Faceless workspaces?

The effect of smart robotics on cybersecurity and business

March

2020

Contents

The introduction of 'Artificial Intelligence' for the masses that we have seen over the last few years has instead been a rapid development in machine learning. Machines, robots and software, unlike humans, are designed to fulfil a commercial purpose and need instruction to carry out tasks. Any use of gender that may humanise this technology is little more than strands of code. As it stands, 'AI' lacks motivation and features are programmed – not learnt. To put it simply, an ant has more intelligence than 'AI' to date and anything artificial needs human direction to function.

Eugene Kaspersky, Founder and CEO of Kaspersky

Cultural change

Robots in factories and smart devices designed to help us complete household tasks are no longer the science fiction fantasies they once were. Artificial intelligence (AI) is rapidly taking its place in our technological history. Our favourite brands are embracing the power of smart robotics and machine learning to improve their products and make our lives more convenient.

This report aims to separate the fact from the fiction by exploring both exciting and concerning future possibilities for robotics

It cannot be denied that smarter technology delivers more efficiencies and intuitive solutions. Time once spent by human workers screwing on toothpaste lids can now be used for more lucrative and creative purposes. Yet many workers and consumers have their reservations. From fears around job losses to dystopian futures set out in our favourite fantasy novels, there are a number of scenarios that could worsen the social and economic impact of robotics.

As we become more trusting of the technology, questions are being asked as to whether it can be used against us. Humans often have poor intentions and anyone with a necessary motive can bend technology to their will. This can come from oppressive governments or rogue, yet sophisticated cyberattacks. How much of our lives are we willing to hand over and arguably put at risk? With machines needing data to run effectively, questions still remain over where it is stored and how it could be leveraged to harm human life.

This report aims to separate the fact from the fiction by exploring both exciting and concerning future possibilities for robotics, with expert opinions from AI, machine learning and cybersecurity specialists.

Who's fit for work?

A recent Kaspersky study revealed nearly half (49%) of UK parents are concerned their children will find it hard to get a job in adulthood due to AI technology

It is no secret that white collar jobs have overtaken blue collar roles over the past few decades. Manufacturing positions have been steadily declining across Europe. In the UK, for instance, just one-in-10 workers are now employed in the sector. This has happened not only due to more people seeking office work, but also because organisations have restructured to maximise resources and staff expenditure. With this in mind, the introduction of robotics and AI workforces has the potential to change recruitment patterns and impact both labour-intensive and desk jobs as businesses look to improve efficiencies.

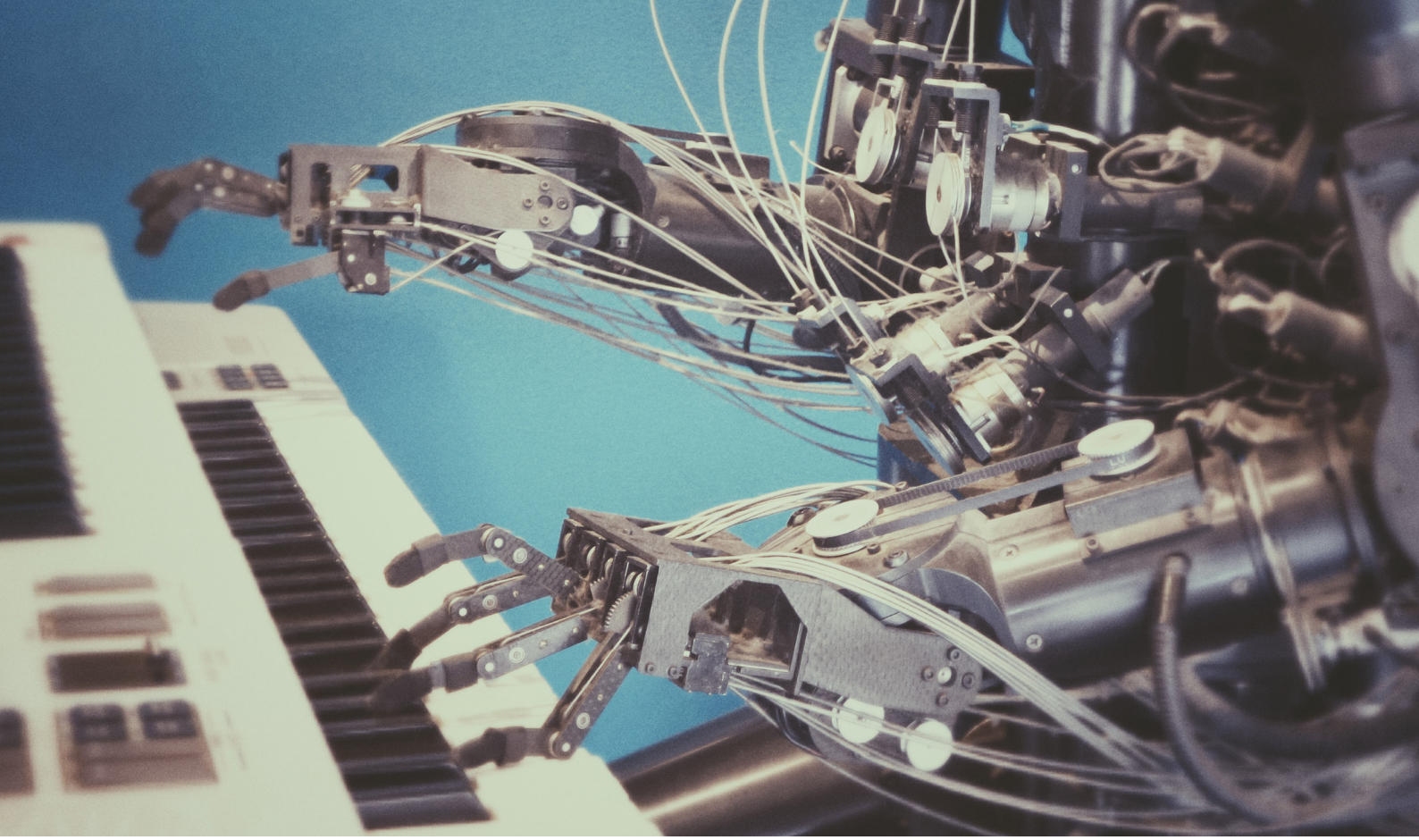
A recent Kaspersky study[1] revealed nearly half (49%) of UK parents are concerned their children will find it hard to get a job in adulthood due to AI technology. Despite consumers' worries, it is believed by many in the technology industry that jobs are not being threatened by machines. Thomas Ramge, the author of Who's Afraid of AI?, believes office roles may be adapted as a consequence, but any change we do see will be transitional and offer humans more opportunities than concerns.

He says, "AI will transform many industries around the world by taking automation to the next level. It will especially affect white-collar workers. They will experience what blue-collar workers have been experiencing for quite a while – machines can take over jobs that once seemed safe for humans. Hopefully that frees up time to allow these workers to be more creative and more sociable."

Anti-malware expert Alexey Malanov agrees and explains how we have seen professions evolve throughout history and there will always new opportunities for humans: "There used to be a lot of professions done by human hand. From textiles and shoe designing to building computers. Now this is all made by robots on conveyer belts.

"Instead people now specialise in marketing, writing, negotiating, programming, teaching, investing and selling. It is not inconceivable that soon taxi drivers, truckers and couriers will be out of business. I hope this job transformation and transition will be gradual and enable people to upskill."

[1]Kaspersky commissioned Arlington Research to undertake quantitative research amongst a nationally representative sample of UK adults to explore respondents' knowledge and perceptions of AI technology. 2,000 UK adults took part in this research.



A human-led threat?

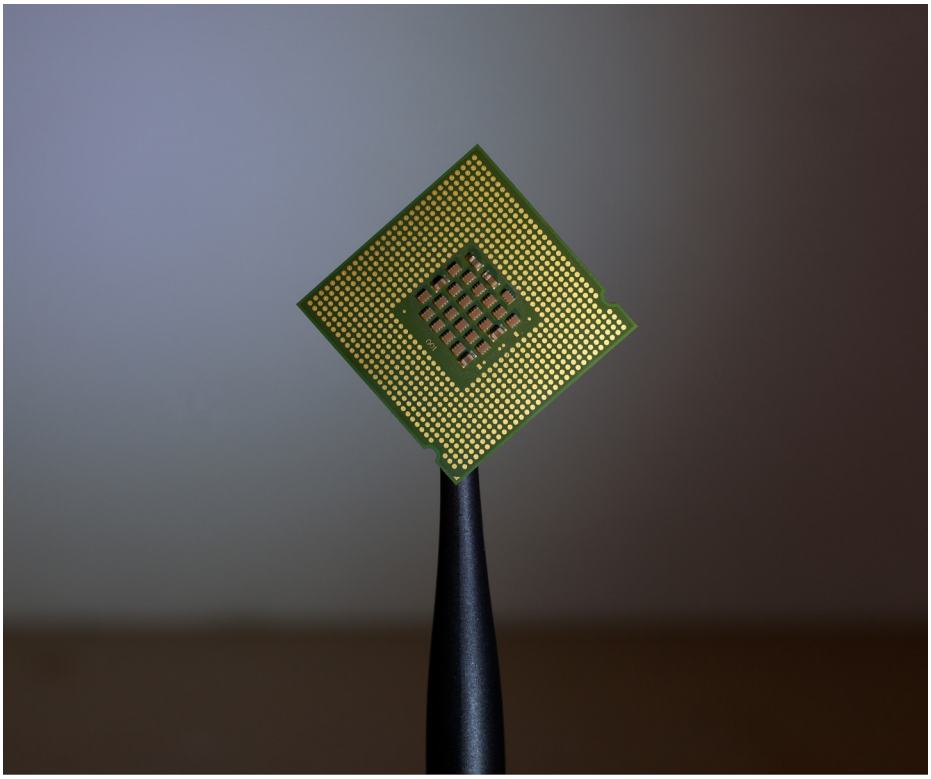
AI currently requires human adoption and influence to work effectively. From factories to smart speakers, smart technology requires human command or code to run a task. So, will AI or machine learning become self-aware? Malanov questions if the validity of cybersecurity and authorisation methods we have become accustomed to will be compromised should there be a rise of the machines. He says, "What if you can use machine learning to look at the way users create passwords, for example. Is there any way to predict an activated password, or change a password?"

As witnessed since the dawn of the internet, cybercriminals are persistent in finding new ways to carry out attacks. For many, AI, machine learning and robotics are new ways of implementing an age-old problem. However, given how effective the technology is in the right hands, Ramge argues the benefits still outweigh potential pitfalls. He says, "By making use of intelligent machines, we will be able to solve difficult and new problems. AI will help humans make better decisions in situations that, in the past, were poorly performed.

"And in many contexts, using intelligent machines will be an ethical imperative.

Autonomous vehicles are a prime example. People die every year in car accidents. When we delegate this task to machines, self-driving cars may well roam the streets more safely than humans who are prone to natural errors."

Malanov is also positive about new technologies and the changes the global workforce is about to experience, yet, still errs on the side of caution. He remains "pretty sure our future life will be better" thanks to AI and robotics, but still identifies examples that show how new technologies could influence human behaviour: "Imagine a machine learning-powered movie suggesting service. At some point, it will only begin to suggest certain types of movies, so you stop watching other movie genres. Your tastes and interests may become narrow."



Humanity may become overly reliant on machine learning and in such a scenario, those creating new technology could be left unable to fully contain its capabilities

As well as the short-term benefits Ramge touches on, David Emm, Principal Security Researcher at Kaspersky, believes AI is still heavily reliant on humans to work effectively. He says, "You've got to keep reprogramming it (AI) to account for new developments if you want to still make it good at doing what it's meant to. You're going to have to keep supplementing the logic that's used to process all these objects."

Emm is concerned about the future, especially if machines and humans remain intrinsically connected. Humanity may become overly reliant on machine learning and in such a scenario, those creating new technology could be left unable to fully contain its capabilities. He adds, "Imagine a future where actually we can build technology, but technology has the ability to keep track of tasks we can't.

"What if AI goes beyond humans, so we can't monitor it and we do not have the brain capacity to hold the information it can? We won't be able to know if it's giving us the right answer. A calculator's fine, we know when we get the wrong answer. We can't do that with some of these advanced machine learning systems. What if you can't tell if the output's valid or not?"

Ramge thinks stopping such a scenario can be done quite simply, by always giving humans the process they need to stay in control: "The machine-control question will be increasingly important and an always be considered as an element of any further development of AI systems. At a certain point, humans might need to build switch-off mechanisms to keep machines safe, just as nuclear power plants need those safety features."

Quality control

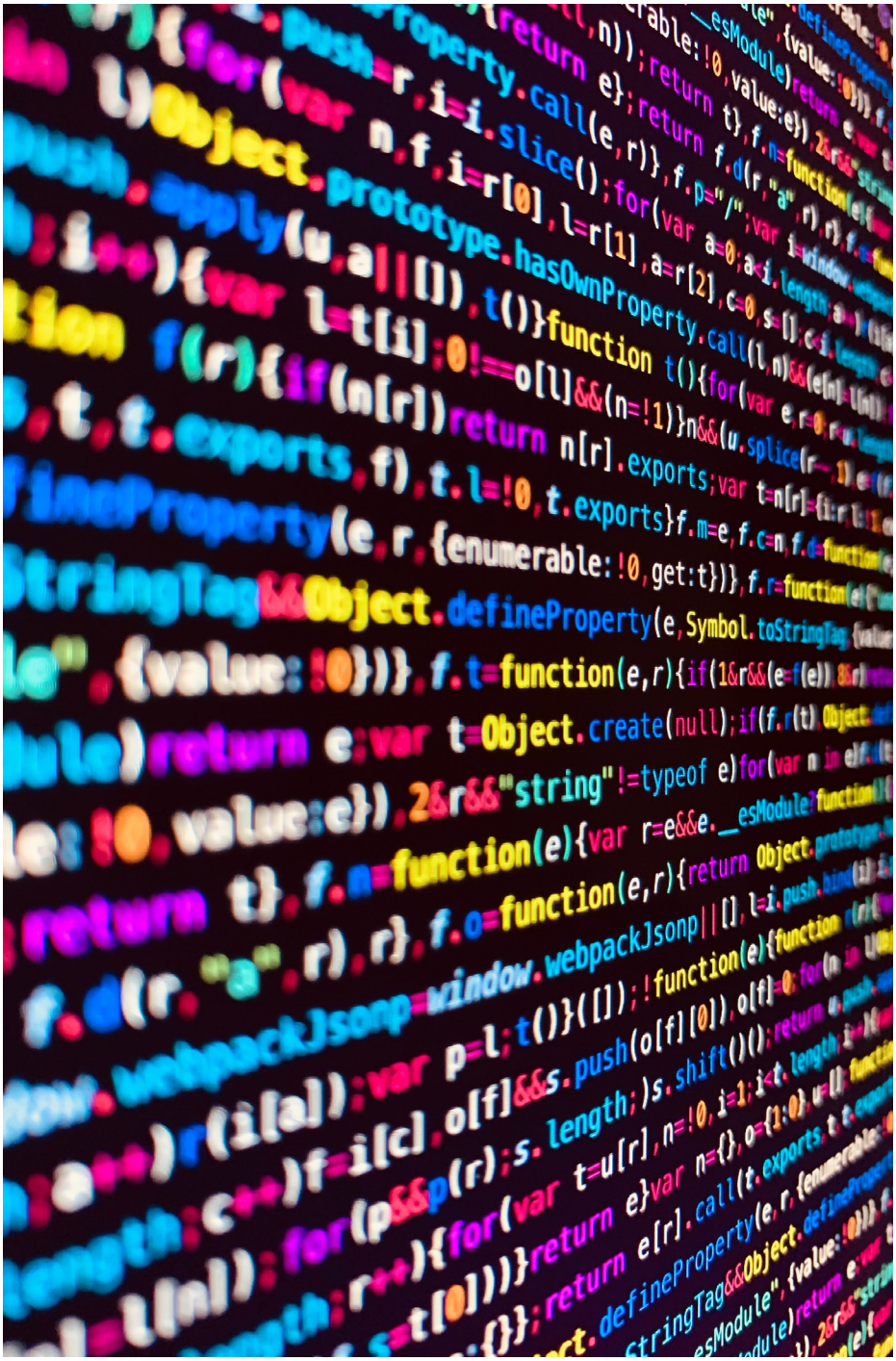
With businesses adopting more smart technology to improve efficiencies, the amount of machine learning software used worldwide is obviously set to rise. Ramge argues as long as AI relies on human input, it is very unlikely that technology will ever find a life of its own and manipulate humanity.

He says, "AI systems that are skilfully programmed and fed with proper data are useful experts within narrow specialties. But they lack the ability to see the big picture. The important decisions, including the decision about how much machine assistance is appropriate, remain human ones. Or perhaps more simply, artificial intelligence cannot relieve us of the burden to think."

Yet, it cannot be ignored that using AI-powered technology comes with great responsibility. The Cambridge Analytica scandal is a prime example of how data and machine learning can be manipulated to target audiences. This incident has led to concerns that there may be too many smart services to regulate - especially if, for example, a corrupt organisation or government prioritises AI to influence customers or citizens.

Legislation and guidelines offer solutions, and Emm suggests that "manipulation is at the heart of cyberattacks right now because the human aspect is so involved". Like all technology, keeping smart solutions out of the wrong hands is essential to ensuring security. The idea of a global or regional transparency board has been mooted in the past, and cybersecurity professionals have already made stong headway in rapidly learning about any potential threats.

While we may be waiting to see what the future has in store for AI and the workplace, organisations can take steps toward understanding the potential impact of the technology they are using. By remaining vigilant over how often personal or sensitive corporate data is shared with smart services and introducing effective cybersecurity solutions will offer control and protection. The workforce seems destined to be transformed, but with the right implementation and security standards it can change for the better.



Contributors

Eugene Kaspersky
Founder and CEO of Kaspersky

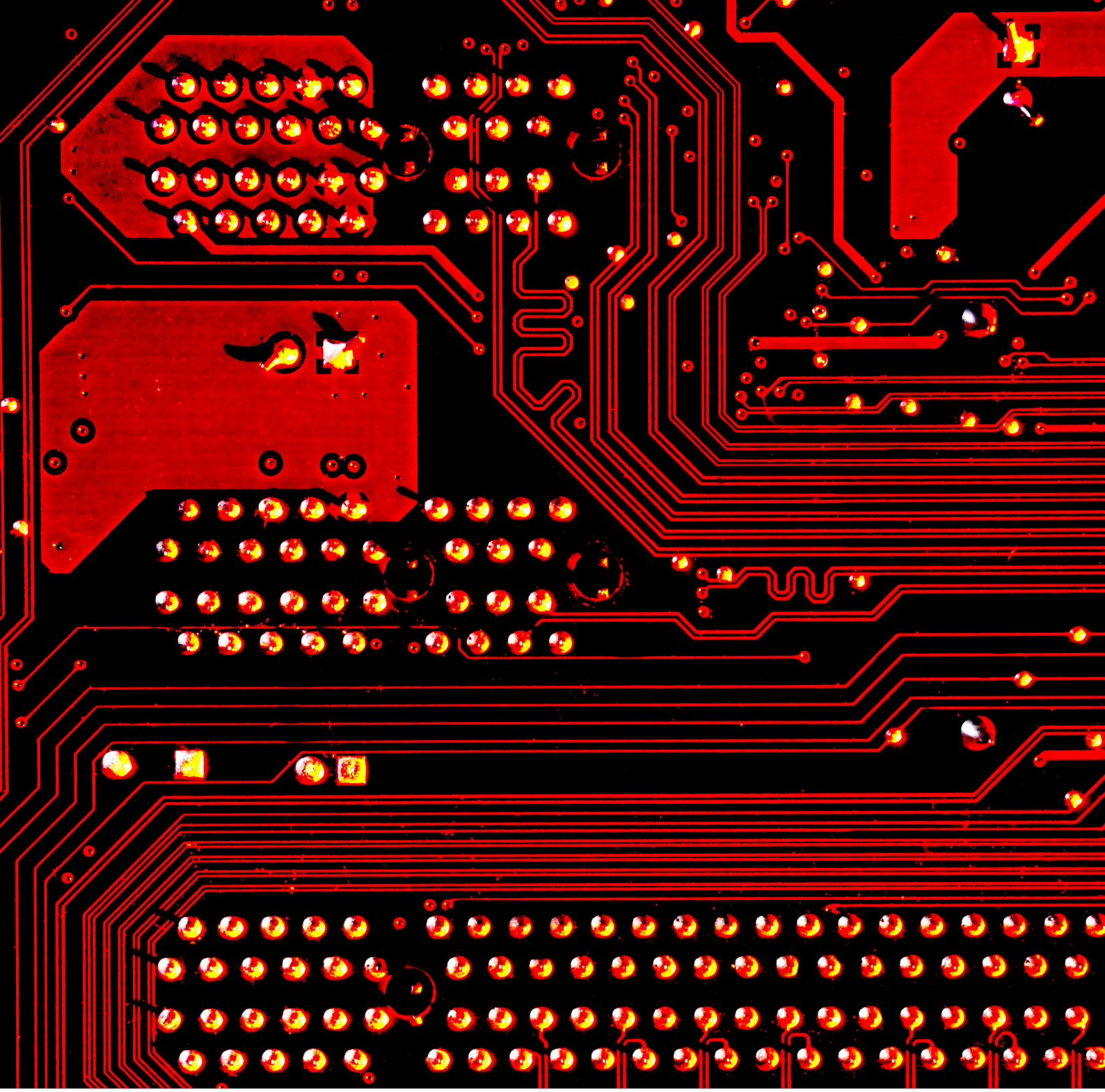
David Emm
Principal Security Research at Kaspersky

Alexey Malanov
Anti-malware Expert

Thomas Ramge
Technology & AI journalist and author of Who's Afraid of AI?

Research methodology

Kaspersky commissioned Arlington Research to undertake quantitative research amongst a nationally representative sample of UK adults to explore respondents' knowledge and perceptions of AI technology. 2,000 UK adults took part in this research.



For more information about Kaspersky products and services contact euhq@kaspersky.com or visit www.kaspersky.com

Kaspersky
Kaspersky Lab, 1st Floor
2 Kingdom Street
London, W2 6BD, UK
www.kaspersky.com

kaspersky