

Fight for Control Threatens to Destabilize and Fragment the Internet



You try to use your credit card, but it doesn't work. In fact, no one's credit card works. You try to go to some news sites to find out why, but you can't access any of those, either. Neither can anyone else. Panic-buying ensues. People empty ATMs of cash.

This kind of catastrophic pan-internet meltdown is more likely than most people realize.

I direct the [Internet Atlas Project](#) at the University of California, Berkeley. Our goal is to shine a light on long-term risks to the internet. We produce indicators of weak points and bottlenecks that threaten the internet's stability.

For example, where are [points of fragility in the global connectivity of cables](#)? Physical cables under the sea deliver [95% of the internet's voice and data traffic](#). But some countries, like Tonga, connect to only one other country, making them vulnerable to cable-clipping attacks.

Another example is [content delivery networks](#), which websites use to make their content readily available to large numbers of internet users. An [outage at the content delivery network Fastly](#) on June 8, 2021, briefly severed access to the websites of Amazon, CNN, PayPal, Reddit, Spotify, The New York Times, and the U.K. government.

The biggest risks to the global internet

We take measurements at various layers of the internet's technological stack, from cables to content delivery networks. With those measurements, we identify weak points in the global internet. And from those weak points, we build theories that help us understand what parts of the internet are at risk of disruption, whom those disruptions will affect, and how severely, and predict what would make the internet more resilient.

Currently, the internet is facing twin dangers. On one side, there's the threat of total consolidation. Power over the internet has been increasingly concentrated primarily in the hands of a few, U.S.-based organizations. On the other side, there's fragmentation. Attempts to challenge the status quo, particularly by [Russia and China](#), threaten to destabilize the internet globally.

While there's no single best path for the internet, our indicators can help policymakers, nongovernmental organizations, businesses, activists, and others understand if their interventions are having their intended effect. For whom

is the internet becoming more reliable, and for whom is it becoming more unstable? These are the critical questions. About [3.4 billion people are just now getting online](#) in countries including Fiji, Tonga, and Vanuatu. What kind of internet will they inherit?

A US-controlled internet

Since at least 2015, the core services that power the internet have become increasingly centralized in the hands of U.S. corporations. We estimate that U.S. corporations, nonprofits, and government agencies could block [a cumulative 96% of content on the global internet](#) in some capacity.

The U.S. Department of Justice has [long used court orders aimed at tech providers](#) to block global access to content that's illegal in the U.S., such as copyright infringements. But lately, the U.S. federal government has been leveraging its jurisdiction more aggressively. In June, the DOJ used a court order to briefly seize [an Iranian news site](#) because the department said it was spreading disinformation.

Due to interlocking dependencies on the web, such as content delivery networks, one misstep in applying this technique could take down a key piece of the internet infrastructure, making a widespread outage [more likely](#).

Meanwhile, U.S.-based technology companies also risk wreaking havoc. Consider Australia's recent [spat with Facebook overpaying news outlets for their content](#). At one point, Facebook blocked all news on its platform in Australia. One consequence was that many people in Fiji, Nauru, Papua New Guinea, Samoa, Tonga, and Vanuatu [temporarily lost a key news source](#) because they rely on prepaid cellphone plans that feature discounted access to Facebook. As these [skirmishes](#) increase in frequency, countries worldwide are likely to suffer disruptions to their internet access.

A splinternet

Naturally, not everyone is happy with this U.S.-led internet. [Russia throttles Twitter traffic](#). [China blocks access to Google](#).

These domestic maneuvers certainly threaten localized meltdowns. India now regularly [shuts down the internet regionally during civil unrest](#). But, in aggregate, they present a more global threat: [internet fragmentation](#). A fragmented internet threatens speech, trade, and [global cooperation in science](#).

It also increases the risk of cyberattacks on core internet infrastructure. In a global internet, attacks on infrastructure hurt everyone, but walled-off national internets would change that calculus. For example, [Russia has the capacity to disconnect itself from the rest of the world's internet](#) while maintaining service domestically. With that capacity, it could [attack core global internet infrastructure](#) with less risk of upsetting its domestic population. A sophisticated attack against a U.S. company could trigger a large-scale internet outage.

The future of the internet

For much of its history, the internet has been imperfectly, but largely, open. Content could be accessed anywhere, across borders. Perhaps this openness is [because, rather than in spite, of the U.S.'s dominance](#) over the internet.

Whether or not that theory holds, the U.S.'s dominance over the internet is unlikely to persist. The status quo faces challenges from the U.S.'s [adversaries](#), its [historical allies](#), and its [own domestic tech companies](#). Absent action, the world will be left with some mixture of unchecked U.S. power and ad-hoc, decentralized skirmishes.

In this environment, building a stable and transnational internet for future generations is a challenge. It requires delicacy and precision. That's where work like ours comes into play. To make the internet more stable globally, people need measurements to understand its chokepoints and vulnerabilities. Just as central banks watch measures of inflation and employment when they decide how to set rates, internet governance, too, should rely on indicators, however imperfect.

[Understand new developments in science, health, and technology, each week. [Subscribe to The Conversation's science newsletter.](#)]

[Nick Merrill](#), Research Fellow, [University of California, Berkeley](#)

This article is republished from [The Conversation](#) under a Creative Commons license. Read the [original article](#).