FEED

Exploring the future of media technology

ISSUE #25 MARCH 2020 £4.99/$13.99 FEEDMAGAZINE.TV

POP-UP CHANNELS

TV DRAMA GOES VR

IRL STREAMING

MIXED REALITY

WHO GOES THERE?

THE CYBERSECURITY SPECIAL

Words by **Neal Romanek**

CYBERWAR IS HELL

Cyberthreats are all around us. You had better come up with a plan

On 8 April 2015, French broadcaster TV5Monde was taken down by a cyberattack. All 12 of the network's channels were taken off the air. The carefully targeted attack delivered malware to the broadcaster's own control systems to try to render them completely and permanently useless.

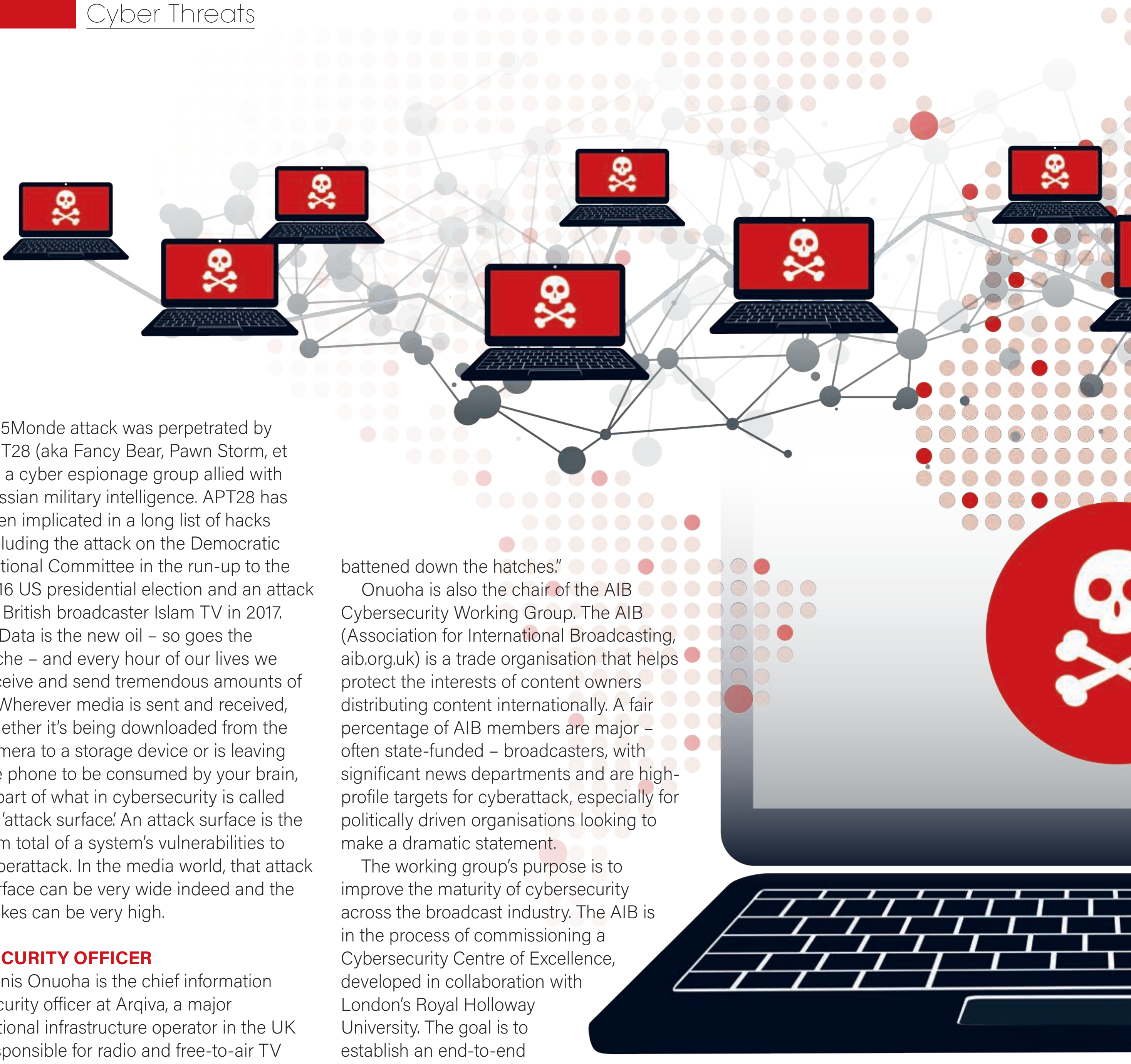
TV5Monde's regular programming was replaced with the message "Je suIS IS" (mocking the slogan "Je suis Charlie [Hebdo]"), and the alleged ID cards of relatives of French soldiers involved in operations against Islamic State terrorists were posted on TV5Monde's social media.

"We were a couple hours from having the whole station gone for good," said TV5Monde director-general, Yves Bigot, in an interview with the BBC.

Something called the 'Cyber Caliphate' claimed responsibility and, with the Charlie Hebdo murders in Paris still fresh in people's minds, the public was only too ready to believe this was the work of ISIS cyberterrorists – despite the shoddy Arabic used in the messaging, which made the claim immediately suspect.

It has since been established that the

DENIS ONUOHA Chief information security officer at Arqiva



TV5Monde attack was perpetrated by APT28 (aka Fancy Bear, Pawn Storm, et al), a cyber espionage group allied with Russian military intelligence. APT28 has been implicated in a long list of hacks including the attack on the Democratic National Committee in the run-up to the 2016 US presidential election and an attack on British broadcaster Islam TV in 2017.

Data is the new oil – so goes the cliche – and every hour of our lives we receive and send tremendous amounts of it. Wherever media is sent and received, whether it's being downloaded from the camera to a storage device or is leaving the phone to be consumed by your brain, is part of what in cybersecurity is called an 'attack surface.' An attack surface is the sum total of a system's vulnerabilities to cyberattack. In the media world, that attack surface can be very wide indeed and the stakes can be very high.

SECURITY OFFICER

Denis Onuoha is the chief information security officer at Arqiva, a major national infrastructure operator in the UK responsible for radio and free-to-air TV transmission as well as services for data comms and satellite uplinking. It's Onuoha's job to oversee the company's information assurance, cybersecurity architecture, incident response and security awareness.

"Part of my job is fending off your day-to day hackers," says Onuoha, "but Arqiva is also potentially a nation state target, so I work across the board to make sure we've battened down the hatches."

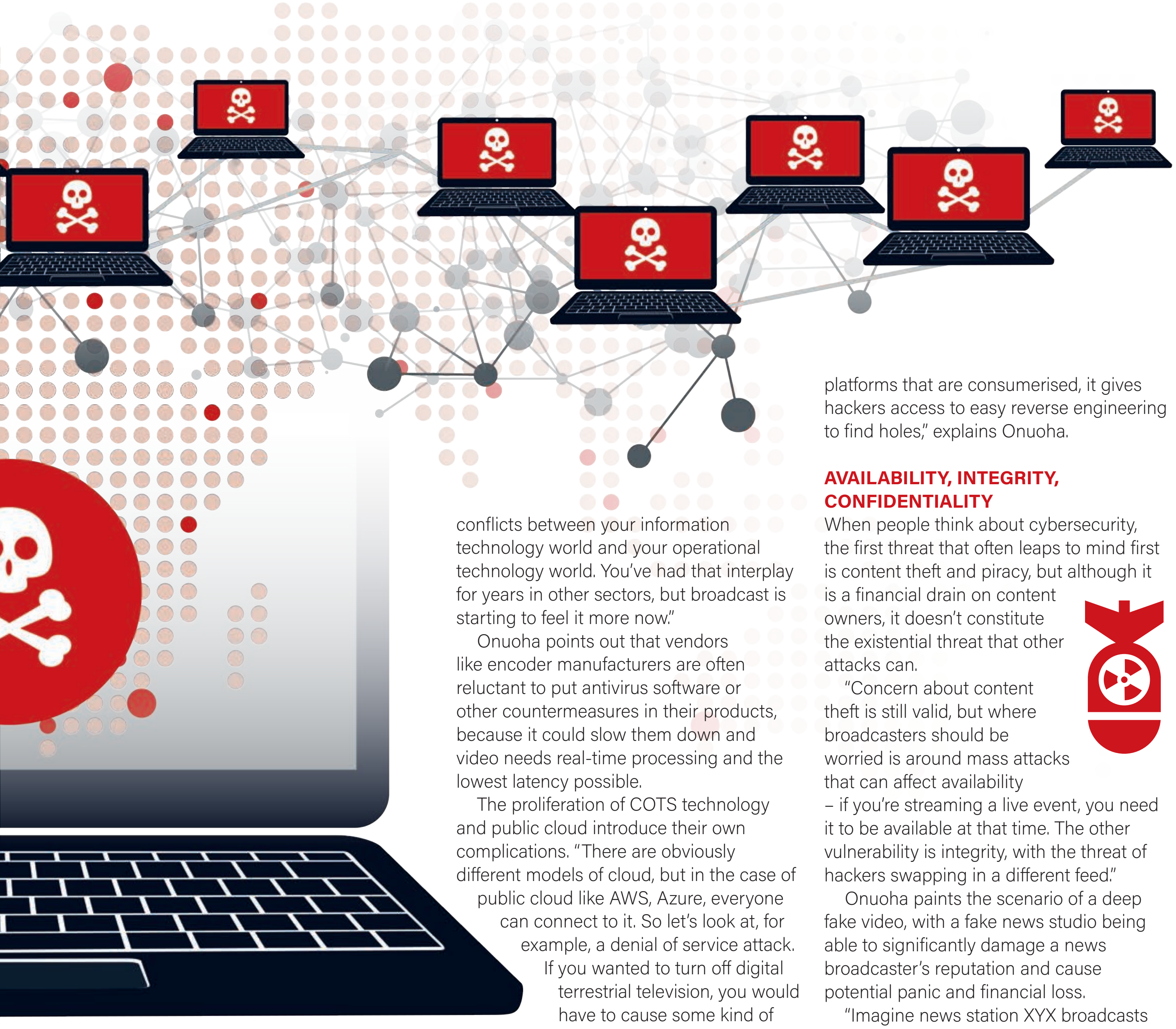
Onuoha is also the chair of the AIB Cybersecurity Working Group. The AIB (Association for International Broadcasting, aib.org.uk) is a trade organisation that helps protect the interests of content owners distributing content internationally. A fair percentage of AIB members are major – often state-funded – broadcasters, with significant news departments and are high-profile targets for cyberattack, especially for politically driven organisations looking to make a dramatic statement.

The working group's purpose is to improve the maturity of cybersecurity across the broadcast industry. The AIB is in the process of commissioning a Cybersecurity Centre of Excellence, developed in collaboration with London's Royal Holloway University. The goal is to establish an end-to-end lab where academia and industry can strengthen the whole media supply chain against digital malfeasance. "The level of maturity for broadcast is different for different countries. Some may care a lot about cyber, but others still don't see cyber as a big threat," explains Onuoha.

The lucrative nature of cybercrime and the increased consumerisation of technology has resulted in a "perfect storm," he says, with many potential points of access available to multiple, highly motivated attackers. He points to ransomware attacks on newspapers last year, including the *Los Angeles Times*. There can be a lot of money to be made and attacks can be very difficult to track.

"We now have a full IP world, so the risk has increased," says Onuoha, "but my perspective, which may be a bit controversial, is that the risk was always there. It's just that now cyberhacking is a multibillion-dollar industry. It's not that the technology is inherently weaker – though

YOU HAVE SO MANY PLATFORMS THAT ARE CONSUMERISED, IT GIVES HACKERS ACCESS TO **EASY REVERSE ENGINEERING TO FIND HOLES**



there are elements of that – now there's more motivation for taking things offline."

Onuoha notes that in the TV5Monde attack, the bulk of the video infrastructure was SDI rather than IP-based, and so fairly safe from attack, but the IT management and control layer was vulnerable.

UP TO THE CHALLENGE

Part of Onuoha's work with the AIB has been to get broadcasters and their vendors on the same page in their cybersecurity response. In an industry with so many moving parts, it's not always easy.

"You have a skills challenge. The traditional media companies are having to upskill their engineers into an IT world and that is further complicated by the historical conflicts between your information technology world and your operational technology world. You've had that interplay for years in other sectors, but broadcast is starting to feel it more now."

Onuoha points out that vendors like encoder manufacturers are often reluctant to put antivirus software or other countermeasures in their products, because it could slow them down and video needs real-time processing and the lowest latency possible.

The proliferation of COTS technology and public cloud introduce their own complications. "There are obviously different models of cloud, but in the case of public cloud like AWS, Azure, everyone can connect to it. So let's look at, for example, a denial of service attack. If you wanted to turn off digital terrestrial television, you would have to cause some kind of electromagnetic interference, or with direct-to-home satellite TV you would have to do satellite jamming, which is expensive and you need the technical know-how.

"But with something like an on-demand streaming player, all you need to do is send that player a lot of requests. And now with the dark web, you can hire compromised machines – we call them bots – and you just overwhelm the service."

BBC iPlayer suffered some DDoS (distributed denial of service) attacks in 2015. And it was a surprise – DDoS attacks had previously been thought of as a traditional IT hack, not something employed against media companies.

"Previously, too, there was a high barrier to entry. Encoders used to cost a lot of money. But now that you have so many platforms that are consumerised, it gives hackers access to easy reverse engineering to find holes," explains Onuoha.

AVAILABILITY, INTEGRITY, CONFIDENTIALITY

When people think about cybersecurity, the first threat that often leaps to mind first is content theft and piracy, but although it is a financial drain on content owners, it doesn't constitute the existential threat that other attacks can.

"Concern about content theft is still valid, but where broadcasters should be worried is around mass attacks that can affect availability – if you're streaming a live event, you need it to be available at that time. The other vulnerability is integrity, with the threat of hackers swapping in a different feed."

Onuoha paints the scenario of a deep fake video, with a fake news studio being able to significantly damage a news broadcaster's reputation and cause potential panic and financial loss.

"Imagine news station XYX broadcasts that British Airways is about to go bankrupt and that's live on a trusted channel with the presenter looking the same as the one you're used to and it has the same ticker, too. People are going to start dumping shares," warns Onuoha.

The security of the data harvested from viewers to personalise content or create other services is another a major vulnerability, says Onuoha. Availability and integrity have been the two pillars of broadcasting that must be protected, but confidentiality is starting to become another key part of preserving a media brand.

"Just as you are able to clear your browser history, broadcasters need to give viewers the ability to clear their data. Personalised data can be used to build profiles on people, which could leave

BROADCASTERS HAVE TO TAKE CYBERSECURITY VERY SERIOUSLY, **BECAUSE WE ARE THE STEWARDS**

them open to being targeted. If someone is watching religious programmes, knowing that could be helpful, say, in an election. Or if everyone streamed a major world sports event and you could access their habits, you had their IP addresses – which is classed as personal data in Europe – that's a problem."

WHO ARE THEY?

The lone nut hacker seeking revenge from his basement is more often the exception than the rule among today's cybercriminals. Attackers fall into several categories.

First, there are the organisations employed or directly run by by nation states. They may be surreptitiously seeking advanced information and intelligence or looking to cause disruption, or their activities may be part of ongoing warfare between two belligerents. Hacking is, by its very nature, a clandestine activity, and rarely are its perpetrators immediately identifiable. It's very easy to hide your tracks, and false flag attacks, where an attacker claims to be someone else, seem almost mandatory.

"If someone is hacking me, they may actually go through Dubai or the Maldives and it will look like someone from there has done it. It's a borderless crime. You can do it from anywhere," points out Onuoha.

Organised crime is another major perpetrator. These operations won't be run by gangsters in a warehouse by the dock, but by computer science graduates from major universities. Insider trading is a big earner. At the end of last year, UK authorities began investigating reported security breaches at the Bank of England, which allowed hedge funds early access to an audio feed of market predictions. As Onuoha says: "Seconds do matter in this day and age, where you can make quick decisions and quick transactions."

Hacktivists – that would be hacker activists – are a third potential threat. These could be anyone from activists trying to get out a message, to political operatives who are trying to take down a major election.

Occasionally, hacks are carried out by young people or someone who doesn't understand the scale or impact of what they're doing. Most of this time this is not much more than digital graffiti. But in the TalkTalk hack in 2015, a 17 year old posted details of a hole in the British telecom's security, which led to a major security breach and the ransoming of stolen data. TalkTalk estimated its total loss at £70 million. "Some kids do it for kudos. Or some kids from a neurodiverse spectrum might do it because they can, but they don't understand that it's a crime," says Onuoha.

But the hacker that is the most common is the one inside, an employee – or ex-employee – with a grudge to settle or a desire to steal or destroy a company's assets or reputation.

DEFENDING TRUST

A hack can create damage to brands and real physical damage to infrastructure, but the real damage in an attack on broadcasters, Onuoha says, is to public trust and confidence.

"We've read enough in the news to realize that there's fake news, there are bot farms. We're wary of that. The real danger is in breaking that highly trusted relationship with a reliable news source. Those are the attacks that undermine people's confidence in the institutions. It's a psychological attack," he explains.

"If there is a cyberattack on a major broadcaster in the UK or the US, it will rock people's minds. They'll feel like they've been burgled. It creates vulnerability. When we look at it from a risk perspective, it's not that the BBC would lose advertising money – they have no ad revenue – it's more the psychological attack, that we're vulnerable. And no one likes to feel vulnerable."

He concludes: "Broadcasters have to take cybersecurity very seriously, because we are the stewards. Sure I have analysts and influencers I follow, but when I want to get the whole picture of the news, I go to that trusted source."