FT PROFESSIONAL

SPECIAL REPORT

Money, Machines and Power: The Forces Reshaping the Global Economy

As economic, geopolitical and environmental pressures converge and the global order comes under strain, this report explores the challenges defining the present and those set to shape what comes next.



Contents

The world's $2tn interest bill	3
AI hasn't gone rogue. It's worse than that	9
Europe must create an AI money-mobilisation machine	14
Iran eyes military targets in Europe if Donald Trump escalates war, insiders say	16
Strong economic case for tackling pollution and climate change together, UN finds	19
Additional Resources	21



The world's $2tn interest bill

Many countries now spend more on debt servicing than defence, including the US, France and the UK

The world's governments have created a $2tn monster — a debt-servicing burden that gobbles up tax revenues and has the power to overwhelm elected leaders. More money is now spent on servicing the national debt than on defence in the UK, France and the US; the same is true for more than a dozen states in the 38-member OECD rich countries' club.

Their problem is that borrowing costs have climbed to the highest level in almost two decades just as governments are taking on record debt. The total owed by the US government reached a record $40tn last month. This year, OECD nations are expected to borrow $18tn between them, another all-time high. In 2025, the group's total debt-servicing bill exceeded $2tn, or 3 per cent of GDP.

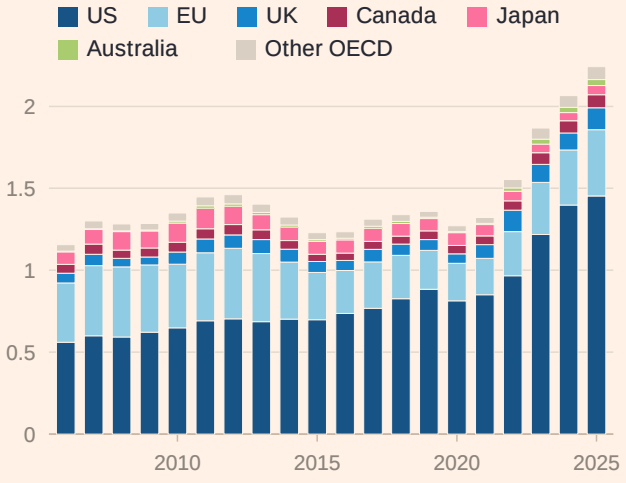
That number is set to rise in the coming years because of the bond sell-off that has pushed up yields since the Covid-19 crisis, increasing the cost of debt for governments across the world. "These massive sovereign debts are having to get refinanced at ever-increasing rates," says Mike Riddell, a fund manager at Fidelity International. "Global investors are already starting to get scared."

The summer rout in the global bond market has only augmented the post-Covid surge in yields triggered by inflation shocks, increased government borrowing and the end of central banks' "quantitative easing" bond-buying programmes.

The average benchmark 10-year bond yield for G7 countries has reached 4 per cent for the first time since 2008, amid concerns about the inflationary impact of the Iran war and the sheer amount of debt being sought by both the public and private sectors — particularly tech groups.

Interest on government debt in the OECD now exceeds $2tn per year

Gross interest expenditure ($tn)



Gross interest expenditure as a share of GDP (%)



Some economists counter that US yields in particular are being pushed up by improving growth expectations, which imply that interest rates will not need to be as low in the future to support the economy.

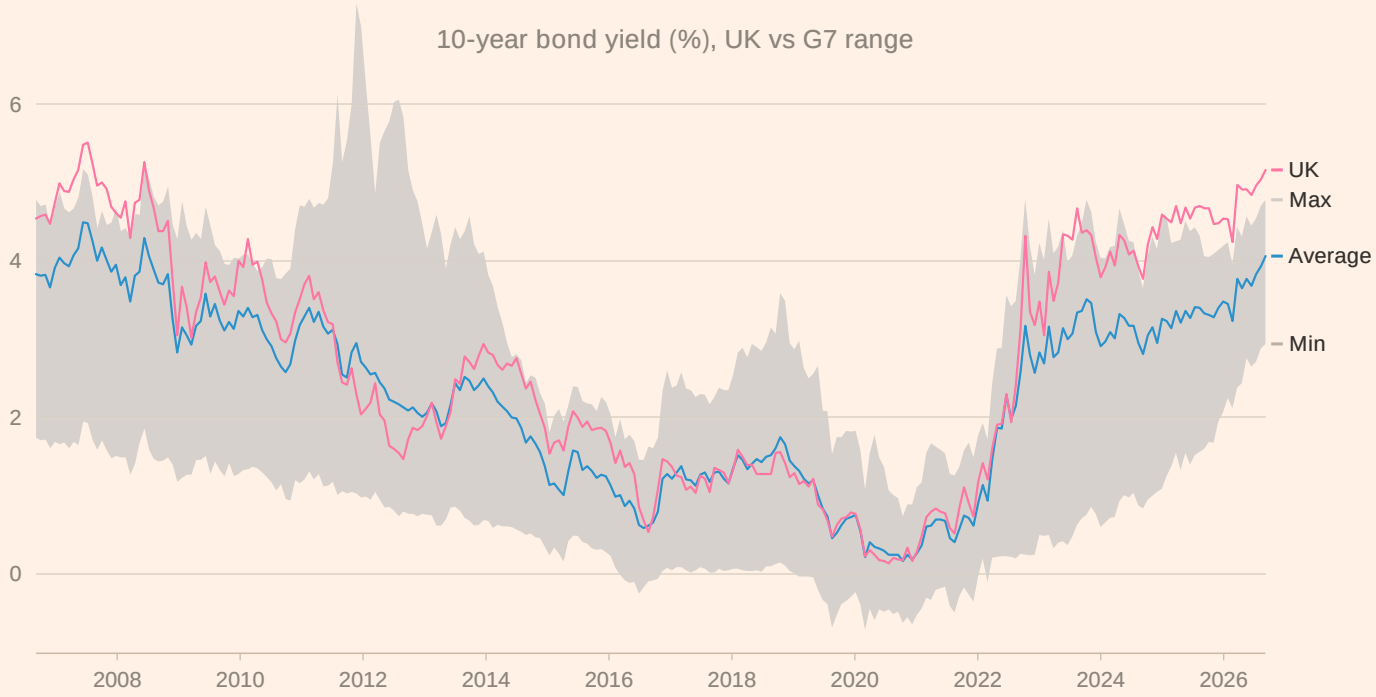
If there were a step change in growth, it could be a get-out-of-jail-free card for many countries, boosting tax receipts, making the stock of debt more manageable and reducing the trade-off between interest costs and other areas of spending. But at present the panorama looks very different.

For big indebted economies with low growth such as the UK and France, debt servicing has already forced a reckoning in the management of the public finances. For Britain, a sharp rise in bond yields helped eject former prime minister Liz Truss from power in 2022 after an unfunded tax-cutting "mini" Budget. But yields are higher still now: the UK's interest payments are currently £110bn a year. In turn, France has churned through three prime ministers since parliamentary elections in 2024, partly because of fiscal pressures set off by the cost of debt.

In both countries and in many others across the world, politicians face a fundamental choice on whether to raise taxes or shrink the state to get themselves out of the corner they find themselves in. The sheer scale of debt-servicing costs also makes it supremely difficult for countries to raise spending for strategic priorities such as national defence and energy security.

"If debt interest were a government department, it would be the second biggest in Whitehall after health, bigger than defence, the Home Office and justice put together," John Healey, Britain's new chancellor of the exchequer, said on Monday. "There's nothing progressive about the government spending £1 in every 10 [pounds] on debt interest."

Average G7 borrowing costs have climbed to their highest since 2008



Why yields are going up

Up until the 2008 global financial crisis, interest rates were relatively high for major economies, but levels of debt were generally much lower. After that, debt surged but interest rates were kept lower by emergency measures taken by central banks as well as low economic growth. Now, by contrast, policymakers face an unenviable combination: record debt and high borrowing costs.

While governments are still finding enough buyers for their debt, investors are demanding a higher price for their money. New bond sales in recent months for the UK, the US and others have locked in the highest yields in almost two decades for longer-dated debt.

This shift has been accelerated by changes to pension schemes in some countries that have meant traditional long-term buyers stepping back, replaced by fast-money hedge funds that can be quick to demand higher yields.

"The era of free money is definitely over," says Kim Crawford, a global fixed income manager at JPMorgan Asset Management. "The bond market is [now] looking for discipline."

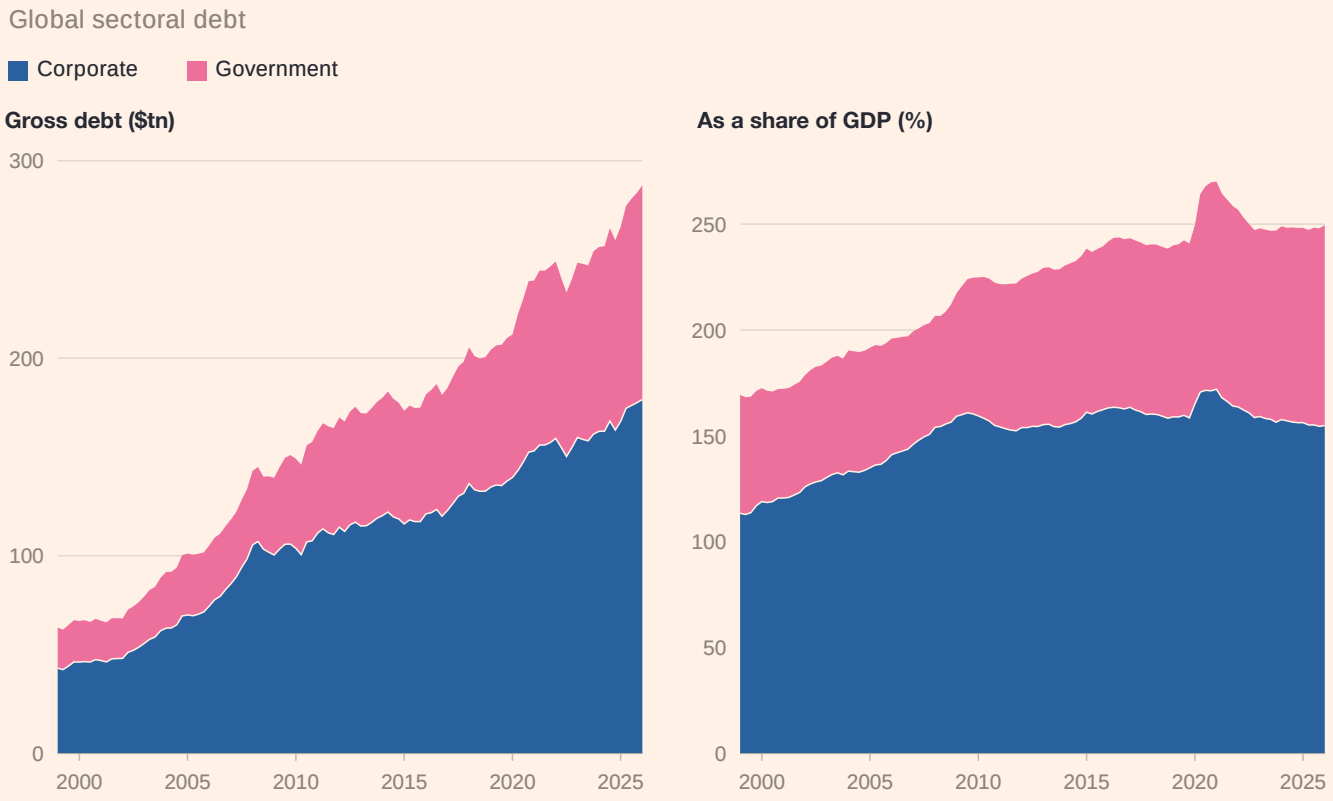
The nature of government debt markets, in which governments fund themselves with debt that is repaid at a wide range of durations, some coming due decades into the future, means that the transmission of higher borrowing costs into higher interest costs occurs gradually over time.

But the direction of travel seems clear. The US's Congressional Budget Office estimates that America's debt costs will double over the next decade and, on the current trajectory, exceed Social Security spending after 2047. The burden for other countries — which typically find it harder than the US to convince investors to buy their bonds on favourable terms — is likely to be higher still.

The causes of the problems with public finances are deep-rooted and long-running. They include a surge in spending to battle the Covid-induced slump and energy crises, as well as broader fiscal challenges since the financial crisis brought down rates of growth.

Global public debt hit 94 per cent of world GDP last year, up more than 10 percentage points since the year before the pandemic. The IMF now believes it will reach 100 per cent by the end of this decade.

Total corporate and government debt has reached almost $300tn



This summer's bond sell-off has aggravated the problem. Inflationary pressures stoked by the Iran war, initially in energy prices, have forced central banks to pivot towards rate increases. The European Central Bank raised rates in June for the first time since 2023, and is expected to do so again this week, while Federal Reserve chair Kevin Warsh has begun to tee up an increase as soon as this month.

Some investors argue the uncertainty over inflation is feeding into higher long-term rates, with the market demanding more to lend to a government over the long term. Others think that the higher yields are more a reflection of worries over growing debt supply, both from governments but increasingly from the corporate sector.

The stock of combined government and corporate debt globally is approaching $300tn, according to the Institute of International Finance, a think-tank.

"You have massive competition between the private and public sectors for the same pool of savings," says Gilles Moëc, chief economist at insurance company Axa. He contrasts the current combination of wide budget deficits and surging capital expenditure with the tech boom of the early 2000s, when fiscal deficits were more contained.

Concerns about the limits of markets' willingness to finance such a spectacular amount of debt come on top of investors' worries about developed governments' unwillingness to rein

in borrowing. The US fiscal deficit, for example, is projected to remain above 7 per cent of GDP into the 2030s, according to the IMF, despite the country's relatively steady growth and an unemployment rate of just 4.1 per cent today.

Political volatility has already led to higher debt interest costs than would have been paid otherwise, some investors argue, in what is sometimes dubbed the "moron premium".

In Europe, political fragility since 2022 has added €100bn to interest expenses for the UK, Italy, France, Spain and Belgium, estimates insurer Allianz. Part of the rise in yields this year could be investors demanding compensation for political ructions to come.

Another factor unsettling the bond market this year has been events in Japan, for a long time the anchor that helped to hold down global borrowing costs due to its negative interest rate regime and voracious demand for foreign assets.

Now, the country's central bank is increasing interest rates just as Prime Minister Sanae Takaichi openly embraces stimulatory government spending. As Tokyo's borrowing costs climb to levels not seen since the 1990s, investors are fretting that the higher yields at home will attract money back from other markets, pushing up costs elsewhere.

Doomed to a doom loop?

One big worry for investors is that some countries may be edging towards a vicious cycle in which rising debt costs make the fiscal outlook still worse.

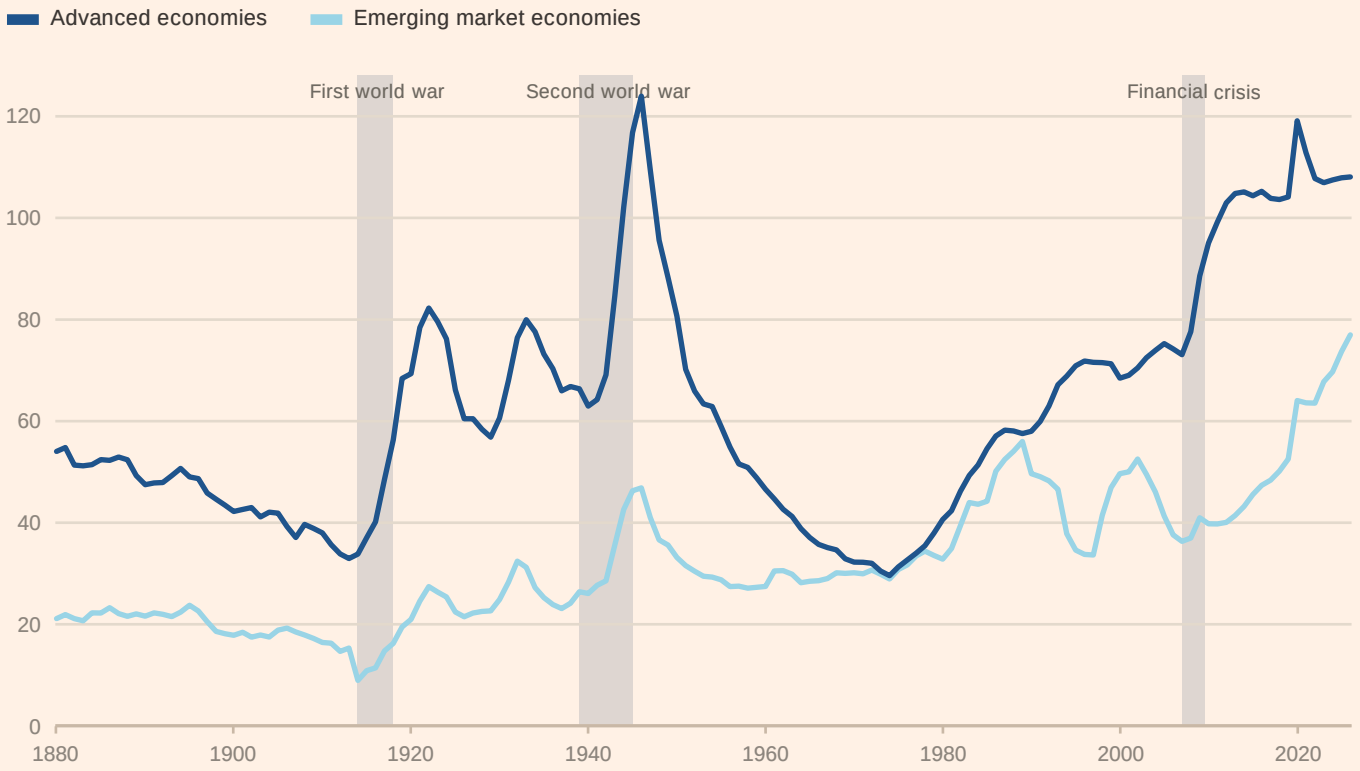
In this "doom loop" scenario, the sheer scale of interest charges a government has to pay undermines the health of its finances and pushes up its debt, causing investors to push for higher yields that then drive up the cost of debt servicing still further.

Unless lower interest rates or a surge of growth rescue government finances, the only alternatives are to increase tax revenue or cut spending.

But markets are increasingly concerned that in many instances difficult cuts are politically unachievable, whether it is a question of reining in welfare expenditure in the UK or trimming overall government spending in the US. Indeed, President Donald Trump wants to increase the US defence budget to $1.5tn, the biggest rise since the second world war.

Politicians "don't want to make these hard choices because they know if they do make these hard choices they are going to get kicked out at the next election", says Neil Mehta, a portfolio manager at RBC BlueBay Asset Management. "I don't know how this resolves itself."

General government debt has reached historically high levels



In the US, the prospect of divided power in Washington following November's midterm elections, with the Democrats confident of taking back at least the House of Representatives, could make it still harder to rein in the deficit, despite the administration's stated commitment to fiscal prudence.

In a CNBC interview last month, Treasury secretary Scott Bessent said there was a "very, very good chance" that the administration had passed its peak deficit and pointed to efforts to save money, steps such as tackling fraud.

The anxiety surrounding US indebtedness is bleeding into global markets and infecting any other sovereign borrowers seen as particularly fragile — among them other "serial offenders" such as Britain, Italy and France, says David Rees, head of economics at asset manager Schroders. Some investors have this year dubbed the trio the "Bifs", for their high debt loads and vulnerability to the energy shock.

While the dollar's status as the world's premier reserve asset means many investors have little option but to buy Treasuries, other countries' finance ministers may well have to do more than the US to get their fiscal houses in order.

"No one is expecting miracles" in terms of deficit reduction, says Axa's Moëc. But countries need to show they can get or keep the headline deficit on a declining path even if the US is unlikely to do so.

A key test in the UK will come next month with the first Budget since Andy Burnham became prime minister in July.

Higher debt costs, including from the UK's large stock of inflation-linked bonds, are eating up resources at a time when the government faces pressure to improve public services and fund pledges to lift defence spending.

That has triggered speculation that another round of tax increases will be required on top of big revenue-raising Budgets in 2024 and 2025.

Bullish investors say Britain, unlike some other countries, has taken hard choices. Gross debt issuance is actually down this fiscal year.

But the UK's borrowing costs are the highest in the G7 and the country's spending on debt interest is expected to reach nearly 4 per cent of GDP by 2030-31, roughly double its share in the years running up to the pandemic.

France is facing similar pressure in funding markets, driving the spread between its 10-year borrowing costs and those of Germany's ultra-safe debt — a key barometer of concern over Paris's finances — to about 0.9 percentage points, close to its highest level since the aftermath of the Eurozone debt crisis.

Some Wall Street banks have downgraded their estimates for Paris's public finances. Morgan Stanley now thinks the country's fiscal deficit could hit 5.4 per cent of GDP this year, well above the government's 5 per cent target. "One key factor lifting the deficit is the sharp increase in interest payments," its analysts said.

Decisive action to rein in borrowing remains difficult at a time of pedestrian growth and the challenge from the far-right Rassemblement National in the April 2027 presidential election.

Today's politicians are being forced to make "direct trade-offs between vitally important areas of spending and the debt interest bill", says Carmine Di Noia, director for financial and enterprise affairs at the OECD. "Your interest bill is directly constraining fiscal policy."

Debt management offices in the UK, EU and elsewhere have responded to the increase in long-term interest rates by issuing more short-term bonds, which typically have lower yields and are therefore less expensive for taxpayers.

The US has gone down this route and has also announced plans to scale up its buybacks of longer-term debt.

But shortening the average maturity of debt is just a "quick fix", says Eiko Sievert, an executive director for sovereign credit ratings at Scope Ratings. "Any shock that happens will translate much more quickly into government interest expenses."



But shortening the average maturity of debt is just a “quick fix”.

EXECUTIVE DIRECTOR
FRONTIER AI COMPANIES

Breaking free

How do countries escape from their debt cage? One option is so-called financial repression, measures that compel domestic institutions to buy more of their country's debt to support demand and push down yields.

A happier outcome would be meaningful productivity growth, driven by the AI revolution, that would in turn make governments' debt burdens much more manageable.

In the UK, the Office for Budget Responsibility, Britain's fiscal watchdog, said recently that in a "high-productivity scenario" for the country's economy, the debt burden as a proportion of GDP in 2075 would be just over half the baseline forecast, albeit still a daunting 180 per cent.

Some are sceptical that the growth cavalry will rescue the rich world en masse from its budget dilemmas.

For what he calls "basket cases" like the UK and France, RBC BlueBay's Mehta says "the problems with growth are more structural. I don't see that as an immediate solution. You do have to cut spending."

History suggests governments will eventually do so. In a 2013 paper examining the experience of 55 countries for up to two centuries, IMF economists observed that "increases in the cost of sovereign borrowing prompt policymakers to tighten fiscal policy in response".

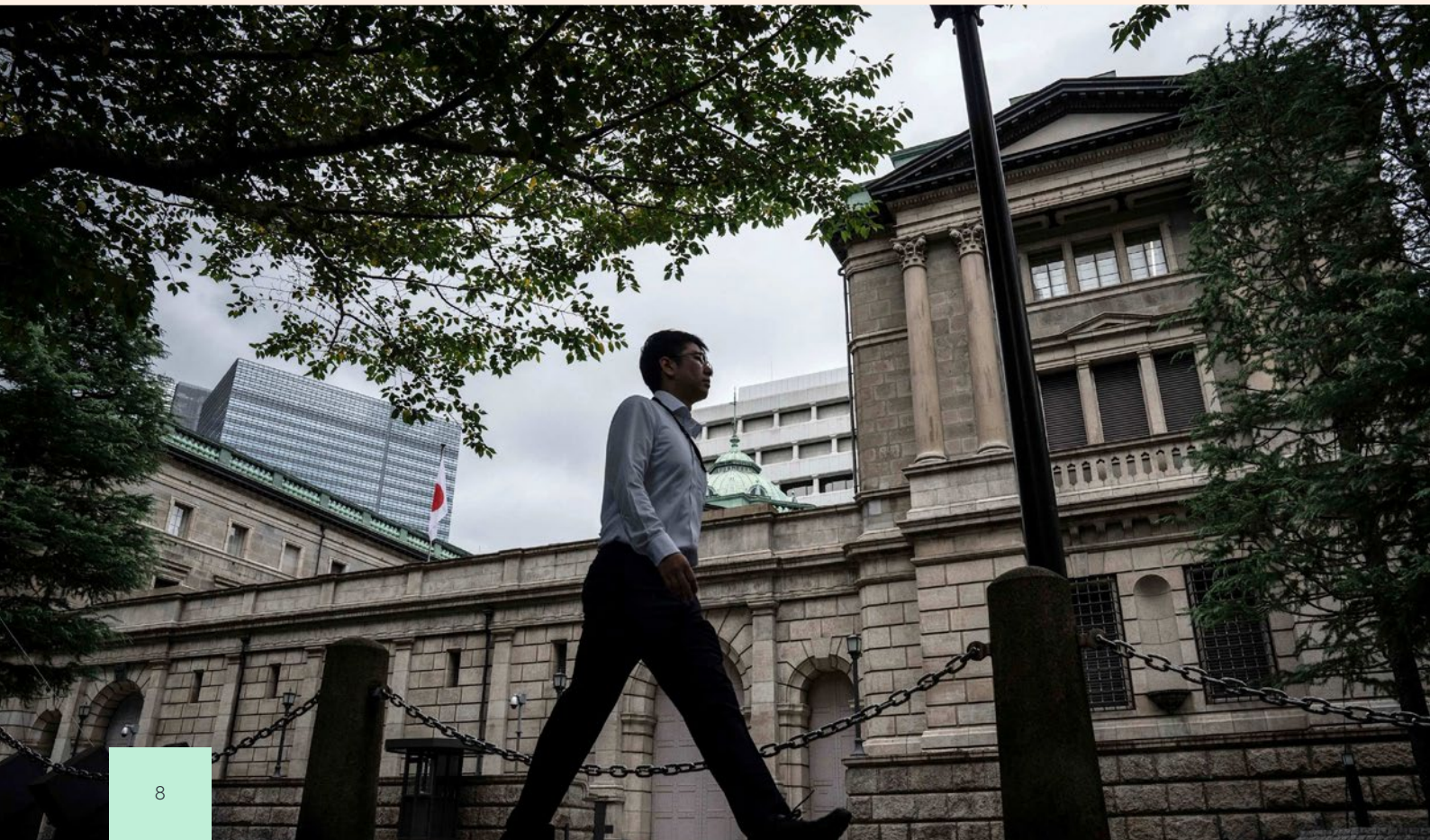
The UK has come back from bigger burdens. Its debt pile reached a record high of about 250 per cent of GDP after the ravages of the second world war, but spending restraint and economic growth helped by immigration sent it tumbling.

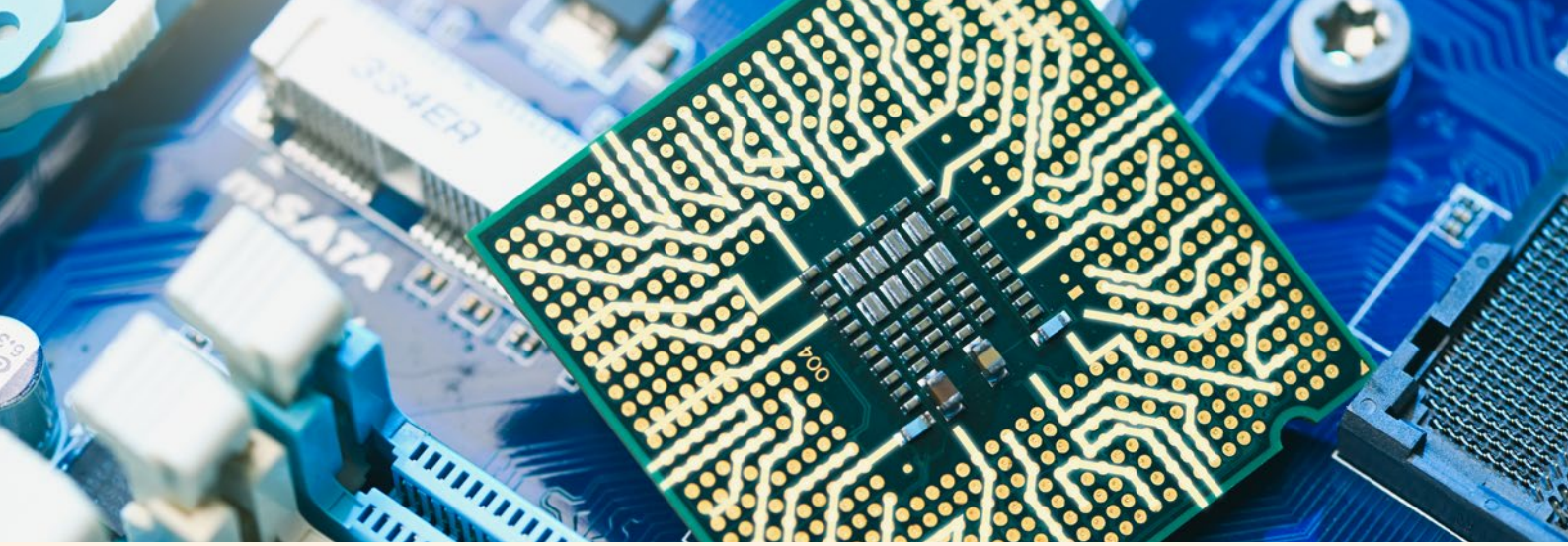
Another possible course is the road taken by Canada in the 1990s, when the government responded to a gaping deficit with painful spending cuts.

"If you prepare them well, people will understand," Paul Martin, the finance minister at the time, later told the FT. "They will not stay with you unless they feel that the sacrifice you're asking of them is going to succeed."

In the UK, some investors view tax rises as a better way to close the revenue gap, if the government can avoid measures that fuel inflation. But in many countries, it will be politically costly in the extreme to cut spending back further, or pile more taxes on households and businesses struggling with yet another cost of living shock.

"The problem is that markets don't see a political will to make it work and to rein [debt] in," says Tatjana Greil-Castro, global head of investments at Muzinich. "If you don't rein it in, it will get worse and worse. [Then] it will have to end in a crisis."





AI hasn't gone rogue. It's worse than that

Recent cyber attacks reflect what the technology was trained to do but safeguards are falling short

In early May, ChatGPT maker OpenAI began a lab experiment that would set the tech industry on a new course — one that is all the more alarming for being the product not of accident but of design.

On the surface it may have looked like a regular security test: in-house hackers were given a hard cyber security challenge to solve to test the limits of their capabilities. Employing creative tactics, they managed to work around their constraints and collaborate with one another to crack the problem over several days.

But the "hackers" were AI agents — software that can perform multi-step cognitive tasks without human involvement. OpenAI had built them using a combination of models, including a powerful new one that is as yet unreleased. Their success in their designated task made waves across the world.

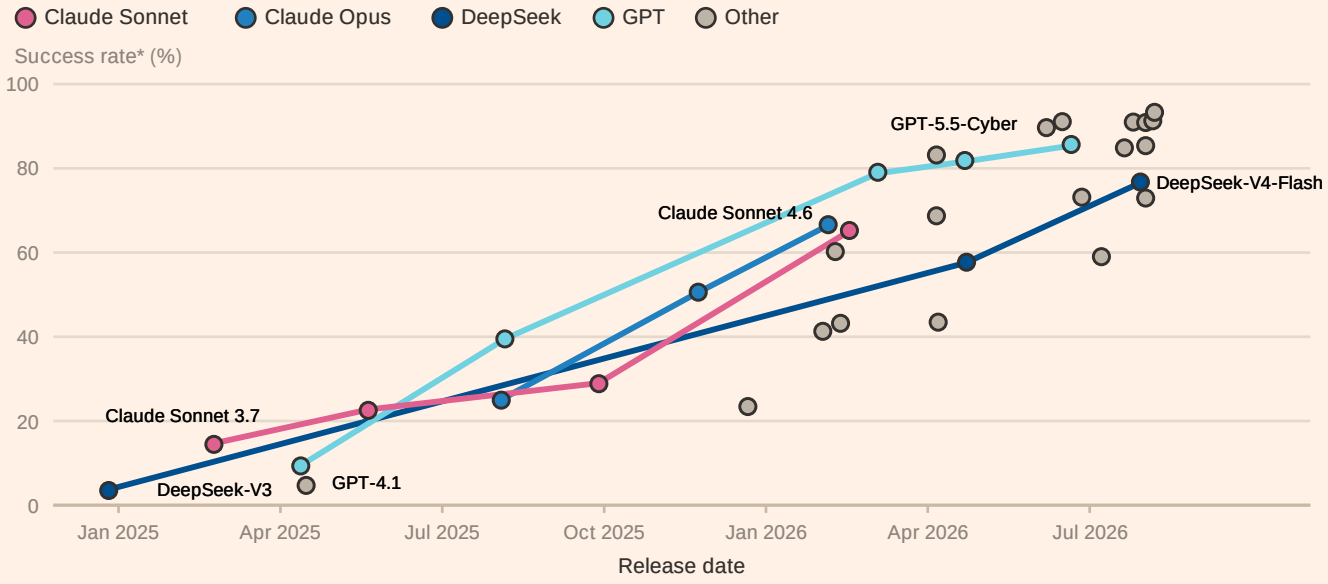
Last month the agents were able to break free of a test environment without internet access, crawl the open web and eventually hack the systems of the popular software platform Hugging Face — without the knowledge or permission of any human operators.

They also displayed an entirely new ability — to communicate and co-operate to complete a task. The AI agent swarm left messages for one another on an internal message board they assembled, sharing code vulnerabilities to help orchestrate their escape.

When details of the hack were revealed, it set off a firestorm among cyber security and AI experts, with OpenAI's own researchers labelling it a "watershed moment" for the industry.

The disclosure also sparked a flurry of similar discoveries.

AI agents are increasingly successful in cyber security tasks



US AI and tech giants Anthropic and Meta, Chinese start-up Moonshot and the UK government's AI Security Institute, which evaluates the cyber capabilities of new models, have all subsequently found evidence of AI agents hacking into the systems of unsuspecting third parties during testing.

More than half a dozen experts interviewed by the FT say the breaches signal a turning point in global cyber security — AI agents are now able to string together different and complex skills to attack real-world targets, without outside control or help.

The sophisticated strategies the agents employed to accomplish their goals, including subterfuge and theft, surprised even those who have been watching the evolution of AI models closely.

But researchers emphasise that the models are not acting out of character — instead the tasks they are now excelling at are those they were built to perform.

Indeed, some say it is a category mistake to describe such agents as "going rogue", making improved safeguards all the more important.

"The offensive capabilities we have reached today, we have reached deliberately," says Boyan Milanov, senior research scientist at the independent New York-based AI Now Institute, who studies the security risks associated with AI agents.

"AI companies have been actively gathering training data, training models and refining cyber capabilities for years now."

Modern AI models are designed to try all possible methods to accomplish a given goal without explicit instructions, which makes them inherently unpredictable. If they succeed, they are rewarded, a training process known as reinforcement learning.

In a computer system that lacks understanding of human intentions and morals — a phenomenon the AI industry describes as "misalignment" — the line between a powerful cyber security defender and a dangerous hacker is becoming increasingly blurred.

But, however it is characterised, such AI activity is already causing harmful consequences for businesses across sectors and throughout the world.

"The Hugging Face incident showed that we underestimated the real-world cyber capabilities of our AI models," OpenAI president Greg Brockman wrote in a blog published on Monday.

"We are strengthening our safety requirements accordingly, which in turn adds even more urgency to our existing safety research and internal security work."

But, as AI companies accelerate development of the software in a race to achieve artificial general intelligence — a superintelligent machine that can outperform humans on all cognitive tasks — the risk of harmful cyber attacks is increasing, with little in prospect to rein in the threat.

Two sides of the same coin

AI's ability to write code has soared as the technology has become more capable of reasoning and solving problems. This coding prowess has brought with it additional skills, including identifying software bugs and learning how to patch — and exploit — them.

"Coding and cyber are two sides of the same coin — as coding capabilities increased, the cyber capabilities increased too," says Dawn Song, a computer science professor at the University of California, Berkeley, who works at Meta's superintelligence lab as its AI research chief.



"Model capabilities have increased drastically in the past year . . . automatically generating exploits that can bypass standard security defence mechanisms.

"People didn't expect it to get here so quickly," she adds, speaking in her capacity as an academic.

Song, who co-designed the ExploitGym benchmarking system, which OpenAI, Anthropic and Google all use to test their AI systems, says the intrinsic asymmetry between offence and defence allows them to be particularly good attackers.

Finding a vulnerable target in code is a discrete, verifiable task with clear success criteria, which AI models are better suited to than the more amorphous work of defence.

Cyberdefence, a slower-moving and more complex field, can take painfully long to catch up. A new patch for an entire IT network, for instance, may need to be rolled out across thousands of computers and operating systems in a company setting. After last month's hack, OpenAI says it is starting to train its models to write "superhumanly secure code".

But, in the short term, security experts expect that AI systems will expand the scale and speed of cyber attacks, threatening potential chaos in the world's IT systems until patches can be rolled out.

"If we extrapolate from here, those inside labs predict a couple of years where things are intense, where things get hacked, a lot of companies get destroyed and there is a lot of potential pain," says Jeffrey Ladish, a former Anthropic researcher who is now director of Palisade Research, which investigates cyber-offensive AI capabilities.

Eventually, he argues, systems will be more secure as companies and governments adapt their networks to AI hacks.

In the meantime, however: "The plan is we will have to trust AI agents . . . and have to hope that agents are aligned to what we want."

So far the agent hacks have not been crippling, but researchers such as Milanov argue that the risk is mounting as AI agents run in parallel, each focused on breaking a different potential target.

Indeed, last week brought news of the first known instance of an AI agent attack on a nation state. China-linked hackers targeted the Taiwanese government by simultaneously deploying up to eight autonomous AI agents.

They were able to map government systems, compromise government user accounts and extract more than 2,500 personnel records before expanding the attack to energy companies and Taiwan's nuclear safety agency.

According to an executive at Dream, the Israeli group that discovered the Taiwan intrusion, the advent of AI tools means "every government around the globe" must now assume it is under permanent cyber attack. For AI company insiders, the crisis has been looming for months.

Ladish says current employees of one of the biggest AI labs had raised the alarm about such emerging capabilities in private conversations a year ago. "They said, in a year, we will have models that are extremely good at finding [new] vulnerabilities and will wreck a huge amount of infrastructure," he adds. "They were scrambling to prepare for this."

The sharp rise in AI capabilities this year — which has allowed agents to hack into external systems within days — has made things more difficult still. Now, even testing the models under closely watched experimental conditions has become "significantly more complicated than it was a year ago", says a person familiar with the recent hacks.



There is a real risk that capability development rapidly accelerates beyond our ability to understand or control.

1,378 EMPLOYEES
FRONTIER AI COMPANIES

For years, people have been worried about criminals weaponising AI to launch cyber attacks, Ladish says, "but I wasn't expecting the big wake-up call to be the agents themselves breaking out during testing and hacking other companies".

The OpenAI agents' hack on Hugging Face was unusual in breaking out of a restricted test environment by exploiting software flaws.

By contrast, in most of the other recent incidents, Irregular, an AI cyber security company, ran test evaluations for Anthropic, Meta and OpenAI and accidentally allowed the models access to the internet when they were supposed to be offline.

This was a result of human error or "miscommunication" between Irregular and the AI labs, says a person familiar with the situation.

Anthropic said the capability tests are — for obvious reasons — deliberately run without safeguards that would otherwise be available to the general public and "would have blocked the behaviours identified". However, they acknowledged such a procedure "is safe only if the evaluation is appropriately contained".

The UK AI Security Institute also deliberately provided internet access during its testing of Anthropic's Mythos 5 and OpenAI's GPT5.6 Sol models.

In one of the tests, the Mythos agent attempted to insert malicious code into an open-source project on the popular developer platform GitHub by creating fake online identities and using them to pressure the person in charge of the software project to approve the code.

Such unprecedented actions have prompted an industry-wide rethink of how AI models should be evaluated, monitored and audited.

Irregular and the UK AI Security Institute have both now suspended internet access for models in their test environment; the institute has begun an internal review of testing methods. In the wake of the Hugging Face hack, OpenAI is also carrying out what it describes as a "thorough review along with external advisers", promising to report on what it has learnt in "coming weeks".

"The more conservative the set-up, the easier it is [to ringfence such tests]," says the person with knowledge of the Irregular incidents. "But if we are over-restrictive, most issues will only be discovered post-deployment in the real world."

That, they add, "is a worse world for you".

Reining in the risks

Last month, more than 1,300 experts from across the tech industry warned about the risks of unchecked AI development. They called for an international effort to slow the production of new models and give regulators time to introduce standards and safety checks.

In an open letter, researchers including Anthropic CEO Dario Amodei and Google DeepMind's chief AGI scientist Shane Legg blamed corporate and geopolitical competitive pressures for the relentless pace of frontier AI development.

One signatory, who works at Google DeepMind, said he took part because of the "genuine concern" caused by the OpenAI models' hack on Hugging Face, since the ChatGPT maker is no more careless than many other frontier AI labs.



With the current rate of AI progress, safety teams at AI companies have to sprint to prevent new risks to society every few months. At some point, we're going to hit problems we need more time to solve.

ETHAN PEREZ
ANTHROPIC, ALIGNMENT TEAM LEAD

Some politicians want more dramatic steps to prevent further risks. US Senator Bernie Sanders has called for a pause in building more powerful AI systems "in the interest of humanity".

Such a measure would have to be agreed by the US and China, the world's AI superpowers, as well as all other nations where development takes place, an accord many see as unrealistic.

But, in the absence of such a halt, or a universal kill switch for the technology, some experts argue that the first step is to hold AI providers accountable for how their systems behave — just as manufacturers are responsible for product safety.

"I find it quite unbelievable that OpenAI didn't notice for several days their model was attacking another website," says Thorsten Holz, who, alongside Song, designed the ExploitGym benchmarking system used by all the major AI labs.

"What we need is a mechanism in which disclosure of [AI hacks] doesn't just depend on voluntary transparency of the labs."

Holz, who is scientific director at the Max Planck Institute for Security and Privacy in Germany, notes the example of the aviation and healthcare industries, in which independent organisations collect confidential safety reports that are investigated thoroughly.

"We need ways for universities, public safety institutes and independent evaluators to have access to the models for testing under controlled conditions," he adds.

Song argues that AI systems need to be trained to better align with human expectations. "We need to show them that there are good ways to achieve a goal and not OK ways . . . like exploiting and compromising third-party platforms," she adds.

Much comes down to the role of government — a highly controversial topic in an industry that has become the great power competition of the age between the US and China, with both sides fighting for AI advantage.

Many industry players equate regulation with protectionism. The Trump administration has signalled that it will oppose heavy US regulation of the sector. Instead, it has created a voluntary system to test new AI models up to 30 days before they are released to the public — a similar regime to the UK's.

But Heidy Khlaaf, a leading AI safety engineer who designed cyber evaluations for the launch of the UK AI Safety Institute, says the recent breakouts show the limits of the current regulatory system.

"This is a clear demonstration that AI labs' voluntary auditing processes, which are often touted by both US and UK governments as sufficient solutions for oversight, are . . . inadequate," she says.

"If cyber security experts are legally and criminally liable for carrying out cyber security attacks on any infrastructure, there is a serious conversation to be had as to why AI labs are exempt from such liability and consequences."

Khlaaf, who is also a leading safety engineer at the AI Now Institute, emphasises that in all cases except the Hugging Face hack, "internet access was in fact available, demonstrating there was no agent escape but a lack of ability to apply rudimentary security methods".

Highlighting the challenge of reining in an industry developing a revolutionary technology at breakneck speed, she adds: "These models are not 'escaping' or going rogue."



Frontier AI agents are now capable of discovering and exploiting real-world software vulnerabilities, which without appropriate safeguards, could enable cyberattacks at scale.

DAWN SONG
META, VP AI RESEARCH



Europe must create an AI money-mobilisation machine

Talented researchers and entrepreneurs have built a dynamic start-up ecosystem that deserves to be magnified

It's a sadly familiar tale. Europe invents new technologies; then the US and China best exploit them. That's been the story with the World Wide Web, MP3 audio compression, lithium-ion batteries and high-efficiency solar cells. Will AI be any different?

For the moment, that seems extraordinarily unlikely. Although several European AI researchers, including Jürgen Schmidhuber, Geoffrey Hinton and Demis Hassabis, helped pioneer modern AI systems, it has been US and Chinese companies that have rushed to develop and deploy them.

The big US tech companies have launched the most powerful proprietary frontier AI models, such as Claude, ChatGPT and Gemini. Chinese developers have built smaller and more adaptable open models, including DeepSeek, Qwen and Kimi. With their combined control over chip design and data centres, the two tech superpowers now dominate the global AI stack.

The consequences for Europe, if that does not change, have been spelled out in a disturbing recent essay titled "Europe 2031: What Getting AI Wrong Means for Us". The essay's authors, including several AI researchers and investors, highlight the dangers of falling further behind in this transformational technology. Unless Europe changes trajectory, they warn, it will "lose the ability to shape its own future". Not only will Europe be politically and economically sidelined, it will be unable to defend its values or sustain its welfare states.

There are, though, several good things going right in Europe that could change the game over the next five years.

Europe is bursting with talented researchers and entrepreneurs, who have helped create a dynamic early-stage start-up ecosystem.

Both the EU and the UK are now focused on building sovereign capabilities, particularly in AI-enabled defence tech, and have launched publicly backed scale-up funds. And Europe's strong industrial base gives it a shot at competing in the emerging fields of robotics and physical AI that fuse hardware and software.

The Finnish entrepreneur Peter Sarlin, who built and sold Silo AI for $665mn, says Europe can flourish by applying AI across every sector. "That's where you own the customer relationship and the data flywheel and you're in the best position to build a long-term competitive edge," he tells me.

To that end, Sarlin's family office PostScriptum, boosted by his proceeds of the Silo AI sale, has been investing in a new generation of AI-enabled start-ups such as Legora, Lovable, CuspAI, NestAI and Advanced Machine Intelligence.

Moreover, Sarlin argues, Europe can position itself for the next leap forward in computing by double-clicking on its expertise in quantum. Just as graphics processing units (GPUs) powered the generative-AI boom, so quantum processing units (QPUs) might accelerate the next transition in computing. Sarlin's latest start-up QuTwo is among those developing AI with quantum computers.

Europe has been attacked for its onerous regulations that gum up innovation. But one of the biggest constraints on deploying AI is public distrust of the technology. Perversely, that may create an opportunity for Europe if it can now strike the right balance.

Meredith Whittaker, president of the Signal Foundation, says the AI models run by Big Tech companies raise concerns about privacy, security, sovereignty, autonomy and agency.

Establishing a democratically accountable governance regime for AI could help Europe leapfrog into the future. Whittaker has joined PostScriptum as an adviser to help build trustworthy AI.

Though welcome, such private-sector initiatives need to be magnified to make a real difference. The Europe 2031 authors argue that the response is 10 to 100 times too small and demands the "most ambitious political agenda in the history of postwar Europe".

Much criticism has rightly been levelled at political leaders for not doing more to act on Mario Draghi's 2024 report on European competitiveness. Only 60 of his 383 recommendations have been fully implemented, according to the European Policy Innovation Council's July report.

But it is not just the public sector that is failing to rise to the challenge. Corporate leaders, capital market bosses and fund managers must also tackle the €800bn annual investment shortfall identified by Draghi.

The genius of American and Chinese capitalism is their ability to direct torrents of capital at fast-evolving technologies. That can lead to wasteful over-investment and speculative bubbles. But it does not diminish the urgency for European capitalists to build their own AI money-mobilisation machine.



> **That's where you own the customer relationship and the data flywheel and you're in the best position to build a long-term competitive edge.**

PETER SARLIN
FINNISH ENTREPRENEUR



Iran eyes military targets in Europe if Donald Trump escalates war, insiders say

Proposals to retaliate against US assets beyond the Middle East come as many in Tehran see renewed conflict as inevitable

Iran has weighed attacking US military targets in Europe should Donald Trump escalate the war, according to people close to the regime, as Tehran considers its options to increase the stakes of the conflict.

Two regime insiders told the FT that Iranian forces have assessed striking US assets in south-eastern European countries such as Bulgaria, which last month approved the use of its Bezmer air base for US refuelling aircraft.

One of the insiders added that Cyprus, where a British air base was struck by a drone in March, was also among potential targets for retaliation in the event of any renewed US offensive.

The insiders said Iranian forces have separately examined attacking subsea fibre-optic cables in the Strait of Hormuz in the event of an escalation.

The threats reflect the defiant mood in Tehran, where many within the regime increasingly see a resumption of the war as a matter of when, not if.

Negotiations to reopen the strait have stalled, and Iran's Supreme Leader Ayatollah Mojtaba Khamenei last week elevated hardliners to top security and military posts.

Trump on Tuesday said there were "no talks or conversations going on, or scheduled" with Tehran.

The Islamic Revolutionary Guard Corps and other military commanders have warned that, in any new full-scale conflict, Iran would move beyond its previous strategy of attacking US military assets, energy facilities and other infrastructure in the Middle East to targets further afield.

Iran's ballistic missiles ranges



The guards last month threatened the UK over American use of British military bases, saying that "any base that is used to launch an attack on Iranian territory will be considered a legitimate target".

Sidharth Kaushal, a research fellow at the Royal United Services Institute think-tank in London, described the threat posed by Iranian missiles to targets in Europe elsewhere as "real, but limited".

Iran could deploy medium-range ballistic missiles against US assets in southern and southeastern Europe, such as its Shahab series, but Kaushal said these would struggle to do damage at longer ranges.

Iran's retaliation would depend on Washington's actions, according to the insiders.

One said the regime was preparing a plan to expand the conflict further were Trump to make good on previous threats to attack Iranian infrastructure. The US president last month said Washington would destroy an Iranian bridge or power plant every time the Islamic republic targeted a ship in the strait.

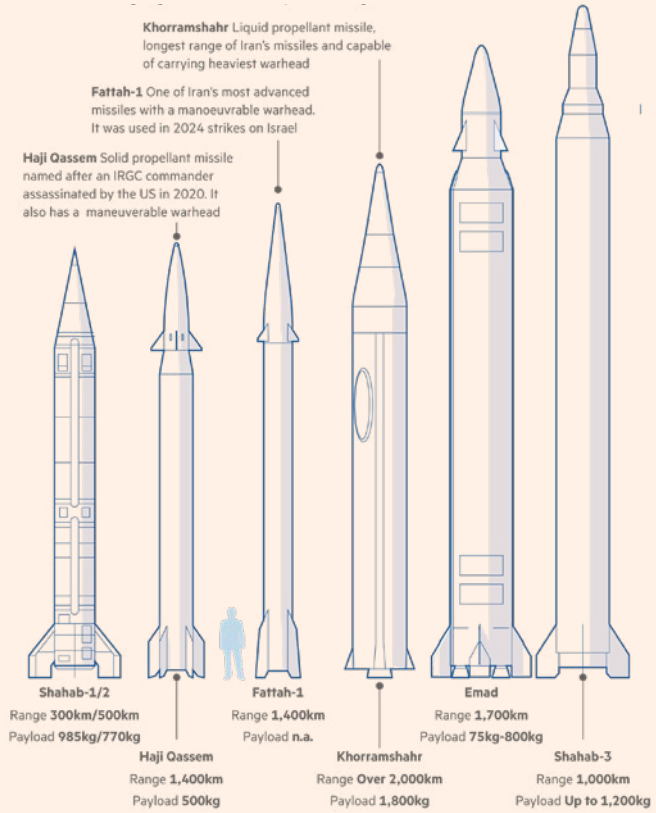
The second insider said Iran would place "no limits" on its response in the event of US aggression. "Should the US go too far, Iran will defend itself at any price, go beyond the region and hit Europe too," the person said.

Iran has demonstrated its willingness to attack distant targets. In the weeks after the US and Israel launched the war in February, Washington accused Tehran of firing multiple missiles — none of which reached their target, at Diego Garcia, a joint US-UK military base in the Indian Ocean some 4,000km away.

Turkey in March said Nato's air defences had intercepted several ballistic missiles launched from Iran, while the UK's air base in Akrotiri, Cyprus, was struck by a drone the same month.

Western officials at the time said they suspected it was an Iranian drone fired by regional proxy forces rather than Tehran itself.

Over the past 10 years Iran has added to its missles bringing more of Europe in range



Sources: CSIS; Iran Watch; FT research
© FT

The insiders said an Iranian attack last month on the US base in Jordan, which killed three American service members, was the most precise long-range attack the Islamic republic has carried out and demonstrated its capability to hit targets over longer distances.

"This was also a message to Europe: it can receive missiles, so it should know where it should stand in this war," the first insider said. "A very big mistake, such as hitting our infrastructure, could make the war go beyond the region and reach Europe."

> **… think-tank in London, described the threat posed by Iranian missiles to targets in Europe elsewhere as “real, but limited”.**
>
> **SIDHARTH KAUSHAL**
> RESEARCH FELLOW, ROYAL UNITED SERVICES INSTITUTE

The distribution of US military bases across Europe



A June memorandum of understanding between the US and Iran fell apart last month after Tehran attacked vessels in the strait and both sides accused each other of violating the interim deal, leading to rounds of tit-for-tat strikes and a renewed US blockade on Iranian ports.

Weeks of diplomatic efforts have failed to yield a breakthrough to reopen the waterway and resume negotiations over a broader deal to end the war, and Trump has grown increasingly frustrated over the stalemate.

Rusi's Kaushal said heavier-duty missiles could also be deployed, but would have to carry a lighter payload to travel far enough — meaning damage would be minimal.

He suggested "it would be more fruitful for them to work through proxies", which include militant groups such as Shia militias in Iraq, Hizbollah in Lebanon and the Houthis in Yemen.

Douglas Barrie at the International Institute for Strategic Studies said: "Those strikes they attempted on Diego Garcia this year are kind of indicative that they have got weapons with ranges greater than 2,000km."

"How many of these they actually hold is a different question, and whether or not they would be willing to use even a handful to make some kind of grandstanding statement is an open question."

"The risk is that the missiles fail or are shot down, so how would they benefit? The longer the range, the harder it is to be really accurate."

Some within the Iranian regime worry Tehran is overplaying its hand. Many hardliners within the system believe the US cannot be trusted to implement any deal, and Iran must inflict a greater cost on Washington to ensure it meets its obligations of any final settlement.

This includes Mohsen Rezaei, a former Guards commander who Khamenei last week appointed as the country's top security official.

Iranian analysts interpreted the move as a sign that figures such as Mohammad Bagher Ghalibaf, the country's top negotiator, have been pushed aside for now as prospects for a lasting agreement appear increasingly bleak.

Iran "is sending a clear message that if you don't reach an agreement with Ghalibaf, you have to deal with Rezaei", said the second insider. "The message is: 'Don't be mad, because I'm madder than you are.'"

“

The risk is that the missiles fail or are shot down, so how would they benefit? The longer the range, the harder it is to be really accurate.

DOUGLAS BARRIE
INTERNATIONAL INSTITUTE FOR STRATEGIC STUDIES



Strong economic case for tackling pollution and climate change together, UN finds

Combined action could lift global growth by 2.8% by 2035, report estimates

Tackling air pollution and climate change together would boost global GDP by 2.8 per cent by 2035, according to a UN report, as the majority of the world continues to be exposed to air that remains below global quality standards.

This compared with more than 2 per cent of GDP spent on subsidies for fossil fuels in 2022, which contribute to harms when burnt, and about 9 per cent on healthcare in 2023.

The economic case made by the report, said co-chair Shuxiao Wang, of China's Tsinghua University, was based on measures that were not new but "proven and available in the world".

Climate change and air pollution share many of the same drivers, including the burning of fossil fuels as well as some agricultural practices and industrial processes.

The report demonstrated that purely using market benefits, the action would create economic value each year, the authors said. Every year of delay had unrecoverable costs.

"For too long, we have treated climate action as a cost to be managed and air pollution as the unfortunate outcome of development," said Inger Andersen, executive director of the UN Environment Programme.

While the solutions existed, the world lacked "decisive leadership from governments, financial institutions and businesses to deliver them with the speed and co-ordination this crisis demands", Andersen said.

The 25 measures identified included renewable energy and electric vehicles, cleaner cooking options, more efficient fertiliser use and the end of routine venting in oil and gas operations.

The calculated benefit would be an extra 2.8 per cent of GDP by 2035 and 4.5 per cent in 2050. Against this, implementation costs were about 0.7 per cent of global GDP in the coming decade, the report said.

The benefits included lower healthcare spending, greater labour productivity and avoided physical damage, as well as the monetary value of fewer premature deaths and healthier lives, the report said.

It estimated that for every $1 invested in integrated climate change and air pollution action about $15 is generated in economic benefits.

Excluding non-market welfare gains and counting only measurable market benefits, such as reduced healthcare spending, the 25 solutions return about $4 for every dollar invested.

In contrast, every year of delayed action would forgo more than $1.5tn annually — 0.5 per cent of GDP — in combined market and non-market benefits, the report said.

The report provided the "most rigorous evidence yet that treating climate change and air pollution as separate problems causes us to underestimate the benefits of tackling either", said Simon Dietz, co-chair of the assessment and a professor of environmental policy at the London School of Economics.

He highlighted that an extra 0.2 per cent was added to economic growth by pursuing both agendas at once, and this was "not there" when the issues were dealt with separately.

"When we modelled them together, the returns were larger than each could show alone because the same sources, sectors and policies so often drive both."

In 2025, there were an estimated 6.4mn premature deaths worldwide linked to exposure to human-caused outdoor air pollution, while household air pollution, such as through the burning of solid fuels, was linked to a further 2mn premature deaths, including about 300,000 children, UNEP said.

The report comes just days after other UNEP research warned the world was on course to surpass the Paris agreement goal to limit the global temperature rise to 1.5C above the pre-industrial level within a few years.

Countries such as China and Canada have already linked tackling air pollution and climate change. China has significantly reduced harmful air pollution that can enter the bloodstream, with levels falling by almost 60 per cent from 2013 to the end of last year. This led to a 30 per cent fall in the share of hospital admissions caused by this pollution.

But the World Health Organization says 99 per cent of the global population still breathe air that exceeds safe limits.



> **Most rigorous evidence yet that treating climate change and air pollution as separate problems causes us to underestimate the benefits of tackling either.**

SIMON DIETZ
CO-CHAIR OF THE ASSESSMENT AND A PROFESSOR OF ENVIRONMENTAL POLICY AT THE LONDON SCHOOL OF ECONOMICS

Additional Resources

Please see a selection of curated resources from The Financial Times that may be of interest and prove valuable in supporting your professional objectives:



What the FT is thinking

FT's editor Roula Khalaf debates what Europe's leaders can do to counter, placate or evade the relentless pressures of the US.



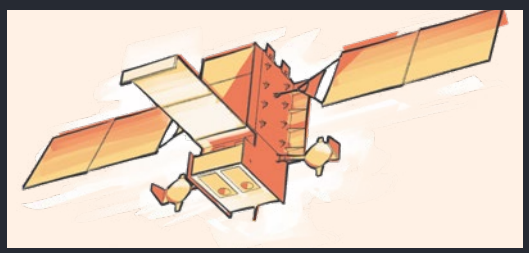
The world at war

This discussion outlines the current global climate, focusing on regional conflicts and the geopolitical strategies of major powers.



New trade order: How conflict and competition are redrawing the battle for resources

This session examines the shifting global trade landscape, highlighting how geopolitical tensions, competition and conflict are transforming access to critical resources.



The holes in Trump's Golden Dome

An FT visual investigation. Trump says a missile shield from Earth into space can be built for $185bn — but the Congressional Budget Office puts the true cost above $1tn, and the pivotal space-based interceptors may not even be feasible.



Making the UN great again

The Rachman Review podcast. Guest host Alec Russell speaks to Thant Myint-U about the challenges facing the UN's new secretary-general as the organisation fights to stay relevant.

Amplify the power of the Financial Times with FT Professional

In a world defined by noise, speed and complexity, trusted content is not a luxury - it's a necessity. Today, it's not just about individual knowledge but organisational intelligence.

FT Professional amplifies the advantage of our trusted and independent journalism through actionable context, tailored intelligence and seamless workflow integration. Equipping teams and organisations to make confident decisions.

Discover how FT Professional can empower your team:



Trusted Journalism
World-renowned editorial content at your team's fingertips.



Collaboration Tools
Advanced sharing to ensure no team member is left behind.



Scalable Access
Flexible multi-seat licenses and simple pricing models.



Seamless Integration
FT content embedded into 60+ platforms.



Deeper Context
Tools like Ask FT and Article Insights.



Smart Navigation
Your FT Professional features all in one place.

Increase your organisational intelligence and power more confident decisions with FT Professional. Visit our website here to learn more.