

DIGITAL ASYMMETRY: Future Business Implications of a Balkanizing Internet

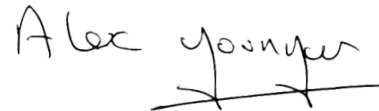
By Collin Barry and Levi Gundert
Foreword by Sir Alex Younger

Foreword

As the internet began to take shape in the early 1990s, national governments, corporations, and individuals alike hailed it as a means to spread digital connectivity globally. Over the last 25 years, the internet has delivered on this promise and more — facilitating an open exchange of ideas, supercharging innovations, empowering individuals, and improving the quality of life for billions when viewed across several key dimensions such as health, education, personal security, and civic engagement. Rising geopolitical tensions over the past decade, however, have heralded a shift in thinking, particularly among authoritarian-style regimes acutely aware of the internet's potential for what they view as subversive and malicious activity.

Consequently, lines are being drawn to protect national assets, critical infrastructure, and information flows. Authoritarian regimes in particular seek to exert higher degrees of control over social unrest, political dissent, whistleblowing, and a free press — all activities they view as counterposed to their conceptions of centrally designed social and political norms and values. As well, the technological innovations and economic considerations underpinning the internet's infrastructure are changing; notably, the United States no longer sits at the center of the internet's technological backbone and ecosystem. Coupled with faltering aspects of internet security, data privacy oversight and regulation, and the deliberate actions of adversarial threat actors, the internet's purpose and resilience, particularly when considering fundamental questions around data ownership and data access, are being called into question.

This "Red Cell" analysis is a thought experiment — a framework for thinking differently about the internet's future. Our intent is to stimulate executive-level thinking on vast geopolitical changes and what we view as a far less certain trajectory concerning global information and commercial flows. The diversity and complexity of these changes are best explored through scenarios — a presentation of alternative narratives as to how the internet's future may unfold. Our effort is to encourage business leaders to think and plan for the long term so that should unanticipated developments occur, their organizations are better prepared for any consequent impacts on the internet's form and function, and by extension their ability to grow and sustain business operations globally.



Sir Alex Younger
Former Chief
British Secret Intelligence Service (MI6)
2014-2020

Executive Introduction

The global order is changing. Over the past decade, we have witnessed a rise in authoritarianism, nationalism, and opposition to the central features and tenets of the international rules-based order. Consider Russia's invasion of Ukraine in April 2022, and more recently, China's military flexing in the Taiwan Strait and more broadly in the South China Sea. Taken together, Moscow's and Beijing's actions¹ reflect a will and intent to undermine the independence and democracy of sovereign nations within their immediate hemispheres². Moreover, their actions reflect a lack of unified and coherent global leadership, which has allowed authoritarian regimes to act with impunity and expose the weaknesses of the international order. Other real-world developments, including the 2008 financial crisis, rising levels of economic inequality, economic insecurity, and status anxiety owing to globalization and technological advancements, have fueled populist sentiment, creating a platform for autocratic leaders such as Vladimir Putin and Xi Jinping to attack the values and norms of liberal democracy as self-indulgent, commercially driven, and ineffectual. These leaders are also promoting nationalist rhetoric that exerts greater influence and control over their respective populations.

We find ourselves, once again, at a critical juncture in human history, where a dynamic interplay of disruptions and discontinuities could lead to widely contrasting futures. We also see a larger rising tide of authoritarian power projection and the return of great power competition, what President John F. Kennedy in his 1961 inaugural address termed a "long twilight struggle" between competing political systems and governing philosophies. Freedom House, a vanguard for tracking political freedoms and human rights, notes that civil liberties have declined globally year-over-year since 2008.³ Thus, the question is not whether democracy is in retreat; the evidence lies with the growing strength of autocratic regimes such as Russia and China, an erosion of liberal institutions in countries such as Poland⁴, Hungary⁵, Turkey⁶, and Brazil⁷, as well as democratic instability in countries such as the United States and India.

This changing global order has profound implications for the internet, and by extension, international business. In our view, it is conceivable that the global internet — a catalyst for progress, development, innovation, and human freedom — can shift to a model of asymmetric openness, where authoritarian regimes freely control not only their own populations, but also exchanges of ideas and economic flows more broadly. In this paper, we explore possible futures of the global internet. Our intent is to foster a deeper strategic conversation in corporate boardrooms about the driving forces and uncertainties that will shape the internet in the years ahead.

1 <https://www.nbr.org/publication/chinas-vision-for-a-new-world-order/&sa=D&source=docs&ust=1661395478164050&usg=AOvVaw35fpAMTz3Tmum3dOD1WRhQ>

2 <http://en.kremlin.ru/supplement/5770>

3 <https://freedomhouse.org/article/new-report-freedom-world-2020-finds-established-democracies-are-decline>

4 <https://freedomhouse.org/article/poland-and-hungary-must-not-be-ignored>

5 <https://freedomhouse.org/article/poland-and-hungary-must-not-be-ignored>

6 <https://www.brookings.edu/research/the-rise-and-fall-of-liberal-democracy-in-turkey-implications-for-the-west/>

7 <https://3A%2Fsuprema.stf.jus.br%2Findex.php%2Fsuprema%2Farticle%2Fdownload%2F162%2F67%2F280&usg=AOvVaw1hGzytDRI6LX35AJxA8Gkk>

Uncertainties and Discontinuities

In the following section we present a summary on the current state of the internet and adjacent ecosystems to better understand the potential for changing business dynamics in the next 5 years.

	Internet Governance Philosophy	Data Regulation ⁸	Supply Chains
China/Russia	Multilateralism + Digital Sovereignty ⁹ + Centralized Control ¹⁰	Data Localization ¹¹ + Data Dependence: Data Protection Act ¹²	Decoupling: semiconductor self-sufficiency desired; state-controlled companies that serve a protected domestic market and international export
European Union	Multistakeholderism ¹³ - Surveillance Capitalism ¹⁴	Data Localization ¹⁵ : GDPR, CIPL, Digital Services Act, Digital Markets Act	Decoupling: semiconductor independence ¹⁶ from US and China
United States	Multistakeholderism + Surveillance Capitalism	Data Dependence: Regional: CCPA, Consumer Data Protection Act	Decoupling: semiconductor self-sufficiency, desired sanctions and trade escalations

Table 1: Approaches, regulatory frameworks, and supply chain considerations for major global internet stakeholders

⁸ <https://www.dlapiperdataprotection.com>

⁹ <https://www.weforum.org/agenda/2021/03/europe-digital-sovereignty/>

¹⁰ <https://www.newamerica.org/cybersecurity-initiative/reports/idealized-internet-vs-internet-realities/ideal-vs-reality-understanding-the-liberal-democratic-gap/>

¹¹ <https://www.finance.senate.gov/imo/media/doc/Samm%20Sacks%20Testimony%20-%20Senate%20Finance%20-%20December%207%202021.pdf>

¹² <https://www.dlapiperdataprotection.com/?t=law&c=RU>

¹³ <https://digitalpeacenow.org/multistakeholderism-what-is-it-and-why-does-it-matter-to-international-peace-and-stability-online/>

¹⁴ <https://news.harvard.edu/gazette/story/2019/03/harvard-professor-says-surveillance-capitalism-is-undermining-democracy/>

¹⁵ <https://www.belfercenter.org/publication/sovereignty-and-data-localization>

¹⁶ <https://www.politico.eu/article/europe-seeks-to-decouple-from-us-china-chip-war/>

Scenario Logic

The nature and distribution of global power is changing as the world becomes increasingly competitive and multipolar. In the next 5 years, we see 4 overarching trends that have the potential to change the trajectories of the internet and the global business landscape:

- **Geopolitical Shifts:** Including China's near-peer power and assertiveness, the US rethinking its role in maintaining international peace, the Indo-Pacific's growing importance to global prosperity, and the continued development of emerging markets creating a growing, global middle class.
- **Technological Change:** Technological development has led to higher degrees of interconnectivity and interdependence of global systems and has reshaped social and economic paradigms — between states, the private sector, and citizens. Smartphones are the precursor to a hyperconnected world, where 5G networks, when fully deployed, will allow for reliable, low-latency connectivity leading to unfathomable scale of data generation.
- **Systemic Competition:** Intensified competition over existing post-WWII international rules and norms and the emergence of rival geopolitical and economic blocs, based on contrasting ideologies and values, will seek to alter if not displace existing security, economic, and trade-based institutions that underpin our way of life. Authoritarian states and malign actors seek to infiltrate and undermine democratic systems. Hybridized conflict has emerged as states use a growing range of instruments (like cyber) to undermine and coerce rivals.
- **Transnational Challenges:** Global food insecurity, climate change, pandemics, illicit finance, and terrorism threaten shared security and prosperity, and they require collective action and multilateral cooperation.

These 4 trends will overlap and interact in ways that are difficult to understand, let alone predict. They also highlight the need for both national leadership and corporate vision to navigate an uncertain future.

The internet is an evolving manifestation of technological development and political fragmentation. In light of a shifting global order, the internet will potentially drift further into a politically defined technological balkanization. However, there is a realistic and more promising scenario: managing these overarching trends through multilateral cooperation, strengthened global governance, and corporate innovation to fulfill opportunities for peace, stability, and economic prosperity.

A Balkanized Internet: Scenarios

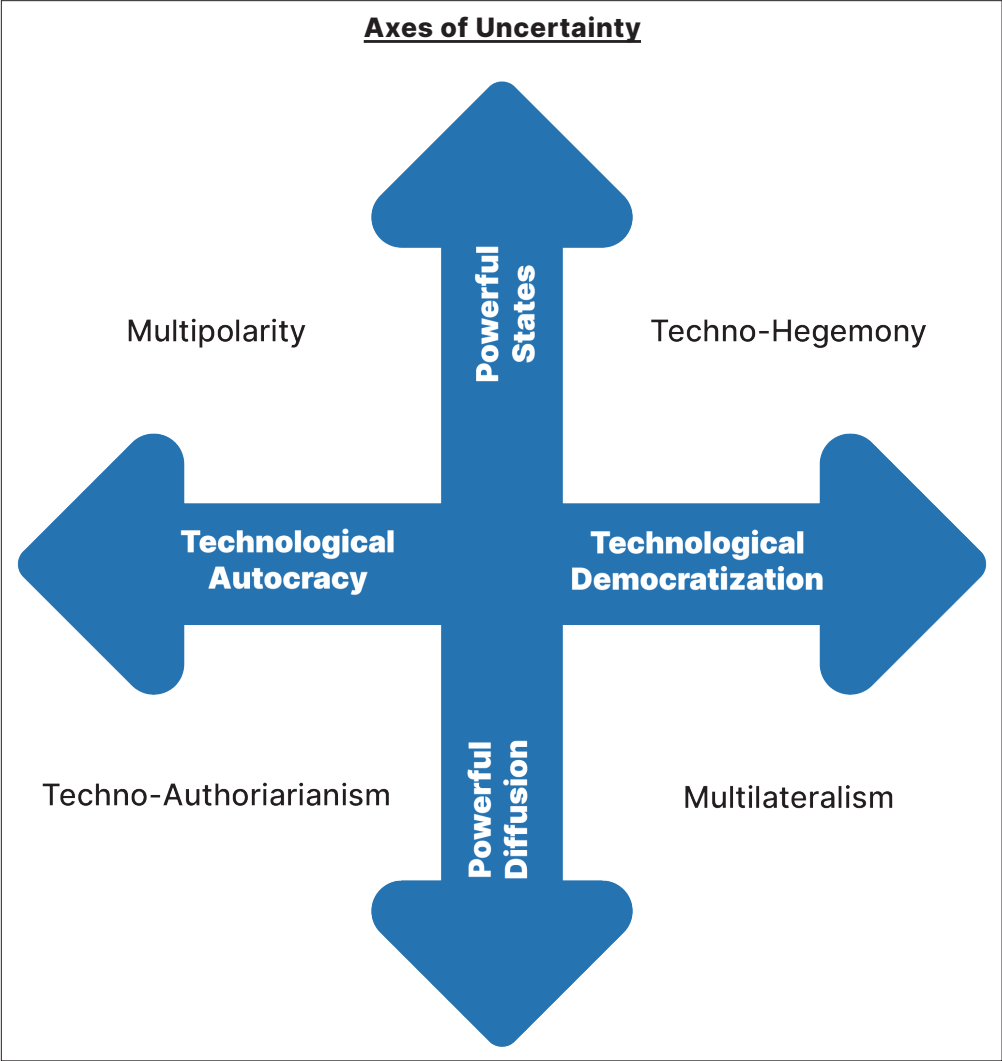


Figure 1: Internet balkanization scenarios matrix

Techno-Authoritarianism

Though mechanisms for central control of a national internet are attractive to autocratic¹⁷ regimes and western¹⁸ democracies alike, the difference lies in the degree of control and desired outcomes. A fully balkanized internet would likely manifest fault lines along major states with minor states joining one or more regional internets based on political or economic alliances. This paradigm would be characterized by localized access to information based on relationships forged through similar ideologies and values.

Maximum balkanization would require companies to iteratively assess tradeoffs and risk in every facet of a particular geography or country. Factors such as data localization and governance would add significant overhead and cost to a profitability calculus. A hyper-balkanized internet would require navigating data transit at national boundaries similar to customs inspection of foreign goods at a port of entry. Permissible data entry or exit from national borders would require verification and transparency certification toward approved routing path traversal using approved hardware (such as servers, routers, and switches) that contains approved semiconductors with a corresponding certified supply chain (including firmware creation). Accessibility of nationalized fiber optic cables would be limited to government-approved internet and hosting service providers. Peer routing between autonomous systems would rely on pre-approved static routes.

Multiple complete walled garden eco-systems would create significant information asymmetries that would affect every facet of life. The largest internet splinters by data volume would experience the greatest advantages in science, commerce, and other fields of knowledge. Adversarial countries might create bilateral data exchanges in specific scenarios to further mutually beneficial outcomes.

Multipolarity

Digital sovereignty is attractive to developed countries to support national goals. A multipolar internet reflects less dramatic technological balkanization and emphasizes cyber priorities via national policy. For example, the EU's focus on individual privacy and online liberty resulted in the General Data Protection Regulation (GDPR), triggering new strategies and tactics for companies straddling multiple poles. Second, creating and benefiting from surveillance capitalism is an important consideration for enterprises aligning somewhere in the multipolarity spectrum. Understanding large-pole overarching objectives and associated strategies in the next 5 years is critical to business planning success. Partial balkanization is likely to continue aligning to national interests in large economies such as China, Russia, the United States, European Union, Brazil, and India. Success in a multipolar world requires foresight toward deft navigation of frequently shifting cyber allies and national policies.

Finally, global supply chains and fiber optic (and satellite) internet access will continue as a centerpiece of mistrust leading to mercantilist technology strategies that prioritize self-sufficiency and internet standards¹⁹ influence. A dispersion of ICANN's authority and responsibilities combined with changing international technology standards will increase competition for influence among the large polarities. Enterprises that contribute to technological national dominance will benefit from government subsidies and assistance.

¹⁷ <https://www.middleeasteye.net/news/iran-google-safe-search-outrage>

¹⁸ <https://therecord.media/eu-wants-to-build-its-own-dns-infrastructure-with-built-in-filtering-capabilities/#:~:text=January%2019%2C%202022-,EU%20wants%20to%20build%20its%20own%20DNS%20infrastructure%20with%20built,the%20general%20public%20for%20free.>

¹⁹ <https://www.csis.org/analysis/international-telecommunication-union-most-important-un-agency-you-have-never-heard>

Techno-Hegemony

In a techno-hegemony world, power is shared between state and non-state actors, the latter including technology multinationals and megacity leaders. This scenario is characterized by an ever-present web — a networked information-latticework world where resilience and pragmatism are the dominant features, and the boundaries between governments, businesses, and individuals blur.

Competition will play out on two levels: countries seeking technological superiority in emerging technology fields such as semiconductors, information and communications equipment, artificial intelligence (AI), and quantum technology, largely in the interest of advancing both national security and foreign policy interests; and corporate competition intensifying, particularly as emerging market entrants and digital disruptors with demonstrated cross-border operational agility scale globally and seek a greater percentage of market share dominated by established industry leaders. Global access to information is driven primarily on economic interests, however, there is a shared understanding that broader cooperation across all actors is required to provide effective digital governance to allow for seamless cross-border flows.

Entrepreneurship and innovation, coupled with higher degrees of collective social and human development, will drive the emergence of new technology regions around the world. Skill sets required for next-generation digital technologies will be harvested nationally and result in decreasing levels of global migration patterns. The digital space lacks global leadership and suffers from poor governance, which leads to accelerated disinformation, unsafe and unethical uses of AI and other advanced technologies, and data privacy infringements. Digital fragmentation will accelerate, and disruptions to economically important supply chains, notably technology, will intensify.

Multilateralism

In a less technologically polarized future world, roughly 190 countries seek international policy and governance consensus, where possible, to promote digital peace and cooperation toward improved holistic outcomes. Certainly powerful states will continue to seek influence in internet governing bodies and standards, but positive network effects from weaker state participation act as a counter-balance to polarization or even extreme balkanization.

In a multilateral digital future, nations continue²⁰ jointly building new fiber optic infrastructure²¹ connecting states and continents, with the understanding that cables and landing stations are natural points of vulnerability during periods of kinetic escalation. Governments prioritize multilateral cyber agreements, similar to intellectual property protection, regardless of geopolitical conflict. Weaker states begin, and stronger states continue, building differentiated offensive cyber capabilities. The digital domain remains a de facto theater for conflict, including information operations, but states invest in defensive capabilities while explicitly recognizing the benefits of relatively free and open information flows across national boundaries. In the event of kinetic conflict, cyber capability and data dispersion in cloud infrastructure across multiple state boundaries may act as a deterrent to escalation, for fear of violating additional national sovereignties.

A future digital multilateralism includes business as a key stakeholder, but with less international influence that a tech-hegemony future would include. Enterprises may increasingly view their digital interests through a stakeholder lens that values ethical digital social and governance behavior for the benefit of not only shareholders, but also an international reputation with customers, partners, and employees.

²⁰ <https://www.reuters.com/world/americas/brazil-joins-chile-building-first-fiber-optic-cable-connect-s-america-asia-2021-05-13/>

²¹ <https://www.submarinecablemap.com>

Business Implications and Outlook

The value of these scenarios is in anticipating alternate emerging patterns, which allows for a clearer identification of both risks and opportunities, and enables an appropriate set of strategic responses to unforeseen challenges. Each of the four scenarios contains characteristic differences, created by the overarching trends behind the axes of uncertainty, and to some degree a creative texturing in an internet portrait that includes the future of business. While cross-border digital expansion has led to scaling advantages, with many corporations deriving more than half their revenues internationally, we believe it worthwhile to explore a future where digital platforms and tools are no longer globally accessible.

Despite sophisticated forecasts and extensive data analysis, the future is likely to surprise us. Contemplating scenarios allows for a dress rehearsal — to build process and skill with anticipating, responding, and adapting to an uncertain future. Success hinges on considerations across 3 dimensions:

- **Global Footprint and Organizational Structure:** Companies may need to decentralize global functions, back-office operations, as well as digital infrastructure to draw on data flows to drive the business and ensure organizational consistency. There could be a return to intranets spanning different regions and countries, lines of business, product groups, and corporate functions.
- **Digital Infrastructure:** Building local digital platforms and data centers, at scale, will be necessary to accommodate digital enclaves. A balkanized internet will also harm big data analytics as a means to generate insights from data being collected as a means to innovate, increase productivity, as well as recruit and retain customers. Data focused on market dynamics, customer relationships, and vendor performance will not be collected and assessed at scale.
- **Risk Management:** External shocks will have less of a ripple effect in an era of a balkanized internet, as the lack of digital linkages will prevent widespread contagion (such as a power grid failure or a natural disaster); however, cyberattacks can be far more harmful to a business if a company's prioritized information assets are housed in one location; the alternative being for companies to bear enormous cost of duplicating their critical assets, to include sequestering data in multiple locations and implementing redundant, protective measures (such as cyber defense technologies and enterprise security teams).

Looking ahead, what will competing in a balkanized digital global landscape look like? What business models will allow for a sustainable and profitable position? What kind of global footprint will be optimal? What does corporate resilience look like in an age of a balkanized internet?

Conclusion

After considering the 4 previous scenarios, we are advocating for a future internet that veers toward multilateralism and technological democracy. Regardless of the significant challenges that a free and open internet must manage, the opportunities to improve human lives are too great to ignore. Additionally, an internet that is free to cross national boundaries may incentivize measured responses in cyberspace. For example, some have speculated that the perceived relative lack of intense Russian cyber aggression against Ukrainian targets is due to Ukrainian data largely being hosted outside of Ukraine's geographic boundaries. Cyberattacks on western cloud infrastructure might be interpreted as a significant conflict escalation with attendant unintended consequences.

The trajectory and shape of the internet in the near-term future is uncertain and unpredictable. The nuanced and diverse outcomes across our four scenarios illustrates how different combinations of uncertainties and discontinuities could shape the internet's trajectory and form in ways that may differ from the implicit assumptions held across governments, private industry, and individuals today. These differences have important implications for the structure of markets, flow of information, and levels of human development and progress.

Our intent is for business leaders to examine these scenarios and orchestrate strategic conversations to ensure an appropriate degree of agility and adaptability in the face of an uncertain future.



Collin Barry is a strategic security leader who has held positions in the US Intelligence Community and private industry. Having lived on four continents and traveled to over 60 countries, Collin has considerable global experience and perspective. Passionate about collaboration, emerging technologies, and leveraging threat research and intelligence to build and sustain enterprise cyber resilience, Collin is driven to push the boundaries of what is possible.

Note: The thoughts and opinions expressed in this paper are solely that of Collin and do not represent the position of Expedia Group.



Levi Gundert is the Senior Vice President of Global Intelligence at Recorded Future, where he leads the continuous effort to measurably decrease operational risk for clients. Levi has spent the past 20 years in both the public and private sector, defending networks, arresting international criminals, and uncovering nation-state adversaries. He's held senior information security leadership positions across technology and financial startups and enterprises. He is a trusted risk advisor to Fortune-500 companies, and a prolific speaker, blogger, and columnist.