TI Observer

October 2023
Vol. 37

by Taihe Institute

Transformation:
Digital Economies & AI

Contents

Digital Westphalia: A Bulwark to the Descent into Digital Barbarism?

Warwick Powell

Adjunct Professor at Queensland University
Chair of Smart Trade Networks
Author of *China Trust and Digital Supply Chains Dynamics of a Zero Trust World*

Wherever we look, the "order" of the unipolar moment is in disarray. Fractures and contests are emerging just about everywhere, so it would seem, with geopolitical and civilization dimensions. This discombobulation of the unipolar order is accentuated at the vectors of modern information technology, whether it be in the *specialized equipment* used to manufacture semiconductors and the associated *raw materials supply chains* (rare earths and other metals), the *protocols and standards* that govern the development and use of "intellectual property," and the various applications of increased *computational capacity* euphemistically described as "artificial intelligence" (AI).

Digital technologies have increased their footprint over many facets of national and international activities over the past few decades. Their impacts have cut across all facets of human existence; from commerce, through public culture and media, and ultimately to military applications. How information is collected, created, validated, stored, disseminated, and used - data ecologies - is now at the heart of what makes societies tick. What happens in the digital arena is expected to shape the possibilities of future generations, as human societies embark on their various journeys towards and through what has been euphemistically referred to as the *Fourth Industrial Revolution*.

The Dystopia That Already Is

Infocracy and the Simulacra

"If we want to comprehend what kind of society we are living in, we need to understand the nature of information," claimed philosopher Byung-Chul Han. He goes on to articulate an increasingly dark perspective on the nature of information in (western) societies, in which he talks of the fragmentation of shared social information integrity and the emergence of "infocracy." He argues that: "We cannot build a stable community or democracy on a mass of contingencies. Democracy requires binding values and ideals, and shared convictions. Today, democracy gives ways to infocracy." His claims echo the critical concerns previously aired by the likes of Jean Baudrillard, who described the plunge of modern societies into the abyss of the simulacra, where the possibilities of common truths - a connection to the shared "sacramental order" - give way to the production of fragmented imaginaries that are very real in their effects, even if they are surreal in their detachment from the possibilities of a shared discursive - let alone ontological - world.

The *promise* of the internet, emanating mainly from Western scholars, politicians, digital industrialists, and observers, of a borderless world of information flows, democratizing data and bringing peoples across the world closer together, resemble more wishful utopias than the realities of ballooning information discordance, social tribalism, cyber fraud and intensified societal and cross-societal antagonism. Information has proliferated, and with this, we have borne witness to an explosion of algorithm-shaped segmentation and tribes, each creating, curating, and consolidating discordant narratives in which echo chamber effects and reinforce the never-ending momentum of tribal simulacra. Through social media, data volume creates a false impression of common social truths, but in reality, these algorithms drive social fragmentation into irreconcilable truth camps. In this environment, fear and paranoia are the leitmotifs of the digital era rather than the promises of democracy and liberation.

Conspiracy theories find succor in the "long tail" effects of a networked world, with heretofore isolated and fragmented pockets linking and fusing into resilient and throbbing networks of simulacra-fueled energy and "calls to action." Rather than open a vista of human liberation, the internet has fueled conspiracies that have in fact turned on the internet itself: the *dead internet theory* is an online conspiracy that claims the internet is now dominated by bots automatically generating content. The internet, armed with Large Language Models and audience analytic algorithms is a Simulacra Machine *par excellence*, the digital embodiment of the *ouroboros* - the ancient icon of a serpent devouring its own tail.

Without a mechanism for the forging of common social truths, a cohesive and functional society at large becomes increasingly problematic. Habermas' ahistorical modernist fantasy of dialogic democracy crumbles when the historical limitations to rationality are confounded by the realities of each historical conjuncture. In the present moment, one of the limits is the unraveling of the informational foundations of common and mutual knowledge formation as hermetic truth-camps proliferate.

Techno-feudalism and the Protective Monarch

If "infocracy" is white-anting the very foundations of the possibility of democratic politics, the emergence and dominance of *techno-feudalism* reinforces in economic terms the fragmentations that are at the heart of contemporary Western modernity. Techno-feudalism speaks to the power of a small number of big technology firms - major platform developers and operators - to extract rents and other forms of power due to their dominance of foundational data infrastructure. The power of Big Tech can be seen clearly in the U.S., where hordes of lobbyists have successfully stymied congressional efforts to introduce antitrust bills.

Such tech-landlords do more than just collect rent, however. They extract value from all aspects of the supply chains that intersect with the channels of the digitized platform economy, reducing the economic welfare of all others. Having done so, they mobilize their newly acquired "cloud capital" - data - to extend their reach into the wallets of enterprises, households, and individuals, shaping desires and preemptively nudging purchase decisions that transfer value and create new pools of data for future valorization. The circuits of capital and data circulation emasculate the supply chains of the real economy, while Big Tech valorizes the power of data.

Techno-feudalism isn't restricted to national polities either. It can have cross-border impacts. That's why many countries are introducing regimes to curtail the autonomy and power of these data "landlords." However, the U.S. and Europe continue to be the largest beneficiaries of the current feudal state of the global digital landscape. American companies historically dominate the creation and setting of standards, conferring upon their clear commercial benefits garnered through licensing revenues and ecosystem lock-in (and competitor lock-out). Their power is in part shared with their state counterparts, who - like the monarchs in the era of agrarian feudalism - act as sponsors and protectors of the estate governors. State agencies are able to regularly compel big tech companies to provide data on individuals, and when they can't, the state turns to the marketplace. As explained

recently by Anne Toomey McKenna, the personal information of US citizens has been sold by commercial data brokers to numerous government agencies over the years, including the FBI, the Department of Defense (DoD), and the NSA.

Commercial and state security interests under techno-feudalism have long coincided. It's hardly a surprise, therefore, that the US government and America's big tech industry have a shared interest in maintaining their hegemony. The very public disputes between the U.S. and China over 5G network technologies (involving the sanctioning of the world's leader in 5G technologies, Huawei) is perhaps the most prominent example of this protectionist mindset. The DoD's own Defense Innovation Board even publicly acknowledged in 2019 that the U.S. had already lost first-mover opportunities in both standards and technologies worth hundreds of billions of dollars, and recommended the state rely on attacks like export controls and aggressive intellectual property protection to slow China's telecommunications ecosystem expansion. The Biden administration has followed through on these recommendations.

Is Digital Barbarism all there is?

In his recent book on techno-feudalism, Yanis Varoufakis invokes the spirit of Rosa Luxemburg who posed the question: *after capitalism, is it socialism or barbarism?* For Varoufakis, techno-feudalism speaks to barbarism, with the return of the rentier economy with a vengeance.

While there is much to the critique of techno-feudalism, barbarism isn't the only possibility. That's because the conditions of existence of techno-feudalism aren't globally ubiquitous.

The growth of China's digital economy; its ongoing major role of Chinese firms in the raw materials supply chains that support the manufacture of semiconductors etc.; its rapidly expanding group of science, technology and engineering graduates; its activism in global standards-setting; and its rapid rise up the global ladder of academic outputs and patents registrations, are creating alternative realities and possibilities.

It's a set of possibilities that could be described as a *Digital Westphalia*.

Digital Westphalia points not to a utopia against the dystopian abyss of techno-feudalism, but is suggestive of a practical bulwark against the slide towards barbarism. As a bulwark, Digital Westphalia resists the presupposition that

technology is borderless *per se*, while at the same time, creates the possibilities of open source systems limiting the power of digital *rentiers*. Indeed, Digital Westphalia, as the name suggests, reasserts the primacy of nation-states in the governance and operationalization of information and associated technology systems while also insisting on protocols that make possible inter-national interoperability in a world lacking in trust.

Digital Westphalia has at least five main features:

1. *Digital Sovereignty*: Unregulated data flows nurtured the rapid spread of the Internet and digitization post-1996. American Big Tech commercially benefited by monopolizing the infrastructure upon which data was created and flowed, then consolidated that system, connecting people around the world as they grew their platforms. Their supra-national reach, while still benefiting from the support of US techno-nationalists, now faces opposition within the EU and China as they each pursue stronger digital sovereignty. The EU's General Data Protection Regulation (GDPR) subordinates data governance to sovereign polities in a manner that enables global interoperability via collaborative multilateral framework development. China's Position on Global Digital Governance has an even wider-ranging framework than GDPR but readily accommodates the GDPR and other such national or pan-regional measures.

2. *Open Source*: In addition to regulating international value flows, the information systems themselves must also be reformed to bring to heel the monopoly powers of techno-feudalism. To truly move away from the current order, new systems must be both transparent and accessible to the relevant stakeholder community. Rather than use intellectual property to inhibit social participation in the design, implementation, and operationalization of data ecologies, open-source paradigms encourage continual engagement and reflection. While certain open-source technologies, like Linux Kernel, have long underpinned digitalization, others have lagged behind proprietary systems in many domains, in terms of adoption and development speed. This situation may well be coming to an end. Many firms, particularly from China, actively embrace the possibilities and benefits of open-source technologies and platforms. Huawei and Intel were the top two contributors to the Linux Kernel 5.10, the core of the Linus open-source operating system when it was released in December 2020. Apple, Intel, Google, and Nvidia have recently joined Baidu and Alibaba in backing the open-source chip architecture RISC-V.

3. *Foundations for Collective Truths*: "Infocracy" under conditions of unregulated social media has undermined the conditions of functional democratic politics. The impact it has had on what can be called "collective truths" cannot be understated. While governments themselves do not need to regulate "truth" for their citizens, the need for commonly recognized authorities that others can rely upon for truthful claims is critical to a functioning society. Most social truths, particularly those that involve information consumption "at a distance," presuppose some form of what Julian Baggini describes as "authority truths." There are always the challenges of authority reductionism. What ultimately is the source of this or that authority? But in practice, authorities are accepted in the applicable social milieu when the actors involved exercise a form of information claim triage. It is therefore imperative that we more explicitly engage with the discussion about what conditions are necessary for persons with expertise, experience, and credibility to be recognized as authorities within a given milieu.

4. *Distributed Ledgers*: There is chronic distrust and mistrust. Creating conditions of trust is increasingly fraught. The practical alternative is to create institutions that can enable the formation of functional communications and transactions in an environment of *zero trust*. Such an environment enmeshes technological possibilities of items like distributed ledgers, with age-old forms of social organization by way of associations of stakeholders with shared interests; and whose interests are enmeshed in wider networks of social intercourse and value flow. Expect cryptography to play an elevated role in this context. As the exchange of data is constrained by national sovereignty concerns, technologies like *zero knowledge proofs* can be reasonably expected to enable cross-border transactions without "spilling the beans."

5. *Data ecologies as public goods*: Techno-feudalism works when the critical infrastructure is dominated by a slew of private interests, with the backing of the state. An alternative frame is needed, one which envisages data ecologies as public goods that need to be designed and governed in ways that continually open the elements of data ecologies to expanded public consideration and concern. Subordinating rent-seeking interests to public interest, at national and global scales, is the most pressing of governance challenges today.

Digital barbarism isn't the only possibility. Digital Westphalia offers hints of an alternative.

The Digital Economy: Opportunities and Challenges in a World Without Borders

Rémy Trichard

Serial entrepreneur and IT executive
Formerly VP of Monetization at KaiOS
Co-Founder at Terark and ex-Renren
Co-Founder of La French Tech Beijing
Advisor to the GSMA Inclusive Tech Lab

According to the Digital Economy Report 2021 by UNCTAD[1], the digital economy was valued at $14.5 trillion in 2021, and is expected to be worth $20.8 trillion by 2025. This represents about 15.5% of global GDP in 2021 and is projected to increase to 18.5% by 2025. The digital economy grew two and a half times faster than global GDP over the previous 15 years, almost doubling in size since 2000. It is a powerful tide that seems to be lifting all boats and yet, this Third Industrial Revolution, as it is sometimes called, is fundamentally different from anything that came before. It encompasses profound changes for the people and societies experiencing it, pushing them to adapt or become obsolete.

Some of the key distinctive features that differentiate the digital economy from the traditional economy are:

- the intangibility of digital goods and services, which means that they can be easily replicated, modified, and distributed at near-zero marginal cost. This enables the production and consumption of digital goods and services to take place anywhere, anytime, and by anyone;

- the low barrier to entry, anyone with a computer and internet can partake;

- the explosive growth that can result from network effects, which has already minted scores of millionaires and billionaires;

1 UNCTAD. “Digital Economy Report 2021.” unctad.org, August 2021. https://unctad.org/system/files/official-document/der2021_en.pdf.

- the data intensity of digital activities, which led some to refer to data as the "new oil";

- and the global reach, enabled once everyone and everything is interconnected in just one virtual "global village" where borders, just like other "physical" concepts don't quite seem to apply anymore...

Some people, such as Holland-born Peter Levels, have been able to take full advantage of the new opportunities offered by the digital economy. After teaching himself software development from online resources and experimenting rather than formal education, Levels built more than 70 digital services, eventually finding success with five of them and becoming a self-made millionaire, all without an office or even a residential address, all the while traveling around the world as a "digital nomad." He is not an isolated case: in just the U.S., the MBO Partners 2023 State of Independence research study[2] found that 17.3 million American workers currently describe themselves as digital nomads. The COVID-19 pandemic has led to a boom in "remote work," and for some of these workers, "remote" means a sunny beach in Bali. Governments at all levels have taken notice, realizing that digital nomads spend more money than tourists, create jobs for locals, and even start local businesses. Fifty-eight countries have decided to embrace the trend and created special digital nomad visas and other incentives for digital nomads to locate in their countries. But it also creates thorny challenges: it used to be said that only two things are certain in life, death and taxes, but digital nomads who work in multiple countries and have no clear home base certainly make it challenging to determine tax residency.

Without going as far as switching to digital nomadism, many people have been able to leverage the digital economy to generate supplemental income and even make a living (or a fortune) from it. For instance, just on YouTube, over two million channels[3] from almost a hundred countries (often individual content creators) are monetizing and receiving a revenue share from the platform. The highest-earning one, known as MrBeast, pulled in an estimated $82 million over the past year.[4]

Previously, video production was a complicated and expensive endeavor that could only be undertaken with the support of television networks. However, with the rise of digital platforms like YouTube, Twitch, and

2 MBO Partners. “Digital Nomads Report 2023.” mbopartners.com, July 2023. https://info.mbopartners.com/rs/mbo/images/2023_Digital_Nomads_Report.pdf.

3 Lyons, Kim. “YouTube Says Its Partner Program Now Has 2 Million Members.” The Verge, August 23, 2021. https://www.theverge.com/2021/8/23/22636827/youtube-partner-program-2-million-members-creators.

4 Spangler, Todd. “MrBeast Annual Earnings Hit Whopping $82 Million, More Than Double Any Other Digital Creator.” Variety, September 26, 2023. https://variety.com/2023/digital/news/mrbeast-earnings-digital-creator-income-ranking-2023-1235735506/.

TikTok, anyone with a smartphone camera and an internet connection can create and distribute content globally, with almost no barrier to entry and a global reach from day one. Even language is not as much of a barrier anymore, given the tremendous progress in AI-powered translation: companies like Spotify and Camb.ai are already offering services to translate and dub videos in more than 78 languages, with accents and dialects, all the while preserving the original creator's own voice. This has led to a democratization of content creation, where anyone can have a voice and find an audience. To put things into perspective, MrBeast has over 207 million subscribers and Comcast, the largest cable network in the U.S., has 17.5 million pay-TV subscribers. The other side of the coin is that with the "public forum" being now so open, it is now possible and even trivial for some parties (external, or not) to influence public opinion and democratic debate in some countries.

The digital economy is not only about immaterial, intangible constructs. It has a huge impact on how people buy and consume very tangible products. Coupled with the improvements in global logistics and trade networks, and programs such as the Belt and Road Initiative, it has enabled anyone to sell anything to anyone anywhere, regardless of physical or cultural borders. For example, China has long been the "factory of the world," with many global brands manufacturing their products in China, but it has historically been a challenge for Chinese brands to successfully market abroad, and only the largest and most mature companies could afford costly acquisitions and navigate culture shocks both in dealing with foreign workforce and understanding foreign customers' tastes. However, in recent years Chinese online marketplaces like Aliexpress (from Alibaba), or Temu (from PinDuoDuo) have become global e-commerce giants and are now making these products directly available to customers globally, cutting out intermediaries, reducing costs and opening new markets and opportunities, regardless of physical location. This has been a chance in many places to promote rural revitalization. For example, in the Rongjiang county of Southwest China's Guizhou province, the Moon Hometown workshop, a social enterprise co-founded by the local government and a designer of the Miao ethnic group[5] has been able to lift 120 elderly people out of poverty by providing them employment making handicrafts sold online and promoted by live streamers. On the other hand, an open global marketplace also made it easier for customers to switch to the

5 China Daily. "Social Enterprise Quells Poverty via Handicraft Sales Online." chinadaily.com.cn, September 24, 2020. https://govt.chinadaily.com.cn/s/202009/24/WS5f6c055d498eaba5051bb69c/social-enterprise-quells-poverty-via-handicraft-sales-online.html.

lowest cost producer, which has impacts on the labor market and the displacement of workers, mandating up-skilling and adaption, or a tangible risk of becoming unemployed.

One of the additional benefits of the digital economy is that it allows emerging markets to bypass some traditional stages of development and adopt new technologies quickly. For example, mobile banking has become increasingly popular in emerging markets, allowing people to access financial services without needing to visit a physical bank branch. This can reduce transaction costs, increase financial inclusion, and improve economic opportunities for the unbanked population. According to the World Bank, there are still over 1.6 billion unbanked adults, which largely excludes them from participating in global trade. As personally witnessed firsthand in my roles both as an advisor to the GSMA's Inclusive Tech Lab and as VP of Monetization at KaiOS Technologies, there is massive overlap between the unbanked and the unconnected, and once these populations are able to access the Internet, usually wirelessly through a mobile device, they are immediately able to access some kind of mobile banking or digital "value" transfer (even if just in the form of prepaid airtime or data credits) and this opens up a new world of possibilities for them, from trading beyond their local physical market, to access to credit scoring which enables them to raise capital to invest and expand their business beyond just a subsistence activity. This indicates that financial inclusion is first and foremost a matter of digital inclusion and that common connectivity is a prerequisite to common prosperity.

In an age where e-commerce parcels are delivered to the other side of the world in an average of two weeks' time (and sometimes much faster), and when more and more economic trade is in the form of impalpable digital goods and services, it is neither practical nor desirable to transfer physical currency, especially if the exchange rate is volatile. This is why a digital currency is essential for the proper functioning of a digital economy. One cannot go without the other. Currently, the global currency for the digital economy is predominantly the US dollar in some digital form, through America-led payment gateways like SWIFT, Visa, Mastercard, etc., but if Ray Dalio's book "The Changing World Order: Why Nations Succeed and Fail" is to be believed, this may not be the case forever.

The digital economy is where change is most likely to happen, due to its distinctive features of low barrier to entry, powerful network effects, and almost unlimited global reach. After all, who could have imagined in early 2008 that a pseudonymous white paper published on the Internet (Bitcoin) would lead to the creation of a multi-trillion dollar asset class of cryptocurrencies with no central banks, no government, and no central authority or backing of any sort?

Of course, a mishmash of meme coins will not be able to provide (or indeed store) much value in the long term, and it is telling that most of the exchange volume in digital currencies is realized in so-called "stablecoins" ($32 out of $38 billion over 24 hours in November 2023 according to Coinmarketcap), but the "crypto experiment" showed the appeal and convenience of a digital native currency for a digital economy.

Many countries are developing or exploring CBDCs (Central Bank Digital Currencies), which is the digital form of a country's fiat currency that is issued and regulated by the central bank, but in a digital manner similar to cryptocurrencies. For example, China has launched a pilot program for its e-CNY. The European Central Bank is considering a digital Euro that would rely on a permissioned blockchain network operated by licensed financial institutions. On this front, Asia is clearly leading the way: the Hong Kong Monetary Authority (HKMA), besides launching a pilot program for its e-HKD, has already completed a successful pilot in October 2022 for a multi-CBDC initiative, called m-Bridge, that aims to improve cross-border payments using a common platform based on distributed ledger technology (DLT), in cooperation with the Bank for International Settlements Innovation Hub (BISIH) Hong Kong Centre, the Bank of Thailand, the Digital Currency Institute of the People's Bank of China and the Central Bank of the United Arab Emirates.

Besides the opportunities and challenges evoked so far, this new digital world has sadly also brought new digital threats and requires appropriate measures for the protection of privacy, security, and trust.

Cyberattacks, data breaches, and identity theft are increasingly common and more dangerous as we become more interconnected. The technological progress, in particular now with AI, makes it trivial to create convincing deepfakes and undermine trust, as demonstrated by

a video of former president Barack Obama delivering a speech that he never actually gave[6].

Just as it can be a force for good, low barrier to entry and powerful network effects provide an opportunity for asymmetric results that can wreak havoc. There are no digital borders so to speak, and since nefarious activities can now be perpetrated by anyone from anywhere, it makes it all the harder to defend against.

How to regulate, and most importantly, enforce and police, against new forms of crime when the pace of technological change advances so fast? How to identify and catch the criminals when they are located in a different country, and maybe even leveraging compromised servers in yet another third-party nation? The only way forward will be through closer international cooperation between countries, as demonstrated by the recent joint effort between China and Laos that led to the arrest and extradition of 164 individuals suspected of defrauding Chinese citizens online[7]. One can't help to wonder what would have happened, had these suspects been digital nomads from a third-party, less cooperative nation. Is it even possible for all countries to cooperate on this when their values or interests may differ in no small way? Will this lead to the emergence of a splintered Internet and a multipolar world?

In conclusion, though the digital economy has, and will certainly continue to produce tremendous economic value for an increasingly large number of people as it becomes more inclusive, this is not without pitfalls. Its immaterial, intangible nature, which blurs physical, national, cultural, economic, and legislative borders, creates a slew of thorny challenges for governments at all levels to address without killing the golden goose, but this also opens up a vast array of new opportunities for individuals and governments to challenge the status quo, build a more inclusive and prosperous future for everyone and maybe, make one world one dream a reality. Or it could lead to a multipolar world of wary blocks trying to isolate from each other by building walls into the ether. The choice is ours: do we want to use the digital economy as a tool for cooperation and integration, or for conflict and fragmentation? That question is left as an exercise for the reader. The answer will shape the destiny of our planet and humanity.

6 Fagan, Kaylee. "A Viral Video That Appeared to Show Obama Calling Trump a 'dips--' Shows a Disturbing New Trend Called 'Deepfakes.'" Business Insider, April 18, 2018. https://www.businessinsider.com/obama-deepfake-video-insulting-trump-2018-4.

7 Zekun, Yang. "Fraud Suspects Handed over to Chinese Police by Laos." Asia News Network, September 12, 2023. https://asianews.network/fraud-suspects-handed-over-to-chinese-police-by-laos/.

Geotechnological Rivalry in the Data Economy

Daniel Araya

Senior Partner with the World Legal Summit
Senior Fellow with the Centre for International Governance Innovation (CIGI), Canada

"There are decades where nothing happens; and there are weeks where decades happen."

—Vladimir Lenin

The world has entered a new period in history, marked by the gradual emergence and ascendance of a new global order. With the rise of Asian economies especially China, a new architecture of economic, political, and technological integration is taking shape. Beyond the bipolar order of the Cold War or the unipolar order of American hegemony, the global system is now becoming "multipolar." This essay argues that the rise of technology rivalry between the United States and China provides a framework for understanding the contours of this new order.

Transformation in the name of innovation is critical to understanding this new era of great power rivalry. Where conventional forecasts on technological change often assume that innovation replaces old

technologies on a one-to-one basis, the reality is that general-purpose technologies like artificial intelligence (AI) and machine learning tend to disproportionately replace old systems with dramatically new architectures, boundaries, and capabilities.

As AI and robotics move geopolitical competition onto a new playing field, the scramble to dominate a data-driven economy is now reshaping the global balance of power. Rather than centering on any one country alone, power itself is becoming increasingly fluid as nations compete and cooperate in the pursuit of *geotechnological* advantage. Governing this global innovation economy across a contested multipolar system could prove especially daunting.

China and the Commanding Heights

As innovation moves to the core of the global economy, geopolitical leadership is now interdependent on technological leadership. Much like the mechanization of steam power in the late 18th century, and the electrification of mass production in the mid-19th century, new technologies are now restructuring the *commanding heights* of the global economy.

No country is more fundamental to this new era than China. Even as the US continues to lead in cutting-edge sectors such as machine learning, biotechnology, and quantum computing, China has emerged as a new center of gravity. This shift in the global balance of power reflects the rise of new centers of influence and the decline of America's "unipolar moment."[1] In this new multipolar era, power is not equally distributed, nor is there a lack of hierarchy among global centers of influence. Rather, power is increasingly becoming embedded within competitive multilateral networks.

No resource is more important to a multipolar era than AI. Together with quantum computing and biotechnology, AI is advancing quickly and represents uncharted territory in the evolution of a data economy. In fact, for many experts in the field, the recent acceleration in both the power and scope of AI has raised fears that the technology is evolving too quickly. What is obvious is that as AI continues to underwrite the convergence of human and machine intelligence, it will continue to reset the global order.

1 Krauthammer, C. (1990). "The Unipolar Moment," Foreign Affairs, Vol. 70, No. 1 (Winter), pp. 23–33.
Khanna, P. (2019). The Future is Asian. New York: Simon and Schuster.

Building on advances in semiconductor chips and improvements in machine learning protocols, AI now sits at the epicenter of a vast innovation economy. The capacity of AI to both automate labor and accelerate innovation portends far-reaching changes in the global order. "Machine knowledge capital"— which is essentially industrializing the process of learning itself— has begun accelerating the pace of innovation.

Where innovation in the knowledge economy ensured that intellectual property (IP) captured the lion's share of economic rents, AI has begun to transform the nature of innovation itself. In fact, both industrial production (manufacturing) and knowledge-based innovation (IP) are becoming subsumed by competition to control the global data economy.

Figure 1: Stages of Technological Change

Industrial Revolution	Time Period	Key Characteristics
Industry 1.0	Late 18th century - early 19th century	Introduction of mechanization powered by water and steam. Transition from hand production methods to machines. Development of iron and textile industries.
Industry 2.0	Mid 19th century - early 20th century	Mass production through electrification and assembly lines. Advancements in transportation and communication technologies. Rise of steel, oil, and automotive industries.
Industry 3.0	Late 20th century - early 21st century	Automation and computerization with the advent of electronics and information technology. Introduction of computers, robotics, and programmable logic controllers. Growth of telecommunications and internet industries.
Industry 4.0	Mid 21st century - present	Integration of cyber-physical systems and advanced digital technologies. Internet of Things (IoT), big data analytics, artificial intelligence (AI), and machine learning. Smart factories, autonomous systems, and decentralized decision-making.

Multipolarity and the Rise of China

No country is more fundamental to this multipolar era than China. Bolstered by its dynamic innovation sector and an unrivaled export economy, China's ascendance is exerting a gravitational pull on the global order.[2] As a recent report for 2023 by the Australian Strategic Policy Institute concludes, "China has built the foundations to position itself as the world's leading science and technology superpower."[3] With 60 percent of the world's total 5G base stations (2.73 million), 50 percent

2 One clear example of this shift is the struggle to dominate the semiconductor industry. China's recent breakthrough with the Kirin 9000S signals a new phase in Chinese innovation. Competition in the semiconductor industry is not just about economic dominance but also about technological leadership, national security, and geoeconomic influence over frontier technologies.

3 Australian Strategic Policy Institute (2023). ASPI's Critical Technology Tracker: The Global Race for Future Power. Retrieved from: https://www.aspi.org.au/report/critical-technology-tracker

of installed industrial robots, and 66 percent of the world's high-speed rail (40,000 km), China is now a global technology leader.

The intensifying rivalry between the United States and China mirrors a palpable shift in the global balance of power.[4] Where the US emerged as a "global hegemon" at the end of the Cold War, China's rising technology and manufacturing capacity is drawing much of the world into a shared orbit. China's enormous market and expansive technology industries are moving it into direct competition with both the United States and Europe.

In truth, the development and application of frontier technologies have always been intimately tied to changes in the global order. Like sedimentary layers, each new stage of technological advancement reshapes the balance of power, leading to increasingly complex social relations (Figure 1). As each new substrate of innovation builds on the last, new disruptive technologies take root, driving a creative explosion in commercial applications.

Leveraging decades of investments in manufacturing, telecommunications, transportation, energy, and education, China's signature Belt and Road Initiative (BRI) is now underwriting a new multipolar trading system. Together, Chinese-led initiatives such as the Asian Infrastructure Investment Bank (AIIB), the BRI, the Global Security Initiative (GSI), the Shanghai Cooperation Organization (SCO), and the BRICS[5] trading blocs are integrating what geopolitical strategist Halford Mackinder once described as the "World Island." Comprising the interlinked continents of Africa, Asia, and Europe (Afro-Eurasia), Mackinder saw this economic configuration as the largest and most powerful geopolitical combination possible.

Rivalry between the US and China has catalyzed widespread fear that a new Cold War is on the horizon. Indeed, for many in the West, a new Cold War era has already begun. However, even as heightened tensions and divergent strategic interests undermine U.S.-China relations, geopolitical rivalry between the two countries faces significant limits. Taken together, (i) a tightly coupled global trading system, (ii) the expanding influence of regional powers (e.g., India, Saudi Arabia, Russia, Iran, Türkiye, Brazil, Indonesia, and South Africa), and (iii) the existential

4 It is important to recognize that multipolarity does not mean that major powers possess equal strength or influence. Rather, multipolarity signifies a world where there are multiple actors with varying levels of power and capabilities.

5 The BRICS bloc includes Brazil, Russia, India, China, South Africa and now six additional countries: Argentina, Egypt, Ethiopia, Iran, Saudi Arabia, and the United Arab Emirates, with more countries expected to be included next year.

risk of nuclear confrontation, places specific constraints on U.S.-China rivalry.

Competing in the Data Economy

China's growing influence in the data economy has been met by a US strategic focus on export controls and calls for "economic decoupling" across many Western capitals. Taken together, US and Chinese companies dominate the global data economy. The market capitalization of US firms, Apple ($2.8 trillion), Microsoft ($2.4 trillion), Amazon ($1.3 trillion), Alphabet ($1.6 trillion), and Meta ($754 billion) is increasingly balanced by rising Chinese firms like Alibaba ($228 billion), Tencent ($423.23 billion), Meituan ($102 billion), and Baidu ($50.4 billion).

With the rollout of 5G edge networks, it is anticipated that there will be an explosion of data created, collected, processed, and stored. Indeed, even though the Internet of Things (IoT) encompassed 10 billion devices in 2018, it is projected to reach 64 billion by 2025 and possibly many trillion by 2040 (National Intelligence Council 2021). Measured by bandwidth, cross-border data flows grew roughly 112 times over 2008 to 2020.[6]

Just as fossil fuels powered the rise of combustion technologies, data now feeds the computational engines that drive technological discovery. Nations that possess extensive data repositories or have the kinds of companies that dominate IP regimes gain enormous leverage in shaping a changing geoeconomic landscape. More to the point, nations that lead in this new computational era have the capacity to shape the contours of the global economy.

Strategies for Competing in the Data Economy Include a Focus on:

1. **Market Dominance:** An acute understanding that market competition in the race for technological dominance— particularly in emerging technologies such as AI, 5G networks, quantum computing, and autonomous robotics— will have significant implications for economic competitiveness, national security, and geopolitical leverage.

6 In 2018 alone, 330 million people made online purchases from other countries — each transaction involving the transmission of data driving $25.6 trillion in cross-border sales — even though only 60 percent of the world is online.

2. **Data sovereignty:** Control of data. As centers of deep technological innovation, both the US and China now seek to protect their data and establish control over data flows, often through regulatory measures. This includes an intense focus on data localization requirements, cross-border data transfer restrictions, and data protection regulations.

3. **Cybersecurity and surveillance:** Extensive cyber surveillance and cyber warfare activities in order to access valuable data, disrupt information systems, and protect data from espionage. This includes hacking, intelligence gathering, and the deployment of offensive cyber capabilities.

4. **Soft power:** Data is seen as a tool for geopolitical influence and soft power projection. This includes the use of the media to shape global narratives, control information flows, and influence international public opinion through the use of social media campaigns, media manipulation, and targeted attacks.

Even as the move from mass industrialization to knowledge-based innovation enabled the outsized influence of US research universities and the unipolar moment, the global economy is increasingly being reconfigured around data. As Harvard scholar Shoshanna Zuboff explains, data has been transformed from "data exhaust" into a feedstock for computation.[7] "Data is the new oil."[8]

As the world's major powers compete to harness and control data, technology platforms have become critical to geostrategic leverage. Notwithstanding the fact that most of the world's leading tech firms were formed only relatively recently (e.g., Facebook in 2004; Twitter in 2006; Instagram in 2010; TikTok in 2016), the data they manage has become critical to great-power rivalry. Indeed, the technology industry and its global supply chains now rival the oil and gas industry in terms of their importance to the global economy.

Rather than controlling single industries, tech platforms use "competitive bottlenecks" to aggregate and harvest user data.[9] The value of this data to commercial enterprises is obvious. The collection and analysis of user data enables commercial firms to continually optimize and

7 Zuboff, S. (1988). In the Age of the Smart Machine: The Future of Work and Power. New York: Basic Books.

8 Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs.

9 Iansiti and Lakhani, (2017). Managing Our Hub Economy. Harvard Business Review. Retrieved from: https://hbr.org/2017/09/managing-our-hub-economy?utm_medium=social

tailor their products and services. While this powerful feedback loop can dramatically improve existing business models, it also ensures that personal data can be monetized, often without the consent or awareness of users. Struggles over the issue of digital surveillance and personal privacy have become fundamental to debates on the data economy, and governments have been balancing between national security and individuals' right of privacy. In the US, Edward Snowden's disclosure of the PRISM[10] program exposed the enormous scale of surveillance deployed by the National Security Agency (NSA) and other US agencies in monitoring both its domestic population and populations abroad. Many global tech giants are also broadly seen as tools of the governments to strengthen their power.

Governing the Data Economy

Much as AI is now critical to economic development, so the data economy has become fundamental to debates on global governance. Unleashing a plethora of new tools for driving propaganda and behavior modification, data-driven technologies have dramatically expanded the potential for social and political fragmentation. The current scramble to regulate tech firms in the context of a rising data economy has awakened many of the world's governments to the very real challenges that data-driven technologies pose.

Notwithstanding US and Chinese leadership in innovation, no country will have a monopoly on data-driven technologies. Given extensive cooperation among researchers and leading commercial enterprises, advancements in AI and machine learning will continue to diffuse globally. As digitally networked technologies become cheaper and more widely available, technology proliferation will democratize access to AI and other disruptive technologies across a multipolar system.

With these challenges in mind, policymakers have begun moving to align digital technologies with a raft of new standards. However, given the scale and scope of the data economy, no single nation or region will have the capacity to regulate the data economy alone. Indeed, as regions with divergent approaches to privacy and data protection clash over global standards and regulations, geopolitics is becoming a particular concern. Ultimately, the resolution of these tensions will

10 PRISM is an acronym for Planning Tool for Resource Integration, Synchronization, and Management.

determine whether technological innovation is marked by collaboration or fragmentation.

Conclusion

What is clear is that we are living through an interregnum— a period in history that bridges a fading industrial era dominated by Western countries and a new digital era underwritten by China and a vast Asian trading system. Since the end of World War II, American predominance has depended on a network of alliances overseen by a sprawling US military. As the U.S.-led order winds down, Western influence over the global system is beginning to wane.

As AI and machine learning move geopolitical competition onto a new playing field, the scramble to dominate a data-driven economy will continue to reshape the global balance of power. In the decades ahead, frontier technologies including AI, robotics, quantum computing, 6G telecommunications, genetic engineering, renewables, and nanotechnology will be the basic building blocks of a competitive multipolar order.

Intensifying rivalry between the United States and China underscores a seismic shift in the global balance of power. As data-driven technologies proliferate, power is being redistributed from older centers of influence to newer centers of influence. Nations that do not have a strong presence in the data economy could find themselves marginalized or dependent on players that do. This likely risks a return to hard power diplomacy and the competition for resources. For this reason, regulating the data economy could prove daunting.

Whether the world's governments collaborate in the pursuit of global governance or simply yield to the temptation to centralize power will depend on our shared capacity to build multilateral engagement. In this increasingly unstable environment, the pursuit of national interest at the expense of managing shared technological, economic, and environmental challenges could prove disastrous. Indeed, even as a global data economy sets the stage for a new digital battleground, multilateral cooperation will remain vital to maintaining peace and security across an ever-changing multipolar system.

References

Araya, D. (2018). *Augmented Intelligence: Smart Systems and the Future of Work and Learning*. New York: Routledge.

Araya, D. and P. Marber (Eds) (2023) *Augmented Education in the Global Age: Artificial Intelligence and the Future of Learning and Work*. New York: Routledge.

Australian Strategic Policy Institute (2023). ASPI's Critical Technology Tracker: The Global Race for Future Power. Retrieved from: https://www.aspi.org.au/report/critical-technology-tracker

Chin, J. and L. Lin (2022). *Surveillance State: Inside China's Quest to Launch a New Era of Social Control*. New York: St. Martin's Press

Ciuriak, D. (2023) How the Digital Transformation Changed Geopolitics. Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4378419

Herman, E.S. & Chomsky, N. (1988). *Manufacturing Consent: The Political Economy of the Mass Media.* New York: Pantheon Books.

Iansiti and Lakhani, (2017). Managing Our Hub Economy. Harvard Business Review. Retrieved from: https://hbr.org/2017/09/managing-our-hub-economy?utm_medium=social

Khanna, P. (2019). *The Future is Asian*. New York: Simon and Schuster.

Krauthammer, C. (1990). "The Unipolar Moment," *Foreign Affairs*, Vol. 70, No. 1 (Winter), pp. 23–33.

Levine, Y. (2018). *Surveillance Valley: The Secret Military History of the Internet*. New York: PublicAffairs.

Mayer-Schönberger, V. and Ramge, T. (2018). *Reinventing Capitalism in the Age of Big Data.* New York: Basic Books.

Menn, J. (2020). Spy Agency Ducks Questions About 'Back Doors' in Tech Products. Retrieved from: https://www.reuters.com/article/us-usa-security-congress-insight-idUSKBN27D1CS

National Intelligence Council. 2021. *Global Trends 2040: A More Contested World*. March. Retrieved from: www.dni.gov/files/ODNI/documents/assessments/GlobalTrends_2040.pdf.

Price, D.H. (2022). *The American Surveillance State: How the U.S. Spies on Dissent*. New York: Pluto Press.

PRC State Council (2015). Made in China 2025. Retrieved from: https://cset.georgetown.edu/wp-content/uploads/t0432_made_in_china_2025_EN.pdf

Romei, Valentina and John Reed. 2019. "The Asian century is set to begin." *Financial Times*, March 25. www.ft.com/content/520cb6f6-2958-11e9-a5ab-ff8ef2b976c7.

Seymour, R. (2019). The Twittering Machine. London: The Indigo Press.

Slaughter, Matthew J. and David H. McCormick. 2021. "Data Is Power: Washington Needs to Craft New Rules for the Digital Age." *Foreign Affairs,* May/June. www.foreignaffairs.com/articles/united-states/2021-04-16/data-power-new-rules-digital-age.

Srnicek, N., (2017). *Platform Capitalism*. London: Polity.

Thadani, A. and G. Allen (2023). Mapping the Semiconductor Supply Chain: The Critical Role of the Indo-Pacific Region. Retrieved from: https://www.csis.org/analysis/mapping-semiconductor-supply-chain-critical-role-indo-pacific-region

Yergin, D. and J. Stanislaw (1998). *The commanding heights: the battle between government and the marketplace that is remaking the modern world* (1). New York: Simon & Schuster.

Zuboff, S. (1988). *In the Age of the Smart Machine: The Future of Work and Power.* New York: Basic Books.

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* New York: PublicAffairs.

TIO Spotlight Talk

AI and Digital Economy: Technologies Threatening and Shaping the World

Thorsten Jelinek

Senior Fellow and Europe Director, Taihe Institute
Former Associate Director at the World Economic Forum (2011-2014)
Author of *The Digital Sovereignty Trap*

TIO The White House has recently issued an executive order on AI, the United Kingdom had an AI safety summit on November 1, The UN has set up an AI advisory group, and Xi Jinping addressed AI governance at the 3rd Belt and Road Forum for International Cooperation (BRF). How do you see the role of policy and governance affecting the future of AI?

Jelinek I would add the following to that list: Firstly, the EU AI Act's final negotiation, or trialogue, is set for December 6. Additionally, China is increasingly implementing comprehensive AI regulations, including rules for foundation models. Notably, during the UK AI Safety Summit in November, U.S. Vice-President Kamala Harris announced a 31-country declaration to establish guidelines for the military use of AI, addressing what the Pentagon terms as "Battle-ready AI." This is a significant issue, although the U.S. stops short of supporting a full ban on autonomous "killing robots."

Globally, we are experiencing a second wave in discussing, and increasingly implementing, AI principles and regulations. The current surge is driven by the breakthroughs in generative AI, whose potent technology and natural language-based, intuitive user interface impacts societies directly. Access to this technology is widespread, at least in more affluent nations. The first wave, peaking around

2020, saw a myriad of non-binding, human-centric AI frameworks emerge, propelled by various governments, large businesses, and international institutions. This initial response was a reaction to substantial advancements in AI, fueled by machine learning and big data, and primarily due to irresponsible use in consumer spaces, especially social media. The first wave made us aware of the inadequacy of existing regulations and values in ensuring responsible, safe, and secure AI development and application.

Now, the Bletchley Declaration from November 1, the U.S. President's Executive Order on AI, the G7's International Guiding Principles and International Code of Conduct for AI, and the final phase of the EU AI Act negotiations exemplify this second wave. These developments emphasize AI risks and the need to transition from principles debates to concrete actions. Regulations serve dual purposes: mitigating potential and existing risks and creating certainty and trust, necessary for beneficial technology use. Legal guardrails not only constrain behavior but are often essential for markets to function properly.

There are tremendous benefits associated with AI, however, we can rather observe a public discourse that focuses predominantly on the immediate and existential risks that have been attributed to AI technologies. Obviously, the industry tends to emphasize the former and wouldn’t like to be constrained, especially in Europe which is lagging behind the U.S. and China. To strike a balance between innovation and regulation, Europe is considering a "tiered approach" that broadly differentiates between foundation and generative AI models, or between the general AI technology and its applications. This approach focuses on regulating both areas, incorporating measures for AI safety, transparency, and specific risk categories. However, there remains a debate over whether the regulatory provisions for foundational models should be mandatory or voluntary. In addition to addressing the issue of discriminating large AI models, originating from the U.S., the regulation of foundation models presents challenges, as providers of these models cannot foresee all potential use cases and the associated risks.

Furthermore, smaller businesses that develop AI applications based on these foundation models are concerned about being held liable for risks inherent to the foundation models themselves, seeking clarity on responsibility distribution. Contrary to months of extensive deliberations in the EU Parliament and the stance of numerous leading AI experts advocating for the regulation of large-scale foundation models, Germany, France, and Italy have recently put forward a proposal advocating a voluntary approach towards the regulation of these models.

From a big tech perspective, there's been a noticeable shift in attitudes towards AI governance over the past years. Initially, AI advancements led to technology optimism, then shifted to technological realism, marked by self-governance and the emergence of ethics boards due to public pressure and regulatory gaps. Interestingly, despite the absence of formal regulations, big tech is now urging lawmakers to impose them. This paradox—excitement about generative AI coupled with warnings from its creators about its risks—reflects AI's disruptive nature. However, some argue this paradox indicates big tech's desire to maintain competitive advantages, as they are better equipped to comply with regulations. Regulations could not only privilege existing large-scale AI providers, but also hinder AI technology transfer to less affluent regions, potentially creating new asymmetries.

This situation mirrors historical precedents. The early U.S. telecommunications and railway industries were initially unregulated, almost leading to chaos. Subsequent government regulation introduced certainty but also led to monopolies that lasted almost the entire 20th century. This not only created a rent-seeking environment domestically but also established a technology hegemony internationally, hindering technology spread to smaller and developing countries. Therefore, we must approach with caution when businesses push for their own regulation. Beyond the realm of regulations, there's a pressing need for a revamped approach to business ethics.

A new ethical framework should not merely be rooted in goodwill. Instead, what is required is a new moral political economy that fundamentally rethinks the interplay between technology, society, and economic systems. This approach should integrate ethical considerations into the very fabric of business operations and decision-making processes, especially in the context of powerful technologies like AI. Such a shift is essential not just for mitigating risks, but also for ensuring that AI and other emerging technologies contribute positively to societal progress, global equity, and sustainability.

TIO With multiple interest groups seeking to govern AI, where do you see possibilities for multilateral intersect, if any? In your recent book, *The Digital Sovereignty Trap*, you talk extensively about technology silos. Will AI follow a siloed path, and should it?

Jelinek The recent UK AI Safety Summit was a significant success, marked by the signing of the Bletchley Declaration on AI Safety. This event was notable for the involvement

of global stakeholders, including major competitors like the U.S. and China, who jointly endorsed such AI declaration for the first time. This development is encouraging, signaling shared concerns about AI safety and security, and the collective responsibility of stakeholders. Although the declaration is non-binding and doesn't fully address the immediate challenges associated with AI, its symbolic significance highlights a positive shift towards dialogue and consensus in global AI governance.

And yet, I believe for now we are still moving towards greater division and fragmentation in global collaboration. This trend is evident in the UK government's intention to establish itself as an international AI testing hub for foundation models and generative AI during the launch of the UK AI Safety Summit. This initiative would have implied testing AI models for vulnerabilities, a role the UK is not formally mandated to perform. It's highly unlikely that U.S. and Chinese AI technology firms would submit their models for safety inspection. Contrarily, the UK established its own safety institute, and the U.S. followed suit with its own under the National Institute of Standards and Technology (NIST). Meanwhile, China enforces regulations for testing AI models in its own technology sector. In Europe, France, in collaboration with Canada, initiated a Global Partnership on AI (GPAI) in 2021, focusing on multistakeholder engagement. The competition has extended beyond AI technology leadership to normative aspects like values, regulations, and operation testing. The EU, with its AI Act, akin to the General Data Protection Regulation (GDPR), aims to extend its regulatory approach globally in AI.

If the development is left unchecked, we could be heading towards a techno-polar world, dominated by a few major technology companies, exerting substantial influence over the economy and society. However, it's unlikely that governments and societies will permit such a scenario. Instead, we might see the AI landscape largely divided between the U.S. and China influences. In such fierce competitive context, the Global South is advocating for its own digital sovereignty, unwilling to be subordinate to either the U.S. or China, and seeking control over their own data, a vital element in AI. Despite the legitimate demand for digital sovereignty, such divisions and fragmentation could be detrimental to innovation, creating barriers rather than fostering collaborative advancements.

TIO In your book, you also talked extensively about information security. Do you have any thoughts on how AI will disrupt this?

Jelinek The Bletchley Declaration underscores the significance of AI safety and security, a

theme that resonated strongly at the UK AI Safety summit, distinguishing it from other gatherings. This attention mirrors societal and governmental concerns about the crucial role of cyber-security and the preservation of societal integrity. Similar with nuclear energy before, there is currently no other technology that has reached such global alignment despite the fierce competition for AI leadership. Present challenges such as hate speech, disinformation, bias, and the psychological and societal impact of the attention economy are pressing. As I explore in my book, these evolving risks mark a pivotal shift in the cyber-security and privacy landscape, disrupted by AI. This includes both an intensification of existing threats and the emergence of new threats, new dilemmas and unforeseen accidents. Arguably, the most significant and hazardous AI threat might be its intentional, malicious use, rather than AI inadvertently causing harm. I think this was also the consensus at the UK AI Safety Summit.

With OpenAI's success, we are generally witnessing an even faster and broader adoption of even more powerful AI, including the rise of open-source models. This evolution further alters and amplifies the risk landscape, alongside unprecedented liability issues. Thus, we also see demands to regulate not only proprietary, but also open-source models due to safety and liability concerns. Who should be regulated most, the providers or the application developers and users? It is challenging for foundation model providers to predict every potential use case of generative AI. A tiered regulatory approach, as proposed by the EU and highlighted in the Biden-Harris Executive Order, advocates for imposing strict guardrails on the largest models, thereby safeguarding against risks while allowing for continued innovation in smaller models. This could be a way forward without stifling innovation.

Just because various risks associated with AI have been identified doesn't necessarily mean that all of them will materialize. There is also an explanation why we see both utopian and dystopian projections of AI. This has something to do with our often-times one-sided understanding of our own existence as humans. We are once again gravitating towards physicalism and neuralism, asserting that we are solely a product of the mind and not matter. This perspective posits that our brain and body are mere algorithms, comprehensible through math and statistics. However, such dominant scientific posture inherently presents a paradox, which is using abstract ideas to bridge the mind-matter gap to understand the latter, like a “divine” act for which we don’t have any proof.

It is essential to recognize that today’s AI merely represents statistical relationships among the artifacts of human thought or models of thought. It does not replicate

human thinking, which is a biological sense process akin to sight, smell, hearing, taste, and touch. The new dualists place algorithms at the core of human existence, effectively embracing post-humanism as utopia or dystopia. This outlook challenges the notions of human agency and self-determination, and these fundamental aspects of our humanity are currently at risk of being eroded by such radical images of human existence. Consequently, it's important to recognize AI for what it is: a powerful enabling technology with a significant societal impact, rather than an entity with human-like cognition or consciousness.

TIO Do you feel AI could lead to inequality in the digital economy, or lead to other problems with national equality?

Jelinek Less addressed in the discourse is how previous economic development models, relying on the industrial absorption of rural labor in developing countries, risk obsolescence due to rapid advancements in AI-driven automation and a renaissance of industrial policies. This shift, coupled with the growing trend towards digital sovereignty, has already begun to blur the lines between the legitimate right of self-determinacy and protectionism or technology nationalism. Such changes pose significant challenges to the existing paradigms of global economic development. For a better understanding of what is happening today, it is worthwhile to look back on the history of telecommunications, which I have also done in my book.

In the past century, the telecommunications sector was controlled by Western nations such as the U.S., UK, Germany, France, as well as Japan. These countries focused on maintaining their monopolistic structures nationally and limited competition internationally, and showed little interest in transferring technology to the developing world. This stance was, in part, supported by the International Telecommunication Union (ITU), which didn't facilitate technology transfer for accelerating development in less affluent nations. The monopolistic structure and high investment barriers prevented many countries from entering the telecommunications sector and developing their own nascent technologies. China, however, was an exception, breaking through this global technology asymmetry with national technology programs, importing foreign technology, and fostering local competition and ecosystems.

Eventually, the telecommunications sector underwent deregulation and liberalization, driven by the rise of liberal values and the advent of the Internet in the 1980s and 1990s. However, what I describe as a "return of sovereignty" or "the

great re-regulation" today risks repeating the past century's pitfalls by erecting new barriers and asymmetries. In light of the telecommunications history, the criticism of China for coercive and unfair practices rather mirrors past Western industrial practices. This reflection raises concerns about potentially repeating these patterns in the current era of AI-driven digitalization.

TIO What would be your suggestions for avoiding these pitfalls?

Jelinek Effective collaboration cannot be left to chance; it requires political will and strategic foresight. As Walter Benjamin aptly put it, sometimes on history's train, one must pull the emergency brake. This is particularly true for pressing issues like climate change, where prolonged inaction has been detrimental. Our experience with climate change underscores the vital need for collaborative approaches, a lesson equally applicable to AI, given its profound impact already today and as a future frontier technology. These are multifaceted challenges that no single government can tackle alone.

Reflecting on the era of neoliberal capitalist globalization during the 1990s and 2000s, which came to a halt post-2008, thus overturning the brief Fukuyamaist period, it is crucial to distill lessons not only from this era, but also from previous industrial revolutions that caused damages to the world. The global economy continues to grapple with the repercussions of this seismic shift. While neoliberalism and capitalism represented progress over nationalist values and feudalism, governments succumbed to the pitfalls of hyperglobalization, undermining social cohesion and destroying nature. Today’s global system is still faltering, burdened by its own moral deficiencies. Technology itself is not to blame, but technologist behavior with old incentive structures, which has failed to take seriously, counter and mitigate externalities. We are now confronted with a similar risk in the realms of hyperdigitalization. It is imperative for governments to step in and collaborate effectively to address these challenges.

However, navigating the 21st century requires more than just emphasizing collaboration and goodwill. As mentioned earlier, a one-sided appreciation of humanity – like understanding human nature as a set of algorithms – provokes dystopian and utopian views, which are not helpful in tackling today’s challenges. Without a balanced approach to technology and economics, AI capability and value alignment, thus coupled with a shared moral framework and political intervention, we risk letting technology evolve without ensuring it serves society's best interests.

I believe we might only witness the establishment of a global AI regulatory body, similar to the International Atomic Energy Agency, as we approach the development of Artificial General Intelligence (AGI). The timeline for when this will occur remains speculative. Recent discussions on AI safety have underscored the need for businesses to ensure the safety of AI systems, not mainly regulators proving their unsafe. Clearly, reliance should not be placed on lawmakers alone to constrain businesses in the face of a system that motivates abusive behavior. For this to happen, we do need a new set of incentives, and those incentives must promote a new moral political economy that ensures that AI is used for the benefit of society, and promotes resolving humanity's greatest challenges, including climate change, health, hunger, and inequality.

This interview was conducted by Evan Tangen, TI Youth Observer - Digitization and Analytics.

Youth Voices

Artificial Intelligence and Infinite Monkeys

Black Boxes, Open Source, Information Security Flow, GPU Class Wars, Training Packages, and Infinite Monkeys

Evan Tangen

TI Youth Observer - Digitization and Analytics

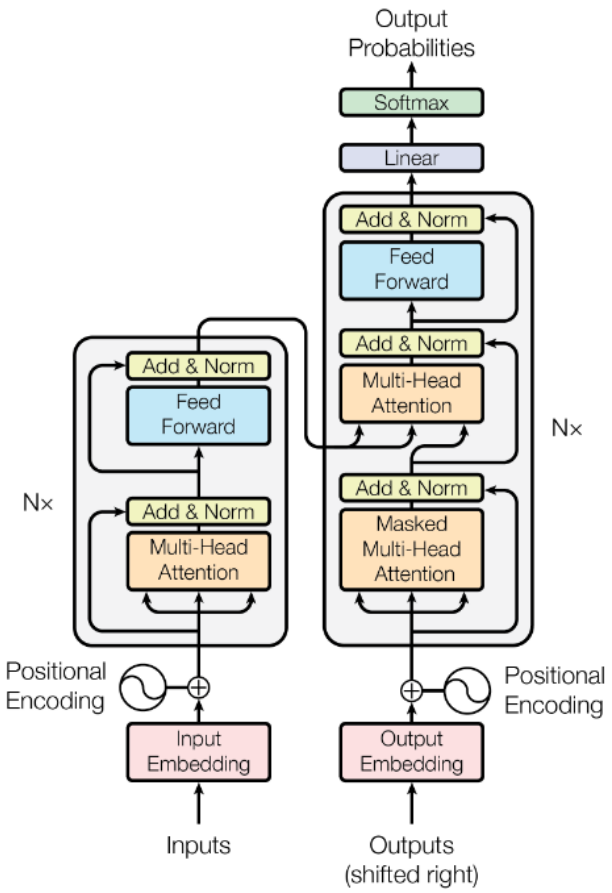
What Is "AI" in 2023?

“AI” has become the in-vogue buzzword of 2023. Spurred by the advent of ChatGPT, everyone from machine learning (ML) engineers, to venture capital investors, to former NFT hawkers clad in colorful brand-name jumpsuits have begun rebranding themselves as “AI” experts or enthusiasts.

The term "AI," as it is commonly understood following the emergence of ChatGPT, refers to large language model (LLM) programs utilizing a transformer or transformer variant architecture capable of producing generative outputs when queried in natural language (any communication form not optimized for digital interpretation). The term “AI” is in fact misleading, as it is not actual artificial intelligence. Open AI, Google, and Meta’s “AIs” are better described as high-end automation with outstanding natural language processing (NLP) systems.

Transformer model ML systems and the components needed to assemble them have been around for years. Google first published a paper detailing the transformer model, the core of ChatGPT, in 2017.[1] What brought “AI” into prominence was not innovation, but actually clever marketing and a consumer-friendly interface that Open AI executed almost flawlessly at launch.

1 Vaswani, Ashish, Shazeer, Noam, Parmar, Niki, Uszkoreit, Jakob, Jones, Llion, Gomez, Aidan N, Kaiser, Łukasz and Polosukhin, Illia. "Attention is all you need." Paper presented at the meeting of the Advances in neural information processing systems, 2017.



In addition to a transformer or variant deep learning model, an LLM also requires a training package. These are typically assembled utilizing a staggering amount of low-cost human oversight. ChatGPT's training package was assembled using companies including Sama[2], a US-based outsourcer who assembled a veritable army of low-cost laborers from countries including Kenya to wade through incalculable amounts of content and outputs. The use of low-cost overseas outsourcing for training is not new. Indeed, it is widely used by Meta, Google, and almost every other company that assembles large-scale automations.[3]

Black Boxes

The base components and structure of LLMs are known to the public, but specific insights into the weights and controls implemented by Open AI and Google are opaque. Justifications for black boxes are multifaceted, but the primary stated objective is always some variation of warding against emulation and tampering.

What is inside a black box is not always as sophisticated or effective as

2 Perrigo, Billy. "OpenAI Used Kenyan Workers on Less than $2 per Hour: Exclusive." Time, January 18, 2023. https://time.com/6247678/openai-chatgpt-kenya-workers/.

3 Tan, Rebecca, and Regine Cabato. "Behind the AI Boom, an Army of Overseas Workers in 'Digital Sweatshops.'" The Washington Post, August 29, 2023. https://www.washingtonpost.com/world/2023/08/28/scale-ai-remotasks-philippines-artificial-intelligence/.

marketed. Sometimes it is an advanced proprietary system, sometimes it is a legacy system supported by lots of manual labor, and sometimes it is "empty." A drastic example of an empty black box is Alameda Research, where a supposed top-secret investing algorithm turned out to be nothing more than appropriated funds from users on the FTX platform, supported by manipulation of a self-produced cryptocurrency.[4]

Black boxes create an environment where unethical actors can create fabrications by presenting output, or a supposition of output, as proof of process because "a proprietary system did it." It is worth noting that in the case of Open AI and Google LLMs, we know the black box (training package + transformer model) is not "empty," but the controls and influences on the outputs are not transparent.

Open Source

Some maintain that the black box model currently employed by Google and Open AI could be overtaken by the collective user consciousness or "infinite monkeys" of the internet, clacking away at independent open-source LLM projects. Meta, in contrast to Google and Open AI, embraced this paradigm with the release of Llama 2, a compact, open-source LLM explicitly intended as a development base for independent LLM projects.[5] In short order, Llama-based independent LLM projects began popping up, including Vicuna, an open-source LLM that reports operating at 90% quality relative to ChatGPT.[6]

The agility and inherent modularity granted by being open source means independent projects improve at a breakneck pace and at a fraction of the cost Google and Open AI pay. In addition, attrition from researchers at top firms with backbox LLMs ensures that despite precautions, confidential pieces of LLMs steadily enter the wild. A recent anonymous leak from a Google engineer outlined these concerns.[7]

Infinite Meddling Monkeys and Information Flow Security

A fundamental issue LLMs face is how to mitigate damage from "infinite monkeys," many of whom seek to negatively manipulate LLMs. We already know Google's LLM can be fooled.[8] Targeted LLM manipulation is the next inevitable evolution.

4 Kharif, Olga, Yueqi Yang, and Hannah Miller. "FTX Collapse Shows Sam Bankman-Fried Made Empty Promises." Bloomberg.com, November 16, 2022. https://www.bloomberg.com/news/articles/2022-11-16/ftx-collapse-shows-sam-bankman-fried-made-empty-promises.

5 Meta. "Meta and Microsoft Introduce the next Generation of Llama." Meta, July 18, 2023. https://about.fb.com/news/2023/07/llama-2/.

6 Chiang, Wei Lin et al. "Vicuna: An Open-Source Chatbot Impressing GPT-4 with 90%* Chatgpt Quality." LMSYS Org, March 30, 2023. https://lmsys.org/blog/2023-03-30-vicuna/.

7 Patel, Dylan, and Afzal Ahmad. "Google 'We Have No Moat, and Neither Does Openai.'" SemiAnalysis, May 4, 2023. https://www.semianalysis.com/p/google-we-have-no-moat-and-neither.

8 Coulter, Martin, and Greg Bensinger. "Alphabet Shares Dive after Google AI Chatbot Bard Flubs Answer in Ad." Reuters, February 9, 2023. https://www.reuters.com/technology/google-ai-chatbot-bard-offers-inaccurate-information-company-ad-2023-02-08/.

Black boxes and their inherent lack of transparency are more difficult for bad actors to manipulate but forgo access to independent good actors who actively optimize LLMs at no cost. It is worth mentioning that while black box models hamper and resist attacks, they do not completely safeguard against tampering.

Open-source LLMs reap engineering benefits by allowing "infinite monkeys" to use their platform as a development base, but this model also opens troubling doors. Access to source code greatly assists bad actors seeking to poison LLMs. Subsequently, Llama 2 and its open-source "children" are extremely susceptible to attacks and manipulation.

It is important to note that LLM tampering is not a question of "if" but "when." Search engine optimization (SEO) has been a thorn in Google and Microsoft Bing's side since search engines have existed. Despite search engine algorithms not being public and many spirited attempts to "kill" SEO, including the Google Panda[9] and Penguin updates[10], a strong, constantly evolving industry built around influencing search engine results remains. LLM manipulation will follow a similar path.

LLM tampering poses an existential threat to information security flow. For shorthand, this article refers to LLM developers and manipulators as "infinite monkeys" to represent scale and median technical expertise, but a few of these entities will be decisively sophisticated and well-funded. Some of these sophisticated manipulators will be aggravating but relatively benign, such as private entities attempting to get brand recognition, but others will be decidedly more malevolent.

Emerging attack vectors on LLMs include hypnosis[11] (manipulating an LLM to regurgitate confidential or malicious outputs) and poisoning[12] (altering LLM outputs by manipulating source data or other decision-making processes). The most realistic future scenario is that sophisticated LLM manipulators will wage a constant cat-and-mouse game with LLM providers on fronts ranging from simple phishing to advanced mass psyops.

Government, Sovereign Internet, and LLMs

A predictable range of reactions to ubiquitous LLMs will crop up. Every

9 Singhal, Amit, and Matt Cutts. "Finding More High-Quality Sites in Search." Official Google Blog, February 24, 2011. https://googleblog.blogspot.com/2011/02/finding-more-high-quality-sites-in.html.

10 Cutts, Matt. "Another Step to Reward High-Quality Sites." Official Google Blog, April 24, 2012. https://search.googleblog.com/2012/04/another-step-to-reward-high-quality.html.

11 Lee, Chenta. "Unmasking Hypnotized AI: The Hidden Risks of Large." Security Intelligence, August 8, 2023. https://securityintelligence.com/posts/unmasking-hypnotized-ai-hidden-risks-large-language-models/.

12 Wan, Alexander et al. 'Poisoning Language Models During Instruction Tuning'. arXiv E-Prints, May 1, 2023. arXiv:2305.00944. https://doi.org/10.48550/arXiv.2305.00944.

large-scale private LLM provider will wage an unending war against bad actors. Governments will inevitably become involved as security risks develop.

Imagine a world where one or two general-purpose LLMs reign supreme in each national territory, much as search engines like Google, Naver, and Baidu currently do in their respective regions. Control of information flow and confidential training data suddenly becomes vulnerable to bad actors able to reverse engineer a generative robot.

Governments will unilaterally favor black box LLMs for their increased security against manipulation. This adds an interesting dimension to the black box versus open-source dilemma. True sovereign internet governments will implement state-owned or nominally state-owned LLMs which will be used almost exclusively in their country of origin. Large private LLM providers will be forced to accept individual invasive control mechanisms. Though the wording, implementation, and transparency will vary, the result is that every nation or grouping of nations with the required leverage will lobby for a siloed or "soft siloed" LLM model unique to them.

The eventual endgame for LLMs is an implementation of increasingly invasive "source and quality" weights that ignore algorithmic data on certain prompts to resist manipulation. A heavy portion of LLM training already includes this to avoid situations like Microsoft TAY[13] and controls will be expanded as new vulnerabilities are discovered.

China and GPU Class Wars

In addition to training packages and a transformer model, large-scale LLM research requires significant resources in the form of prohibitively expensive industrial graphic processing units (GPUs). Not all are equal in this fight for GPUs. It is worth noting that while independent Llama 2-based programs like Vicuna can emulate scale LLMs, these represent economic and processing optimization and not functional innovation. To create innovative projects and functions, never mind scaling them, massive amounts of GPUs are required. To this point, Open AI's daily hardware operation costs for ChatGPT are estimated to be roughly 690,000 USD.[14]

13 Lee, Peter. "Learning from Tay's Introduction." The Official Microsoft Blog, March 25, 2016. https://blogs.microsoft.com/blog/2016/03/25/learning-tays-introduction/.

14 Patel, Dylan, and Afzal Ahmad. "The Inference Cost of Search Disruption – Large Language Model Cost Analysis." SemiAnalysis, February 9, 2023. https://www.semianalysis.com/p/the-inference-cost-of-search-disruption.

As of 2023, China and the US are engaged in a no-holds-barred race to hoard GPUs for LLM innovation. The US has leveled restrictions on the distribution of high-end GPUs to China and multiple "unspecified Middle Eastern countries,"[15] indicating an era of GPU throttling has arrived. Despite this, if we define a "GPU-rich" company as having over 20,000 Nvidia A/H100 GPUs, multiple China-based organizations are still projected to have the equivalent of over 100,000 industrial-grade GPUs by the end of 2024.[16] While Google, Meta, and Open AI will still possess more GPUs, this is enough processing power to compete with top Western automation companies.

Eyes on the Future

As powers compete for information flow hegemony, the most likely outcome for LLMs will be siloed implementation subject to ever-expanding regulatory controls. Western nations will utilize private enterprises subject to moderation and weights at varying levels of transparency to guard against psyops. China will adopt a sovereign black box LLM that has the same, if not stricter guard rails, but will have fewer pretensions about moderation.

The largest losers of the LLM development boom will be nations without the leverage to implement controls, the capability to develop their own LLMs, or the ability to "play the line" between China and the U.S., leaving them subject to extranational LLM information flow regulation. The notion of nations without the leverage or capability to implement their LLMs being left at a disadvantage is a tangible concern. This could potentially exacerbate existing digital divides and contribute to a new form of information imperialism.

For private enterprises, LLMs represent pure opportunity. Though we often think of the LLMs made by Google and Open AI as chatbots or query engines, LLMs open doors in many niche applications, including software programming, hardware operation automation, legal dispute settlement, accounting, design, and education. Private sector companies will also be important players in the upcoming war to manipulate LLM responses. Brands that successfully influence key queries will see massive returns, and computer-savvy marketers will flock to this new niche.

15 Nellis, Stephen, and Max Cherney. "US Curbs AI Chip Exports from Nvidia and AMD to Some Middle East Countries." Reuters, September 1, 2023. https://www.reuters.com/technology/us-restricts-exports-some-nvidia-chips-middle-east-countries-filing-2023-08-30/.

16 Murphy, Hannah, and Qianer Liu. "China's Internet Giants Order $5bn of Nvidia Chips to Power AI Ambitions." Financial Times, August 10, 2023. https://www.ft.com/content/9dfee156-4870-4ca4-b67d-bb5a285d855c.

Independent open source LLM projects will continue to exist, but are unlikely to displace the big LLM players. Governments will vastly prefer regulated black box projects over independent open-source LLMs, which governments will view (not incorrectly) as potential disinformation machines. It is conceivable that digital throttles, legislation, and other tools could be used to neuter or regulate open-source LLMs aiming for mass public adoption.

Private enterprises, governments, and "AI" manipulators will follow an intersecting, diverging, and reconvening pattern as advancements are made in LLM manipulation tactics. Open-source advocates will be upset by the probable siloed black box model, but this approach provides the information flow security governments demand. It will be policy, risk mitigation, and information security that rule the future of LLMs. The only roadblock is a consortium of infinite meddling monkeys.

About this volume

TI Observer would like to thank the following individuals for their time and insights.

Commentators

Warwick Powell

Adjunct Professor at Queensland University
Chair of Smart Trade Networks
Author of *China Trust and Digital Supply Chains Dynamics of a Zero Trust World*

Rémy Trichard

Serial entrepreneur and IT executive
Formerly VP of Monetization at KaiOS
Co-Founder at Terark and ex-Renren
Co-Founder of La French Tech Beijing
Advisor to the GSMA Inclusive Tech Lab.

Daniel Araya

Senior Partner with the World Legal Summit
Senior Fellow with the Centre for International Governance Innovation (CIGI), Canada

Thorsten Jelinek

Senior Fellow and Europe Director, Taihe Institute
Former Associate Director at the World Economic Forum (2011-2014)
Author of *The Digital Sovereignty Trap*

Evan Tangen

TI Youth Observer - Digitization and Analytics

TIO Executive Committee

Please note: The above contents only represent the views of the authors, and do not necessarily represent the views or positions of Taihe Institute.

Taihe Institute

www.taiheinstitute.org/en

太 和 智 库
Taihe Institute

Taihe Institute

Address

23/F, ShunMaiJinZuan Plaza,
A-52 Southern East Third Ring Road,
Chaoyang District, Beijing

Postcode

100022

Telephone

+86-10-84351977

Fax

+86-10-84351957