The internet is surprisingly fragile, crashes thousands of times a year, and no one is making it stronger

July 18 2019, by Vasileios Giotsas

Credit: AI-generated image (disclaimer)

How could a small internet service provider (ISP) in Pennsylvania cause millions of websites worldwide to go offline? That's what happened on June 24, 2019 when users across the world were left unable to access a large fraction of the web. The root cause was an outage suffered by

Cloudflare, one of the internet's leading content hosts on which the affected websites relied.

Cloudflare traced the problem to a regional ISP in Pennsylvania that accidentally advertised to the rest of the internet that the best available routes to Cloudflare were through their small network. This caused a massive volume of global traffic to the ISP, which overwhelmed their limited capacity and so halted Cloudfare's access to the rest of the internet. As Cloudflare remarked, it was the internet equivalent of routing an entire freeway through a neighbourhood street.

This incident has highlighted the shocking vulnerability of the internet. In 2017 alone there were about 14,000 of these kinds of incidents. Given it is mission-critical for much of the world's economic and social life, shouldn't the net be designed to withstand not just minor hiccups but also major catastrophes, and to prevent small problems turning into much bigger ones? Governing bodies such as the EU Agency for Network and Information Security (ENISA) have long warned of the risk of such cascading incidents in causing systemic internet failure. Yet the internet remains worryingly fragile.

Like a road network, the internet has its own highways and intersections that consist of cables and routers. The navigation system that manages the flow of data around the network is called the Border Gateway Protocol (BGP). When you visited this website, BGP determined the path through which the site's data would be transmitted to your device.

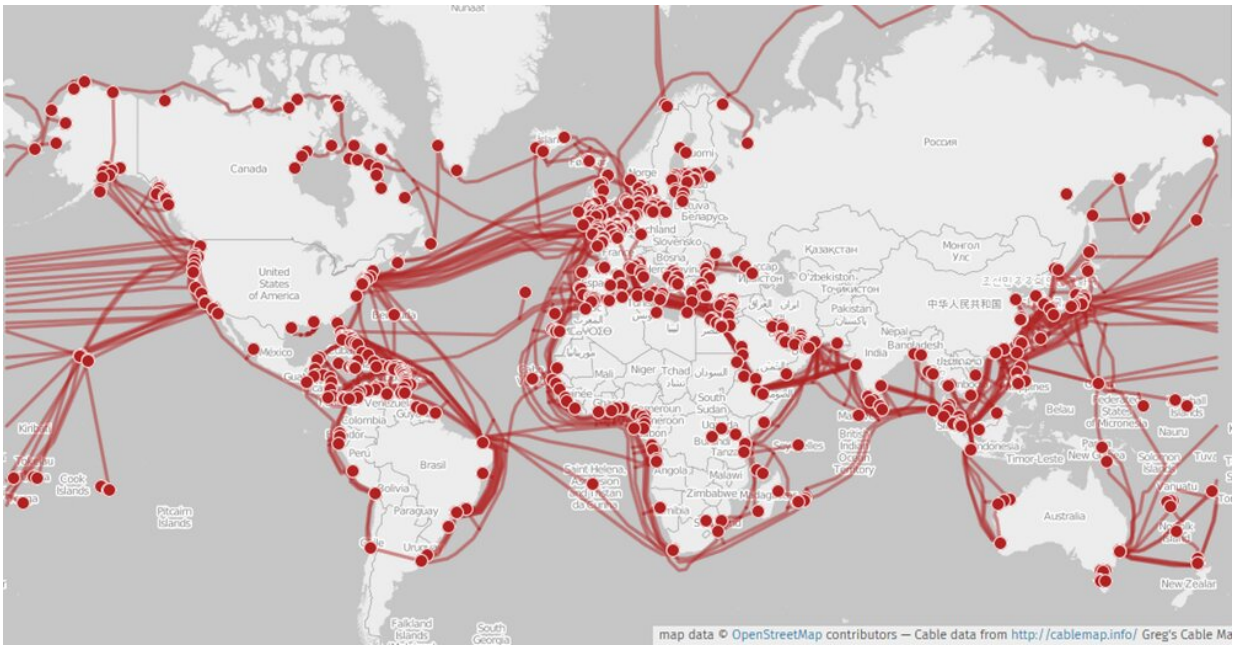
The problem is that BGP was designed only to be a temporary fix, a "good enough" solution when the internet was rapidly growing in the late 1980s. It then proved good enough to help the net sustain its explosive expansion and quickly became part of every backbone router that manages the flow of data down the internet's principal pathways. But it wasn't built with security in mind, and mechanisms to ensure that the

paths BGP sends data down are valid have never been added. As a result, routing errors go undetected until they cause congestion and outages.

Even worse, anyone who can access a backbone router (and doing so is trivial for someone with the right knowledge and budget) can construct bogus routes to hijack legitimate data traffic, disrupt services and eavesdrop on communications. This means the modern internet operates using an insecure protocol that is exploited on a daily basis to compromise communications from governments, financial institutions, weapon manufacturers and cryptocurrencies, often as part of politically-motivated cyber-warfare.

These issues have been known about at least since 1998, when a group of hackers demonstrated to the US Congress how easy it was to compromise internet communications. Yet, little has changed. Deploying the necessary cryptographic solutions turned out to be as hard as changing the engines of an airplane in mid-flight.

In an actual aviation issue, such as the recent issues with Boeing's 737 MAX aircraft, regulators have the authority to ground an entire fleet until it is fixed. But the internet has no centralised authority. Different parts of the infrastructure are owned and operated by different entities, including corporations, governments and universities.



Many paths to choose from. Credit: Greg Mahlknecht/Openstreetmap, CC BY-SA

The tussle between theses different players, which often have competing interests, means they don't have incentives to make their own part of the internet more secure. An organisation would have to bear the significant deployment costs and operational risks that come with a switch to a new technology, but it wouldn't reap any benefits unless a critical mass of other networks did the same.

The most pragmatic solution would be to develop security protocols that don't need global coordination. But attempts to do this have also been impeded by the decentralised ownership of the internet. Operators have limited knowledge of what happens beyond their networks because of companies' desires to keep their business operations secret.

As a result, today nobody has a complete view of our society's most

critical communications infrastructure. This hinders efforts to model the internet's behaviour under stress, making it harder to design and evaluate trustworthy solutions.

Improving security

The direct implications of this bleak situation on national security have led government agencies to intensify their activities to protect their critical internet infrastructure. For example, the UK National Cyber Security Centre (NCSC) recently launched the Active Cyber Defence (ACD) program, which puts the security of internet routing among its top priorities.

As part of this program, my own research involves mapping the internet at an unprecedented level of detail. The aim is to illuminate hidden locations where the infrastructure is particularly susceptible to attack and responsible for cascading failures.

At the same time, new initiatives are attempting to make security a more routine consideration for people who work for organisations controlling internet infrastructure.

As we become more economically dependent on the internet, the cost of outages will grow further. And the advent of cryptocurrencies, whose transactions are fundamentally vulnerable to BGP hijacking attacks, could finally make resolving this problem a priority for internet infrastructure businesses.

It's no exaggeration to say that the internet is currently a cyber Wild West. But after two decades of ineffectual efforts, there's a chance the outlaw days may slowly be nearing to an end.

Commons license. Read the original article.

Provided by The Conversation

Citation: The internet is surprisingly fragile, crashes thousands of times a year, and no one is making it stronger (2019, July 18) retrieved 18 April 2024 from https://phys.org/news/2019-07-internet-surprisingly-fragile-thousands-year.html