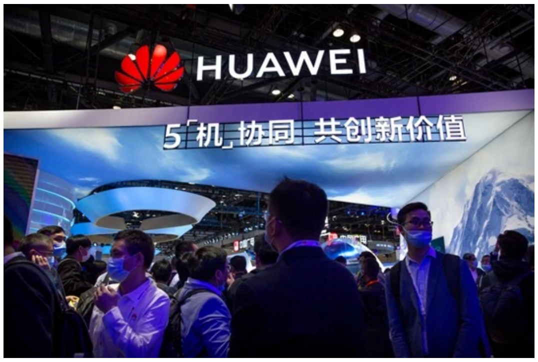
WPR
WORLD POLITICS REVIEW

Tech-Nationalism Threatens the Internet Itself

Emily Taylor | Tuesday, March 2, 2021



Huawei's booth at the PT Expo in Beijing, China, Oct. 20, 2020 (AP photo by Mark Schiefelbein).

"Keep the politics out of the network"—that was the mantra of the tech community back in the day. There was wisdom in that sentiment, and it worked fairly well for the first 20 years of the internet's build-out. But today, controversies over next generation 5G networks and how many of them will be built by China's telecom giant, Huawei, have demonstrated how far geopolitics have infected digital infrastructure. The latest tensions are now over undersea cables.

The argument over digital networks goes like this. It's to be expected that politics, culture, language and all sorts of complex, contested issues will be present at the points where people interact with technology—that is, the things you can see, and increasingly summon with your voice. For the engineering community, this is called "the application layer," and is the world of tech's household names: Facebook, Google, Twitter, TikTok, Alexa, Zoom.

In the ordered minds of the engineering community, the people who built the protocols and standards that enable today's internet, the application layer is distinct and separate from the deeper architectural layers. If regulators come your way, send them up to the application layer, where they can puzzle over intractable policy issues to their hearts' content. Hopefully, they will stay there forever and leave us alone to just build out the network and make things work.

This is not a mere pipe dream, and if you carefully demarcate between the internet's layers, there are wonderful examples of the technical community working effectively across political barriers. CENTR, the European organization for country domain name registries, boasts among its membership the Iranian, Israeli and Palestinian registries—that's .ir, .il and .ps in domain-world. Together, these friends and colleagues sit down together, share good practices about domain names and enjoy trusting relationships. At the Internet Corporation for Assigned Names and Numbers, or ICANN, the Arabic script community—spanning members from Iran, Saudi Arabia, and Pakistan through to North Africa—has been collaborating for years to agree on code points to bring the Arabic script (https://www.icann.org/sites/default/files/packages/lgr/lgr-second-level-arabic-language-13jan21-en.html) into domain names without creating cross-language problems.

Another example is the collaboration between Facebook and China Mobile, one of China's three major state-run telecom companies, on bringing a superhigh bandwidth undersea cable from the U.K. (https://www.prnewswire.com/news-releases/2africa-a-transformative-subsea-cable-for-future-internet-connectivity-in-africa-announced-by-global-and-african-partners-301058889.html) right around the entire coast of Africa, back through Suez and eventually landing in northern Spain. In what universe can you imagine the freewheeling Silicon Valley giant as a bedfellow of a Chinese state-owned mobile operator? On digital infrastructure, though, interests converge. There is no downside to connecting Africa, except that it costs a fortune and takes years to achieve.

As connectivity improves—and one positive aspect of the coronavirus pandemic is that it has driven digital uptake in Africa—investment and innovation increase (https://www.ft.com/content/8845a8fb-ae12-423b-a7c9-6cfb5c149827), and economic development goals are achieved (https://www.ft.com/content/8845a8fb-ae12-423b-a7c9-6cfb5c149827). According to the GSMA, the mobile operators' industry body, sub-Saharan Africa accounts for almost half of the global population not covered by a mobile broadband network (https://www.gsma.com/r/wp-content/uploads/2020/09/Mobile-Internet-Connectivity-SSA-Fact-Sheet.pdf). So, it makes sense to collaborate in the massive investment needed to improve connectivity on the continent.

But meanwhile, there's trouble in paradise, specifically many Pacific islands, whose connectivity woes have been a focus of concern for decades. In the final days of the Trump administration, the United States issued a warning that an undersea cable linking many Pacific islands and built by Huawei Marine—which recently divested from its better-known namesake, but is still Chinese owned—represented a "security threat." (https://www.reuters.com/article/us-china-pacific-exclusive-idUSKBN28R0L2) Last year, Facebook and Google initially withdrew from a multiyear project (https://www.bloomberg.com/news/articles/2020-08-29/google-facebook-dump-hong-kong-cable-after-u-s-security-alarm) to connect the West Coast of the U.S. with Hong Kong, then rapidly changed course to reroute the undersea cable (https://www.bbc.co.uk/news/technology-53972238), connecting to Taiwan and the Philippines only, because the Trump administration expressed security concerns about risks of China's access to data carried by the cable.

> ***The insertion of politics into the physical infrastructure of the internet poses its own security threats and could even hasten a fragmentation of the internet along national lines.***

For those who subscribe to the now-dominant narrative that Chinese companies in any networks pose a security threat by definition, the assertion of national security concerns over undersea cables is a logical extension. But the insertion of politics into the physical infrastructure layer poses its own security threats and could even hasten a fragmentation of the internet along national lines.

This view of protecting networks from apparent security threats like Huawei is based on a fallacy that you could make a network secure by simply removing one company or country from it. People who understand the cybersecurity of networks, like the former head of the U.K.'s National Cybersecurity Centre, Ciaran Martin (https://www.techregister.co.uk/ncsc-ceo-suggests-opposition-to-uk-huawei-tech-ban/), point out that standards of cybersecurity in networks are far below what they should be. It could create a false sense of security to adopt a nationalist approach. The U.S.-based cybersecurity specialist, SolarWinds, would have flown through any nationality-based security test, yet it turned out to be a single point of vulnerability for major government departments across the West after last year's massive hack.

There are three other reasons why these undersea cables stories should cause concern. First, the assertion of tech-nationalism over infrastructure breaks a fundamental tenet of internet protocols. Data needs to travel indiscriminately across networks for it all to work. Creating artificial barriers imposes cost and latency into networks. It starts to make the internet look and feel more like traditional telecommunications networks, with single points of control, and therefore single points of vulnerability.

Second, what's sauce for the goose is sauce for the gander. An increasingly strident China, determined to become a technological superpower, is building out undersea cables itself. The PEACE Cable—"Pakistan & East Africa Connecting Europe"—is a Chinese-led project that will, as its name suggests, connect Islamabad to southern France, via stops along the way in the Horn of Africa and Egypt, before it crosses the Mediterranean. Some see it as an extension of China's sweeping infrastructure program, the Belt and Road Initiative. Since it will also connect Pakistan to France "beyond India's reach," according to some observers, it looks like evidence of geopolitical tensions between the South Asian neighbors (https://asiatimes.com/2021/02/huawei-digitally-connects-pakistan-beyond-indias-reach/).

Finally, the growing presence of tech giants from the application layer—Google, Facebook and others—moving into the internet's architecture (https://www.tandfonline.com/toc/rcyb20/5/1?nav=tocList) and right through to undersea cables risks undermining the resilience of the internet as a network of networks. Traditionally, these companies existed only at the content layer, relying on networks built by others. While it is welcome that they are using their massive financial resources to invest in connecting the unconnected, the collapse of those distinct architectural layers into the control of a few companies also introduces new vulnerabilities. The companies become too big to fail, and the consequences of business failure or a service outage become more severe than a website or app going dark: It could, instead, take out a whole continent.

And if you are concerned about China's access to the data flowing across undersea cables, wouldn't you also worry about Google and Facebook's access to the same data?

Emily Taylor is the CEO of Oxford Information Labs, and an associate fellow with the International Security Program at Chatham House. She is also the editor of the Journal of Cyber Policy, a research associate at the Oxford Internet Institute, and an affiliate professor at the Dirpolis Institute at the Sant'Anna School of Advanced Studies in Pisa. She has written for The Guardian, Wired, Ars Technica, the New Statesman and Slate. Follow her on Twitter @etaylaw (https://twitter.com/etaylaw). Her guest column will appear each Tuesday.

MORE WORLD POLITICS REVIEW

Cameroon's Ethno-Political Tensions and Facebook Are a Deadly Mix

(https://www.worldpoliticsreview.com/articles/29412/in-cameroon-conflict-along-ethnic-lines-may-be-stoked-by-facebook)

'Watching People Become Citizens': Clubhouse's Brief Run in China

(https://www.worldpoliticsreview.com/articles/29429/watchin people-become-citizens-clubhouse-s-brief-run-in-china)

Why Did Rwanda Abruptly Change the Language in Schools—Again?

(https://www.worldpoliticsreview.com/articles/29440/in-rwanda-language-change-in-schools-leaves-students-and-teachers-struggling)

How the Pandemic Is Accelerating a ‘Splintering of the Internet’

(https://www.worldpoliticsreview.com/trend-lines/29214/how-the-pandemic-is-accelerating-a-splintering-of-the-internet)

China’s Road to ‘Cyber Superpower’ Status

(https://www.worldpoliticsreview.com/articles/29408/under-xi-china-aims-for-cyber-superpower-status)

Deplatforming Pro-Trump Extremists Could Drive Them Underground

(https://www.worldpoliticsreview.com/articles/29354/deplatfo pro-trump-extremists-could-drive-them-underground)