

Claire Wardle, co-founder of First Draft

ONSPIRACY THEORIES HAVE LONG BEEN CIRCULATING ALL

AROUND THE WEB. On 6 January 2021, at least one of them burst into the real world. That was the day a group of insurgents stormed the US Capitol after being duped into believing the election was rigged.

'We knew it was coming, but it still was deeply shocking, says Claire Wardle, co-founder of First Draft, a non-profit organisation dedicated to combating misinformation and disinformation. 'And I think for somebody like myself, who talks a lot about misinformation, the way we've been thinking about it is unhelpful. This [wasn't] just about false claims, or even conspiracies [that we can debunk], but many people at the Capitol are now part of a completely alternate reality."

Thanks to the internet, conspiracy theorists tend to spend a lot of time in a different information ecosystem. It's not straightforward like the old media of newspapers and TV. Instead, it's a participatory environment in which individuals can collaborate, share, and watch their lies bounce from person to person until someone gets hurt. This is radicalisation, and needs to be treated as such.

'What happened at the Capitol is a direct extension of disinformation and coordination online,' says Graham Brookie, director and managing editor of the Atlantic Council's Digital Forensic Research Lab, a leading platform for opensource research with a focus on where governance, technology, security, and

social media intersect. 'It wasn't

just one group of people ... It was a number of groups ranging from the most violent and unlawful militias, to political and ideologically driven actors who are enthusiastic to the extreme, to outright conspiracy theorists. Grappling with each kind of segment, even

though there's a lot of overlap between those groups, is going to be important."



Governments aren't always the most credible messengers or the greatest experts when it comes to what is happening in a particular country or community. That's why it's important to rely on partnerships. It's also why the US State Department is excited to announce its first US-Africa Tech Challenge, scheduled to take place in Nairobi this year.

The US State Department relies on a network of local partners who have special insights into what's happening in a specific place, and the credibility and relationships to counter propaganda and disinformation. It has conducted a number of international tech challenges. The goal is to identify relevant technologies as they are being developed locally and to support them.

The challenge encourages participation from eight promising technology companies, up to three of which will be awarded \$250 000 for their solutions to the problem of misinformation, disinformation, and fake news. This is just one of the tools that form part of a much broader suite of initiatives. The State Department also has a technologyengagement team that's constantly looking for different solutions, from social listening and web annotation tools to blockchain-based content validation and more.

'We're engaged in seeking innovative tech solutions to this problem,' says Daniel Kimmage, principal deputy coordinator of the US Global Engagement Center. 'We don't see any of these as a silver bullet [that solves everything]. But each one is part of an incremental move toward . a better armed and more secure user who is able to approach information with critical tools. disinfocloud.com

Preparing for a long fight

Tech companies and social-media platforms are surely blamed for making this possible. It's the reason many have updated their policies, from app stores blocking Parler to Twitter and Facebook banning Donald Trump. However, for the change to have lasting impact, it needs to be less about knee-jerk reactions and more about deeper societal conversations.

Specifically, there needs to be an oversight framework and structure so that private entities aren't making big decisions that affect the public without input from the people they're supposed to serve. There needs to be a coming together of researchers who've been looking into this for years and already have ideas on how to design regulation that's driven by data and facts. It's also valuable to learn how conspiracy theories spread online and use this knowledge to spread the truth instead. This involves using social media the way it was designed to be used. While the easy response might be to just tweak a few algorithms to prevent the spread of fake news, the effective response goes further. It's about one-to-one community interventions and engagement on the ground, where listening and empathy are at the core.

'You cannot deradicalise people quickly,' Claire says. 'And I think it's hard to hear because people are scared and they want a quick fix. There isn't.'

Speaking the language

Understanding the problem starts with understanding people, many of whom feel as though they don't have a sense of agency or a part in the information ecosystem. They grow tired of waiting for the gatekeepers and trusted experts to tell them what to think. That's when they take matters into their own hands and the lies begin to spread.

Indeed, we all have a friend or family member who forwards text messages that are demonstrably false. This non-deliberate spread of falsehoods is misinformation, which Graham says can be thought of as a sort of 'accidental fake news' – a term that comes with a lot of baggage, is hard to measure, and has been weaponised against journalists who are just doing their jobs. Meanwhile, disinformation is the deliberate spread of information that the sender knows is untrue.

'In a conspiracy theory, you have each type of actor creating that vocabulary to show that spectrum or to show that kind



of causal effect across the board is important, he says. 'And one thing that we see with those who spread disinformation is that when they get caught, they try to wash their hands of it and say, "Oh, I didn't know" or "It's just misinformation" or "It was a joke." But it's not a joke. The deliberate pattern of behaviour over time proves disinformation intent.'

Fixing the internet

So, if people can't be trusted to police themselves, is government regulation the answer? Of course a collective challenge requires a collective solution. This means that the government, especially in a democracy, has a key role to play. The problem is that democracies around the world don't have normative standards.



TEG: primer

Twitter's response to COVID-19

The problem of misinformation and disinformation has become more challenging during the coronavirus pandemic. That's why Emmanuel Lubanzadio, Twitter's head of public policy for sub-Saharan Africa, has been working with a number of partner organisations on the ground.

We can all agree that the world is going through something simultaneously, which requires a collective response,' he says. That's why Twitter responded quickly by updating its policies and sharing more data to ensure that experts and the public can better analyse how discussions around COVID-19 continue to evolve.

In supporting the community with the overall goal of reducing the spread of harmful misinformation related to COVID-19, Twitter doesn't just focus on the removal of harmful information. It also elevates sources of helpful information by verifying credible accounts. Twitter has also worked in concert with others by building partnerships, raising relief funds, and even granting pro bono advertising grants to support governments and non-profit organisations. This has ensured that people are getting the right messages from the right sources at the right time.

In addition to helping reporters and journalists use the platform to maximum effect, Twitter launched different campaigns and challenges to encourage handwashing and other good behaviour during the pandemic. Emmanuel has also conducted training sessions and webinars for various organisations and the youth, all as part of a drive to use the pandemic as an opportunity to create positive engagement that leads to change.

'Partnerships are central,' he says. 'It's how we make sure we look into different issues not only from a San Francisco company-based perspective but also based on the realities on the ground.' twitter.com

d and the control of the control of

The European Union has made a move, for better or for worse, on global privacy with the GDPR, while South Africa has made its own strides with POPI. And yet the United States remains a strong leader when it comes to the First Amendment and free speech. Until we have a uniform set of standards of what it means to be a democracy – an open society with privacy and free speech – we're going to be at risk.

There are a number of things that branches of government could do, whether it's the executive branch, the legislative branch, or even the judiciary, Graham says. 'This isn't just foreign policy or domestic policy or tech policy but policy that strengthens the foundations of democracy.'

Graham Brookie, director and managing editor of the Atlantic Council's Digital Forensic Research Lab

And yet those actions can backfire. For example, Germany passed a law in January 2017 that ended up having a chilling effect on speech because its definition was too broad. Platforms were so worried about getting fined that they pre-emptively took down content that should have stayed online.

At the same time, it's not helpful to just remove content when much of it will end up in darker corners that are hard to police. There needs to be broad and collective agreement on the issues first so that governments, just like the platforms, don't have knee-jerk reactions without thinking through what the implications are. The last thing we want is to look back in ten years and reflect on the internet as something we damaged beyond repair because we took the wrong steps to fix it.

I wish there were easy answers but there aren't, Claire says. 'Smart regulation is hard [and] I worry that we move at speed on these issues. We regret it while at the same time recognising we do have to do more than we're doing now.' **T**