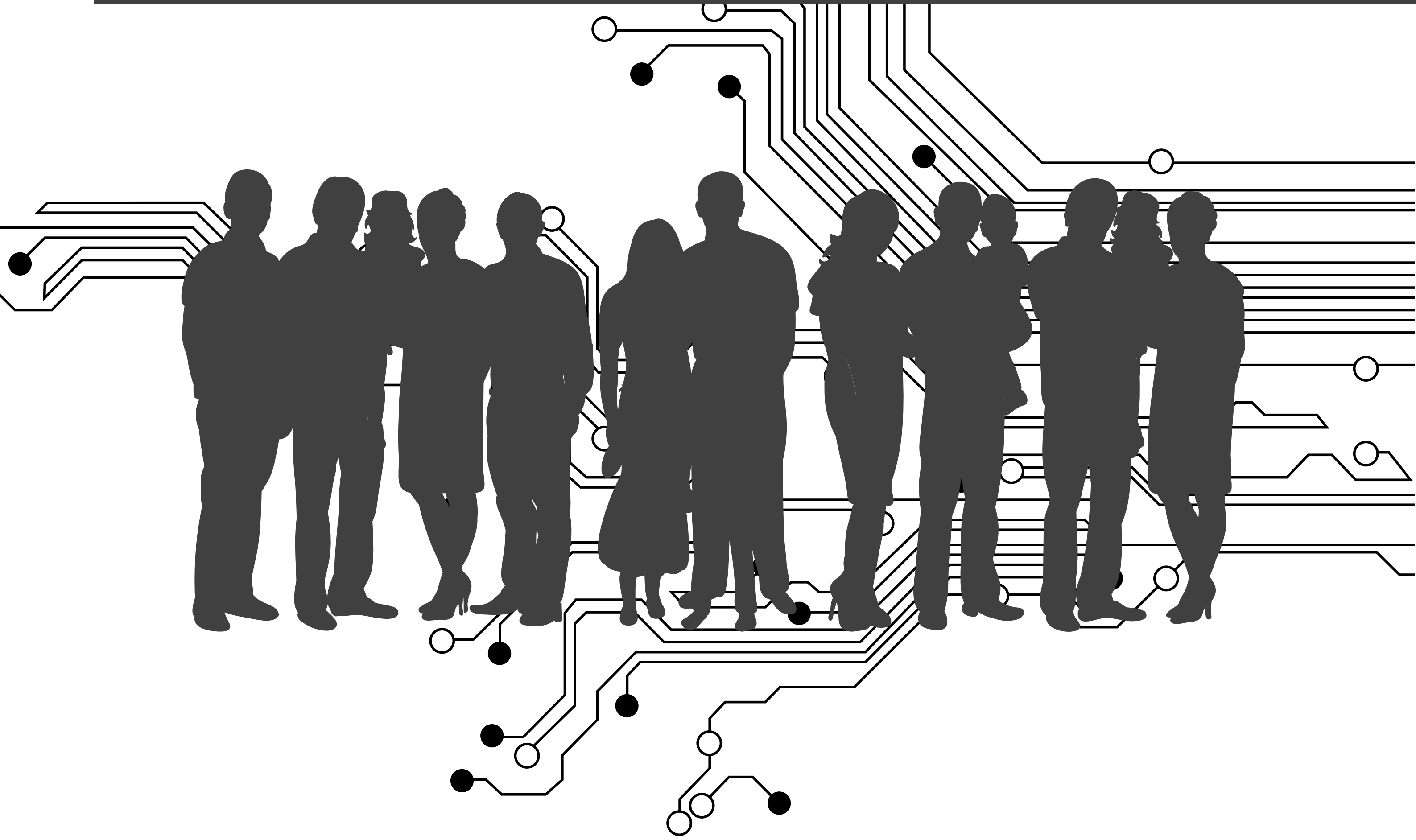
BAE SYSTEMS

Technology has been the engine room that powers society, the economy and government for decades. But the past few years have witnessed an explosion in digital advances driving consumer and enterprise innovation that will transform the way we all live and work.

The creation and dominance of hyper-scale platforms, combined with technologies like artificial intelligence (AI), quantum computing, 3D printing and 5G communications, are driving an ever more seamless integration between technology and humanity, bringing disruption to organisations large and small, public and private.

At BAE Systems Applied Intelligence, it's our job to anticipate the consequences of these profound shifts – which is where The Intelligence Network comes in. At a recent roundtable event, in partnership with RUSI, we brought together some of the world's leading experts in this field to analyse these systemic changes via **six key lenses.**

Click here to find out more about The Intelligence Network and how your organisation can get involved



I. Hidden complexity

With the democratisation of these technologies, what are the inherent risks in hiding complexity from users and how do we protect against them?

The significant trends towards the democratisation of technology – from the Internet of Things (IoT) to the proliferation of cloud utility services – has meant that the barrier to adopt and integrate new digital advances has dropped precipitously over the last few years. However, those who do adopt these technologies, as well as the technology providers themselves, can overlook security challenges, and the ability of users to understand and manage that risk is harder than using the technology itself.

Even before the pandemic, governments and businesses were wrestling with issues around global supply chains. The dependence on other countries for key technologies and other goods, as well as the lack of sovereign capability in critical areas, has also prompted increasing concern. A key element is having the right skills in place – there is a big skills agenda in the UK but there is scope to do more, particularly as remote working means that organisations can source these skills from anywhere.

But it's not just the skills gap. There are many skilled people, especially in security teams, but their voices aren't being heard because the consequences would lead to painful reorganisations and budget reallocations – senior leaders sometimes appear not to want to hear the message. Ironically, the backdrop to this is that in many ways the goal of technology is to eliminate users' skills.

From turning the lights on to driving a car, the whole point is to make it as simple and unskilled as possible. This means that solving these issues via enhanced skills goes against the grain of wider technology trends. It's not just a user issue either – it is difficult for professionals to understand what is going on in multi-layered systems and technologies because of their sheer inherent complexity. If IT professionals can't understand algorithms, for example, consumers aren't going to either.

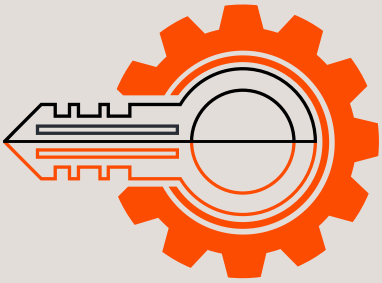
There also tends to be an assumption that security issues and risk get managed automatically. In reality, they don't get managed at all unless someone deliberately does so. When trying to decide whether or not to spend more money to manage this issue, there is no economic incentive for a leader to increase spending levels because there is nothing requiring their competitors to do the same. This means there is an economic hurdle working against companies doing what, in theory, is the right thing in order to manage complexity and risk in new technologies.

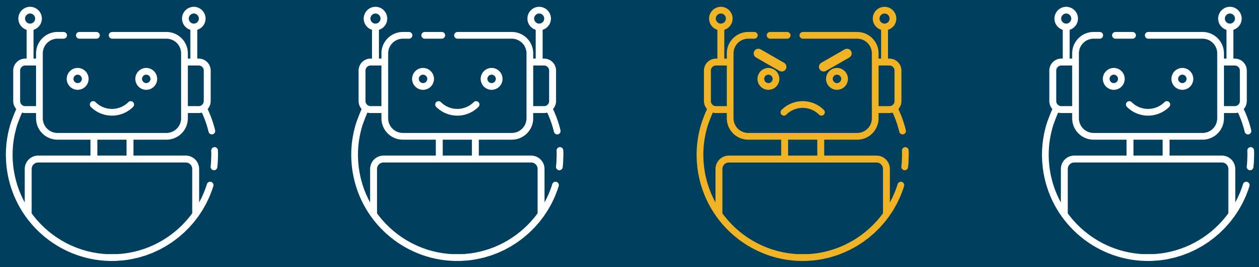
The only real way to make it happen consistently is through some form of standards. For example, the UK's National Cyber Security Centre (NCSC) has a code of practice for consumer IoT but this is only a British-based standard. Progress is only really made at scale if some combination of the European Union or United States puts forward a new standard which means that for organisations it's simply not worth not meeting it – like GDPR, for example. On its own, a single domestic market isn't big enough to drive suppliers towards extra cost.

With technology taking an increasingly significant role in how we run our lives, so the risk increases of something going wrong. In virtually every other aspect of life – healthcare, transportation, industry – there are accidents; it's impossible to eradicate them entirely so they are all insured against. Interestingly, this is something the technology sector has been slow to consider – yet – but certainly the cyber insurance market can learn from the example of other parts of the economy. The reason we as consumers of the technology should care, is that in other sectors, it is the insurers who apply pressure to raise standards. In areas such as car safety requirements and building codes, they have the incentive to minimise their losses.

2. Enabling bad things

How do we best understand the malevolent unintended uses of technology and how do we guard against them?





Government is always looking to see if there will be unintended side effects of new technologies, particularly when the rush to take new inventions to market is very powerful. An example is digital twins – digital replicas of a living or non-living physical entity – an issue which is particularly pertinent in the electric vehicle market. Every Tesla car, for example, has a digital twin and this means data is sent back and forth to the car and can potentially change its behaviour. So if someone got access to the digital twin they could damage or break all or indeed a particular car. But digital twins are also seen as the saviour of validating complex artificial intelligence (AI) as well – they are a go-to engineering tool for engineers when monitoring in-field equipment, for example. This all means that it is difficult to prevent some bad things occurring when new technology is implemented.

Money often underpins the malevolent corners of the internet. Most of the bad things online are rooted in people trying to make money in illicit ways – in transactions via cash or bitcoin. If such transactions could be eliminated, particularly those involving bitcoin, then that would remove one of the main mechanisms of cyber-crime and would be extremely effective – ransomware wouldn’t exist if bitcoin wasn’t there. So there are things that can be done in terms of the nature of payments and transactions that would make it harder to do bad things.

It’s also important to remember that no technology comes to market without overcoming many difficult hurdles. This prompts its creators to pro-actively sell the benefits of their idea and encourages them to minimise any downsides. Similarly, designers mostly design with the positive user in mind – it’s very rare for them to consider what someone with nefarious motivations could potentially do with their product; only cyber intelligence teams do this and even then this isn’t commonplace. The challenge is that if new applications and technologies are sold as “magic” then it puts the onus on technologists and engineers to understand how it works and decide whether it is a good or bad thing. Opening it up, though, would encourage more responsible decision-making, as well as greater consumer education and awareness – which is currently non-existent.

3. The human impact

When it comes to the introduction of automation, ML and AI, what are the risks to individuals and workers and how best to protect them?

People have been predicting for literally hundreds of years that technology is going to destroy all employment. The burden of proof is on those who believe that technology and automation are now suddenly going to eliminate jobs, which is something they struggle to do as there is very little evidence this is the case, even today.

The impact of technology is often submerged into the impact of globalisation – and globalisation has destroyed large numbers of jobs in particular communities – but the blending of the two is unfortunate. As an example, AI is already having less of an impact than was predicted three or four years ago. As researchers experiment with potential applications, in virtually every field, the combination of AI and the human has been found to be the best way to do just about anything.

By way of example, three or four years ago, the work looking at the impact of AI on security and defence was about replacing people. But now it has been found to be much more impactful when augmenting and optimising the human involvement. AI is very effective in a closed environment but the larger the environment, the more that augmentation comes to the fore – as opposed to taking over entirely.

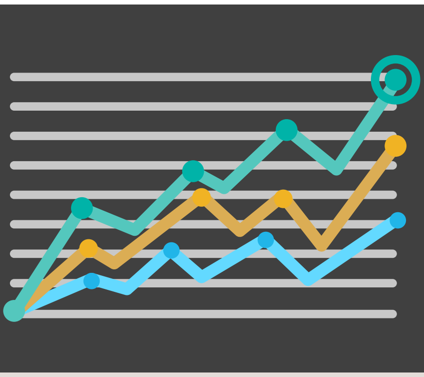
Looking at the effect on society as a whole, you can see the impact on social media and the way algorithms are being used to drive people's attention to feed them a constant reinforcing set of messages. Government has to intervene to some extent if and when emerging technology is having a detrimental effect on society, but it should only do so via intelligent and prescriptive regulation tailored to each individual challenge.

When it comes to understanding the role of government, it starts with the education system, which is not fit for purpose – particularly for the technologies we are building and creating, as well as the skillset that needs to be developed. Government has a crucial role to play in designing a curriculum that better equips citizens to understand AI. Of course, the problem here is that this will help in 10 to 20 years' time but governments are measured by and need more immediate results.

But if we aren't educating children in school, if we're not educating people in the workplace, and if we're not educating journalists to offer better analysis, then we're setting ourselves up for a problem. This raises other challenges, such as how to explain AI to the younger generation? How can we get it on CBBC? It's important to remember that it's not just for kids – it's for their parents and their teachers as well, akin to a public health message aimed at the young but which can also help educate the wider population. The bottom line is that there are 67 million people in the UK who need to understand modern technologies like AI, and this can only occur through some form of collaborative ecosystem made up of academia, industry and government.

4. Economic side-effects

What are the economic risks, how do we mitigate them and focus on maximising the economic benefit?



Countries in the West are not going to be able to compete with China and India without more automation and productivity, the economic product of which is required to pay for improved living standards. Higher productivity is associated with higher wages and, along with automaton, is really the only path going forward. In the end, governments need virtually all the automation possible – from agriculture to the energy grid to education – in order to accelerate economic growth.

Prosperity and economic strategy should be at the heart of cyber strategy and this means becoming a data-driven digital society with greater investment in new technologies. This involves government becoming the customer of first choice for start-ups, purchasing their services and helping them on their way to becoming medium sized companies, while also doing things like working closer with academia and encouraging the private sector to take on more risk.

Big tech is often incorrectly painted as the enemy, something to be wary of and controlled. It will be interesting to analyse the impact of the French government's move to tax large corporations and whether it leads to increased tax revenues or new rules to minimise their exploitation of markets. After all it has been the sheer strength of certain large companies – such as Amazon and Microsoft – which has helped get us through the pandemic. Imagine how much worse things would have been without the ability to move seamlessly to cloud enabled remote working or the use of hyper scale computation platforms to run the enormous simulations required to support genome sequencing and vaccine development.

Looking at the approaches of China and the US, there are actually some similarities between the two different models but the "dirty secret" of AI is that it requires vast amounts of data in order to thrive. This runs contrary to the reality that data is also a security risk and notion of privacy by design. The more data and the more diverse the data sets that you are able to provide to researchers, the faster they will develop AI models and the better they will become at using technology to deliver productivity enhancements to benefit their economy. Resolving this inherent conflict requires the acknowledgement that it exists – which doesn't always happen – and these questions are only now starting to be raised.

5. Global power

What are the risks and implications for global power structures? Are globalisation and the rise of China and India heralding change?

Over the next decade there will be fragmented and competing supply chains. Companies have to plan for a context of increasing Chinese domination of emerging tech, with a competing Western model alongside it. There also needs to be the acknowledgment that there is no such thing as untrusted tech – there is risk in all the tech we use, no matter who makes it. So it is a very interesting global context which demands strong cyber security, greater vendor diversity in supply chains, and resilient Critical National Infrastructure.

It's also clear that the old traditions of sovereign control and freedom to act as a sovereign nation may be less relevant than they were. In the technology space, the UK, for example, has done very well. It has companies which still provide massive elements of infrastructure and technology so it still maintains its own capability but it's all subject to the ups and downs of the market.

It's increasingly difficult for countries even as powerful as the US to have complete freedom and control. This means that countries are likely to need to work closer together to ensure they have plurality in supply options and that they have the freedom to control whatever is deemed in the national interest – the pandemic and supply chains have certainly focused a lot of minds. And the sheer size of many companies means they can't be influenced by any one country – they will have to work together to enjoy any measure of control.

The foundations of the digital economy are such that only two countries in the world – China and the United States – have a horse in the race, leaving it very difficult for others to compete. As part of the emerging cyber security strategy there will be a need to expand beyond traditional areas seen as sovereign, such as the very tightly controlled defence and security core, into other things like Critical National Infrastructure. It's not about building competitors to things that are already won but more about looking at the layers above things like Azure and AWS, identifying what new intellectual property can be developed in new areas.

However, despite the size and power of China and the United States, not all is lost, other countries have a role to play too. India believes it will be in a position to catch up within 5-10 years and even now, the third largest producer of technology in the world is Taiwan – America is more dependent on Taiwanese manufacturing than it is on China. Small countries, then, can play a tremendous role as well, and nations such as Japan and South Korea would not hesitate to say they will be self-sufficient when it comes to building their computer networks.

6. Navigating to benefit

Are there any overarching elements that can help governments tip the balance in favour of the benefit for business and society whilst minimising the risk?

Getting the regulation right is really important. It's the role of government to raise cyber standards and governance across the digital economy – particularly relating to Critical National Infrastructure. This means there is a need to invest in skilled regulators to enforce these regulations but they need to be intelligent and prescriptive – there shouldn't be regulations for the sake of it.

Government also needs to change its narrative. Technology is what has helped us through the pandemic, is the thing that will help countries compete against China and is the thing which will help deliver a decarbonised economy. Yet the government narrative is that technology is destroying jobs, privacy and even our culture – a message which is then amplified back and forth by the media and, as a result, has become the dominant way people think about technology.

The diversity of people working in technology also has a role to play. This challenge has been around for decades, but making technology more attractive as a sector would help bring more people into this conversation and help spark new ideas and approaches. Yet despite abundant initiatives, women still only make up 20% of the workforce in Silicon Valley and that includes traditionally more diverse areas like HR. Tech is not just about coding, it's about working as a strategist and bringing in the thinking of social scientists and much more. Government can and should help encourage young talent, especially girls, into the sectors like cyber security.

Governments find it hard to change their course. They are there to respond and have to have time to do that but the challenge is that emerging technology doesn't wait. It's highly likely that emerging technology will be part of the solution for climate change, for example, but it's also going to come with negative things – and it's these which are difficult to control and predict – but that is the challenge our elected leaders need to grasp and successfully navigate.

But it's not just about government. Civil society has a role to play as the answers to these challenges are not going to be found in one place; it will need that full spectrum of different perspectives to be brought together, including the pro and anti-technology minds, in order to have a proper argument rather than conversations occurring only in echo chambers.

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
Level 1
14 Childers St
Canberra, ACT 2601
Australia
T: +61 1300 027 001

BAE Systems
Suite 905 Arjaan Office Tower,
Dubai Media City
Dubai
T: +971 (0) 4556 4700

BAE Systems
1 Raffles Place #42-01, Tower 1
Singapore 048616
Singapore
T: +65 6499 5000

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

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

in linkedin.com/company/baesystemsai

twitter.com/baesystems_ai