TV5 Monde take-down reveals key weakness of broadcasters in digital age

April 21 2015, by Laurence Murphy

Attack on TV5 Monde is seen in France as an attack on media freedom. Credit: Yoan Valat/EPA

In what was one of the most severe outages of its kind, French national television broadcaster TV5 Monde was recently the target of a well-

planned and staged cyberattack that took down its 11 television channels, website, and social media streams.

The hacker group responsible claimed to support the Islamic State, and proceeded to broadcast pro-IS material on the hijacked channels, while also exposing sensitive internal company information, and active military soldiers details.

It took TV5 three hours to regain control of its channels. The scale and completeness of the attack, and that it involved hijacking live television broadcast channels, has shocked the industry and prompted heated discussion on what steps might prevent or at least limit the likelihood of this reoccurring.

The shift from analogue

The fact that a major European public service broadcaster could be taken down so efficiently flags up an underlying weaknesses in modern broadcasting.

For years the industry has been moving away from traditional, analogue audio-visual broadcasting technology towards digital-only, network-based infrastructures. This is a logical and necessary process for broadcast companies to keep pace with technological development, and to benefit from the efficiencies of digital media network distribution. But any system based on delivering digital media over the internet is potentially vulnerable to cyberattack from outside.

The Max Headroom hijacker – still on the loose. Credit: Youtube

These sorts of events often prompt moves that seem to be a case of bolting the stable door after horse has left. For example, when planning a new building or station installation, it's common for there to be an argument over the value of a robust uninterruptable power supply system, or UPS. They are expensive and often seen as unnecessary – until the power fails, at which point a UPS redundant battery backup is worth, quite literally, its weight in gold (and batteries are heavy).

Similarly the reaction to the assault on TV5 has been a call for immediate and widespread cybersecurity improvements, including new collaborations between European security and law enforcement agencies

in order to react faster and more effectively when such attacks occur.

The question must remain as to how the many, almost daily examples of hacking and cybercriminal attacks on firms hadn't prompted broadcasters to take the threat seriously before now.

Old idea, new tech

There have been television broadcast signal hijacks before these modern, internet-enabled times. In 1977, the evening programming from broadcaster Television South in the UK was cut across by a hoax signal overriding the programme's audio, claiming to be from an alien civilisation and demanding world disarmament. In 1986, HBO's east coast satellite feed was interrupted by a hacker calling himself Captain Midnight, actually satellite engineer John R. MacDougall, protesting at cable television fees.

In 1987, a Chicago television broadcast was interrupted by a man wearing a Max Headroom mask. He has never been identified. In these instances hijacking the signals involved physical access to or tampering with the transmitters uplink sites, or broadcast feeds. For example, MacDougall worked at firm that uplinked programmes onto satellite feeds and so had access to all the equipment needed.

There are other means of interrupting broadcasts, such as intentional jamming of signals by using one transmission of a higher power to block out another. During the Cold War it was common for the Soviet Union and Eastern European governments to use high-powered antenna to cancel out Western media such as Radio Free Europe east of the Iron Curtain.

More recently, the BBC World Service coverage of the contested Iranian election of 2009 was quashed by stronger signals causing interference

throughout Iran and surrounding countries.

There are relatively few examples of incidents like these because it's difficult to interrupt a television or radio broadcast chain – not so in our new, all-digital, internet-connected media infrastructure. The scale of this intrusion into a major European public service television station is unprecedented, and a worrying escalation of the scope and capability for politically-motivated attacks on the media and freedom of speech.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation