Global Future Council on the Future of Complex Risks

OCTOBER 2024

Complex risks in the changing world

The world is undergoing structural change across multiple dimensions. As identified in the World Economic Forum's *Global Risks Report 2024*, four structural forces – geostrategic, climatic, technological and demographic – are impacting all geographical regions. These structural forces are pervasive in sectoral scope and influence a wide range of economic and societal issues. Their ramifications are persistent, with no simple way to change their trajectory, making them viable candidates for long-term projections beyond 10 years.

It is the mandate of the **Global Future Council on the Future of Complex Risks** to explore potential "future shocks" that could arise at the intersections of these structural forces. The complex risks that emerge from the often unpredictable interactions between these structural forces could outpace our ability to understand – and govern – related threats to economies and societies.

Rapid change often leads to heightened risks. The Global Future Council on the Future of Complex Risks has produced this paper to explore potential complex risks and emphasize the urgent need to scale up adaptive and proportionate risk governance to manage them effectively.

"Complex risks" refers to emergent or established global risks that would negatively impact a significant proportion of global gross domestic product (GDP), population or natural resources beyond the 10-year horizon. More specifically, complex risks share three key characteristics:

1. **Interdependence**: the presence of interconnected risks across multiple domains, requiring sophisticated, multi-dimensional solutions and interventions

2. **Non-linearity**: the risk's impact accelerates as the risk materializes

3. **Uncertainty**: significant difficulties in identifying and quantifying the causes and adverse effects – can be due to feedback loops and tipping points or less predictable and emergent behaviours

This paper focuses on the complex risks that could arise if there are future shocks at the intersection of two of the structural forces listed above, namely:

- **Technological acceleration**, relating to the development pathways of frontier technologies, including general-purpose applications

- **Geostrategic shifts**, referring to evolving sources and concentration of geopolitical power, including the offensive and defensive projection of soft and hard power

Technological acceleration

Technology is accelerating at a remarkable pace. For example, in 2016, custom-trained artificial intelligence (AI) models could not pass primary school tests. In 2023, however, GPT- 4 succeeded at dozens of highly competitive university and job exams without being specifically trained for them.[1]

Experts expect the development of 1,000 times more powerful models incorporating imagery, video, audio and sensor data within the next five years.

Critically, the absolute metrics of artificial neural networks may soon approach a tipping point compared to biological neural networks. Several drivers are strengthening the momentum of this trajectory, from the commercialization of AI applications to the pursuit of scientific knowledge for addressing healthcare, education and climate challenges.

Looking 10 years ahead and beyond, models could become a million times as powerful as they are today,[2] potentially overwhelming our adaptive capacity.[3] The two key aspects of this challenge are often expressed as the "black box problem" and the "pacing problem".

The black box problem extends to both intelligibility and predictability; that is, "Why does a model do what it does?" as well as "What will it do?".[4] As the ability to train ever-larger neural networks increases, it will likely outpace the technical ability to understand how they arrive at outputs. The models will likely exhibit some emergent capacities and behaviours that cannot be predicted based on experience.

The pacing problem describes the speed of governance processes being unable to keep up with models' exponential growth – creating regulator gaps and unmanaged societal risks. This problem could apply across many fields, as AI is an invention that improves the method of invention.[5] For better or worse, as models become more powerful and more widespread, they will also accelerate the timelines of capabilities in other fields. This will both catalyse new scientific discoveries and proliferate existing scientific knowledge. For example, humanity discovered 190,000 protein structures over approximately 60 years, while AI capabilities determined the structures of around 200 million proteins in 2022 alone.[6]

This pace of change is too fast for legislative processes to keep up: current models can potentially increase 1,000-fold in complexity between the start and the end of a legislative process, as is the case with the EU AI Act.[7] Autonomous intelligence and recursive self-improvement will only increase this challenge.

Geostrategic shifts

Shifts in geopolitical power will influence the speed and spread of frontier technologies. International tensions could accelerate unchecked deployment as governance efforts are constrained by eroding international cooperation.

Challenges may arise due to different regulatory systems, values and norms at a national level. Existing legal differences (e.g. regarding hate speech and intellectual property) are likely to persist in an age of large language models. Countries may have different interpretations of what is socially harmful – does a particular application infringe on individual human rights or disrupt social harmony?

Furthermore, deteriorating security dynamics are strengthening the perception that access to the latest military technology is needed to ensure national security. Even the widespread understanding of joint existential interests – in limiting dangerous technological arms races, avoiding misunderstandings and preventing the uncontrolled proliferation of dangerous capabilities – could be under threat.

Complexity and governance

Self-regulation by the private sector alone will not be sufficient to contain these risks. In practice, AI consists of a stack of multiple layers. As with other industries, frontier technology firms are likely to push responsibility on to other layers – not unlike large layers. emitters of greenhouse gases, highlighting the responsibility of individuals to adjust their lifestyle to mitigate climate change. When profit motives collide with ethical concerns, self-regulation cannot be a load-bearing pillar, let alone the only pillar, of addressing complex global risks.[8]

As with other industries, frontier technology firms are likely to push responsibility on to other layers – not unlike large emitters of greenhouse gases, highlighting the responsibility of individuals to adjust their lifestyle to mitigate climate change. When profit motives collide with ethical concerns, self-regulation cannot be a load-bearing pillar, let alone the only pillar, of addressing complex global risks.[8]

As warned by many of the world's senior frontier technology researchers, there is no reliable system currently in place that could prevent the loss of control over, or catastrophic misuse of, the next generations of AI models.[9] While the fact that an anonymous user can create artificial agents and give them potentially destructive aims may not seem like a pressing issue yet, it could become a serious concern if such capabilities remain inadequately regulated over the coming 10 years, if not before.

Across all levels of governance, regulation should seek to ensure:

1. **Access to information**: big tech companies have the data on how their systems perform and interact with users and society. To derive and implement effective policy, governments should have legal access to this data, which is required to define, monitor and enforce compliance with social goals. In addition, individuals need simple, clear information to make safety-informed consumer choices.

2. **Independence and impartiality**: recognizing that the same technology companies leading AI development also own the "digital town squares" where political discussions take place, it will be important to ensure that all stakeholder groups' voices are heard.

3. **Capacity building**: even if public and private sector actors are equipped with the necessary information and the mandate to manage the complex risks of technological acceleration and geostrategic shifts, they must also have the capacity to act effectively. This means possessing adequate human resources, infrastructure and tools to protect and analyse the datasets provided by big technology companies.

Regulations must be forward-looking and adaptable to a rapidly evolving risk environment. They must also avoid imposing a disproportionate burden on start-ups and other market entrants that would stifle innovation.

In such a multifaceted and uncertain long-term environment, it is essential that key stakeholders regularly discuss the most appropriate ways to navigate the long-term complexities of technological governance amid heightened geopolitical tensions.

Contributors

Lead authors

Grace Atkinson
Insights Specialist, Global Risks, World Economic Forum

Mark Elsner
Head, Global Risks Initiative, World Economic Forum

Global Future Council on the Future of Complex Risks

Global Future Councils are independent foresight and advisory bodies that help the World Economic Forum and the public to anticipate and explore emerging issues.

The Global Future Council on the Future of Complex Risks is mandated to look at complex risks that might evolve at the intersection of structural forces over the next 10 years and beyond.

The World Economic Forum would like to thank all members who contributed to this edition of the Future Shock series through community discussions and reviews.

We are grateful to our colleagues in the Centre for the New Economy and Society for their contributions and support.

The views expressed in this briefing do not necessarily represent the views of the World Economic Forum nor those of its members and partners. This briefing is a contribution to the Forum's insight and interaction activities and is published to elicit further comments and debate.

Acknowledgements

Council co-chairs

Azeem Azhar
Chief Executive Officer, Exponential View

Ngaire Woods
Dean, Blavatnik School of Government,
University of Oxford

Council members

Saif AlDhaheri
Director, National Operations Center of National Emergency and Crisis Management Authority,
United Arab Emirates

Abdullahi Alim
Chief Executive Officer, Africa Future Fund

Franciskus Antonius Alijoyo
Founder and Principal,
Center for Risk Management and Sustainability

Robin Anne Alta Charo
Professor Emerita of Law and Bioethics,
University of Wisconsin

Lisa Donahue
Co-Head, Americas and Asia, Alix Partners

Peter Engelke
Resident Senior Fellow, Scowcroft Center for Strategy and Security, The Atlantic Council

Roya Ensafi
Assistant Professor, Computer Science and Engineering, University of Michigan

Florence Gaub
Director, Research Division, NATO Defense College

Maha Hosain Aziz
Professor, Master of Arts, International Relations, New York University

Alsharif Nasser bin Nasser
Founder and Chief Executive Officer, Ambit Advisory

Mwanda Phiri-Mwewa
Lead, Africa, Charter Cities Institute

Frida Polli
Founder, Alethia

Nayef Al-Rodhan
Philosopher, Neuroscientist, Geostrategist and Honorary Fellow, St Antony's College, University of Oxford

Maxime Stauffer
Co-Founder and Chief Executive Officer, Simon Institute for Longterm Governance

Araz Taeihagh
Assistant Professor of Public Policy, National University of Singapore

Anna Tunkel
Founder and Chief Executive Officer, Sustainable Impact

Ya-Qin Zhang
Chair Professor and Dean, Tsinghua Universi

Production

Laurence Denmark
Creative Director, Studio Miko

Martha Howlett
Editor, Studio Miko

Cat Slaymaker
Designer, Studio Miko

Endnotes

1. OpenAI. (2023). *GPT-4 Technical Report*. https://cdn.openai.com/papers/gpt-4.pdf.

2. Seeking Alpha. (2023). *NVIDIA Corp. (NVDA) Q4 2023 Earnings Call Transcript*. https://seekingalpha.com/article/4580889-nvidia-corp-nvda-q4-2023-earnings-call-transcript; Epoch AI. (2024). *Machine Learning Trends*. https://epochai.org/trends.

3. US Government. (2018). *Artificial Intelligence: With Great Power Comes Great Responsibility. Joint Hearing before the Subcommittee on Research and Technology & Subcommittee on Science, Space, and Technology, U.S. House of Representatives*. https://www.govinfo.gov/content/pkg/CHRG-115hhrg30877/pdf/CHRG-115hhrg30877.pdf.

4. Michael, A. H. (2020). *The Black Box, Unlocked: Predictability and Understandability in Military AI*. UNIDIR. https://unidir.org/files/2020-09/BlackBoxUnlocked.pdf.

5. Bianchini, S., M. Müller and P. Pelletier. (2022). Artificial intelligence in science: An emerging general method of invention. *Research Policy*, vol. 51, issue 10. https://www.sciencedirect.com/science/article/pii/S0048733322001275.

6. Hassabis, D. (2022). *AlphaFold reveals the structure of the protein universe*. DeepMind. https://deepmind.google/discover/blog/alphafold-reveals-the-structure-of-the-protein-universe/.

7. When the EU Commission proposed the EU AI Act in April 2021, the largest AI training run was 341 million petaflops. As of Q1 2024, the largest known training run belongs to GeminiUltra (90 billion petaflops = 300 times larger). By the time the EU AI Act enters into force in 2026, this number could be over 1,000 times larger.

8. World Economic Forum. (2024). *Global Risks Report 2024: 19th Edition*. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf; Schiffer, Z. and C. Newton. (2023). *Microsoft lays off team that taught employees how to make AI tools responsibly*. The Verge. https://www.theverge.com/2023/3/13/23638823/microsoft-ethics-society-team-responsible-ai-layoffs; Lostri, E., A. Z. Rozenshtein and C. Sharma. (2023). *The Chaos at OpenAI is a Death Knell for AI Self-Regulation*. Lawfare. https://www.lawfaremedia.org/article/the-chaos-at-openai-is-a-death-knell-for-ai-self-regulation.

9. Center for AI Safety. (n.d.). *Statement on AI Risk*. https://www.safe.ai/work/statement-on-ai-risk.