



INTEGRATED INTERNET INTERNATIONALISM



July 2023

Melanie Garson, Cyber Policy and Tech Geopolitics Lead, Tony Blair Institute for Global Change

Pete Furlong, Senior Policy Analyst, Tony Blair Institute for Global Change

वश्धेव कुदुम्बकम्

ONE EARTH • ONE FAMILY • ONE FUTURE

Abstract

n the digital age, stability is determined by how the internet is used, and this is most evident during conflicts and crises.

Tech companies' interventions during the Ukraine War to ensure the stability of the internet were essential to the digital and physical security of Ukrainians and their basic communications infrastructure. Yet, as new crises emerge across the

world, governments, multilaterals, and new geopolitical actors such as tech companies find themselves unprepared to play the role of protectors of the global internet. Therefore, a new model of internet internationalism is required that is centred on the engagement across these actors to define a twenty-first century approach to stability and digital resilience.

The Challenge

No stability without internet stability

■ hedigitaleconomyaccounts for 15.5 percent of global GDP and is the fastest growing sector worldwide.1 Digital development is a major contributor to economic and sustainable development, from increasing financial inclusion and reducing poverty, to protecting endangered marine life.2 2.7 billion people still lack basic access to the internet,3 and there is a need to ensure that they are connected and that connectivity is stable and resilient. It is estimated that one hour without connection to the internet would cost the world economy £1.5 billion;4 intentional internet shutdowns in 2022 resulted in a US\$24 billion loss to the global economy.5

The pivotal role played by internet access and resilience is increasingly evident, as basic internet infrastructure has come under stress due to climatic events and conflicts. When Tonga's submarine cable was severed during a volcanic eruption in early 2022⁶ and satellite communications were limited by ash cover, the country's economy ground to a halt; the deliberate

targeting of Ukraine's electricity and internet infrastructure by Russian troops led to Ukraine's troops being reliant on SpaceX's Starlink satellite internet network for military and civilian communications; more recently, Cyclone Gabrielle left parts of New Zealand in complete blackout, with banks, retailers, and even emergency services seeking alternatives such as Starlink.8

Paradoxically, despite its fundamental importance, the proliferation of stable internet has rendered it more insecure and less stable.9 Malicious actors, heavyhanded regulation, competing visions, and geopolitical competition over its basic infrastructure and standards have threatened the already fragile globally maintained ecosystem. The 'gossamer arrangement' of hardware, software, protocols, organisations, and telecommunications¹⁰ is shared across a network of institutions with varying business and operational models. This has led to fragmentation across the user experience, the technical layer, and the internet's governance and coordination,11 the value and weaknesses of which have been exposed in recent conflicts and geopolitical crises. Without the rapid interventions

THE CHALLENGE

of tech companies leveraging their positions across the internet stack stabilise the communications infrastructure, Ukraine would likely have been unable to counter Russia's kinetic and cyber operations. However, without principled decision-making of traditional internet governance players, the very nature of the free, open, and interoperable internet is threatened. As the world moves towards a new UN Global Digital Compact predicated on avoiding internet fragmentation,12 a new model of internet internationalism is needed that balances this complex relationship and centres the protection and resilience of the world's most critical infrastructure, such that the benefits of digitalisation are accessible to all.

Traditional internet governance: Slow and stable

The loose coalition of multistakeholder forums that govern the diverse spaces within the global internet¹³ are generally united in their vision for the internet. Decentralisation, stability, and interoperability are guiding principles for the dominant players of traditional internet governance, which are split between technically focused bodies such as the Internet Corporation for Assigned Names and Numbers (ICANN)

and the Internet Engineering Task Force (IETF), and more socially focused bodies such as the Internet Governance Forum (IGF) and the Internet Society (ISOC). Designed to have no central point of control, like the internet itself, these organisations are structured across similar levels of distribution that are focused on the maintenance, expansion, and evolution of the network and are critical to preserving the global, interoperable internet.

Despite the United Nations General ES-11/4 Assembly Resolution condemning Russia's invasion Ukraine, the responses from internet governance organisations were and **ICANN** restrained measured; rejected Ukraine's request to pull Russian country code domain access, which would have blocked about five million sites from the internet, thus hindering Russia's ability to communicate, noting that "[r]egardless of the source, ICANN does not control Internet access or content."14 Similarly, RIPE NCC, the regional internet registry for Europe, Middle East, and parts of Asia, resisted Ukraine's requests on the basis that it could not take actions that risk undermining internet stability.15 These organisations reiterated their support for Ukraine but reaffirmed their greater obligation to prevent the fracturing of the internet on geographical, political, commercial, or technological lines.

However, this is one of the rare instances where internet governance organisations demonstrated alignment. Over the last 20 years, multistakeholder initiatives have faced challenges in dealing with competing interests that threaten internet stability. These bodies are designed to be stable, with a narrow remit to maintain the foundation of the internet. However, this has also rendered these bodies brittle and inflexible at times, making it increasingly difficult for them to assert the protection of the free and interoperable internet. The organisations suffer from a lack of cooperation and long-term strategic direction, as well as weak internal processes and participation, which prevent them from acting coherently beyond crisis situations.16 A lack of institutional reform among internet governance organisations would result in the foundations of the internet being at risk.17

The speed and scale of new internet actors

The Ukraine War is the first fully internet-enabled conflict, with access

to the internet being pivotal to the strategies of both parties. From basic communications to sophisticated drone technology, access to the internet has been crucial to both successful offence and defence. Additionally, with Russia's strategy encompassing the destruction, rerouting, and control of the information ecosystem, the need to keep the internet secure and open became paramount. The commercialisation of the internet was highlighted, as tech companies stepped in to mitigate the pressure on the internet and balance the risks and opportunities of its myriad applications and devices; Google Maps traffic view was temporarily disabled in Ukraine after researchers tracking traffic and road closures identified the first movement of Russian troops;18 Ukrainians and Russians turned to Telegram for communications and updates, with President Zelensky's Telegram channel growing from 65,000 followers in February 2022 to over 1.5 million in the first month of the war;19 Amazon shifted 10 petabytes of Ukrainian government data to cloud servers to protect citizens' data and enable the continued running of its e-government platform;20 Cloudflare configured Ukrainian servers to wipe local data in the event of a Russian attack;²¹ SpaceX provided satellite internet service to the Ukrainian

THE CHALLENGE

government and military following a Twitter exchange between Mykhailo Fedorov and Elon Musk; Microsoft was working closely with Ukraine's government even before the war started, which enabled the company to neutralise the Foxblade malware that had been intended to paralyse government systems.²²

Compared to governments and multilateral organisations, which were slow and conflicted in their response to the ways in which Russia and the Ukraine War were exploiting and reshaping the internet, private companies were able to mitigate this at an unprecedented speed. Telecommunications and internet 'backbone' providers such as Cogent Communications and Lumen Technologies quickly withdrew their services from Russia, with the consequences for connectivity felt as far as Kazakhstan and Iran.23 Companies rapidly created alternatives to counter information controls following Russia's fake news law, such as Twitter's launch of a website.24 privacy-protected dark Others, such as Cloudflare, halted paid services in line with sanctions but continued to provide free services within Russia to enable information access for people and prevent Russia from using its isolation from the global internet to its advantage.²⁵

The risks of rapid best intentions

The agility of these companies' actions undoubtedly impacted the course of the war, provided a fundamental advantage to Ukraine, and helped manage a humanitarian disaster; however, also put the internet at risk. While the withdrawal of internet backbone providers like Cogent and Lumen was in compliance with sanctions, the speed of the withdrawals pre-empted the General License exemption for internet providers²⁶ that recognised the ramifications of such withdrawals on the free and open internet. Operating under speed has led to opaque, disjointed, and inconsistent positions that have occasionally created confusions destabilised communications and infrastructures; Meta temporarily altered its policy on hate speech to allow users to call for the death of Russian soldiers,27 leading to Instagram and Facebook being barred from Russia and the isolation of Russian people from non-state-controlled information services. In February 2023, SpaceX announced that it would restrict the

use of Starlink by the Ukrainian Army to defensive operations. This seemed to be a reversal from initial policy, but responses from SpaceX were unclear, citing a lack of anticipation for Ukraine's use of Starlink in offensive operations.²⁸

Companies have struggled to articulate clear policies and are now being faced with the realities of financial commitments to a protracted conflict, particularly during a tech downturn. Unlike states and international organisations that are prepared for intervention for "as long as it takes,"29 private companies' obligations to shareholders and commercial interests can limit the sustainability of their support. Although a large proportion of the cost of Starlink terminals has been covered in conjunction with USAID, Poland, and the UK, SpaceX covered approximately 70 percent of the connectivity costs. It has further declared that it may not be able to continue these contributions indefinitely, approaching the Pentagon for support.30 SpaceX would not be able to finance a request from Ukraine for 8,000 additional terminals, and there is concern that the company's commitment might be wavering.31

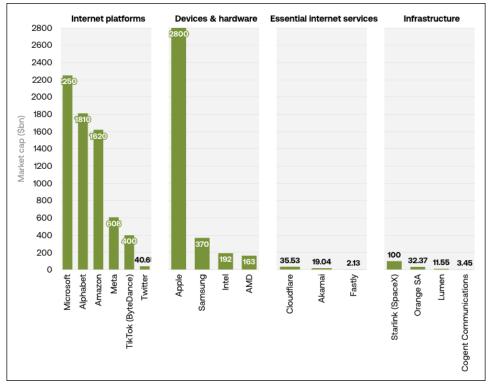
New geopolitical actors are ill-equipped for internet geopolitics

During times of conflict and peace, private companies are the caretakers and underwriters of the secure, free, open, and interoperable internet. While multistakeholder forums may govern aspects of the operational alignment of the internet, the content, hardware, and networks are increasingly controlled by internet platforms, content delivery networks, and internet providers. This changing power dynamic has placed tech companies at the centre of geopolitics as states seek to assert their vision and principles on internet infrastructure and content. The vertical expansion of these tech companies through the levels of the internet has consolidated their technical dominance as well as their influence on geopolitics.

The decentralised internet is now heavily consolidated. Amazon, Meta, Microsoft, and Alphabet have content platforms, branded hardware, cloud services, and ownership stakes in fibre networks. Content providers such as social media and search platforms have an outsized share of influence (Figure 1). Their market capitalisation

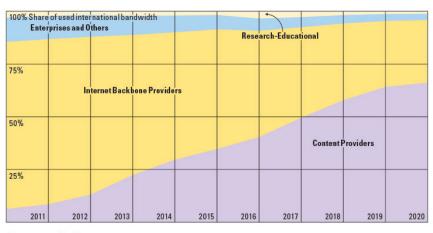
outranks other internet companies, and they even buy bandwidth directly on fibre networks, bypassing traditional telecommunications firms (Figure 2).

Figure 1: Internet Companies' Market Capitalisation



Source: TBI (2022)32

Figure 2: Share of Submarine Cable International Bandwidth



Content Reigns

Content providers' international bandwidth growth has outpaced that of all other customers in recent years. By 2017, content providers had surpassed internet backbone providers as the largest users of international capacity.

Source: Telegeography (2022)33

Addressing an influx of geopolitical crises requires global perspectives that tech companies may not always be equipped to provide despite their power and influence. The same private companies that demonstrated the significance of their involvement in Ukraine have exhibited a lack of engagement that is just as meaningful. The lack of adequate content-moderation resources among social

media platforms in non-Western nations has been a major concern. The Facebook Files noted that, despite more than 90 percent of Facebook users living outside the US and Canada, only 13 percent of content-moderation resources were spent on non-US content.³⁴ Trust and safety teams as well as international offices (such as Twitter's Accra office) have been hit hard by recent layoffs.³⁵

The G20's Role



A G20 approach to internet internationalism

ech companies have changed the geopolitical landscape. The G20 was formulated to address a myriad of global crises and therefore, must adapt to the role of technology in current and future crises. Governments have increasingly responded the power of tech companies with blunt instruments, conducting policy through data localisation laws, internet shutdowns,36 and platform bans.37 These actions are polarising and, in conjunction with complex geopolitics, exacerbate the fissures in the global internet.

Localised control of the internet cuts against the foundational principles

of internet governance and risks, thus hampering the growing digital economy. The G20's mandate as an informal power centre for the global that addresses global economy alignment and governance challenges gives it clear convening power across some of the largest developers and users of internet technologies. A new approach to multilateralism, which is rooted in technology and greater crosscutting ties, is needed digital stability and resilience. This is fundamentally not possible without acknowledging the most powerful and influential actors in the space. The G20 should seize the opportunity to ensure that their investments in the global digital economy are underpinned by a fit-forpurpose, universally accessible, and sustainable internet.

Recommendations to the G20

Coordinating multistakeholder engagement on digital stability

he current model of multilateralism does not sufficiently address the role of tech developers and experts in geopolitical crises. It is the responsibility of companies, states, and international institutions to form a new vision and partnership to address threats to global stability from the misuse and abuse of the internet. The Declaration on the Future of the Internet, signed by 61 countries on 28 April 2022, made strides in increasing commitments to the free, open, and interoperable internet but did not provide a mechanism for oversight or action. There are also concerns that proposals for the UN Global Digital Compact, to be agreed upon at the Summit for the Future in 2024, could undermine the multistakeholder model that is vital for long-term internet access and security. A new independent body is needed to bring together the key stewards of the internet and its governance and to communicate and coordinate across all issues relating to digital stability. By fostering greater ties between states, internet governance organisations, and tech developers, such a body can

ensure the health and stability of the internet ecosystem.

Supporting technology companies in the development of geopolitical strategy and a self-regulatory geotechnology board

It is in global interest to ensure that tech companies are equipped to address evolving crises worldwide. Tech companies have largely intervened on an ad-hoc basis, often depending on the decisions of a single person. geopolitical strategy coherent policies are essential to digital resilience in crises. The G20 can lead through supporting the development of geotechnology boards, similar to Facebook's Oversight Board, in order to aid companies in their review of global geopolitical challenges and balance their interventions.

Aiding countries in tech diplomacy through training and norms development³⁸

Nations need more effective ways to engage with tech developers. However, many diplomats lack the knowledge and capacity to engage fruitfully with the tech industry. This is especially challenging, since smaller and lower income nations are disproportionately impacted by global crises such as climate change and extremism. Providing all nations with the resources and capacity-building to have a voice at the table on global tech issues should be a G20 priority.

Developing a G20 Digital Infrastructure and Defence Agreement (DIDA)

The resilience and defence of international infrastructure requires global awareness and commitment. Existing internet governance forums are designed to be slow and stable. While this is important, more multilateral support is required in the face of crises in order to secure the internet and global communications. A DIDA could provide swift action to support nations in safeguarding the open internet and maintaining connectivity in the event of a crisis.

The internet is at an inflection point. Geopolitical competition on its basic infrastructure stretches from the depths of the ocean into the furthest reaches of space. This competition will expand to the 79.4 zettabytes of data likely to be generated by the 41.6 billion devices that will be connected to the internet by 2025,39 as the final three billion people gain access. The internet will also have to bear the pressure of a new layer of generative Al tools and their effects across a stack that is consolidating in the hands of a few who must balance their commercial commitments with a geopolitical environment for which they are ill-prepared. Thus, it falls to institutions like the G20 to provide support and work with companies and internet governance organisations towards a new model of internet internationalism that puts protecting the world's greatest resource-the stable, open, free, secure, and interoperable internet—above geopolitical rivalries.

Attribution: Melanie Garson and Pete Furlong, "Integrated Internet Internationalism," *T20 Policy Brief*, July 2023.

Endnotes

- 1 International Chamber of Commerce, *ICC White Paper on Delivering Universal Meaningful Connectivity*, May 30, 2022, https://iccwbo.org/news-publications/policies-reports/icc-white-paper-on-delivering-universal-meaningful-connectivity/#single-hero-document.
- "Digital Technologies to Achieve the UN SDGs," ITU, December 2021, https://www.itu. int/en/mediacentre/backgrounders/Pages/icts-to-achieve-the-united-nations-sustainable-development-goals.aspx.
- 3 ITU/UNESCO Broadband Commission for Sustainable Development, *The State of Broadband Report 2022: Accelerating Broadband for New Realities*, September 2022.
- 4 Ian Wright, "The Cost of Shutting Down the Internet," Merchant Machine, November 17, 2022, https://merchantmachine.co.uk/the-cost-of-shutting-down-the-internet/.
- 5 Sebastian Klovig Skeltong, "Internet Shutdowns Cost Global Economy \$24bn in 2022," ComputerWeekly.com, January 11, 2023, https://www.computerweekly.com/news/252529078/Internet-shutdowns-cost-global-economy-24bn-in-2022.
- Jane Wakefield, "How Will Tonga's Broken Internet Cable Be Mended?" *BBC News*, 2022, https://www.bbc.com/news/technology-60069066.
- Amritha Jayanti, "Starlink and the Russia-Ukraine War: A Case of Commercial Technology and Public Purpose?" Belfer Center for Science and International Affairs, Harvard Kennedy School, March 3, 2023, https://www.belfercenter.org/publication/starlink-and-russia-ukraine-war-case-commercial-technology-and-public-purpose.
- 8 Ulrich Spiedel, "Why NZ's Communications Networks Broke Down in Cyclone Gabrielle," *RNZ*, March 3, 2023, https://www.rnz.co.nz/news/national/485259/why-nz-s-communications-networks-broke-down-in-cyclone-gabrielle.
- Andrew Bennett et al., "The Open Internet on the Brink: A Model to Save its Future," The Tony Blair Institute for Global Change, September 30, 2021, https://www.institute.global/insights/tech-and-digitalisation/open-internet-brink-model-save-its-future. 10 Kieron O'Hara and Wendy Hall, "Four Internets: Data, Geopolitics and the Governance of Cyberspace," The Forum Network, August 9, 2021, https://www.oecd-forum.org/posts/four-internets-data-geopolitics-and-the-governance-of-cyberspace-by-kieron-o-hara-wendy-hall.
- "Draft Framework & Discussion Document," IGF 2022 Policy Network on Internet Fragmentation (PNIF), November 2022, https://www.intgovforum.org/en/filedepot_download/256/23770.
- 12 United Nations, *Our Common Agenda Report of the Secretary General*, 2021, https://www.un.org/en/content/common-agenda-report/assets/pdf/Common_Agenda_Report_English.pdf.

- 13 O'Hara and Hall, "Four Internets"
- Göran Marby, "Letter to Mykhailo Fedorov," ICANN, March 2, 2022, https://www.icann.org/en/system/files/correspondence/marby-to-fedorov-02mar22-en.pdf.
- Hans Petter Holen, "An Open Internet Remains the Goal," RIPE Labs, April 6, 2022, https://labs.ripe.net/author/hans_petter_holen/an-open-internet-remains-the-goal/?pk_ vid=146c4dcbec1e224a16811867363f15ef.
- 16 Kieren McCarthy. "Revitalising Global Internet Governance," Tony Blair Institute for Global Change, May 31, 2022, https://www.institute.global/insights/tech-and-digitalisation/revitalising-global-internet-governance.
- Justin Ling, "The Election That Saved the Internet from Russia and China," *Wired*, October 30, 2022, https://www.wired.com/story/itu-2022-vote-russia-china-open-internet/.
- 18 Rachel Lerman, "On Google Maps, Tracking the Invasion of Ukraine," *The Washington Post*, February 28, 2022, https://www.washingtonpost.com/technology/2022/02/25/google-maps-ukraine-invasion/.
- 19 Vera Bergengruen, "How Telegram Became the Digital Battlefield in the Russia-Ukraine War," Time, March 21, 2022, https://time.com/6158437/telegram-russia-ukraine-information-war/.
- 20 Russ Mitchell, "How Amazon Put Ukraine's 'Government in a Box' and Saved its Economy from Russia," *Los Angeles Times*, December 15, 2022, https://www.latimes.com/business/story/2022-12-15/amazon-ukraine-war-cloud-data.
- 21 Matthew Prince, "Steps We've Taken Around Cloudflare's Services in Ukraine, Belarus, and Russia," *The Cloudflare Blog*, March 22, 2022, https://blog.cloudflare.com/steps-taken-around-cloudflares-services-in-ukraine-belarus-and-russia/.
- 22 Brad Smith, "Defending Ukraine: Early Lessons from the Cyber War," *Microsoft*, https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/.
- Doug Madory, "Updated: Cogent and Lumen Curtail Operations in Russia," *Kentik Blog*, March 7, 2022, https://www.kentik.com/blog/cogent-disconnects-from-russia/.
- 24 "Twitter Launches Privacy-Protected Site on Dark Web to Bypass Russia's Block," The Guardian, March 10, 2022, https://www.theguardian.com/technology/2022/mar/09/twittertor-version-russia-block.
- 25 Chris Stokel-Walker, "Russia Inches Toward its Splinternet Dream," *Wired*, April 1, 2022, https://www.wired.com/story/russia-splinternet-censorship/.
- "U.S. Moves to Keep the Russian People Connected despite Sanctions," Access Now, February 10, 2023, https://www.accessnow.org/press-release/u-s-treasury-russia-sanctions-internet/.

- 27 "Facebook and Instagram Let Users Call for Death to Russian Soldiers over Ukraine," *The Guardian*, March 11, 2022, https://www.theguardian.com/technology/2022/mar/11/facebook-and-instagram-let-users-call-for-death-to-russian-soldiers-over-ukraine.
- Joey Roulette, "SpaceX Curbed Ukraine's Use of Starlink Internet for Drones -Company President," Reuters, February 9, 2023, https://www.reuters.com/business/aerospace-defense/spacex-curbed-ukraines-use-starlink-internet-drones-company-president-2023-02-09/.
- 29 "Remarks by President Biden and President Zelenskyy of Ukraine in Joint Statement," The White House, February 20, 2023, https://www.whitehouse.gov/briefing-room/speeches-remarks/2023/02/20/remarks-by-president-biden-and-president-zelenskyy-of-ukraine-in-joint-statement/.
- Alex Marquadt, "Exclusive: Musk's SpaceX Says it Can No Longer Pay for Critical Satellite Service in Ukraine, Asks Pentagon to Pick Up the Tab," *CNN*, October 14, 2022, https://edition.cnn.com/2022/10/13/politics/elon-musk-spacex-starlink-ukraine/index.html.
- 31 Marquadt, "Exclusive: Musk's SpaceX Says it Can No Longer Pay for Critical Satellite Service in Ukraine"
- 32 Melanie Garson and Pete Furlong, "Disrupters and Defenders: What the Ukraine War Has Taught Us about the Power of Global Tech Companies," Tony Blair Institute for Global Change, May 10, 2022, https://www.institute.global/insights/geopolitics-and-security/disrupters-and-defenders-what-ukraine-war-has-taught-us-about-power-global-tech-companies.
- Larry Lairson et al., *Submarine Cable Map 2022*, TeleGeography and Telecom Egypt, 2022, https://submarine-cable-map-2022.telegeography.com/.
- Justin Scheck, Newley Purnell, and Jeff Horwitz, "Facebook Employees Flag Drug Cartels and Human Traffickers. The Company's Response Is Weak, Documents Show," *The Wall Street Journal*, September 16, 2021, https://www.wsj.com/articles/facebook-drug-cartels-human-traffickers-response-is-weak-documents-11631812953.
- Kate Klonick, "The End of the Golden Age of Tech Accountability," *The Klonickles*, March 3, 2023, https://klonick.substack.com/p/the-end-of-the-golden-age-of-tech.
- "Weapons of Control, Shield of Impunity," Access Now, February 2023, https://www.accessnow.org/wp-content/uploads/2023/05/2022-KIO-Report-final.pdf. 37 Shahbaz, Funk, Friedrich, Vesteinsson, Baker, Grothe, Masinsin, Vepa, Weal eds. Freedom on the Net 2022, Freedom House, 2022, freedomonthenet.org. 38 Akos Erzse and Melanie Garson, "A Leader's Guide to Building a Tech-Forward Foreign Policy," Tony Blair Institute for Global Change, March 25, 2022, https://www.institute.global/insights/tech-and-digitalisation/leaders-guide-building-tech-forward-foreign-policy.
- "Internet of Things and Data Placement," Dell Technologies, https://infohub.delltechnologies. com/l/edge-to-core-and-the-internet-of-things-2/internet-of-things-and-data-placement.





वश्धिव कुटुम्बकम् ONE EARTH • ONE FAMILY • ONE FUTURE