



INTRODUCTION

In 1999, the branding agency Interbrand came up with the name “Wi-Fi” as a catchier alternative to “IEEE 802.11b Direct Sequence”, the official name for the wireless networking protocol of the time. It was a sign that wireless communications had finally reached the consumer mainstream. In the same year, Apple launched its AirPort router, with a jubilant Steve Jobs demonstrating this new-fangled wireless networking technology by passing an iBook through a hula hoop and exclaiming: “No wires!”

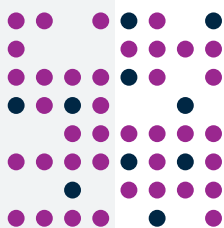
Wi-Fi has come a long way in the two decades since then, allowing ever faster downloads of ever greater volumes of data. It’s not only become an essential part of our personal and professional daily lives, but also enables the Internet of Things. There are currently more than 20 billion connected devices around the world, transforming every area of human existence.

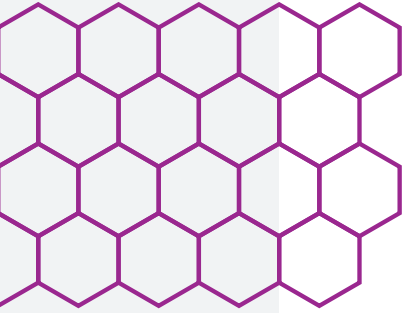
This rapid growth is a perfect example of the Law of Accelerating Returns posited by American inventor and futurist Ray Kurzweil. In an essay published in 2001, he argued that the rate of technological change accelerates exponentially. “So we won’t experience 100 years of progress in the 21st century – it will be more like 20,000 years of progress (at today’s rate),” he wrote.

The last 30 years have brought multiple innovations such as smartphones, cryptocurrency, augmented reality, gene editing, social media platforms... the list is long. Many of these are underpinned by groundbreaking foundational technologies such as AI and cloud computing. Huge steps have also been taken in areas such as robotics, nanotechnology and biotechnology.

So what comes next? According to Elon Musk, one of the prime movers in this explosion of new technology, we will see humans on Mars within the next five years. But what about closer to home? Which innovations and trends will come to the fore in the next few years?

“In previous decades, we have seen cutting-edge science and technology stem from the defence industry, given the large capital budgets that were previously required,” says Mike Sewart, Group Chief Technology Officer, QinetiQ. “As the pace of change increases and technology becomes more prolific, new products, services and business models are increasingly arising from the wider world of commerce. With that being the case, it is vital that the defence and security organisations learn from the global trends around us and, combined with defence and security domain knowledge, use them to protect our national interests for the future.”





This report focuses on six key areas of advancement, exploring the technology behind them and the uses to which they can be put, while also speculating on the opportunities or challenges they may pose to the defence and security sectors.

1 BRAIN-COMPUTER INTERFACES

By controlling machines using nothing but brain waves, we will fundamentally change the way that we interact with technology.

2 QUANTUM TECHNOLOGY

The science of subatomic particles will revolutionise fields such as computing and sensors, transforming many areas of our lives.

3 PROGRAMMABLE MATERIALS

A growing suite of new techniques in material development will enable the integration of smart capabilities into the objects around us.

4 EDGE COMPUTING

As the Internet of Things predominates, the ability to process data as close to its source as possible will become ever more important.

5 BIOMIMICRY

Nature-inspired technology, based on insights from millions of years of evolution, will unlock new areas of innovation in a multitude of fields.

6 ELECTROMAGNETIC INTERFERENCE

Potential new threats will lie in store in a world that is increasingly dependent on sensors and wireless communications technology.

This is by no means an exhaustive list, but all these topics contain considerable food for thought for those in the defence and security sectors and should serve to inspire new ideas for future applications in defence and beyond.





Pager is a macaque monkey who lives with his friend Code. They enjoy swinging from their tree house and napping in their hammocks. Pager is also pretty good at Pong, the 1970s video game involving two moving paddles and a ball. In fact, you could say he's very good at it, considering he controls his paddle simply by using his mind.

A video of Pager playing the game was released by Elon Musk's Neuralink company last April. This wasn't the first time that a monkey had moved a computer cursor using brain control, but it was the first time it had been done wirelessly – via a small device implanted into Pager's brain. It was a significant achievement on the road to a future where we will interact with machines in a fundamentally different way.

Next, Musk hopes, will come experiments with human subjects. Wired neural implants are already familiar in a medical setting – in one case, a man paralysed from the neck down was able to send a text message by imagining moving a joystick with his hand – but Neuralink's solution represents a significant upgrade on current technology, not simply because it's wireless, but because it multiplies by a factor of ten the number of implanted electrodes, hugely improving “bandwidth”.

Neuralink's immediate goal is to help people with paralysis; other companies, such as Austin-based Paradromics, are heading along a similar wireless implant route aimed at enabling new therapies for brain-related disorders. But for Musk, who has invested \$100m of his own money in the company, this latest experiment represented a major step towards his ultimate goal of developing a neural implant that will allow us to control a computer or mobile device anywhere we go.

This is the logical endpoint of the development of a brain-computer interface (BCI), a world in which we interact effortlessly with machines simply by thinking. But will we need an implant under our skull to do it – especially considering the ethical and safety concerns that most of us would have? Jody Medich, CEO of Superhuman-X and a long-time observer of the BCI sector, remains skeptical about this invasive approach to the science.

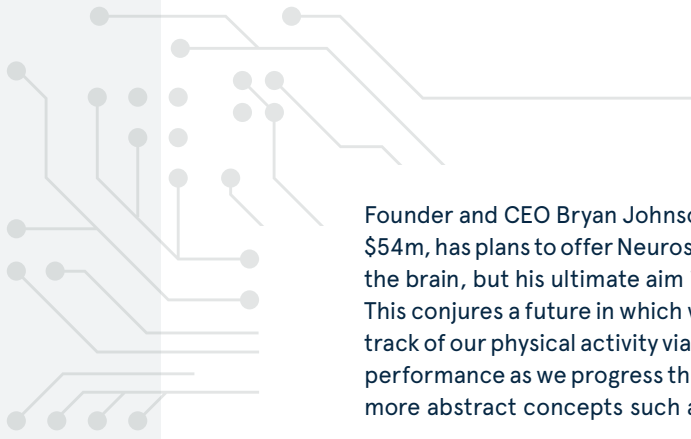
“The idea that everyone in the world would want something like this seems a very distant possibility,” she says. Much more likely, Medich believes, is that our brains will interact with machines via some sort of non-invasive, wearable user interface, starting with headsets: “Once we get used to wearing, say, AR glasses, then that becomes a pretty reasonable idea. What we get from those kinds of systems at the moment is kind of fuzzy data, but the technology will get smoother over time.”

A large amount of research is currently being done to perfect a wearable, portable BCI that could blend efficiently and seamlessly into our daily lives, allowing us to control machines without the need for manual or voice control.

The future lies on our heads... or wrists

“Pong?” began a press release, somewhat satirically, in July announcing “a new era of neuroscience and gaming”. Los Angeles-based Kernel, one of the companies at the forefront of commercial non-invasive BCI technology, was letting the world know that it was partnering on a project with Aim Lab, a training platform for eSports and video gaming.

Kernel's Flow device looks like a space-age cycling helmet and uses infrared light and ultra-sensitive optical detectors to measure blood flow and oxygenation in the brain. In its partnership with Aim Labs, players were able to get real-time access to their brain data to help them measure, quantify and improve performance. In another experiment, Kernel developed an algorithm that could work out which song a person was listening to (from a pre-selected list of ten) just from their brain activity.



Founder and CEO Bryan Johnson, who started the company with a personal investment of \$54m, has plans to offer Neuroscience as a Service via Kernel headsets to scientists studying the brain, but his ultimate aim is “to make measuring the mind as easy as your heartbeat”. This conjures a future in which we monitor the health of our brains in the same way we keep track of our physical activity via wearable devices. That could mean measuring our cognitive performance as we progress through a busy day, but ultimately we might be able to quantify more abstract concepts such as focus, mental health and even pain.

Kernel’s infrared light technology is too slow for controlling machines via the mind, and it’s in France that the dream of mind-controlled technology is closest to becoming an everyday occurrence. Neurotechnology startup NextMind has developed a small EEG sensor worn on the back of the head that measures activity in the brain’s visual cortex. By directing your visual attention, you can then issue digital commands to a computer or VR headset.

The company already sells the technology as a developer kit and is focusing on the entertainment and gaming world. A TechCrunch reviewer described it as “an awe-inspiring glimpse into what could well be the next major shift in our daily computing paradigm”. Mercedes-Benz is working on a concept car that uses NextMind’s technology to allow drivers to trigger functions such as operating the radio or controlling navigation without having to speak or touch anything. “Brain-computer interfaces are going to impact every aspect of our lives and bring incredible benefits to improve our world,” says NextMind founder and CEO Sid Kouider.



But will our BCIs necessarily be worn on our heads? In 2017, the company then known as Facebook announced that it intended to create a non-invasive, head-worn device that would allow people to type at 100 words per minute simply by imagining themselves talking. More recently, however, perhaps following the company’s new focus on the metaverse, an alternative online world based on virtual and augmented reality, it has pivoted towards wrist-based devices powered by electromyography – sensors that can translate the brain’s electrical motor nerve signals, as they travel through the wrist, into digital commands. Contextually-aware AI that works in sync with us, the company believes, will allow us to interact effortlessly with technology using just the slightest movement of our fingers.

“What we’re trying to do with neural interfaces is to let you control the machine directly, using the output of the peripheral nervous system – specifically the nerves outside the brain that animate your hand and finger muscles,” says Thomas Reardon, Director of Neuromotor Interfaces at Facebook Reality Labs.

“Brain-computer interfaces are going to impact every aspect of our lives and bring incredible benefits to improve our world,”

Sid Kouider, NextMind founder and CEO

The company hopes that one day, using AR glasses, we’ll be able to interact with virtual objects, or even type at high speed on a virtual keyboard on a table or our lap. The company is also developing different prototypes for wrist-based haptic technology to make virtual objects feel tangible – currently a holy grail in the VR space and something that will make virtual worlds seem far more “real”.

Perhaps this is how we will ultimately experience the metaverse: sitting silently in AR glasses or a VR headset, as our fingers twitch imperceptibly.

The Defence Perspective

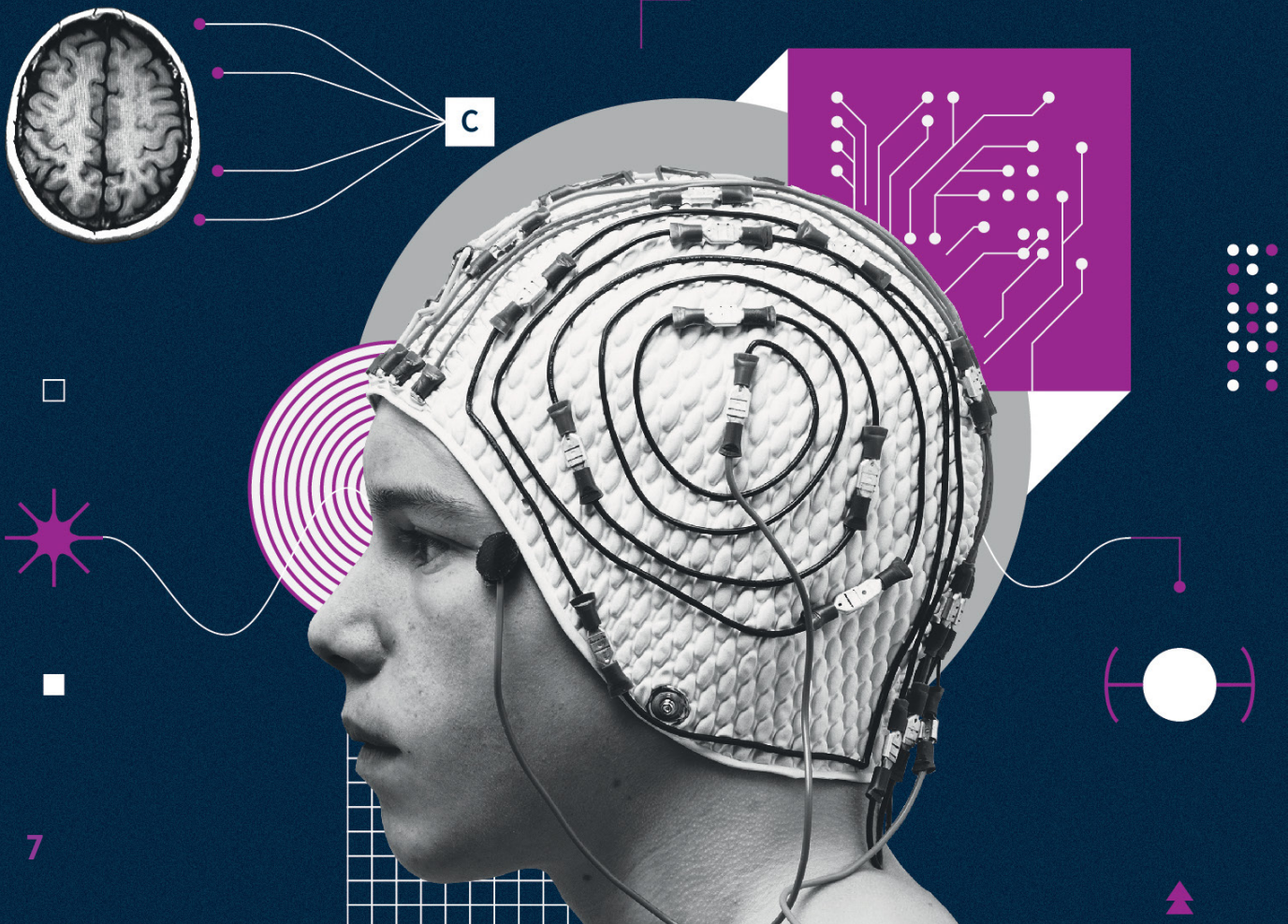
Today's personnel, in defence and beyond, deal with more data (and more data sources) than ever before. This requires fast, accurate decisions and can result in cognitive overload, which can cloud judgement or hamper performance in critical situations.

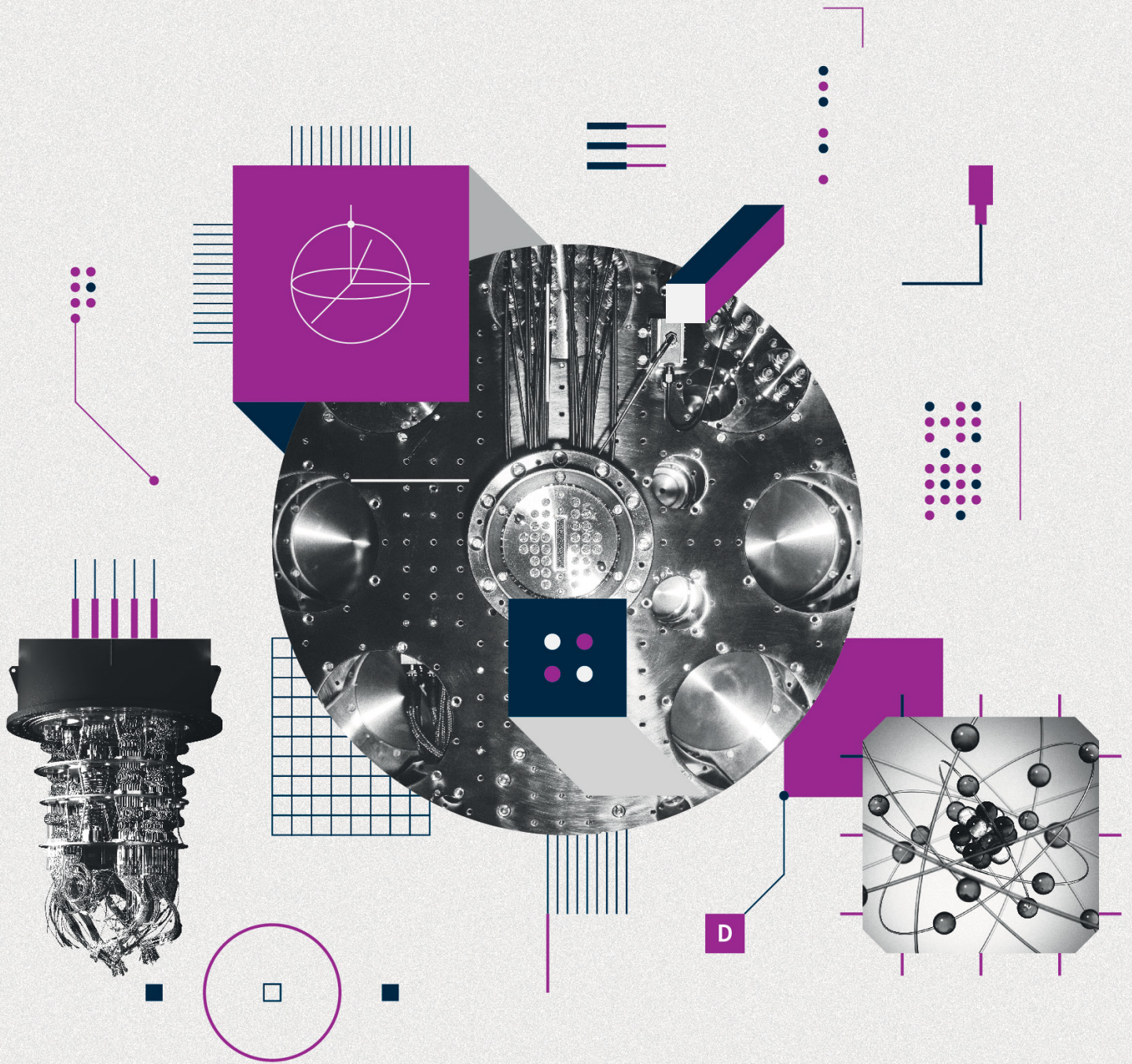
"Adaptive" brain-computer interfaces (BCIs), with the ability to respond to an operator's needs, could help to avoid such cognitive overload (or underload). For example, if the system knows that an operator is overwhelmed, it could reduce the display of information or direct focus towards an area that is more important. BCIs could also provide a control mechanism, for example, freeing up the hands and allowing operation at "the speed of thought", decreasing reaction times. Such a capability would be invaluable for fighter pilots or frontline personnel, where rapid reactions are important.

Electroencephalogram (EEG) "nets" placed on the head to record brain activity, are fairly common and non-invasive; whereas invasive arrays of fine wires to sense neuron (or neuron group) responses are at an early stage of development. The latter face infection and instability problems, which, combined with ethical and risk issues, has led to hesitancy in many countries to test invasive devices. Substantial research has been conducted into non-invasive BCIs over the last few years in the defence industry and we are seeing promising applications in wellbeing and workload management. However, such devices are very much in the early stages and it will be some time until they become commonplace.

Dr Helen Dudfield

Chief Scientist, Human Performance and Protection and Senior Fellow - QinetiQ

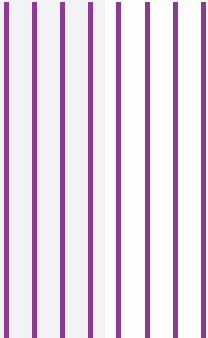




QUANTUM TECHNOLOGY

HARNESSING THE POWER OF SUBATOMIC PARTICLES

The principles of quantum mechanics are increasingly being applied in a wide range of fields, in particular computing, imaging and cryptography. It promises to transform communication, internet security and our everyday lives.



“Quantum computing will enable us to process an almost infinite number of solutions at once,” announced British Prime Minister Boris Johnson in a speech at the Lord Mayor’s Banquet in London in November 2021. “And if we could perfect it, there are so many problems we could solve, including how to turn nitrogen into fertiliser and feed the world without creating so much CO2.”

Johnson went on to announce his ambition for the UK to build a general-purpose quantum computer by 2040, saying the country would “go big” on quantum computing, which paradoxically is based on the behaviour of tiny particles, such as electrons and photons.

Around the world, many corporations and nation states are already going big on quantum, pouring billions of dollars into research aimed at creating quantum computers capable of performing tasks that are beyond the reach of the largest classical supercomputers. Applications would include enhanced artificial intelligence, the development of new chemicals, drugs and alloys, and advanced algorithmic financial trading.

VC funds and private investors have sensed an opportunity, too. In 2021, in the US alone, more than a billion dollars had already been directed into the quantum computing industry by the end of the third quarter, compared to a total of \$187.5m through all of 2019. In October, IonQ, which was spun out of the University of Maryland, became the first purely quantum-computing company to trade publicly on the New York Stock Exchange, raising \$600m in the process.

But there’s still a long way to go, because quantum computers are extremely difficult to engineer and build. By coincidence, the Prime Minister was speaking on the same day that IBM unveiled its latest quantum processor, named Eagle. This is the first processor to pack more than 100 qubits (the quantum version of binary bits) onto a single chip. By 2023, IBM hopes to reach the 1,000 qubit mark. However, to achieve the processing power to truly fulfil its promise, quantum computing will require millions of qubits.

According to Amit Katwala, author of the WIRED guide to quantum computing, it’s likely to be ten, if not 20, years before that goal is achieved. For the moment, many companies are experimenting with quantum computers and running proof-of-concept projects and looking at ways in which quantum could offer solutions to persistent problems. For example, Volkswagen is collaborating with Google and quantum computing company D-wave on ways to reduce traffic congestion, BMW is working with Honeywell on optimising its supply chains, and Bosch has hooked up with quantum software research centre QuSoft to investigate use cases in the engineering and AI/machine learning field.



Quantum beyond computers

Quantum technology isn’t just about computing. Ground-breaking solutions based on quantum mechanics and the way that sub-atomic particles behave are being developed in areas such as imaging, gravimetry, navigation, timing, radar and measurement, and some products are already reaching the market.

QLM is a Bristol-based company that wants to help organisations achieve net zero by mitigating their greenhouse gas emissions. It has developed a camera based on quantum technology that is able to “see” methane gas that may be escaping from oil and gas processing facilities or industrial sites, as well as identifying methane hotspots in agricultural scenarios. And M Squared Lasers, a Glasgow-based company, has developed a range of quantum products, including a gravity sensor that can be used to detect underground objects, which will be of considerable use to surveyors.



Battery company AMTE Power is working with a range of partners to develop testing for lithium batteries on a production line. Quantum sensors can detect the small magnetic field given off by healthy batteries, meaning faulty ones can be quickly rejected. Currently, the process for testing batteries can be time-consuming, meaning wasted energy and higher costs.

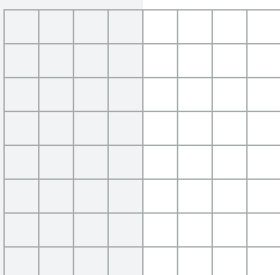
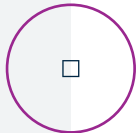
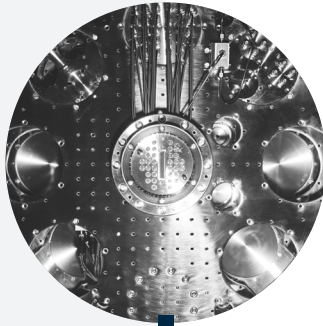
Innovations such as these will not necessarily revolutionise our daily lives in ways we are immediately aware of, but they will improve the infrastructure and professional services upon which we rely, according to Roger McKinlay, Challenge Director – Quantum Technologies at UK Research and Innovation (UKRI). The UKRI's National Quantum Technologies Programme, launched in 2014, aims to have invested £1 billion by 2025 in make the UK a go-to place for the development and commercialisation of quantum technologies.

"I get government ministers who wave their phone at me and say, 'When can I get quantum in my phone?'" he says. "There's a kind of tunnel vision at the moment where people believe that anything that impacts our lives will end up in a smartphone or is about processing data, and they tend to forget the professional services. If, for example, gravity sensing began to prevent the number of roadworks that are in the wrong place, you can see how it would improve our lives significantly."

One area that's ripe for growth is the field of quantum cryptography. In the future, traditional public key cryptography may be vulnerable to being cracked by large-scale quantum computers. One answer is to develop quantum-safe cryptographic algorithms, and research is already progressing on this. Another way around the problem lies in so-called quantum key distribution (QKD), which uses physics rather than maths to solve the problem. Here, cryptographic keys are transmitted and exchanged between parties by means of laser-generated light photons, and because of the nature of quantum mechanics, it is theoretically impossible for a third party to see or tamper with a key without the original parties being aware. The global market for this technology is anticipated to increase from practically nothing today to going on for \$4 billion by 2028, according to market research company Inside Quantum Technology.

As with quantum computing, the technical difficulties of making QKD work are considerable. China has been leading the way with research based around its Micius satellite, and the European Space Agency is building its own satellites as part of a secure end-to-end quantum communication infrastructure with a pan-European reach.

According to Roberto Viola, Director-General of the European Commission's communications arm, the new infrastructure will have multiple uses beyond cybersecurity, such as digital signatures, authentication and clock synchronisation. Ultimately, this technology is likely to be the foundation of the quantum internet, a future global network powered by the laws of quantum, with added security into the bargain.



The Defence Perspective

Quantum is a very broad category but can be divided roughly into two parts. The first part is quantum sensing, timing and communications. These are all things we can do right now with classical techniques, but quantum enhancement could provide greater sensitivity, accuracy and range to such systems.

The second part is more speculative. If a suitably large quantum computer could be built, it might be revolutionary – letting us do things we simply can't do with classical computing. For example, quantum information processing could enhance machine learning, leading to better image recognition.

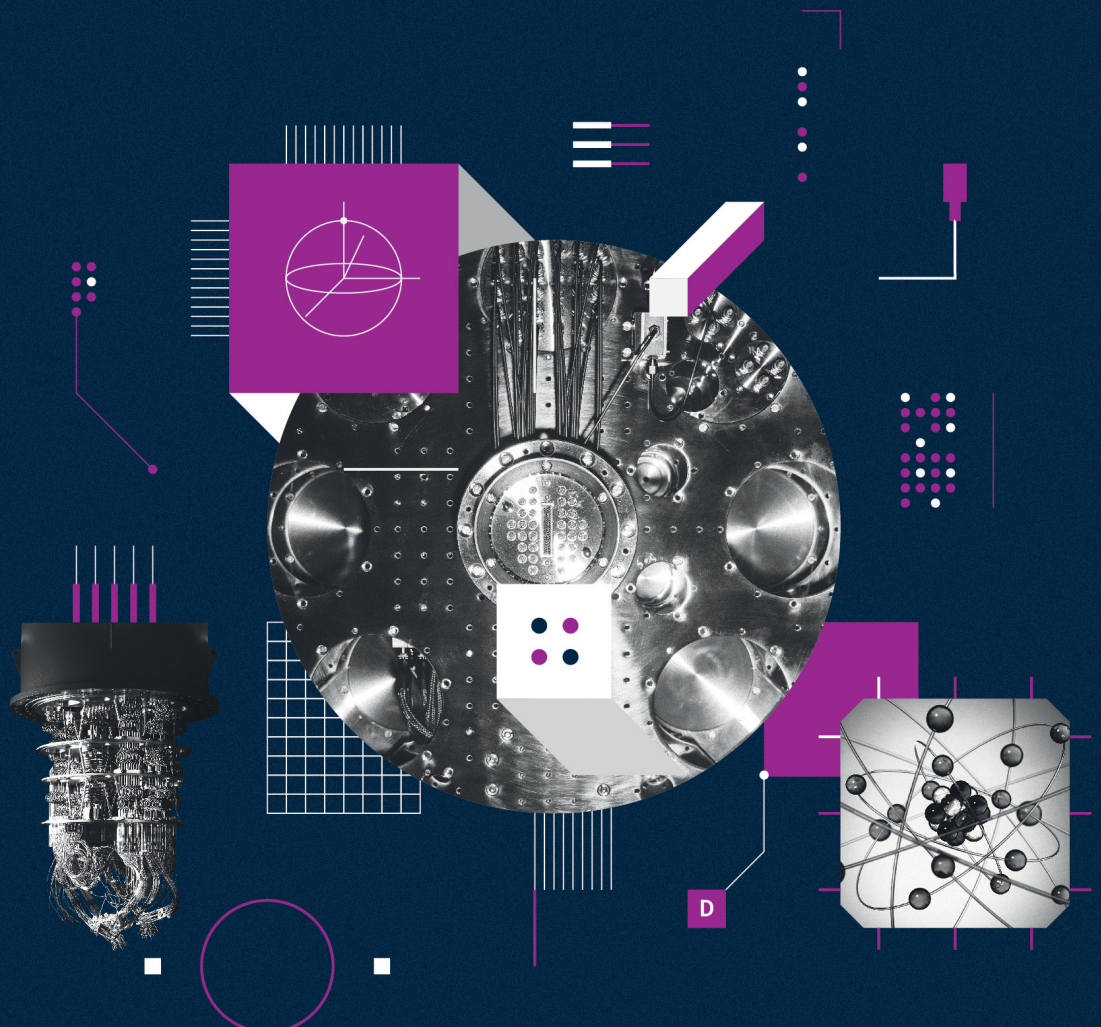
There are now people in the early stages of their careers who will be in the industry when true quantum computing arrives. Therefore, we must be "quantum ready" for the debut of a suitably advanced quantum computer.

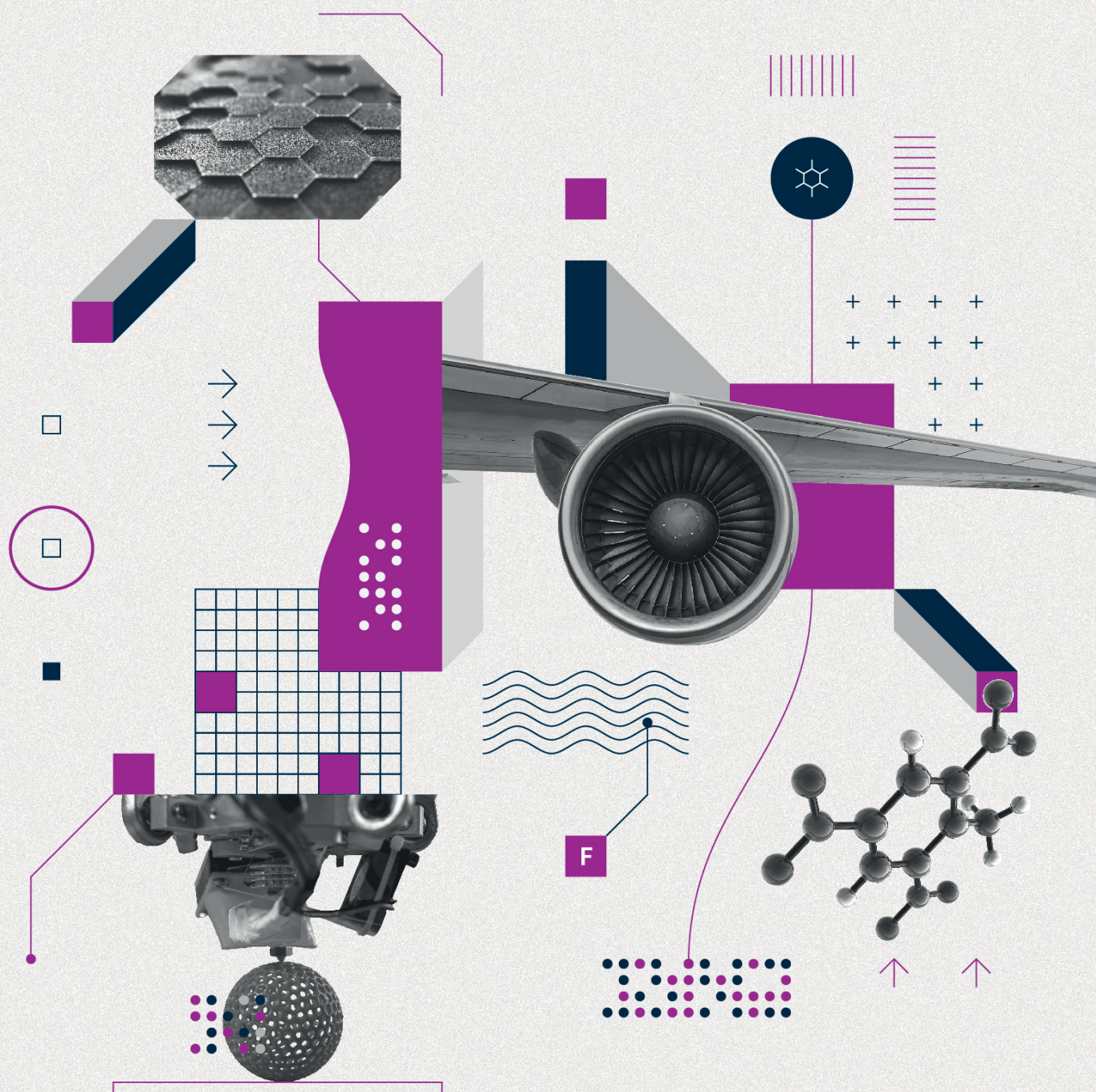
One key element of quantum readiness for defence includes being able to assure a quantum computer. The verification, validation and trust of quantum computers is of significant importance in the defence arena. We must be able to ask and answer: has the quantum computer done what it was told to do? Has the quantum computer been told to do the right thing? And has the result of the quantum computer been tampered with, intercepted or spied on?

As such, we're looking to partner or collaborate with other organisations, and to train quantum specialists for just this purpose. People are going to be one of the biggest factors in the realisation of quantum.

Dr Gillian Marshall

Head of Quantum Technologies and Fellow – QinetiQ






PROGRAMMABLE MATERIALS

SEAMLESSLY INTEGRATING SMART CAPABILITIES
INTO EVERYDAY OBJECTS

Through new structural patterns and additives, scientists can transform properties in materials to make them behave like electromechanical devices – but without the need for electronics.



Imagine a day some time in the future when you're on a family trip in your autonomous vehicle. Gone are the days when people sit facing forward in rows in their car. In this future, you can all face one another and chat or play games as you pass the time on your way to your destination.

Nobody in your vehicle is worrying about safety – and that's not just because they trust the autonomous technology. They also know that their seats are made from a material that has special properties that will respond to a collision. Triggered by the rapid deceleration of impact, it will change shape and stiffness, swiftly cocooning them from harm.

This is just one example of the ways in which the materials around us might become increasingly adaptive in the future. This is because we will be able to embed properties in them that make them reconfigure themselves in response to heat, pressure, moisture or other external factors – allowing them to act like machines. According to Professor Chris Eberl, the Scientific Coordinator of the Fraunhofer Cluster of Excellence for Programmable Materials in Germany, the possibilities are endless.

"We need to get away from thinking of a material as something that is fixed in terms of its properties and never changes throughout its lifetime," he says. "In the future, everything around us, from our clothes to our homes and our vehicles, will become adaptive and will be able to change its shape or its stiffness or whatever depending on how we, as users, want to interact with it."

This 21st-century alchemy relies on a convergence of new technologies, including advances in materials science and new capabilities in computer simulation software. Another significant factor has been the development of 3D printing into so-called 4D printing, which allows a material created through the additive process to later change shape or properties. The ultimate aim is to create materials that on their own can perform tasks in the same way as electromechanical devices comprising sensors, controllers and actuators.

"Robots without robots," is how Skylar Tibbits, Co-Director and Founder of MIT's Self-Assembly Lab, describes it. "It's about tapping into material properties, and the geometry of those materials, using different forms of fabrication, in such a way that they can sense and actuate – just like a robot," he says.

As an example of materials acting like devices, Eberl offers the example of a current project by Fraunhofer's scientists in the field of building insulation – currently a pressing environmental topic. They are experimenting with shape memory polymers which, because of the way the foam is synthesised at a molecular level and the additives that are employed, can be "programmed" to change shape at specific temperatures.



"We need to get away from thinking of a material as something that is fixed in terms of its properties and never changes throughout its lifetime,"

*Chris Eberl, Scientific Coordinator of the
Fraunhofer Cluster of Excellence for Programmable Materials*

Two separate foams are used in conjunction, containing narrow, aligned channels for air flow. In one foam, the channels remain closed at temperatures below 15 degrees C, and then become open at temperatures above that, as the foam changes shape. In the other foam, the channels are open until the outside temperature reaches 28 degrees C, at which point they close. The combination of the two foams means that at very low and very high external temperatures, the air flow channels are closed, so the building will neither overheat nor get too cold. In effect this is an intelligent insulating system, but without electronic sensors or other components.

A world of opportunities

Examples of commercial applications for programmable material technology in operation are currently thin on the ground, or indeed happening at a classified level. However, with some of the world's leading scientific researchers pushing ahead in this field, we can expect a raft of innovation that spawns a wide range of commercial use-cases in the years ahead.

Fraunhofer scientists are working with a number of industrial partners, looking at areas that could be revolutionised by the use of programmable materials, although much of the detail is protected by NDAs. One project is in the medical field, creating instruments that can change shape as they enter or leave the body. They are also working on car seats that can adapt to different users' body shapes. However, Eberl believes it will be at least two or three years before they are talking about tangible solutions.

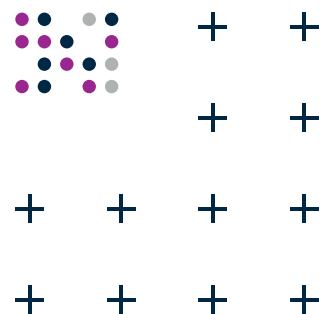
"If we can have materials that have more agency and capability, we can reduce the cost, complexity and energy consumption of all of our traditional systems."

Skylar Tibbits, Co-Director and Founder of MIT's Self-Assembly Lab

"It's still super-early days for this technology," says Tibbits, whose Self-Assembly Lab is examining ways to create self-transforming carbon fibre by applying temperature-sensitive polymers to them. One potential application for this type of material is a morphing jet engine inlet, developed with Airbus, which opens and closes to control the flow of air to the engine in response to changes in temperature or wind-speed pressure. There is typically a component on top of the engines with a hole to draw in air for cooling, but this creates drag. Airbus was looking at other solutions using electromechanical or pneumatic flaps that would open and close, however, these add weight, cost and potential failure with additional mechanisms. The morphing carbon fiber inlet solves the problem without the need for electronic or mechanical components.

Tibbits believes programmable materials are likely to play a major role in our lives in the coming years. "We're seeing a lot of 'smart' technologies, from smart homes to smart shoes to smart seats or whatever, but today all these things rely on electromechanical, robotic devices," he says. "To me, that's a clumsy middle step that no one really wants. I think we're going to shift away from a lot of those devices, and these capabilities will be seamlessly integrated into the materials in our everyday world.

"If we can have materials that have more agency and capability, we can reduce the cost, complexity and energy consumption of all of our traditional systems," he adds. "We can have more with less, basically. It's a much more sustainable approach."



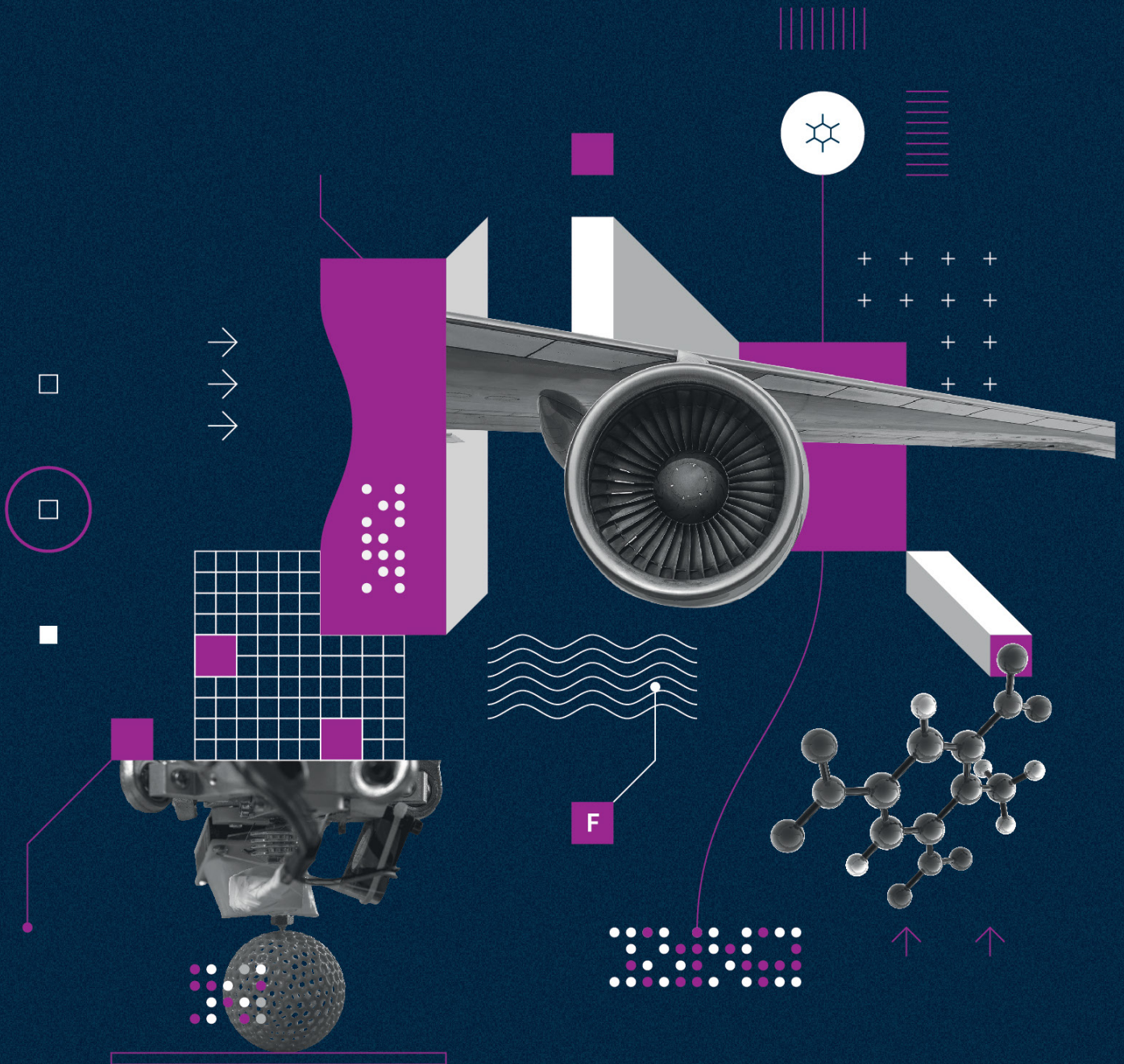
The Defence Perspective

Programmable materials offer many possibilities in defence. For example, a material system could be adapted to changing operational requirements: its strength, size, impact properties, or overall shape could be modified as needed. Imagine an aerial vehicle (like a hypersonic or UAV) that could change its aerodynamic profile by tailoring its leading edge so that it travels faster at certain points. Or an antenna that uses metamaterials (materials that are engineered to have properties which cannot be found naturally), which could modify its radiation pattern, change the band/frequencies in which it transmits, or direct the beam at a specific target.

There's also a sustainability angle to new material development. If you wanted to upgrade a military platform in the future, you could tailor that platform by changing its properties, instead of swapping out some (or all) of its components and materials. Lots of work is being done in the field of metamaterials and a range of applications are being evaluated, including secure communications, IoT, and various classified applications too.

Professor Sajad Haq

Head of Advanced Materials and Senior Fellow - QinetiQ





EDGE COMPUTING

TECHNOLOGY TO ENABLE A SENSOR-RICH WORLD

Emerging technologies such as the Internet of Things, enabled by distributed micro-computing, can benefit from processing as close to the source of data as possible. Even in outer space.



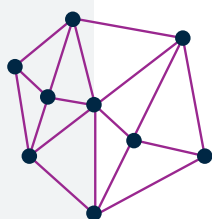
On 18 February 2021, after a journey of 293 million miles, NASA's Perseverance rover made its descent to the surface of Mars. Back on Earth, scientists held their breath as they waited to hear the outcome of a complex series of operations known as the "seven minutes of terror". It takes more than 11 minutes to get a radio signal back from the Red Planet, which meant Perseverance had to handle everything itself, with every manoeuvre commanded by onboard computers guided by cameras and sensors.

When the rover's safe touchdown was finally confirmed – some minutes after it had actually happened – there was jubilation back at NASA's Jet Propulsion Laboratory in Southern California. It had been a remarkable example of cutting-edge space technology successfully deployed.

And it had also been a perfect demonstration of edge computing.

As its name implies, edge computing is processing that's done as close to the source of data generation as possible – whether that's in an actual device such as a sensor or smartphone, or in a nearby small-scale data centre (cloudlet) or a cellular base station.

In recent years, companies and organisations have come to rely more and more on cloud-based infrastructure, where computing happens a long way away on a centralised network of remote servers and is reliant on a robust connection between the cloud and the client end-points. Edge computing reduces that reliance and, while it is not a new technology, it is becoming ever more important as the amount of data that we produce increases, with the advent of new technologies such as AI, machine learning and blockchain. The number of devices connected to the Internet of Things (IoT) is also growing: semiconductor company Arm has predicted that there could be a trillion IoT devices by the end of 2022, each collecting data on its environment.



"Processing the data closer to where it is generated means processing information faster and having the ability to make decisions more quickly,"

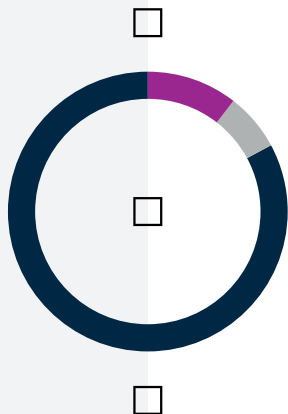
Matías Díaz, Global Head of Edge Security in Security Architecture at digital bank BBVA

Edge computing enables that raw data to be rapidly processed and filtered close to the source. "Processing the data closer to where it is generated means processing information faster and having the ability to make decisions more quickly," says Matías Díaz, Global Head of Edge Security in Security Architecture at digital bank BBVA. And there's an added sustainability benefit – by reducing the total amount of data traversing a network, energy consumption is also reduced.

In security terms, it's a double-edged sword. On one hand, edge computing reduces the amount of sensitive information transferred between devices and the cloud. However, others worry that a proliferation of sensors and devices will bring new vulnerabilities. According to Santhosh Rao, Senior Research Director at Gartner, "Extending your footprint using edge computing exponentially increases the surface area for attacks."

The edge has no limits

Research company IDC has forecast that annual worldwide spending on edge computing hardware, software and services will reach \$250 billion by 2024, and the sector is already a hotbed of innovation. Use cases span pretty much every industry sector – wherever sensors are collecting data, there's likely to be a need for computing at the edge.



San Jose-based Edgeworx has developed a device the size of a paperback book that includes video, thermal and sound sensors together with user-friendly machine learning software that can process data locally. At a local school, following its reopening after lockdown, it was used to monitor students entering the premises and was able to scan their unique QR code, use a thermal camera to scan for fever and also use a video camera to check for a face mask, all in less than 100ms.

“The testing can create around half a terabyte of data and previously all that data had to come down to the ground and then hop to data centres and it would be several weeks before they got the results,”

*Naeem Altaf, Distinguished Engineer
and CTO of the IBM Space Tech team*

In Australia, Fleet Space is bringing the power of IoT and edge computing to places where connectivity is slow or non-existent. Its Portal device is a small white box that can be mounted on a pole and provides wireless connectivity to hundreds of sensors within a range of 15km. Included is an edge server that can aggregate and compress selected data before beaming it onward via one of the company’s fleet of nanosatellites.

As we have seen, edge computing’s applications are not limited to processing data on earth. A couple of days after the Perseverance rover landed on Mars, a Cygnus rocket was launched from Wallops Island, Virginia, taking cargo to the International Space Station. Included in the payload was HPE’s Spaceborne Computer-2, designed for use in space, which would be used to run a custom edge computing solution created by IBM for the DNA sequencing of microbes on the ISS.

“The testing can create around half a terabyte of data and previously all that data had to come down to the ground and then hop to data centres and it would be several weeks before they got the results,” says Naeem Altaf, IBM Distinguished Engineer and CTO of the company’s Space Tech team. By designing computers and processes powerful enough to carry out this work on board, that time was cut to just a couple of days.

Space has become the final frontier for edge computing R&D, and Altaf believes that important lessons will be learned from the ISS project, with implications for future trips to the Moon and beyond. “If we can speed up communication with our far-flung space explorers, it will accelerate how much we can learn and discover,” he says.

And it won’t just be time that’s saved. By cutting down on transmissions, edge computing can also save energy – an even more precious resource in space than it is on Earth.

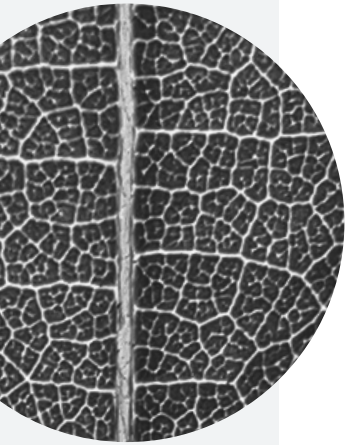




A 6x6 grid of dots. A 2x2 square is highlighted in the bottom right corner, with its bottom-right dot also highlighted in red.

Head of AI, Analytics and Advanced Computing and Senior Fellow - QinetiQ





We tend not to notice honeybees as they live their lives, pollinating flowers, carrying nectar back to the hive, and creating new colonies. And in the future we may be similarly oblivious as autonomous machines move around us, cleaning, carrying and generally making our lives easier.

The ambition of Opteran, a Sheffield University spinout, is that its technology will, quite literally, be the brains behind this new era of “ubiquitous autonomy”. But rather than employing machine intelligence based on deep learning that imitates the mammalian brain, as is usual in autonomous machines, Opteran’s solution uses what it calls “natural intelligence”, reverse-engineered from the brains of the aforementioned honeybees and transferred to a silicon chip.

As CEO David Rajan points out, the human brain contains 86 billion neurons, whereas a honeybee’s has just a million. “But they’re extremely smart,” he says. “They’re amazing navigators and builders. They exhibit autonomous behaviour, and they do it with a brain the size of a pinhead, while expending very little energy.”

Adopting this pared down approach to intelligence and energy-saving, the company has installed its development kit on a robot dog, giving it 360-degree stabilised vision based on the compound eyes of insects, while its honeybee brain uses optic flow motion detection to navigate around naturally without colliding with objects – and all this without the need for GPS or the huge datasets associated with deep reinforcement learning. In the near future, Opteran intends to add honeybee-style decision-making to its autonomous machines.

Although Opteran was only founded in 2020, its work is based on eight years of research led by co-founders Professor James Marshall and Dr Alex Cope. As Rajan points out, nature-inspired solutions generally tend to involve such long periods of research and require specialised knowledge, often across several disciplines. “But it’s worth the effort,” he says, “Because what nature has spent hundreds of millions of years figuring out usually works so much better than what a team of software engineers can come up with.”

“They’re amazing navigators and builders. They exhibit autonomous behaviour, and they do it with a brain the size of a pin head, while expending very little energy.”

David Rajan, CEO at Opteran

Technology solutions inspired by nature are nothing new, but they are growing in number. Research by the UK’s Biomimicry Innovation Lab, “The State of Nature-inspired Innovation in the UK”, found a 170 per cent increase in patents over the last ten years, with China and the US leading the way. In the UK, the predominant area for biomimicry research is engineering, followed by medicine and computer science. However, it’s possible to find applications for nature-inspired innovation in just about every industry sector.

But while research is progressing apace, the road to commercial success for nature-inspired technologies can be a long and winding one. “Many projects are unable to transition from validated technology to system completion,” says the Biomimicry Innovation Lab’s Founder and Biofuturist, Richard James MacCowan.

The journey to nature inspired success

Finding the appropriate application for an innovative, nature-inspired technology can be problematic. When Dr Anthony Brennan, a materials science and engineering professor at the University of Florida, was asked by the US Office of Naval Research to look at ways

to reduce the drag on ships caused by barnacles and algae, he came up with an answer inspired by the skin of sharks, which features a slippery, diamond-shaped micropattern of millions of tiny ribs.

Some years later Brennan serendipitously discovered that an artificially created surface using the micropattern could also resist human pathogens. Today, Sharklet Technologies produces a germ-resistant, adhesive-backed film that can be attached to multi-touch surfaces such as elevator buttons and door knobs, and has found a ready new market in the era of Covid-19.

From a drone designed to mimic the flapping wings of a dragonfly, to a greenhouse inspired by a desert beetle's shell, to wind turbines designed to look like sycamore seeds, nature-inspired solutions are increasingly proliferating. Perhaps not surprisingly, many are specifically aimed at making the world more sustainable.

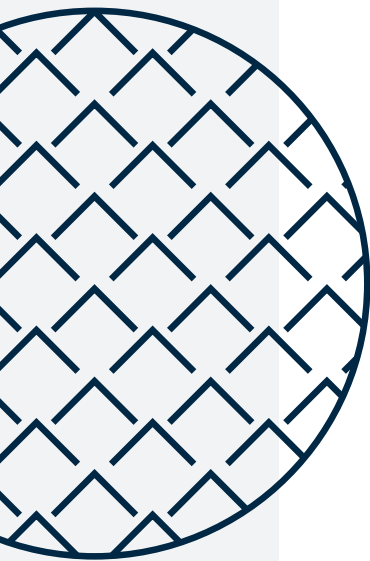
Arborea, based at Imperial College's White City Campus in London, is addressing the problem of providing food for a growing world population by producing organic, healthy ingredients with the smallest environmental impact. It has developed what it calls BioSolar Leaf technology, a solar panel-like platform made up of nutrient-rich microalgae that mimics the functioning of a real leaf, absorbing carbon dioxide and releasing oxygen. The panels can be installed pretty much anywhere and at any scale, and use a thousand times less water than soil-based plants. An acre of Arborea's BioSolar Leaf is about 120 times better at sequestering carbon dioxide and producing oxygen than an average forest of the same size.

When you see white products in daily life, from the lines on the road to sunscreen and toothpaste, it's likely the paints and pigments used to colour them contain titanium dioxide. However, titanium mining has an environmental cost and nanoparticles of titanium dioxide, which is non-degrading, have recently been labeled as a potential carcinogen. Looking for an alternative, Cambridge University spinout Impossible Materials took their lead from the bright white Cyphochilus beetle, which makes its home in the forest floors of southeast Asia. Its scaled exoskeleton acts as a highly optimized light-scattering structure, giving the beetle its brilliant whiteness, which can be reproduced using cellulose, offering a safe alternative to titanium dioxide.

"what nature has spent hundreds of millions of years figuring out usually works so much better than what a team of software engineers can come up with."

David Rajan, CEO at Opteran

Creating synthetic fabrics for materials such as rayon, polyester and lycra requires large amounts of energy and water, as well as producing carbon dioxide and a lot of waste. Oxford University spinout Spintex is emulating the spider, which can produce an extremely strong thread at room temperature with only protein and water. Using a unique biomimetic spinning mechanism, Spintex can create a fibre from a liquid gel just by pulling, with water the only byproduct. The process is a thousand times more energy efficient than the production of synthetic plastic fibres and no hazardous chemicals are used. As Spintex puts it, it's a product backed by 300 million years of R&D.



Chief Scientist Advanced Services and Products and Fellow – QinetiQ





ELECTROMAGNETIC INTERFERENCE

THE INVISIBLE THREAT TO OUR WIRELESS WORLD

The radio waves on which our increasingly wireless lives depend are also the means of potentially devastating – and untraceable – attacks on our infrastructure and personal security.



Last April, a model aeroplane enthusiast was flying his pride and joy, a 1:5 replica of a WWII-era T-6 training aircraft, near Lichfield in Staffordshire, UK, when something strange happened. Suddenly the remote-controlled plane became unresponsive and flew in a straight line before colliding with the trailer of a lorry parked at a nearby distribution centre.

Crashes of unmanned, radio-controlled aircrafts have to be reported to the UK aviation authorities, and in its subsequent report, published in November, the Air Accidents Investigation Branch (AAIB) noted that the pilot of the model plane and other club members were unable to identify any faults that could explain the loss of communication. However, the pilot had said that he suspected jamming devices were being operated by some of the companies at the distribution centre to prevent staff from using mobile telephones.

The AAIB dismissed this explanation, saying it had been told no such devices were in operation, and adding that in any case it is illegal in the UK to use a jammer. Which of course is not the same as saying such a device could not have caused the plane to be unresponsive.

Jamming devices, although illegal in many countries, are readily available to buy online. They work by sending out electromagnetic signals on the same frequency as a targeted device, effectively drowning it in “noise”. Even if a cell phone jammer (cost: a couple of hundred pounds) wasn’t being used on this occasion, the model plane could just as easily have been brought down by a drone jammer (cost: around a few thousand pounds).

The loss of a single model aircraft may not seem particularly important, but the episode points to a wider phenomenon of much greater potential significance. We live in a world that is increasingly dependent upon a wireless, digital infrastructure, and the radio waves on the electromagnetic spectrum on which this infrastructure depends are vulnerable to disruption. Electromagnetic interference (EMI) can be caused by faulty or unshielded electronic equipment, or even by devices battling amongst themselves for space on an ever more crowded spectrum. Last January, a Federal Aviation Authority team investigating interruptions in the GPS service near Wilmington Airport, North Carolina, traced the problem to a nearby utility company’s wireless control system, which was unintentionally jamming GPS within a two-mile radius of the airport.

“If you can control that voltage from outside the system, you can control that system’s view of the world,”

*Kasper Rasmussen, Associate Professor at
Oxford University’s Computer Science Department*



EMI can also be both deliberate and malicious. Governments are aware of this and some have taken action: for example, following the introduction of a radio-based signalling system on European railways, the EU constantly monitors it for potential EMI events. But while companies and organisations collectively spend billions countering online cyber threats, most pay little attention to their vulnerability to EMI.

And the damage that could be caused by a targeted EMI attack is potentially huge. As Kasper Rasmussen, Associate Professor at Oxford University’s Computer Science Department, acknowledges, at the most basic level, this could involve remotely jamming signals at, say, a factory that is heavily reliant on automation – an ever more likely scenario with the advent of Industry 4.0. The science is the same as that applied to jamming model aircraft or mobile phone reception, and in this case it would simply require more power.

"You could definitely do that," Rasmussen says. "Say you have a factory producing cars in a semi-automatic way, and all the robots suddenly don't do what they're supposed to do, not only do you lose time, but you could also damage some of the cars that are being built, and that could cost the company millions."

A new danger – signal injection attacks

Rasmussen believes jamming attacks such as these are unsophisticated compared to other ways in which EMI can be used maliciously. "Those kinds of things are just about overwhelming control systems with so much noise that they can't receive any normal commands," he says. He is far more concerned about ways in which electronic devices, in particular sensors, which are increasingly proliferating in the world, can be taken over and controlled remotely by bad actors using radio waves.

Rasmussen cites a research project by scientists at the University of Michigan and the University of Louisiana at Lafayette, in which they were able to remotely manipulate the temperature sensor of an unoccupied infant incubator from the other side of a wall in a laboratory experiment. The equipment needed was relatively basic and could easily be purchased or made at home, and was used to direct radio signals towards the incubator's temperature sensor.

A temperature sensor measures the ambient temperature in the form of changes in resistance in a thermocouple. The resistance generates a voltage, which is measured by the sensor's microprocessor. In this case, depending on the voltage, the incubator will either increase or decrease the amount of heat it produces to maintain a set temperature. But by directing radio waves of a specific frequency towards the wire between the sensor and the microcontroller – which acts as an antenna – the scientists were able to induce a voltage and spoof the system into raising or lowering the temperature – which in the real world could be deadly.

"From a distance away, we could inject a waveform of human speech and issue OK Google commands to the phone. It can be 'OK Google, delete all my contacts' or any mischief you can think of. It's early days for this kind of research but already we can do a lot of damaging things."

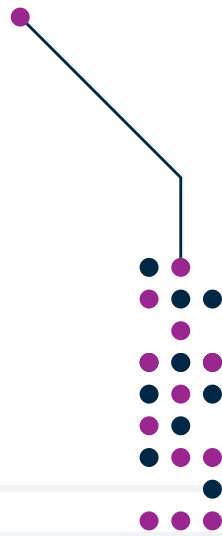
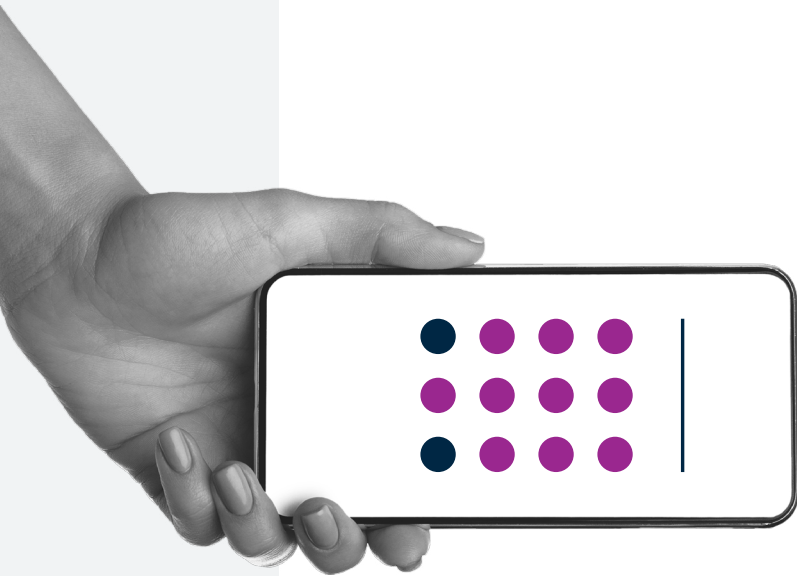
*Kasper Rasmussen, Associate Professor at
Oxford University's Computer Science Department*

"If you can control that voltage from outside the system, you can control that system's view of the world," says Rasmussen. There are many other scenarios in which these kinds of "signal injection attacks" can be used, he adds, from simple operations such as setting off alarms or opening electronic doors all the way up to what he admits is a perhaps overdramatic example – controlling the temperature sensors of fuel rods in a nuclear reactor. And in every case, attacks could be carried out remotely and the perpetrator would be untraceable.

There is also the possibility of attacks on an individual level. Experiments have been carried out in which heart pacemakers were manipulated to deliver defibrillation shocks. And in one of his own experiments, Rasmussen and his team were able to control and issue voice commands remotely to a smartphone, using the wire of a person's headphones as the antenna to receive signals without their knowledge.

"There was no sound at all, we were just sending electromagnetic rays," he says. "From a distance away, we could inject a waveform of human speech and issue OK Google commands to the phone. It can be 'OK Google, delete all my contacts' or any mischief you can think of. It's early days for this kind of research but already we can do a lot of damaging things."

Rasmussen is also working on ways to defend against signal injection attacks, because conventional shielding is often only of limited use in preventing them. The technology constitutes a very real threat, he believes, but as yet it remains relatively unknown. As he puts it, "People are just not aware." The radio waves that enable a sensor-rich world and make our lives easier could increasingly become a means for others to cause commercial or societal harm. In our bright technological future, a new threat is lurking in the shadows.



A complex digital illustration on a dark blue background. The central focus is a hand holding a white smartphone with a grid of yellow dots on its screen. Below the hand is a large, grey satellite dish with a central antenna. To the right of the dish is a 5x5 grid of squares, with some squares highlighted in yellow. Above the grid is a white square containing a triangle of yellow dots. Various abstract geometric shapes, lines, and dots in white and yellow are scattered throughout the composition, creating a sense of digital connectivity and data flow.

E

CONCLUSION

Scientific and technological innovation continues to march forward at pace, yielding a wealth of applications with the potential to advance human capabilities, improve the health of our planet, revolutionise the performance of machines and transform entire industries.

The six areas highlighted in this report bring to life just a few of the disruptive developments that will impact nations, corporations and citizens alike in the years ahead. From brain-computer interfaces that allow humans to control machines with their minds, to programmable materials that adapt to their circumstances – the transformative opportunities are immense. And yet, whilst these technologies will be disruptive in their own right, it is the interplay of these technologies with each other and with foundational technologies such as AI, nanotechnology and robotics that will unlock an array of applications that are almost unimaginable at present.

With investors, corporations and, most notably, Big Tech dialling up their R&D spend, the pace of innovation will only accelerate and, as a result, the commercial use-cases of new technologies will multiply.

For the defence and security industry, this rapidly evolving innovation landscape simultaneously offers a wealth of possibility and a new world of threats. Indeed, looking beyond the defence and security sector itself to learn from global trends and apply these to protecting national interests has never mattered more.



QINETIQ

QinetiQ is a global integrated defence and security company focused on mission-led innovation for defence, security and civil customers around the world. Combining world-leading expertise with a distinct heritage in science, technology and engineering, we create, test and assure new ways of protecting what matters most.

Find out more at [QinetiQ.com/S-T](https://qinetiq.com/S-T).

WIRED Consulting.

WIRED is known for its fresh thinking and deep expertise on the technological, scientific and societal trends shaping our world. WIRED Consulting is a division of WIRED dedicated to taking the unique WIRED network, knowledge and brand to commercial organisations – helping them to build internal knowledge, develop strategy and create thought-leading content that positions their brand at the cutting edge of trends.

Discover more at consulting.wired.co.uk.

