

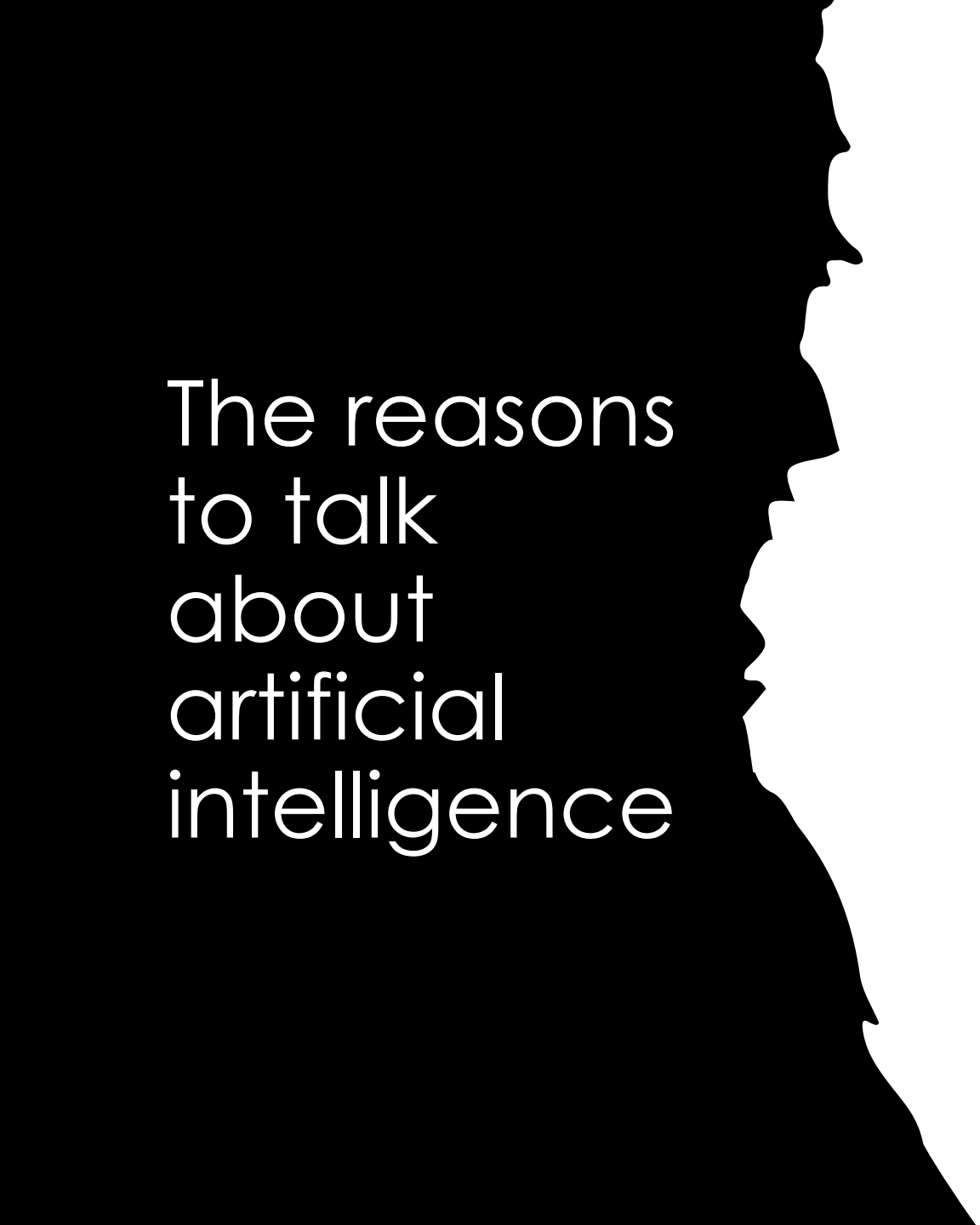


# The challenges and dangers of the artificial Intelligence

Guy Paic  
UNAM, Mexico city

# contents

- Reasons for alarm
- Listing of alarm signals
- Requirements of AI
- Conclusion



# The reasons to talk about artificial intelligence

I believe that this is the most dramatic development in this century and more:

As the internet it will influence our lives, but unlike it, it will drastically change the whole social structure including our manner to do Physics

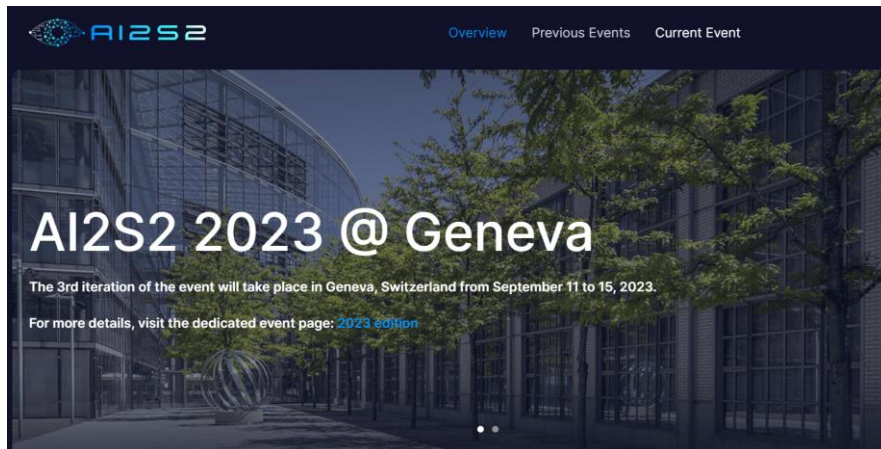
# The history of my engagement in AI



Artificial Intelligence for Science, Industry and Society (AISIS2019)



This event has already proven itself to be of great interest to the interdisciplinary AI community, and has succeeded in attracting major names from each of the three pillars of the event. For example, in [our 2021 edition](#) keynote speakers included Turing medal recipient **Yoshua Bengio**, Fields medal laureate **Cédric Villani** and **Bonnie Lei**, VP and Head of Global Strategic Partnerships at AI for Earth, Microsoft.



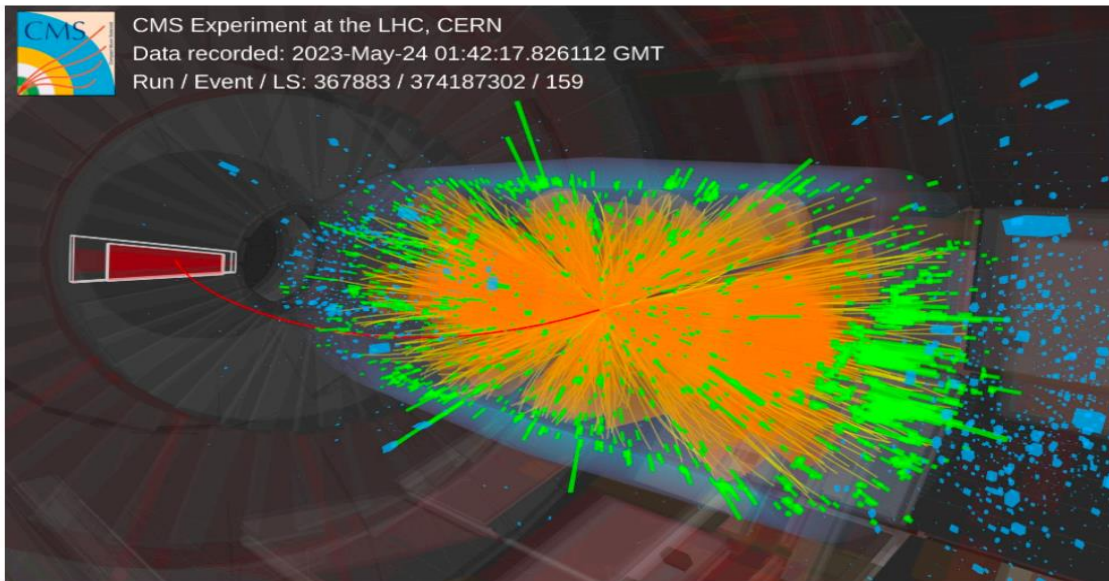
# The beauty of AI

- “A cathedral is built with stones; it is made up of stones; but the cathedral ennobles each stone, which becomes a cathedral stone.”  
Scientific discoveries and technological innovations are stones in the cathedral of human progress.

# AI helping new physics

Event display of the highest anomaly score event that is not selected by the normal L1T menu, from Ephemeral Zero Bias 2023 Run 367883. This event features the maximal number of jets (12), out of which 11 have  $ET > 20$  GeV. It also features a 3 GeV muon. The offline reconstruction identifies 7 jets (reconstructed with the PUPPI algorithm) with  $p_T > 15$  GeV, and 1 muon.

[DP2023\\_079.pdf \(cern.ch\)](#)



**Figure 8.** An event selected by an autoencoder-based anomaly detection hardware triggering algorithm in the CMS Experiment (figure from Ref. [94]).

But,,, there is ample reasons for concern

- Did we reach the point where we might have broken the three laws of Asimov:
  - (1) a robot may not injure a human being or, through inaction, allow a human being to come to harm;
  - (2) (2) a robot must obey the orders given it by human beings except where such orders would conflict with the First Law;
  - (3) (3) a robot must protect its own existence as long as such protection does not conflict with the First or Second Law.”

# Biden's executive order...



- **Artificial intelligence (AI) holds extraordinary potential for both promise and peril.**
  - making us more prosperous, productive, innovative, and secure.
  - but in wrong hands a tremendous potential to exacerbate
  - societal harms such as fraud, discrimination, bias, and disinformation; displace and disempower workers; stifle competition; and pose risks to national security.
  - **Harnessing AI for good and realizing its myriad benefits requires mitigating its substantial risks. This endeavor demands a society-wide effort that includes government, the private sector, academia, and civil society.**



# Artificial Intelligence must be safe and secure

- Testing and evaluations, including post-deployment performance monitoring, will help ensure that AI systems function as intended, are resilient against misuse or dangerous modifications, are ethically developed and operated in a secure manner
- Develop effective labelling and content provenance mechanisms to determine when content is generated using AI and when it is not.

# The concerns

- Elon Musk has raised concerns over the speed at which AI is being developed and the lack of safeguards.
- In their letter published on June 4, the AI experts suggested that risks could be mitigated with guidance from the scientific community, policymakers, and the public.
- "However, AI companies have strong financial incentives to avoid effective oversight," they added.

# Defense may be more difficult than attack! From Joshua Bengio

- we may see these systems used against society in attacks, we will also need some AI to defend us. In the case of bioweapons, for example,
- if AI is used to design a dangerous pathogen, we are going to need another AI to detect that order for synthesising this pathogen. Similarly, for cyberattacks, if there are some that are stronger than our best human programmers, we need AI systems to help us figure that out and find defences and countermeasures.
- It must safe? Even if they behave as intended by those who operate them, those who operate them may abuse the power of these AI systems in many areas, whether it's politics, military, or economic agendas.
- We have to worry about increased power concentration. Right now, we think it's in the hands of a few corporations but in the future, it might also be states or individuals within companies that abuse that power.
- We need to realise that this power concentration problem is **in contradiction with the very objective of democracy**, which is about sharing power. It says we're going to build these tools that give a lot of power to those that use them. This means our democratic institutions need to somehow manage that concentration of power and make sure that power is used in a way that aligns with our collective will, goals, and values. That means that governments need to acquire the muscles, the capability to master these frontier AI systems, to drag them in the directions that we collectively want, and to regulate them properly.

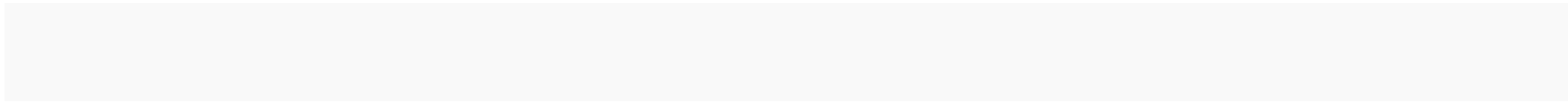
# Some of us reasonably fear various forms of retaliation.

AI-Extinction Threat Letter Signatories

- The letter pointed out that AI firms are fully aware of the harm they can wreak upon humanity.
- "However, they currently have only weak obligations to share some of this information with governments, and none with civil society," the letter said.
- "So long as there is no effective government oversight of these corporations, current and former employees are among the few people who can hold them accountable to the public.
- "Some of us reasonably fear various forms of retaliation, given the history of such cases across the industry."

The letter was signed by Geoffrey Hinton in conjunction with ex-OpenAI engineer Daniel Ziegler, and co-organizer, Daniel Kokotajlo, who quit [OpenAI](#) earlier this year and others...

The requests...



**1. That the company will not enter into or enforce any agreement that prohibits “disparagement” or criticism of the company for risk-related concerns, nor retaliate for risk-related criticism by hindering any vested economic benefit;**

**2. That the company will facilitate a verifiably anonymous process for current and former employees to raise risk-related concerns to the company’s board, to regulators, and to an appropriate independent organization with relevant expertise;**

**3. That the company will support a culture of open criticism and allow its current and former employees to raise risk-related concerns about its technologies to the public, to the company’s board, to regulators, or to an appropriate independent organization with relevant expertise, long as trade secrets and other intellectual property interests are appropriately protected;**

**4. That the company will not retaliate against current and former employees who publicly share risk-related confidential information after other processes have failed. We accept that any effort to report risk-related concerns should avoid releasing confidential information unnecessarily. Therefore, once an adequate process for anonymously raising concerns to the company’s board, to regulators, and to an appropriate independent organization with relevant expertise exists, we accept that concerns should be raised through such a process initially. However, as long as such a process does not exist, current and former employees should retain their freedom to report their concerns to the public.**



# The importance of the Universities

# Example.: University of Florida

The University of Florida has a partnership with NVIDIA to develop the HiPerGator3 supercomputer, the most powerful AI machine in US higher education and a cost overall of 70millions to spend!

The goals UF has set to infuse **the entire curriculum with** AI training and educational opportunities is an example all universities should aspire to follow. It demonstrates that the University of Florida and NVIDIA understand the depth and the breadth of AI's impact as the demand for AI-literate workers will extend well beyond the tech sector.”



# Energy consumption

- "In terms of macro numbers, by 2030 AI could account for 3% to 4% of global power demand. Google said right now AI is representing 10% to 15% of their power use or 2.3 TWh annually."
- the journal *Joule*, estimated that using generative AI such as ChatGPT in each Google search would require more than 500,000 of Nvidia's A100 HGX servers, totaling 4.1 million graphics processing units, or GPUs. At a power demand of 6.5 kW per server, that would result in daily electricity consumption of 80 GWh and annual consumption of 29.2 TWh

# Data and their storage

- The storage requirements for AI systems can vary significantly based on several factors. Here are some considerations:

- 1.Data Volume:** The amount of data being processed plays a crucial role. Large language models (LLMs) and other generative AI systems, such as text-to-image and sound generation models, require massive datasets for training<sup>1</sup>.
- 2.Model Complexity:** The complexity of the AI models matters. Deep learning models, like neural networks, often demand more storage due to their intricate architectures.
- 3.Application Requirements:** The specific application determines storage needs. For example, regression, classification, and multilabel models may require different amounts of data

# AI depends on large scale storage

**Data, computing power and algorithm are the three key elements of AI development**

Storage, like computing, also consumes a large quantity of energy, especially when data needs to be quickly accessed.

Based on its access frequency, data can be classified into hot, warm and cold data.

AI workloads are data driven.

Today's analytics-based AI requires tremendous amounts of [AI storage](#). Without this capacity, you would not be able to benefit from information and knowledge unleashed by AI workloads. Whether you are sequencing human genomes, reading medical imaging, or performing clinical trial research, the amount of data to process is huge. The same is true with machine learning monitoring the Internet of Things (IoT); intelligent agents enabling customer support, purchase prediction, and fraud detection; and business intelligence and other analytical applications. In each case, you can see the commonality of storage at an enormous scale.

# Designing the ideal storage solution

**1. Multiple tiers with a unified namespace:** A single storage system with both a high-performance tier and a large-capacity tier, a unified namespace, and the ability to manage data throughout its entire lifecycle.

-

# What to do

- The scientists are those with the best knowledge of every day use of AI
- The task is to use, promote a sustainable and ethical use of AI
- The task is to address the potential risks and warn the authorities at the global level
- Thank you