Digital
Intelligence

BAE SYSTEMS

BAE Systems Digital Intelligence 2023 Predictions

The BAE Systems Digital Intelligence team lay out their 2023 predictions

Jessica Regan	Project Manager
Neil Sherwin-Peddie	Head of Space Security
John Young	Head of Strategic Campaigns, Space
Elizabeth Seward	Head of Strategy, Space
Adrian Nish	Head of Cyber
James Muir	Threat Intelligence Research Lead
Miriam Howe	Lead Cyber Consultant
Mivy James	Digital Transformation Director
Rob Wythe	Chief Technologist, C5ISR
Andy Lethbridge	Global Head of Consultancy, Central Government
Victoria Knight	Strategic Campaigns Director
Theresa Palmer	Head of Diversity and Inclusion

Space

AI and machine learning to be applied more widely to analyse huge datasets generated in space

"While AI and machine learning are already used in other sectors, practical applications in space are currently in their very early stages. In 2023, however, we will begin to see new capabilities applied more frequently when it comes to analysing huge datasets generated by satellites. Currently, most sensors in space downlink everything they are trying to collect, which makes it difficult for those on the ground to pick out signals from the noise in a timely manner. Using AI and machine learning to analyse this data on board makes it possible to only downlink relevant pieces of information rather than sending the data set. The benefits will be significant for people on Earth, enabling us to better protect citizens in near real-time."

Jessica Regan, Programme Portfolio Manager

The first major satellite hack

"From the attacks on ViaSat via supply chain vulnerabilities which exposed the ground terminal, to more recent threats against Starlink low earth orbit (LEO) satellites, events in 2022 have indicated that the space race is far from over. In 2023, the focus will continue to shift towards satellite compromise, with the first major satellite hack to be expected in the next 12 months. This will likely involve all three main attack vectors: ground, communication links and payload hijacking.

"From the ground station perspective, it is highly possible that vulnerabilities in physical security will be targeted. Leveraging the cost-of-living crisis, malicious actors could exploit insiders to gain direct access to Satellite Operations Centres and Mission Operations Centres.This will enable them to take control of spacecraft, disable communication links or capture all earthbound transmissions.

"Communication links will also be a prime target in the coming years. Earth-to-LEO satellite communications are vulnerable as spacecraft are frequently passing over potentially hostile territory. The adversary can use satellite blinding as these satellites pass to capture critical imagery or radio frequency data.

"Lastly, poorly developed DevSecOps principles could see the introduction of malware based on the reliance on COTs code bases. A lack of understanding around code and applications could allow an attacker to hide on spacecraft payload and run tasks undetected."

Neil Sherwin-Peddie, Head of Space Security

Partnerships and collaboration with SMEs

"In 2023, space innovation will become even more vital for boosting defences and delivering advantages on Earth, especially in a time of increased conflict and tension. We'll therefore see more emphasis on growing the sector in line with the government's National Space and Defence Space Strategies.

"As part of this growth in innovation, a greater focus will be placed on involving smaller organisations in defence programmes and contracts. For this to happen, the relationship between 'primes' and SMEs will need to evolve beyond supply chains, which means working together in a new, dynamic way. Not only will this collaboration help smaller organisations in the space sector to grow, but it will also enable 'primes' to deliver enhanced capabilities to customers.

"The onus is also on customers to encourage collaboration by outlining it in contracts and development programmes. Risk levels increase when working with smaller organisations, which is something customers will have to accept and build into programmes."

John Young, Head of Strategic Campaigns, Space

The investment in reprogrammable satellites to address the issue of space junk and debris

"Within all sectors, there is no doubt that sustainability will be a key focus in 2023 and beyond. For organisations within the space sector, there are two very different areas they need to address.

"The first relates to the organisations themselves. Many will continue to find ways to develop capabilities in a sustainable way to meet the net-zero targets. This might include switching to clean energy sources and electric propulsion to working in partnership with other organisations to introduce new green initiatives"

"The second links to sustainability in space. There is currently a growing amount of junk and debris in space, which is leading to a sustainability dilemma. Over the coming years, we will see more efforts to build awareness around the impact of satellite launches and deploying new equipment, as well as removing dead satellites. We can also expect to see the sector innovate to increase the life expectancy and versatility of satellites. At BAE Systems, for example, we've partnered with In-Space Missions to invest in satellites that are reprogrammable. Moving away from deployment and launch for a single mission, providing reconfigurable, mission-specific satellites that can refuel and re-equip in the longer term will be critical."

Elizabeth Seward, Head of Strategy, Space

Cyber

"Over the last year, we've seen even more examples of how cyber-space is being abused to disrupt individuals, organisations and nations. While their motivations may differ, cyber criminals continue to capitalise on today's tumultuous landscape, whether it's through launching ransomware attacks, threatening critical national infrastructure, or exploiting vulnerabilities in emerging technologies.

"Looking ahead to 2023, cyber attacks will continue to be a challenging facet of our global security. Organisations in both the public and private sector will need to work together to mitigate potential threats, paying close attention to new risks such as adversarial AI, threats to 5G and energy networks, and changes to cyber insurance policies.

"Against this backdrop, the UK will place more emphasis on becoming a 'responsible cyber power' in line with its **2022 National Security Strategy.** A big part of this will involve building greater cyber resiliency across every part of the country. Building up our cyber defences will require a massive team effort; we'll see more collaboration between industry, government and academia to improve cyber capabilities and skills at every level."

Adrian Nish, Head of Cyber

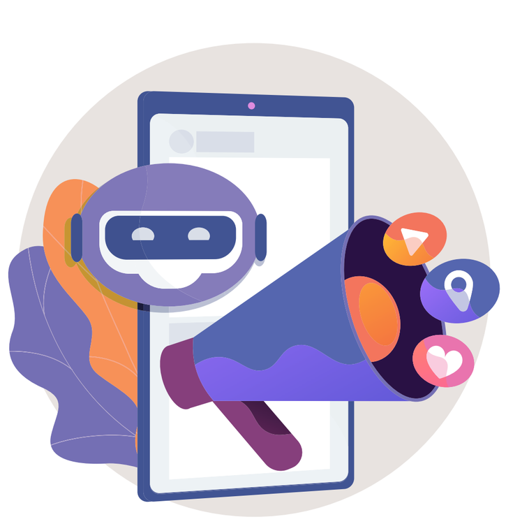
2023 could be the year 'the world is held to ransom'

"Over the last few years, ransomware attacks have risen in both sophistication and frequency. We've seen targets move from individual consumers, to small businesses, to large enterprises. In 2022, we even saw entire countries being held to ransom, including attacks on Costa Rica and Montenegro that crippled multiple government services.

"Today's ransomware criminals are getting bolder, homing in on large organisations that deliver critical value to society. As this landscape evolves, it is not outside the realm of possibility that 2023 could be the year that cyber criminals hold 'the whole world to ransom'; from exploiting flaws in widely-used operating systems, to supply chain attacks in software used globally, to targeting international critical national infrastructure.

"Getting ahead of attackers is therefore paramount. This will involve collaboration between public and private sectors, sharing knowledge and working together to detect and respond to potential threats."

Adrian Nish, Head of Cyber



Adversarial AI reaches a tipping point to become a real world concern

"There is still little evidence around the use of AI for launching cyber attacks. A more concerning aspect to consider, however, is the field of adversarial AI, whereby target AI systems are exploited as part of an attack.

"In 2023, it is possible that this type of threat will reach a 'tipping point', moving from being mainly an academic matter to a real-world concern. We can expect to see more attempts from cyber criminals to poison training data and confuse AI systems with special inputs.

"One way an adversarial AI attack could lead to real-world consequences is if vulnerabilities are found in widely-used AI frameworks or codebases. It is likely that attackers will develop easy-to-use tools to exploit these vulnerabilities, potentially opening up a whole new class of attack. How and when this may happen remains unclear, but the creation of new security policies to mitigate potential threats will become increasingly important."

James Muir, Threat Intelligence Research Lead

Developments within the cyber insurance market will have serious, knock-on impact effects

"In 2022, the rising threat of ransomware attacks led many insurers to raise premiums and reassess coverage. Going into 2023, Lloyd's of London announced that its insurance policies will no longer cover losses from state-sponsored cyber attacks, effective from March. We can expect these dynamics to heavily impact organisations. Many will find themselves without appropriate coverage and be required to use emergency incident response services outside of their existing arrangements.

"The change in cyber insurance policy could also affect government-led attribution of cyber attacks to state entities, which is often a challenging task in itself. All of these factors combined means that if a NotPetya style incident were to occur, the repercussions could be severe."

James Muir, Threat Intelligence Research Lead

Energy security and cybersecurity to converge

"As more focus is placed on building a more sustainable future, the motivations for energy-related cyber attacks will likely increase across the entire threat landscape. At the low end of sophistication, we have already seen numerous scams related to energy bills, including fake emails or texts to steal individuals' personal information. At the high end, the potential for state actors to disrupt energy networks looms large in certain regions.

"As companies across the globe look to green agendas and innovation in 2023 and beyond, new opportunities for threat actors will doubtless arise. Next year, we could see actors find other links between energy security and cyber security, such as espionage efforts into green technology or energy policy, along with environmental hacktivism."

James Muir, Threat Intelligence Research Lead

Retaining and upskilling mid-level cybersecurity employees will be a top priority

"In recent years, the cyber skills shortage has had a serious impact on organisations' abilities to mitigate emerging digital security risks. As the public and private sectors have collaborated to bridge the gap, we have seen more programmes – such as **CyberFirst Girls** – dedicated to helping young people from all backgrounds enter into cybersecurity careers.

"While these efforts are very welcome, many organisations are also struggling to find and retain people with mid-level experience. To truly bridge the cybersecurity skills gap we also need to look at upskilling employees at all levels of their career. In 2023, it is likely that we will see an increasing number of learning and development programmes aimed at mid-level employees."

Adrian Nish, Head of Cyber

5G rollouts will widen the attack surface

"Predicting the direction of travel for the 5G threat landscape is not a straightforward task. The 5G standard itself offers significant security improvements compared to its predecessors like 4G and LTE. But the infrastructure required to implement full 5G rollout – with increased dependence on IT, as well as virtualisation and cloud infrastructure – could increase the attack surface and expose vulnerabilities.

"When looking at radio access networks (RAN), for example, security researchers have pointed to poorly configured virtualised environments in existing OpenRAN deployments, including numerous issues in Kubernetes configurations.

"On the core network side, as the rollout and implementation of new features becomes more complex, it is possible that we'll see security misconfigurations that impact wider 5G networks. Adopters of 5G must therefore pay greater attention to the risks surrounding 5G security, with specific high-threat use cases – such as military scenarios – having been discussed in whitepapers this year, including CCDCOE's research report on Military Movement Risks From 5G Networks."

James Muir, Threat Intelligence Research Lead

The UK government will evolve its cyber capabilities in line with the National Cyber Strategy

"The publication of the **National Cyber Strategy** a year ago embedded cyber power as a key thread throughout the UK government's vision for the future. Since then, we've seen government stakeholders engaging with confidence on their cyber objectives.

"In 2023, we expect that there will be greater focus on stretching and evolving the UK's existing cyber capabilities, which will mean entrenching partnerships and joining up effects across government. As success cannot be achieved by the government alone, we expect there will be a concerted effort to engage and co-opt industry across a spectrum of pursuits and through a range of tools and incentives.

"We can also expect to see more consolidation of cyber and the electromagnetic activities and an integration of this military concept with other cyber pursuits across Defence and government."

Miriam Howe, Lead Cyber Consultant

Defence

Defence to break down data silos to gain advantage

"To stay a step ahead of the adversary in a tumultuous geopolitical landscape next year, defence will double down on creating greater visibility. As a result, we will see the sector move away from siloed systems to a military end-to-end internet of things.

"This will involve securely forming connections with data across a complex environment. The effect will be like weaving digital threads; joining dots between multiple digital domains to bring together different sources of information.

"In practice, this means creating a data fabric that allows intelligence to flow safely between interoperable systems, seamlessly linking sensors with decision makers and "effectors". Importantly, this data flow needs to be audited, trackable and organised, creating a controlled ecosystem where people retain their ownership.

"Defence will seek inspiration from other sectors to make this vision a reality, looking towards the open banking model – and the APIs involved – for ways to enhance interoperability.

"By breaking down silos and safely linking data, the sector can work together to identify patterns, spot problems, and ultimately, find solutions to some of the biggest challenges it is facing today."

Mivy James, Digital Transformation Director

Defence to modernise and transform in line with the tumultuous geopolitical landscape

"All five defence domains – maritime, land, air, space and cyber – are being influenced by a series of technological, climatic, social and economic factors. Priorities for defence organisations are evolving as a result, and will continue to do so next year in line with the tumultuous geopolitical landscape.

"The defence sector will need to keep up with this pace of change to push boundaries, drive innovation and remain secure. Technological evolution in commercial markets is surpassing that of traditional defence markets, and it will become increasingly commonplace for defence applications to adopt and adapt to these developments.

"At the same time, as the speed of warfare and associated need for rapid cross-domain decisions continue to increase, we'll see greater emphasis on the centrality of information. By establishing a controlled, seamless flow of data from across multiple domains, the MOD and wider government organisations will work to create a 'Digital Backbone'. This will ensure users receive the right information at the right time (with different employees having different levels of access). Through enabling better, more informed cross-domain decision making, we will be better placed to swiftly respond and react to the evolving threat landscape.

"Modernising and transforming defence will move to the top of the agenda as governments look to protect national interests and navigate an ever-increasing threat landscape."

Rob Wythe, Chief Technologist, C5ISR

Central Government and Data

Government to prioritise data optimisation to avoid siloed working

"The way in which the government communicated during the pandemic changed the way society think about government data use, creating a complex dynamic as we go into 2023. More than ever, the public is aware of how data-backed insights inform critical government decisions, driving the need for greater transparency and accountability. At the same time, the government is under mounting pressure to make sense of large, often overwhelming, datasets to gain a 'bigger picture' view necessary for solving real-world problems.

"Next year, we expect government to double down on the secure consolidation and optimisation of data. There is now an understanding that data cannot be looked at in isolation, so achieving interoperability will be paramount for enabling information to flow seamlessly between systems, enhancing collaboration and intelligence sharing. Adhering to standards will be key to getting this right, as well as for building a sense of trust, both operationally and with citizens, around where data has come from and how it has been used.

"Finding and retaining people with the right data and problem solving skills is an important part of the puzzle, as well as automating manual processes to ensure these skills are used in the most valuable way."

Andy Lethbridge, Global Head of Consultancy, Central Government

Digital Diversity and Skills

Bridging the STEM skills gap will become a national security priority

"Securing the future of STEM talent has become a top priority. To stay at the forefront of research and innovation, organisations and governments are coming together to encourage people from all backgrounds to enter STEM fields, while promoting alternative routes into education.

"Progress has been made in recent years to improve the quality of these programmes, through digital training courses, apprenticeships and boot camps. However, there is still a lack of information, advice and support out there to help people access careers in cyber and digital. Next year, we will see more programmes with accountability measures put in place to deliver high-quality learning experiences for students.

"Building the future of a diverse STEM talent pool is a rising national security priority. Investing in skills enables organisations and governments to benefit from a richer, more capable defence workforce. Attracting and cultivating a broad range of talent, and diversity of mind sets will be vital to staying ahead of our adversaries.

"To achieve this, organisations need to consciously make cultural changes and investment choices to diversify their talent pools. At BAE Systems Digital Intelligence, we will actively seek to attract more neuro divergent candidates and females into cybersecurity roles. As the skills gap broadens, we must continue to embrace a mix of minds and skills to keep Britain safe."

Victoria Knight, Strategic Campaigns Director

D&I maturity to bolster recruitment and talent pipelines

"Broadening the diversity of business will always be a core focus of any diversity and inclusion strategy. By focusing our efforts in the year ahead on the important role that we all play in creating a culture of inclusion and belonging, we evolve ourselves to the next level of the maturity curve by ensuring responsibility to others and accountability in ourselves. If we can achieve that, diversity in recruitment and talent pipelines will follow."

Theresa Palmer, Head of Diversity and Inclusion

These forecasts are those of the authors personally, and do not necessarily represent the views of BAE Systems

BAE SYSTEMS

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

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