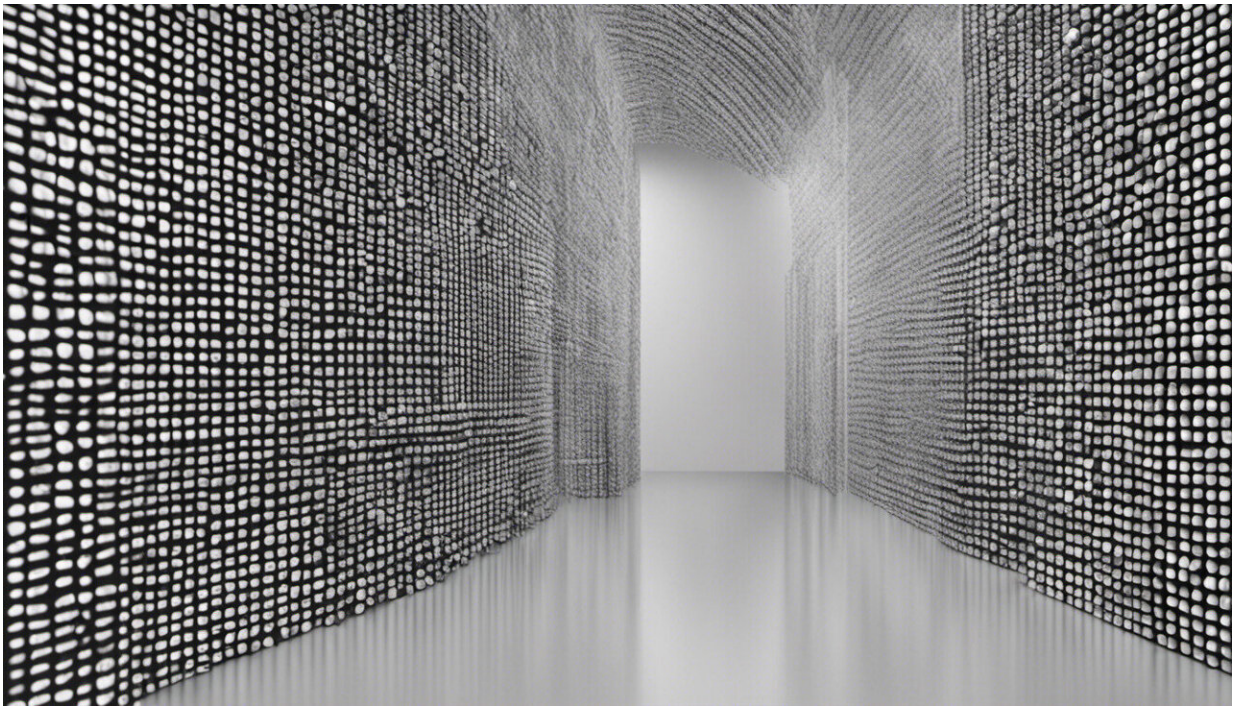
It's not just Facebook that goes down—the cloud isn't as robust as we think

October 1 2015, by Bill Buchanan



Credit: AI-generated image (disclaimer)

The computing cloud we have created supports much of our day-to-day office and leisure activity, from office email to online shopping and sharing holiday photos. Even health, social care and government functions are moving towards digital delivery over the internet.

However, we should be wary that as we become more dependent on it, the cracks will show. The systems are often a patchwork of interconnected services provided by various companies and industry partnerships. A failure of one can lead to a failure in others.

For example, Skype recently went down for almost an entire day, while Facebook was down for more than an hour – the second time in a week – meaning that many sites that depend on Facebook accounts as authentication were locked out too.

Losing Facebook is an annoyance, but interruptions to major health and social care services or energy supply management systems can lead to real damage to the economy and people's lives.

A few weeks ago Google's data centres in Belgium (europe-west1-b) lost power after the local power grid was struck by lightning four times. While most servers were protected by battery backup and redundant storage, there was still an estimated 0.000001% loss of disk space – which for Google's huge data stores meant a few gigabytes of data.

The lesson is not to trust cloud providers to store and provide backups for your data. Your backups need backups too. What it also shows is our dependence on power supply system which, as long runs of conductive metal, are more prone to lightning strikes than you might imagine.

When the lights go out

Facebook response graph, showing outage. Credit: Bill Buchanan

Former US secretary of defence, William Cohen, recently outlined how the US power grid was vulnerable to a large-scale outage: "The possibility of a terrorist attack on the nation's power grid—an assault that would cause coast-to-coast chaos," he said, "is a very real one."

As a former electrical engineer, I understand well the need for a safe and robust power supply, and that control systems can fail. It's not uncommon to have alternative or redundant power supplies for important equipment. Single points of failure are accidents waiting to happen. Back-up your backup.

The electrical supply grid will try to provide alternative power whenever any part of it fails. The power supply system needs to be built with redundancy in case of problems, and monitoring and control systems that can respond to failures and keep the electricity supply balanced.

Cohen fears a major power outage could lead to civil unrest. Janet Napolitano, former Department of Homeland Security secretary, said a

cyber-attack on the power grid was a case of "when," not "if". And former senior CIA analyst Peter Vincent Pry went so far as to say that an attack on the US electrical power supply network could "take the lives of every nine out of ten Americans". The damage that an electromagnetic pulse (EMP) could cause, such as from a nuclear weapon air-burst, is well known. But many now think the complex and interconnected nature of industrial control systems, known as SCADA, could be the major risk.

An example of the potential problem is the north-east US blackout on August 14 2003, which affected 508 generating units at 265 separate power plants, cutting off power to 45m people in eight US states and 10m people in Ontario. It was caused by a software flaw in an alarm system in an Ohio control room which failed to warn operators about an overload, leading to domino effect of failures. It took two days to restore power.

As the world becomes increasingly internet-dependent, we have created a network that provides redundant routes to carry traffic from point to point, but electrical supply failures can still take out core routing systems.

Control systems - the weakest link

Often it's the less obvious elements of infrastructure that are most open to attack. For example, air conditioning failures in data centres can cause overheating sufficient to melt equipment, especially the tape drives used to store vast amounts of data. This could affect anything from banking transactions worth billions, the routing of traffic around a busy city, or an emergency services call centre.

As we become more dependent on data and data-processing, so we are more vulnerable to their loss. Safety critical systems are built with

failsafe control mechanisms, but those mechanisms can also attacked and compromised.

The cloud we have created and upon which we increasingly depend is not as hardy as we think. The internet itself, and the way we use it, is not as distributed as it was designed to be. We still rely too heavily on key physical locations where data and network interconnections are concentrated, creating unacceptable points of failure that could lead to a domino-effect collapse. The DNS infrastructure is a particular weak point, where just 13 root servers worldwide act as master lists for the entire web's address book.

I don't think governments have fully thought this through. Without power, without internet connectivity, there is no cloud. And without the cloud we have big problems.

Source: The Conversation