CARL MILLER LONG READS 14.11.2018 06:00 AM

Inside the British Army's secret information warfare machine

They are soldiers, but the 77th Brigade edit videos, record podcasts and write viral posts. Welcome to the age of information warfare

FUTURE PUBLISHING/GETTY IMAGES/WIRED

A barbed-wire fence stretched off far to either side. A Union flag twisted in a gust of wind, and soldiers strode in and out of a squat guard's hut in the middle of the road. Through the hut, and under a row of floodlights, I walked towards a long line of drab, low-rise brick buildings. It was the summer of 2017, and on this military base nestled among the hills of Berkshire, I was visiting a part of the British Army unlike any other. They call it the 77th Brigade. They are the troops fighting Britain's information wars.

"If everybody is thinking alike then somebody isn't thinking," was written in foot-high letters across a whiteboard in one of the main atriums of the base. Over to one side, there was a suite full of large, electronic sketch pads and multi-screened desktops loaded with digital editing software. The men and women of the 77th knew how to set up cameras, record sound, edit videos. Plucked from across the military, they were proficient in graphic design, social media advertising, and data analytics. Some may have taken the army's course in Defence Media Operations, and almost half were reservists from civvy street, with full time jobs in marketing or consumer research.

From office to office, I found a different part of the Brigade busy at work. One room was focussed on understanding audiences: the makeup, demographics and habits of the people they wanted to reach. Another was more analytical, focussing on creating "attitude and sentiment awareness" from large sets of social media data. Another was full of officers producing video and audio content. Elsewhere, teams of intelligence specialists were closely analysing how messages were being received and discussing how to make them more resonant.

Explaining their work, the soldiers used phrases I had heard countless times from digital marketers: "key influencers", "reach", "traction". You normally hear such words at viral advertising studios and digital research labs. But the skinny jeans and wax moustaches were here replaced by the crisply ironed shirts and light patterned camouflage of the British Army. Their surroundings were equally incongruous – the 77th's headquarters were a mix of linoleum flooring, long corridors and swinging fire doors. More Grange Hill than Menlo Park. Next to a digital design studio, soldiers were having a tea break, a packet of digestives lying open on top of a green metallic ammo box. Another sign on the wall declared, "Behavioural change is our USP [unique selling point]". What on Earth was happening?

"If you track where UK manpower is deployed, you can take a good guess at where this kind of 'influence' activity happens," an information warfare officer (not affiliated with the 77th) told me later, under condition of anonymity. "A document will come from the Ministry of Defence that will have broad guidance and themes to follow." He explains that each military campaign now also has – or rather is – a marketing campaign too.

Ever since Nato troops were deployed to the Baltics in 2017, Russian propaganda has been deployed too, alleging that Nato soldiers there are rapists, looters, little

different from a hostile occupation. One of the goals of Nato information warfare was to counter this kind of threat: sharply rebutting damaging rumours, and producing videos of Nato troops happily working with Baltic hosts.

Information campaigns such as these are "white": openly, avowedly the voice of the British military. But to narrower audiences, in conflict situations, and when it was understood to be proportionate and necessary to do so, messaging campaigns could become, the officer said, "grey" and "black" too. "Counter-piracy, counter-insurgencies and counter-terrorism," he explained. There, the messaging doesn't have to look like it came from the military and doesn't have to necessarily tell the truth.

I saw no evidence that the 77th do these kinds of operations themselves, but this more aggressive use of information is nothing new. GCHQ, for instance, also has a unit dedicated to fighting wars with information. It is called the "Joint Threat Research Intelligence Group" – or JTRIG – an utterly unrevealing name, as it is common in the world of intelligence. Almost all we know about it comes from a series of slides leaked by NSA whistleblower Edward Snowden in 2013. Those documents give us a glimpse of what these kinds of covert information campaigns could look like.

According to the slides, JTRIG was in the business of discrediting companies, by passing "confidential information to the press through blogs etc.", and by posting negative information on internet forums. They could change someone's social media photos ("can take 'paranoia' to a whole new level", a slide read.) They could use masquerade-type techniques – that is: placing "secret" information on a compromised computer. They could bombard someone's phone with text messages or calls.

JTRIG also boasted an arsenal of 200 info-weapons, ranging from in-development to fully operational. A tool dubbed "Badger" allowed the mass delivery of email. Another, called "Burlesque", spoofed SMS messages. "Clean Sweep" would impersonate Facebook wall posts for individuals or entire countries. "Gateway" gave the ability to "artificially increase traffic to a website". "Underpass" was a way to change the outcome of online polls.

They had operational targets across the globe: Iran, Africa, North Korea, Russia and the UK. Sometimes the operations focused on specific individuals and groups, sometimes the wider regimes or even general populations. Operation

Quito was a campaign, running some time after 2009, to prevent Argentina from taking over the Falkland Islands. A slide explained "this will hopefully lead to a long-running, large-scale, pioneering effects operation". Running from March 2011, another operation aimed for regime change in Zimbabwe by discrediting the Zanu PF party.

Walking through the headquarters of the 77th, the strange new reality of warfare was on display. We've all heard a lot about "cyberwarfare" – about how states could attack their enemies through computer networks, damaging their infrastructure or stealing their secrets. But that wasn't what was going on here. Emerging here in the 77th Brigade was a warfare of storyboards and narratives, videos and social media. An engagement now doesn't just happen on the battlefield, but also in the media and online. A victory is won as much in the eyes of the watching public as between opposing armies on the battlefield. Warfare in the information age is a warfare over information itself.

Propaganda published on Facebook by Russian PR firms in an attempt to affect the 2016 US presidential election FACEBOOK

Over a decade ago, and a world away from the 77th Brigade, there were people who already knew that the internet was a potent new tool of influence. They didn't call what they did "information warfare", media operations, influence activities, online action, or any of the military vernacular that it would become. Members of the simmering online subcultures that clustered around hacker

forums, in IRCs, and on imageboards like 4chan, they might have called it "attention hacking". Or simply lulz.

In 2008, Oprah Winfrey warned her millions of viewers that a known paedophile network "has over 9,000 penises and they're all raping children." That was a 4chan Dragon Ball-themed in-joke someone had posted on the show's messageboard. One year later, Time magazine ran an online poll for its readers to vote on the world's 100 most influential people, and 4chan used scripts to rig the vote so that its founder – then-21-year-old Christopher Poole, commonly known as "moot" – came first. They built bots and "sockpuppets" – fake social media accounts to make topics trend and appear more popular than they were – and swarmed together to overwhelm their targets. They started to reach through computers to change what people saw, and perhaps even what people thought. They celebrated each of their victories with a deluge of memes.
The lulz were quickly seized upon by others for the money. Throughout the 2000s, small PR firms, political communications consultancies, and darknet markets all began to peddle the tactics and techniques pioneered on 4chan. "Digital media-savvy merchants are weaponising their knowledge of commercial social media manipulation services," a cybersecurity researcher who tracks this kind of illicit commercial activity tells me on condition of anonymity.

"It's like an assembly line," he continues. "They prepare the campaign, penetrate the target audience, maintain the operation, and then they strategically disengage. It is only going to get bigger."

A range of websites started selling fake accounts, described, categorised and priced almost like wine: from cheap plonk all the way to seasoned vintages. The "HUGE MEGA BOT PACK", available for just $3 on the darknet, allowed you to build your own bot army across hundreds of social media platforms. There were services for manipulating search engine results. You could buy Wikipedia edits. You could rent fake IP addresses to make it look like your accounts came from all over the world. And at the top of the market were "legend farms", firms running tens of thousands of unique identities, each one with multiple accounts on social media, a unique IP address, its own internet address, even its own personality, interests and writing style. The lulz had transmogrified into a business model.

Read more: Inside the online disinformation war trying to tear Sweden apart

Inside the base of the 77th, everything was in motion. Flooring was being laid, work units installed; desks – empty of possessions – formed neat lines in offices still covered in plastic, tape and sawdust. The unit was formed in a hurry in 2015 from various older parts of the British Army – a Media Operations Group, a Military Stabilisation Support Group, a Psychological Operations Group. It has been rapidly expanding ever since.

In 2014, a year before the 77th was established, a memo entitled "Warfare in the Information Age" flashed across the British military. "We are now in the foothills of the Information Age" the memo announced. It argued that the British Army needed to fight a new kind of war, one that "will have information at its core". The Army needed to be out on social media, on the internet, and in the press, engaged, as the memo put it, "in the reciprocal, real-time business of being first with the truth, countering the narratives of others, and if necessary manipulating the opinion of thousands concurrently in support of combat operations."
Then the business of lulz turned into geopolitics. Around the world, militaries had come to exactly the same realisation as the British, and often more quickly. "There is an increased reliance on, and desire for, information," Nato's Allied Joint Doctrine for Information Operations, published in 2009, began. And it reached the same conclusion as the British military memo: wars needed to have an "increased attention on Info Ops". Simply put, information operations should be used to target an enemy's will. "For example, by questioning the legitimacy of leadership and cause, information activities may undermine their moral power base, separating leadership from supporters, political, military and public, thus weakening their desire to continue and affecting their actions," the document explains.

Russia, too, was in on the act. The Arab Spring, the revolutions in several post-Soviet states, Nato's enlargement – each of those had chipped away at the crumbling edifice of Russian power. Russia had a large conventional army but that seemed to matter less than in the past. The Chief of the Russian General Staff, Valery Gerasimov, began to rethink what a military needed to do. Warfare, he argued in an article for *Voyenno-Promyshlennyy Kurier* (*The Military Industry Journal*), was now "hybrid" – blurring the lines between war and peace, civilian and military, state and non-state. And there was another blurring too: between force and ideas. "Moral-psychological-cognitive-informational struggle", as Gerasimov put it, was now central to how conflicts should be fought.

We now know what Russian information warfare looks like. Moscow has built an apparatus that stretches from mainstream media to the backwaters of the blogosphere, from the President of the Russian Federation to the humble bot. Just like the early attention hackers, their techniques are a mixture of the very visible and very secret – but at a vastly greater scale.

Far less visible to Western eyes, however, were the outbreak of other theatres of information warfare outside of the English language. Gerasimov was right: each was a case of blurred boundaries. It was information warfare, but not always just carried out by militaries. It came from the state, but sometimes included plenty of non-state actors too. Primarily, it was done by autocracies, and was often directed internally, at the country's own inhabitants.
A Harvard paper published in 2017 estimated that the Chinese government employs two million people to write 448 million social media posts a year. Their primary purpose is to keep online discussion away from sensitive political topics. Marc Owen Jones, a researcher at Exeter University's Institute of Arab and Islamic Studies, exposed thousands of fake Twitter accounts in Saudi Arabia, "lionising the Saudi government or Saudi foreign policy". In Bahrain, evidence emerged of spam-like operations, aiming to stop dissidents finding each other or debating politically dangerous topics online. In Mexico, an estimated 75,000 automated accounts are known locally as Peñabots, after President Enrique Peña Nieto, flooding protest hashtags with irrelevant, annoying noise burying any useful information.

Disinformation and deception have been a part of warfare for thousands of years, but across the world, something new was starting to happen. Information has long been used to support combat operations, but now combat was seen to taking place primarily, sometimes exclusively, through it. From being a tool of warfare, each military began to realise that the struggle with, over and through information was what war itself actually was about. And it wasn't confined to Russia, China or anyone else. A global informational struggle has broken out. Dozens of countries are already doing it. And these are just the campaigns that we know about.

Read more: From the fires of revolution, Ukraine is reinventing government

On their shoulders, the soldiers of the 77th Brigade wear a small, round patch of blue encircling a snarling golden creature that looks like a lion. Called an A

Chinthe, it's a mythical Burmese beast first worn by the the Chindits, a British and Indian guerrilla force created during the Second World War to protect Burma against the advancing Japanese Army. An army of irregulars, the Chindits infiltrated deep behind enemy lines in unpredictable sorties, destroying supply depots and severing transport links, aiming to spread confusion as much as destruction.

It's no accident that the 77th wear the Chinthe on their shoulder. Like the Chindits, they are a new kind of force. An unorthodox one, but in the eyes of the British Army also a necessary innovation; simply reflecting the world in which we all now live and the new kind of warfare that happens within it.
This new warfare poses a problem that neither the 77th Brigade, the military, or any democratic state has come close to answering yet. It is easy to work out how to deceive foreign publics, but far, far harder to know how to protect our own. Whether it is Russia's involvement in the US elections, over Brexit, during the novichok poisoning or the dozens of other instances that we already know about, the cases are piling up. In information warfare, offence beats defence almost by design. It's far easier to put out lies than convince everyone that they're lies. Disinformation is cheap; debunking it is expensive and difficult.

Even worse, this kind of warfare benefits authoritarian states more than liberal democratic ones. For states and militaries, manipulating the internet is trivially cheap and easy to do. The limiting factor isn't technical, it's legal. And whatever the overreaches of Western intelligence, they still do operate in legal environments that tend to more greatly constrain where, and how widely, information warfare can be deployed. China and Russia have no such legal hindrances.

Equipping us all with the skills to protect ourselves from information warfare is, perhaps, the only true solution to the problem. But it takes time. And what could be taught would never keep up with what can be done. Technological possibility, as things stand, easily outpaces public understanding.

The Chinthe was often built at the entrances of pagodas, temples and other sacred sites to guard them from the menaces and dangers lurking outside. Today, that sacred site is the internet itself. From the lulz, to spam, to information warfare, the threats against it have become far better funded and more potent. The age of information war is just getting started.

Carl Miller is Research Director at the Centre for the Analysis of Social Media, and the author of The Death of the Gods: The New Global Power Grab

More great stories from WIRED

– Why the iPad Pro won't save the free-falling tablet market

– Small robots will make farming efficient and kill tractors

– Scientists explain why Hyperloop is so dangerous and difficult

– China wants to make supersonic trains. They won't work

– Inside the intensely political philosophy of the Fallout games

*Get the **best of WIRED in your inbox** every Saturday with the WIRED Weekender newsletter*

TOPICS LONG READS POLITICS MILITARY RUSSIA

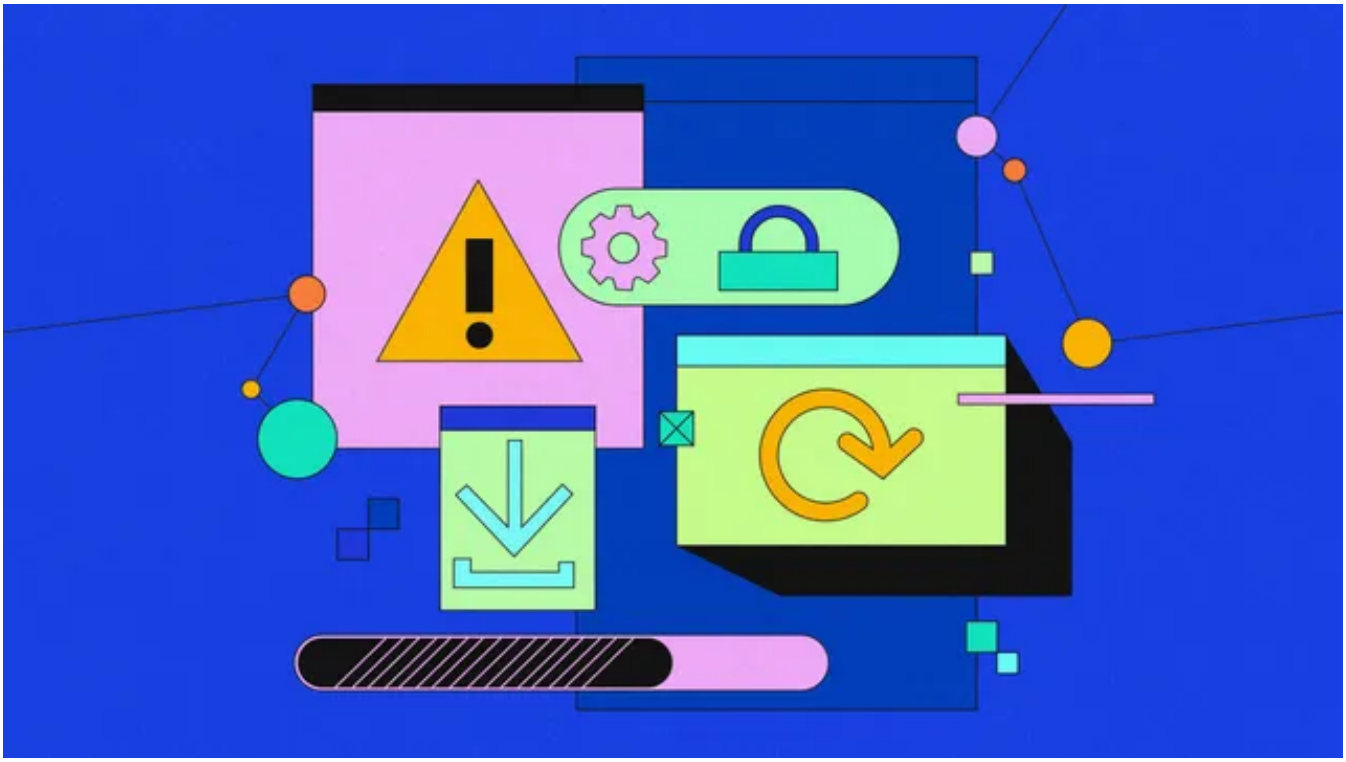
MORE FROM WIRED UK

SECURITY

Don't Panic, but Slack's GitHub Got Hacked

Plus: Russian spies uncovered in Europe, face recognition leads to another wrongful arrest, a new porn ID law, and more.

BY MATT BURGESS



SECURITY

Update Android Right Now to Fix a Scary Remote-Execution Flaw

Plus: Patches for Apple iOS 16, Google Chrome, Windows 10, and more.

BY KATE O'FLAHERTY

BUSINESS

Encryption Faces an Existential Threat in Europe

The CEO of Proton says new competition laws have finally given him a voice in Brussels, even as he fights the EU's anti-encryption campaign.

BY MORGAN MEAKER

IDEAS

The EU's Privacy Protections Must Extend Beyond Its Borders

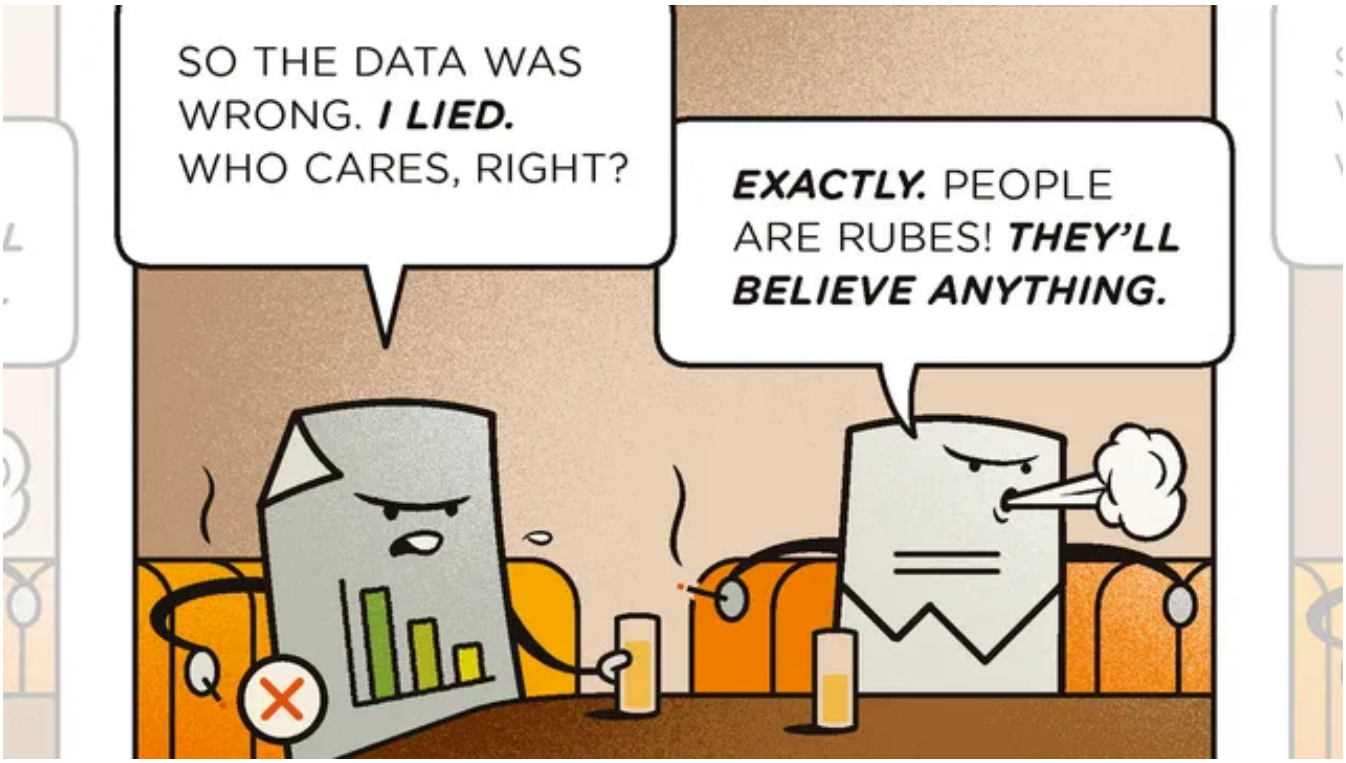
Without more forceful global laws, tech will continue to cause harm to marginalized communities

BY MICHELLE KENNEDY

Hacktivism Is Back and Messier Than Ever

Throughout 2022, geopolitics has given rise to a new wave of politically motivated attacks with an undercurrent of state-sponsored meddling.

BY MATT BURGESS



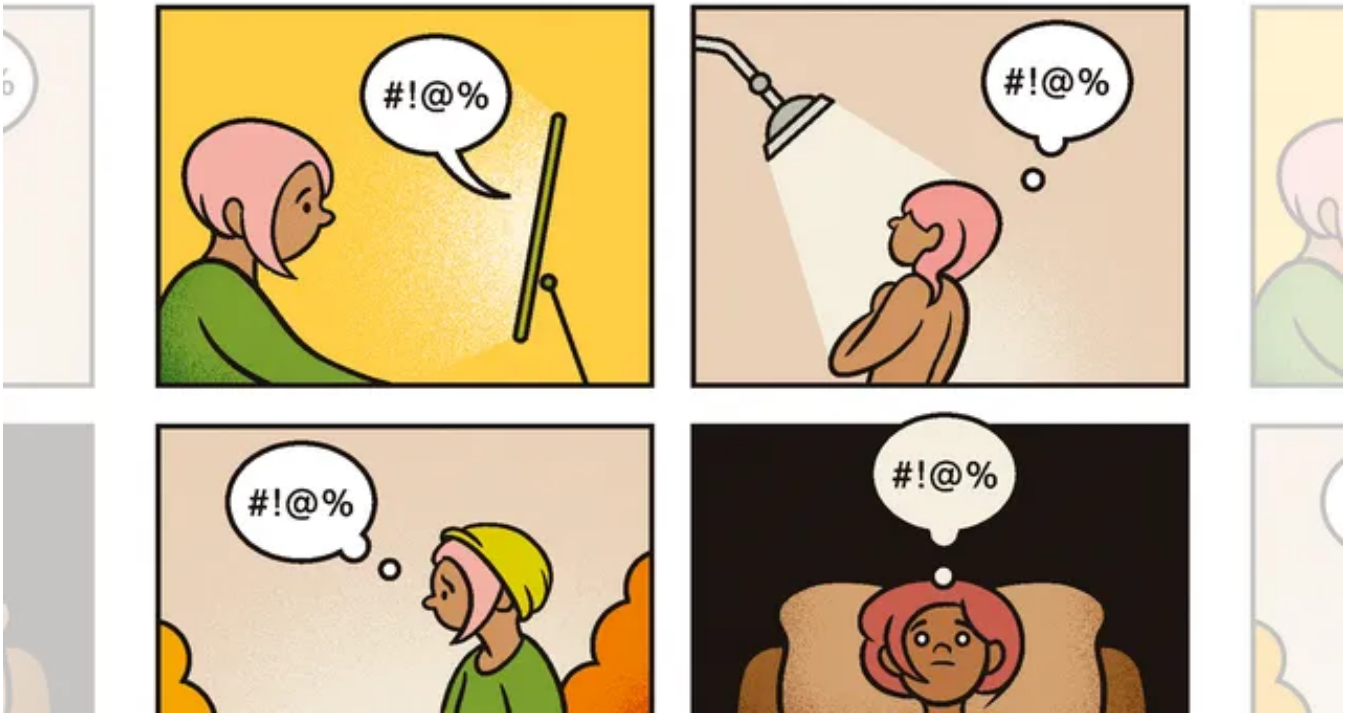
IDEAS

Public Programs Are Only as Good as Their Data

Most governments work off incomplete or inaccurate information, but it's time to plug the gaps.

BY GEORGINA STURGE

The Rebellion Amazon Can No Longer Ignore



IDEAS

An Online Safety Bill Is Coming to the UK—But It's Not Enough

The long-awaited bill is set to pass next year, but its many limitations make it ineffective. It might even set a dangerous precedent for free speech.

BY SEYI AKIWOWO