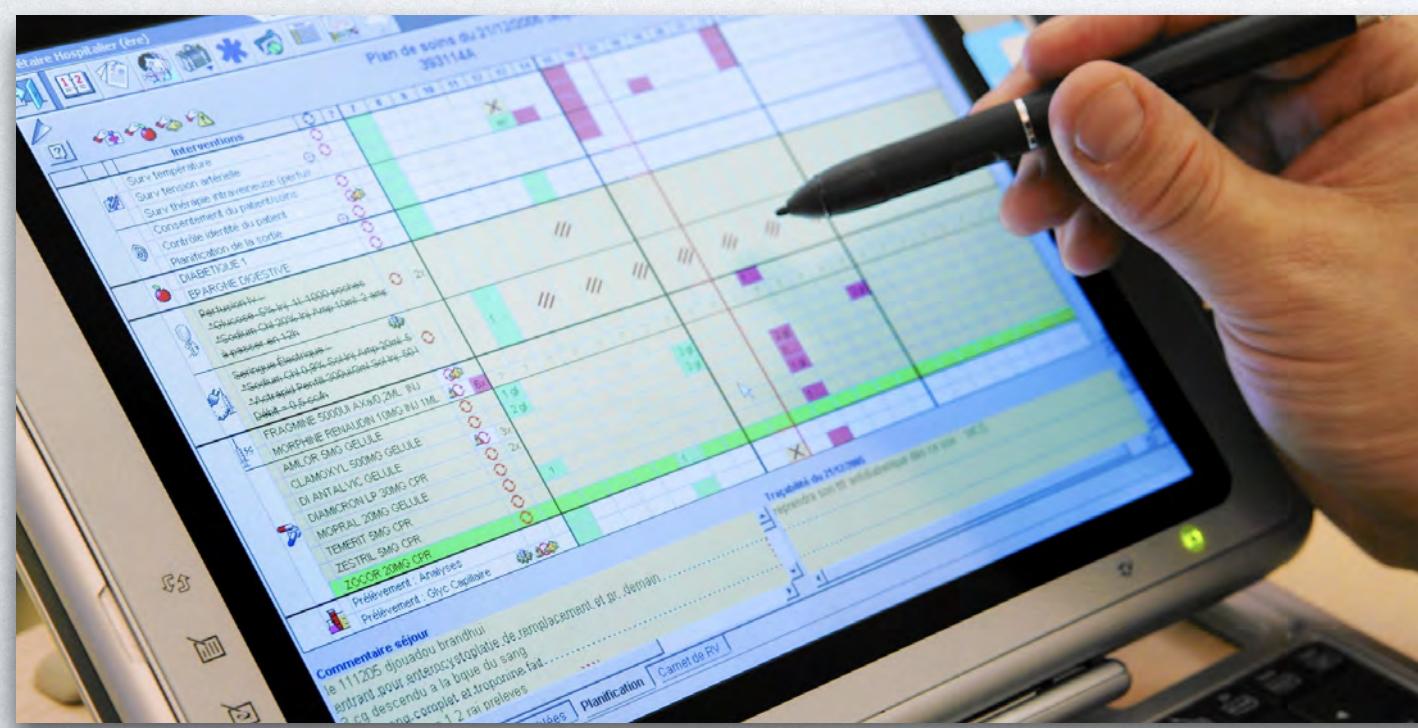
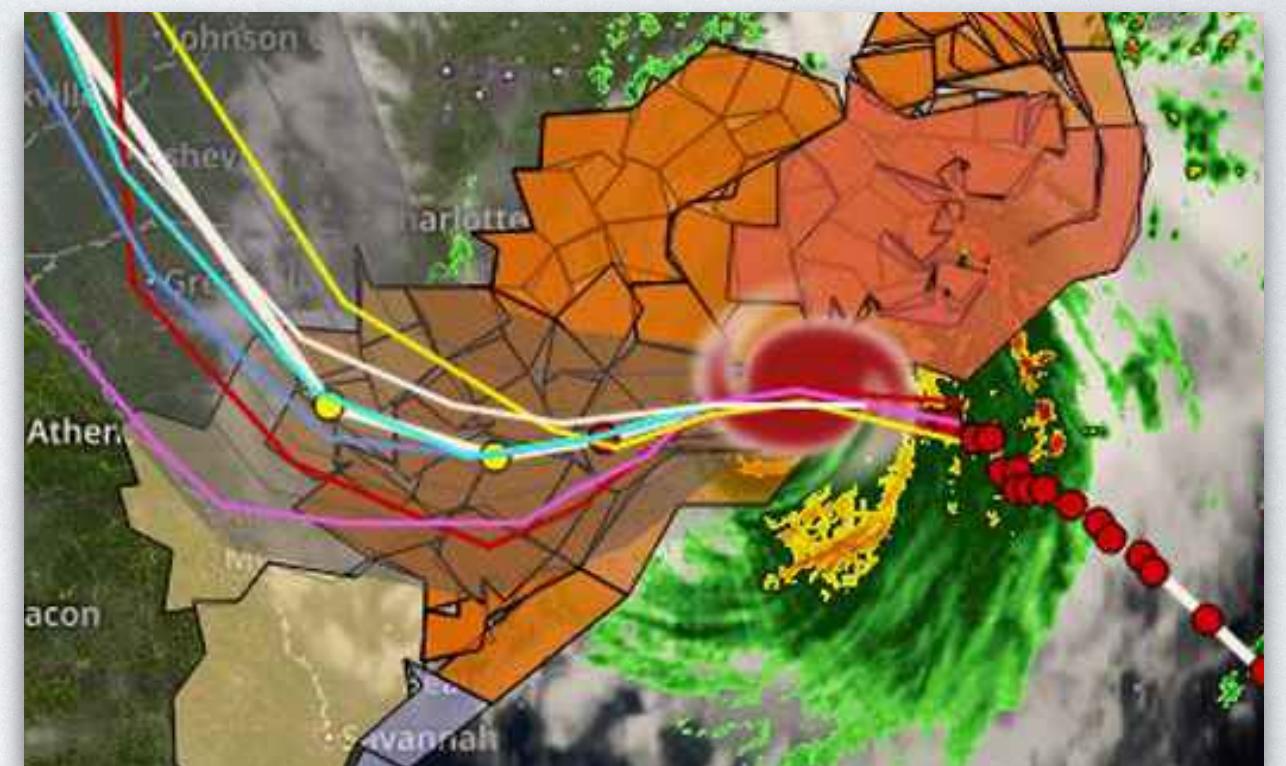
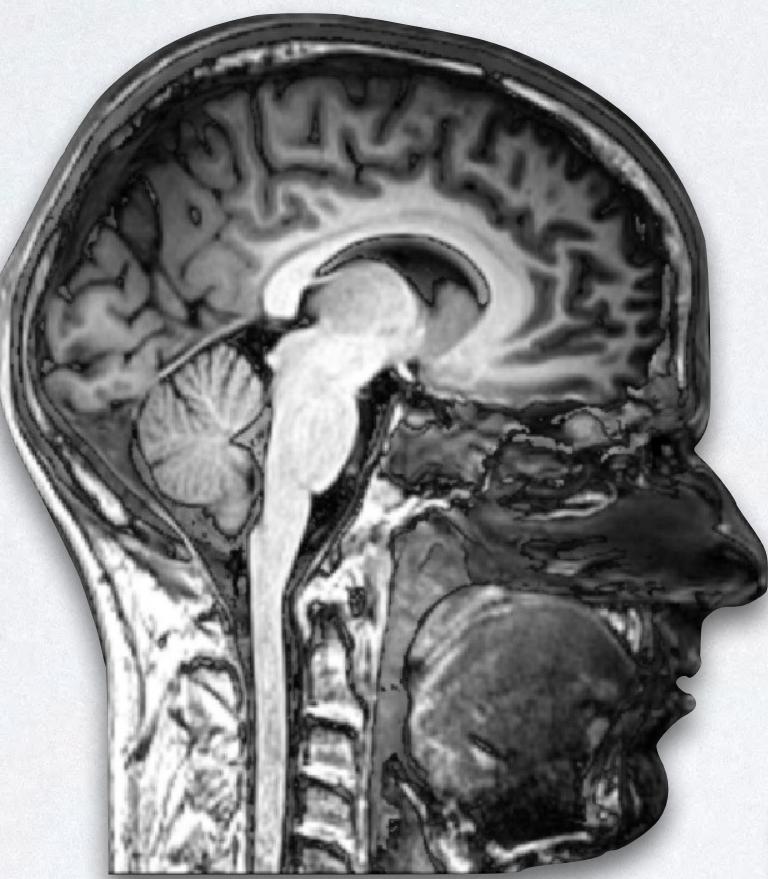
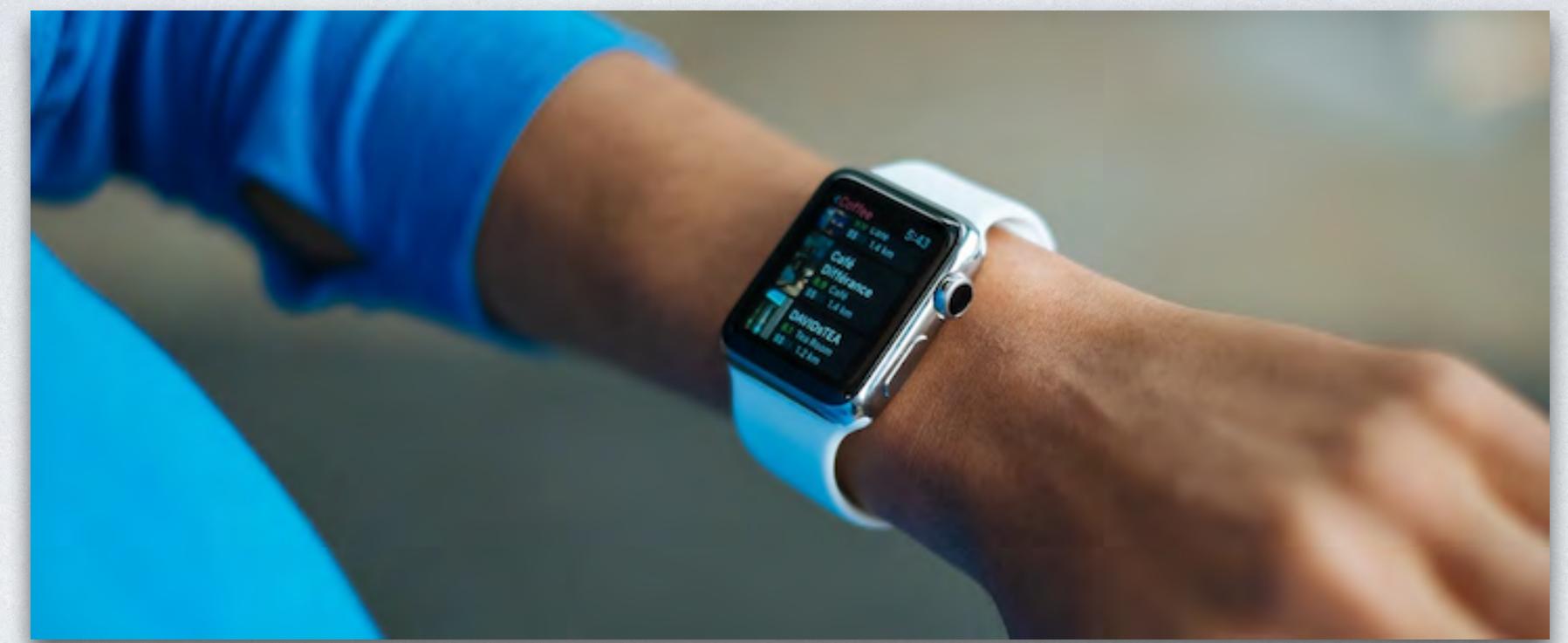
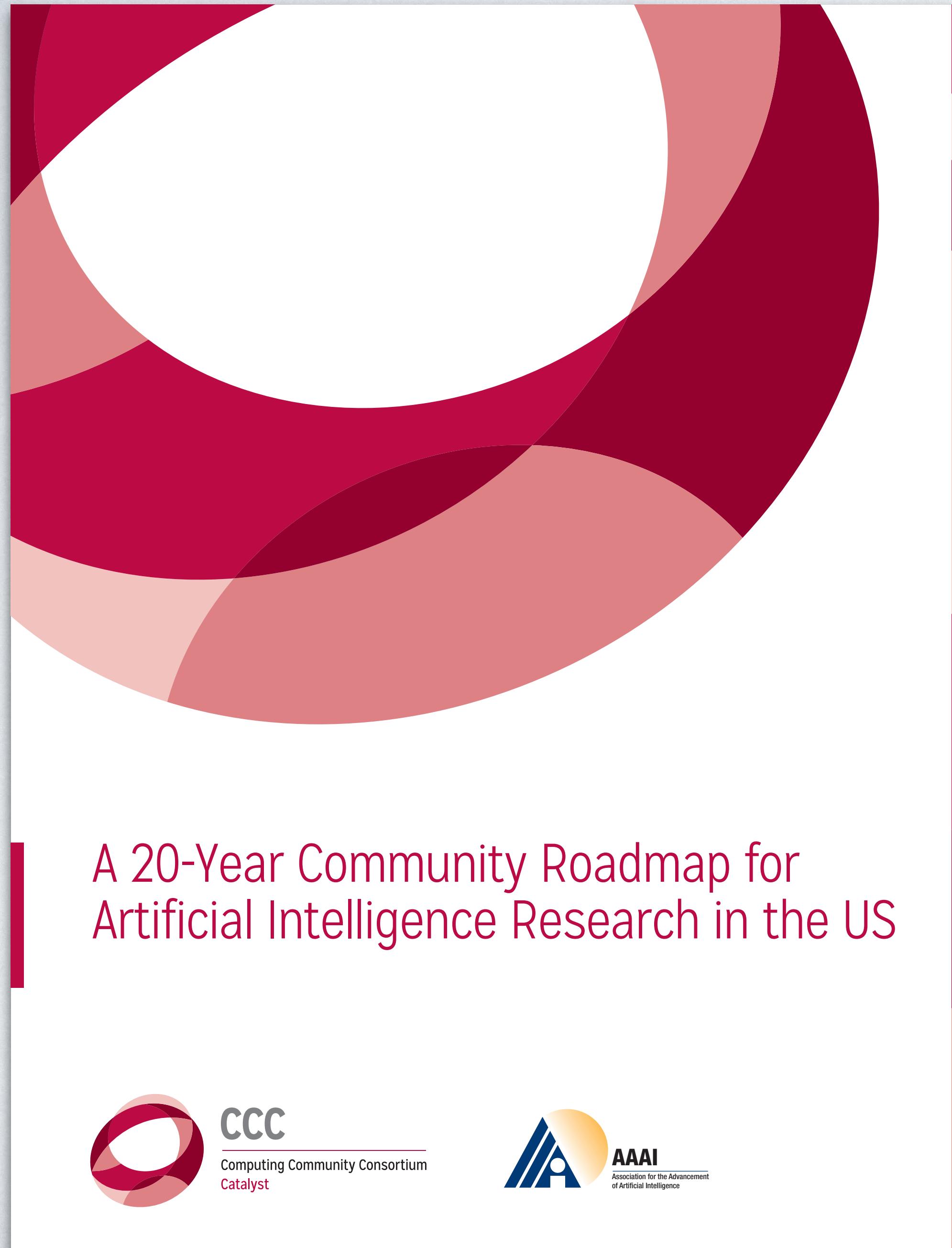


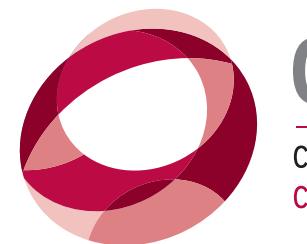
# AI: Challenges, Opportunities, and Partnerships with Academia

Rebecca Willett, University of Chicago





## A 20-Year Community Roadmap for Artificial Intelligence Research in the US



**CCC**  
Computing Community Consortium  
Catalyst



**AAAI**  
Association for the Advancement  
of Artificial Intelligence

# Transformative potential of AI

- boost **health** and quality of life
- provide lifelong **education** and training
- reinvent **business** innovation and competitiveness
- accelerate **scientific** discovery and technical innovation
- expand evidence-driven **social** opportunity and policy
- transform national **defense** and security

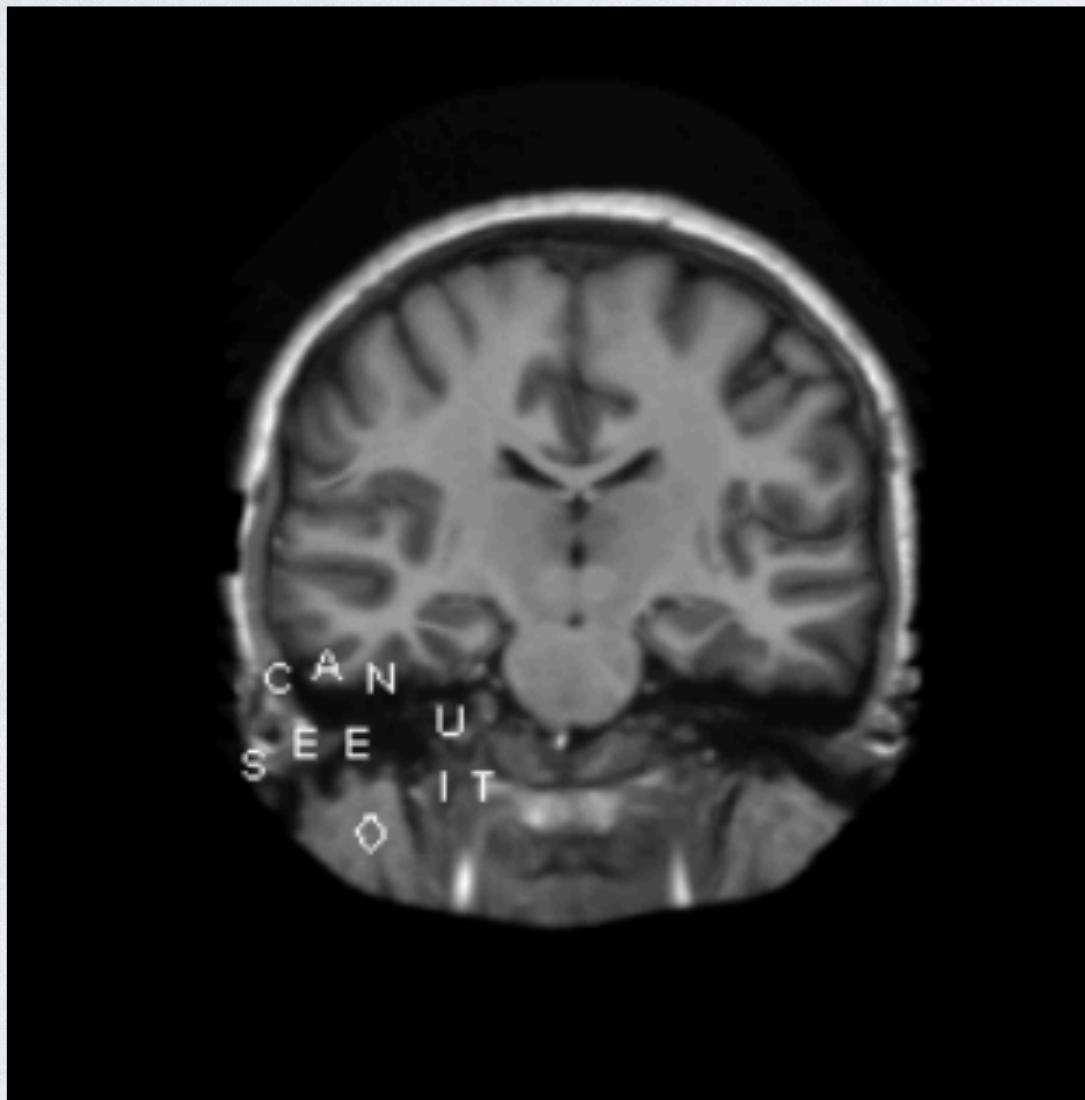
# Exploring AI in action

- hunt for subatomic particles
- malware detection
- lip reading
- seasonal forecasting
- automatic translation
- spectrum estimation for wireless communications
- automatic translation
- robot juggling
- epigenetics
- grammar correction
- describe a photo
- renewable energy
- play go
- play chess
- play poker
- help control prosthetic devices
- analyze vast collections of images of galaxies
- facial recognition
- drug discovery
- advanced transportation systems
- compose music
- speech recognition
- mimic artistic style
- design better batteries
- invent recipes
- home automation
- find new disease risk factors
- recommend purchases
- design new materials
- control the power grid
- predictive policing

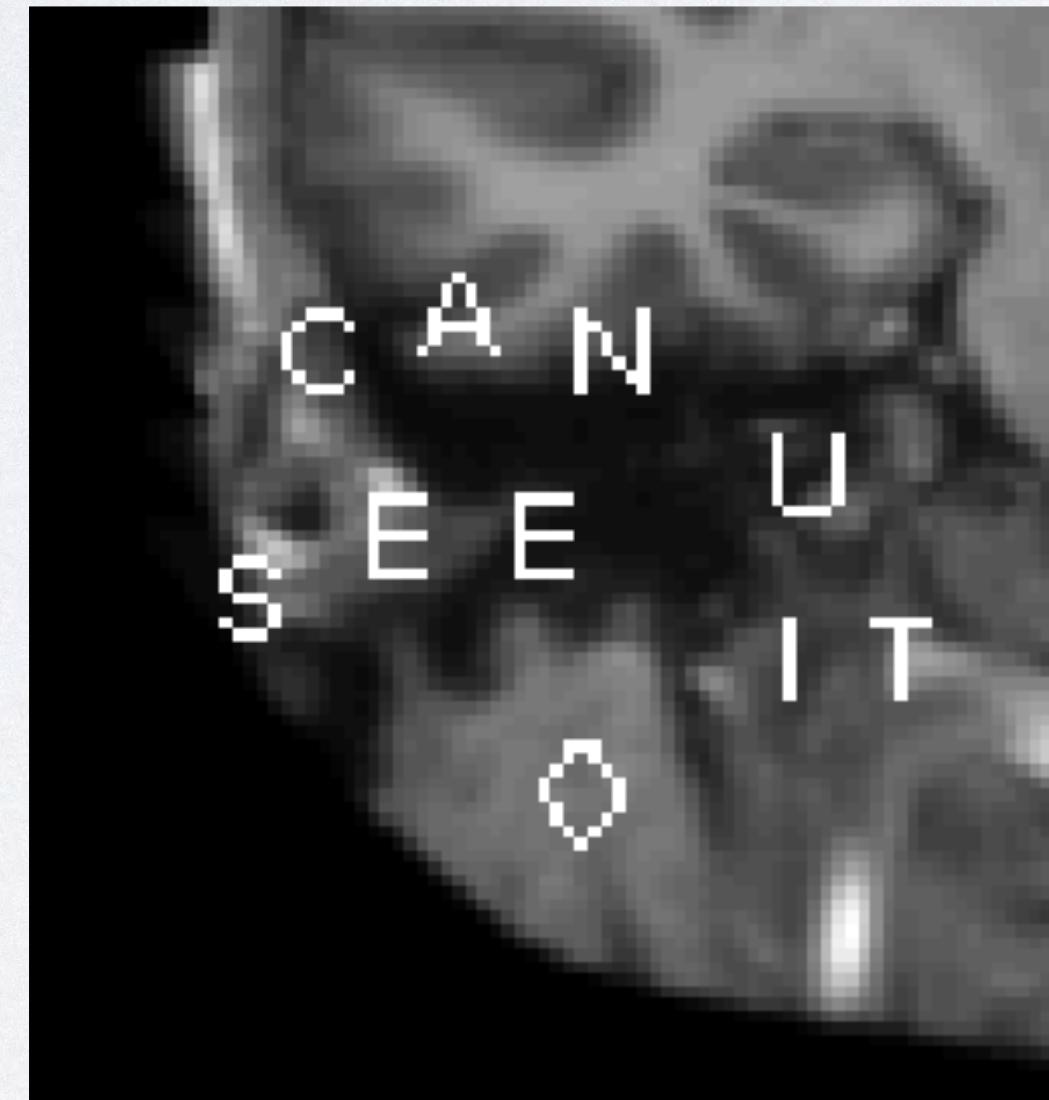
“It's quite obvious that we should stop training radiologists.” — Geoffrey Hinton, an AI luminary, in 2016

“It's quite obvious that we should stop training radiologists.” — Geoffrey Hinton, an AI luminary, in 2016

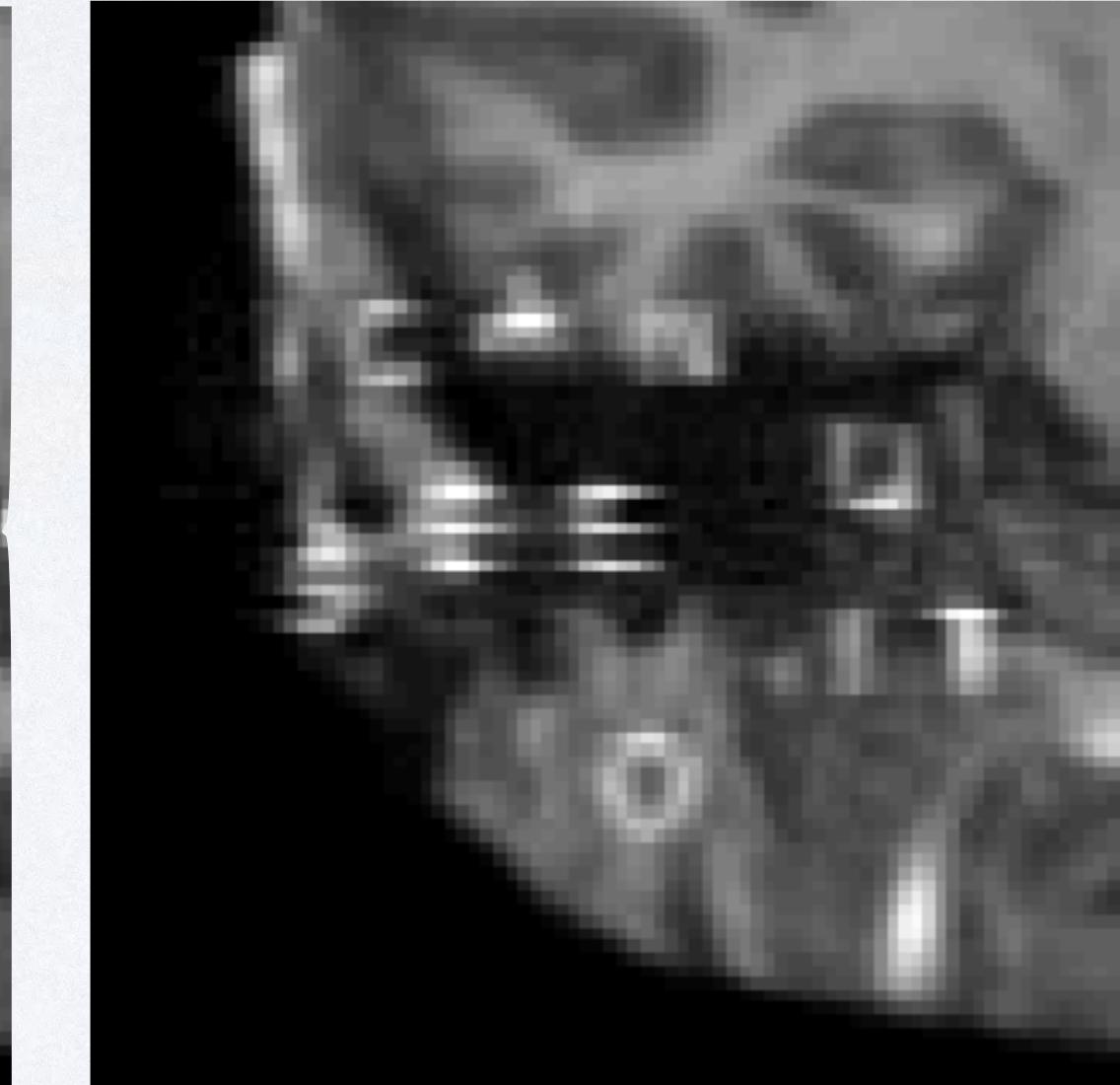
Original



Original (zoomed)

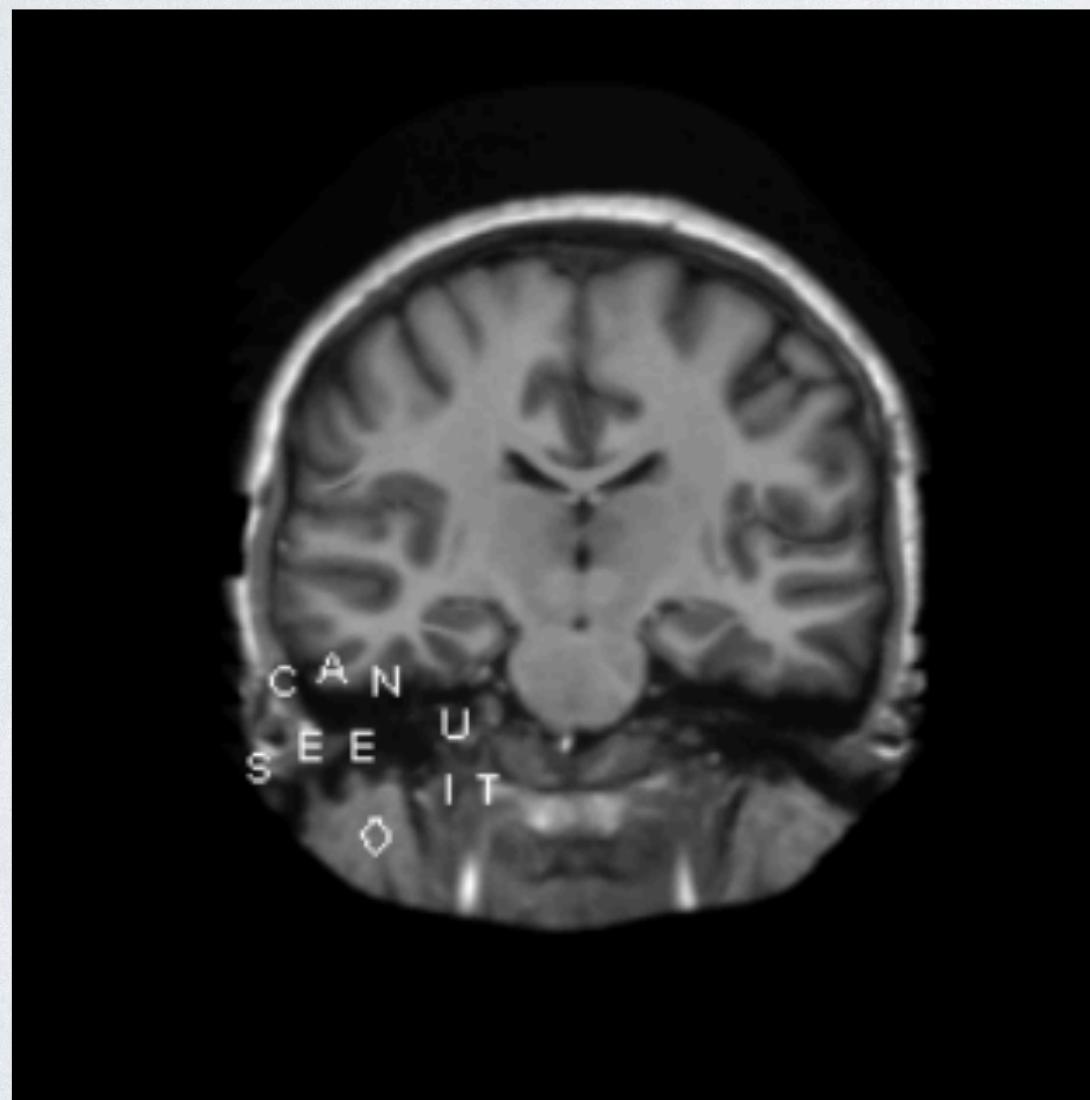


Machine Learning

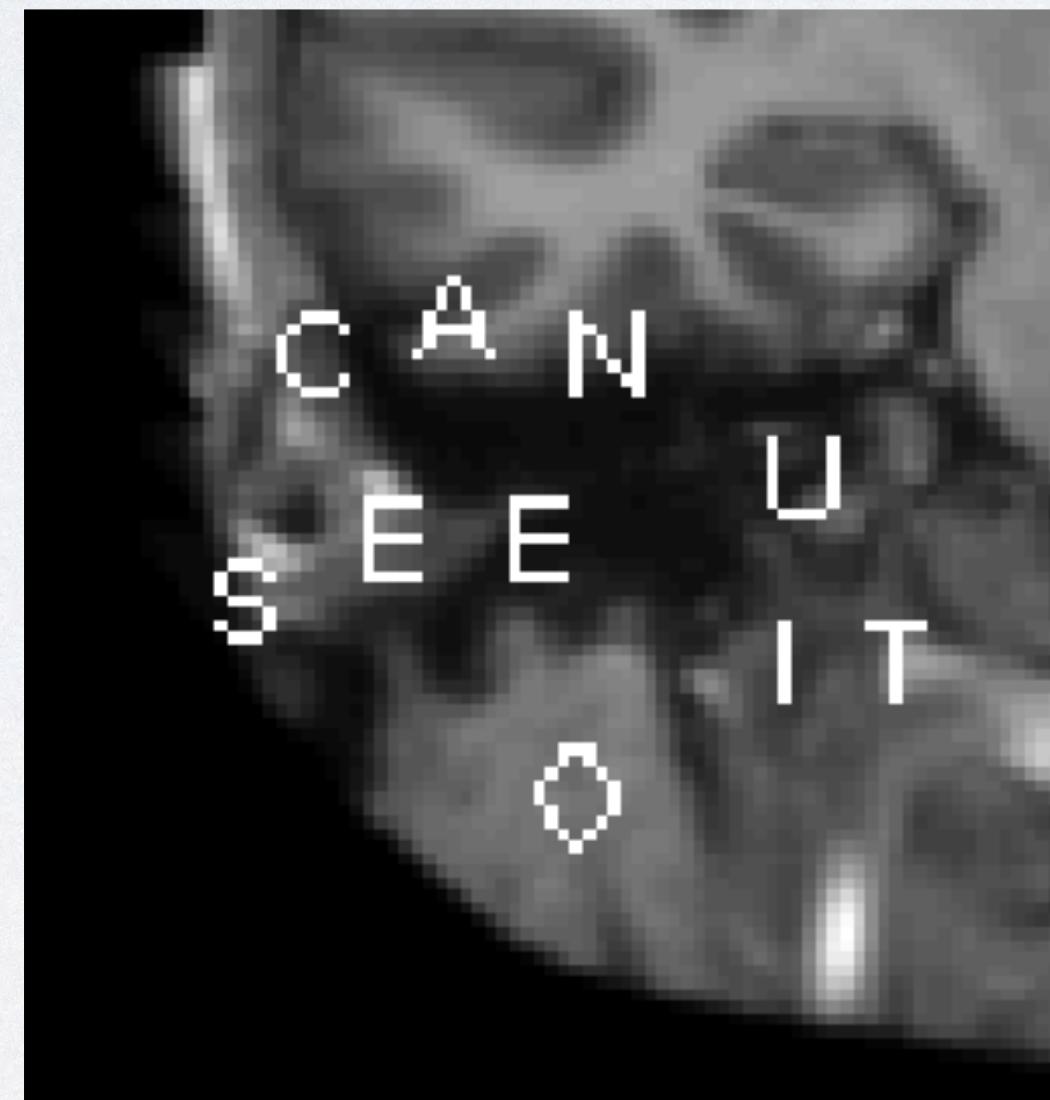


“It's quite obvious that we should stop training radiologists.” — Geoffrey Hinton, an AI luminary, in 2016

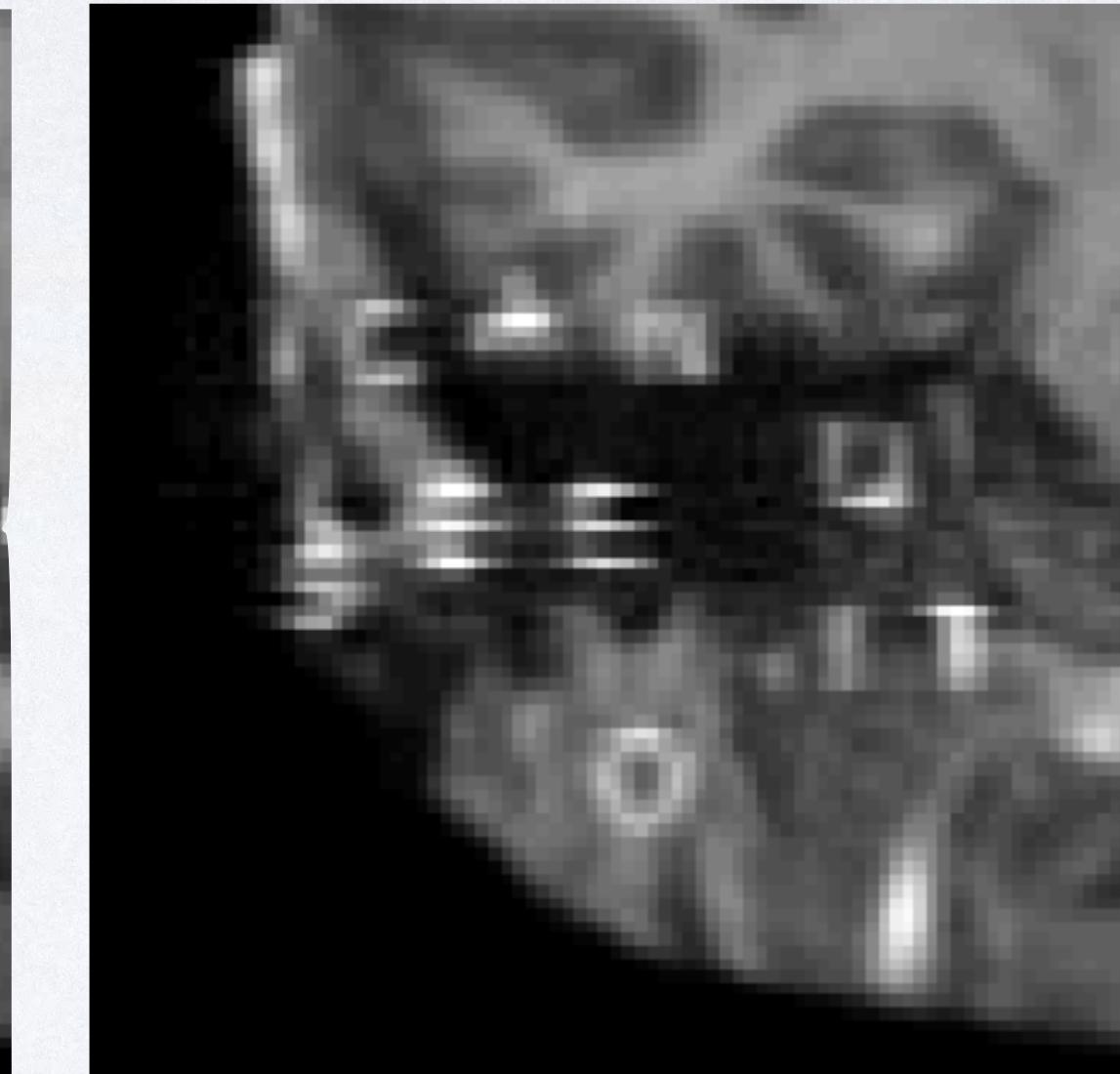
Original



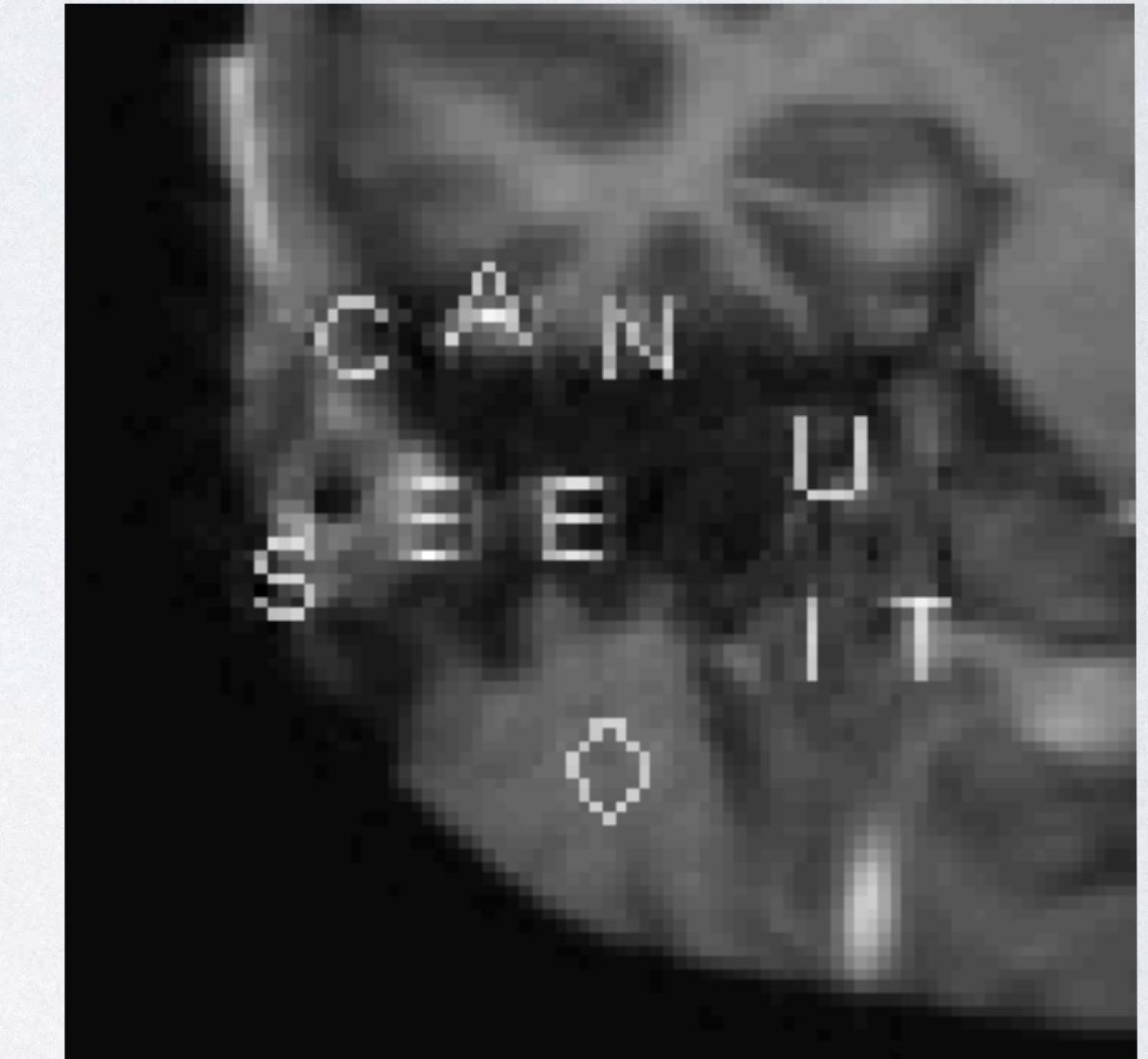
Original (zoomed)



Machine Learning



Classical Method



# Two Viewpoints

AI is Amazing ⇒ Adopt Everywhere!

Focus on deployment and efficiency

More concerned with “could it work?”  
then “might it fail?”

Trial and error mindset

Benchmark performance → innovation

AI is Curious ⇒ Learn More!

Focus on theory, including accuracy  
bounds, sampling efficiency, etc.

Concerned with robustness and  
correctness

The costs of mistakes may be high

Find shortcomings → understanding

Progress depends on both approaches

# Robustness and stability

# Robustness and stability

No one knows exactly how some methods work:  
we cannot predict when outputs will be catastrophically wrong

# Robustness and stability



“panda”

No one knows exactly how some methods work:  
we cannot predict when outputs will be catastrophically wrong

# Robustness and stability



No one knows exactly how some methods work:  
we cannot predict when outputs will be catastrophically wrong

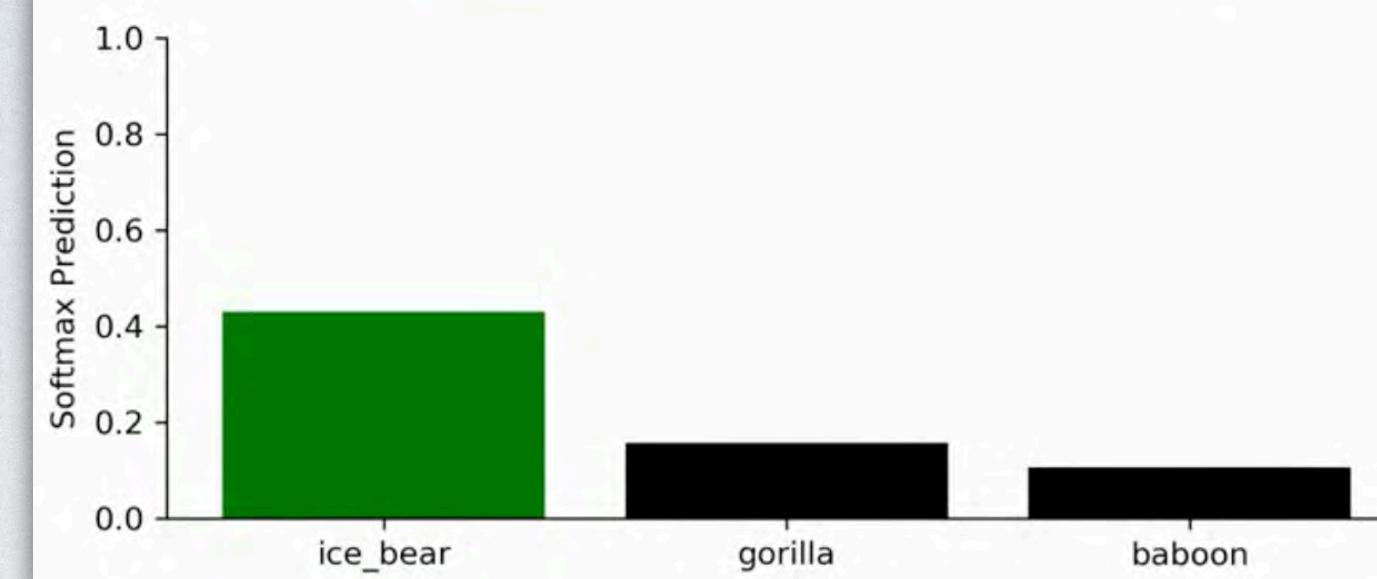
# Robustness and stability



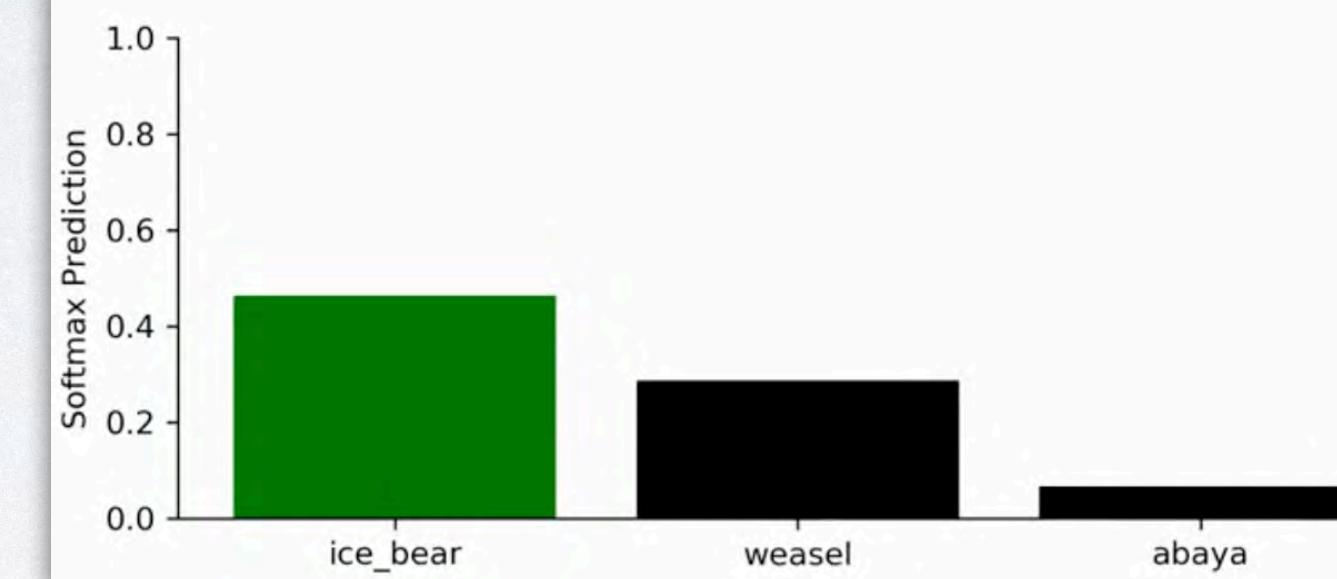
No one knows exactly how some methods work:  
we cannot predict when outputs will be catastrophically wrong

# Robustness and stability

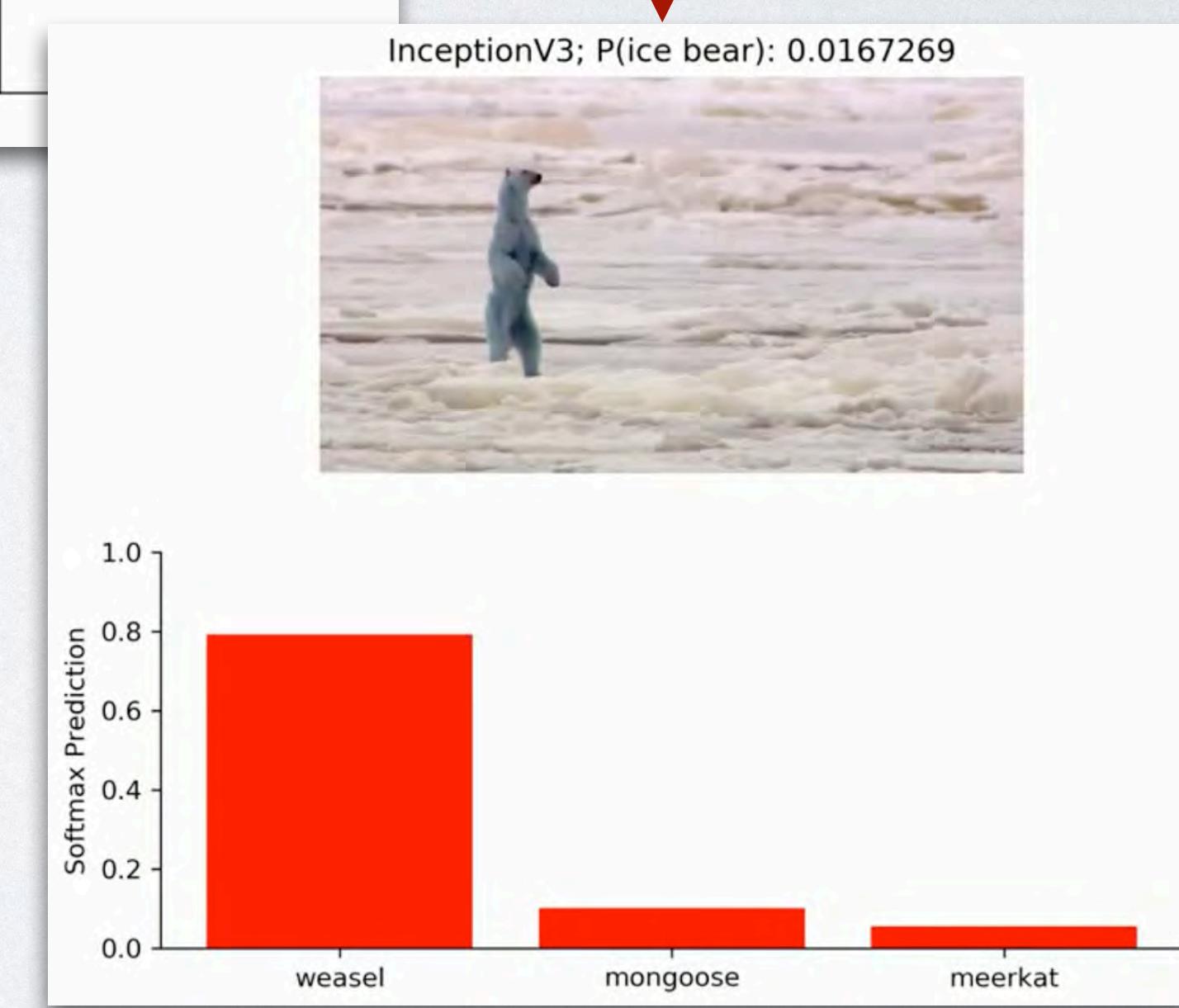
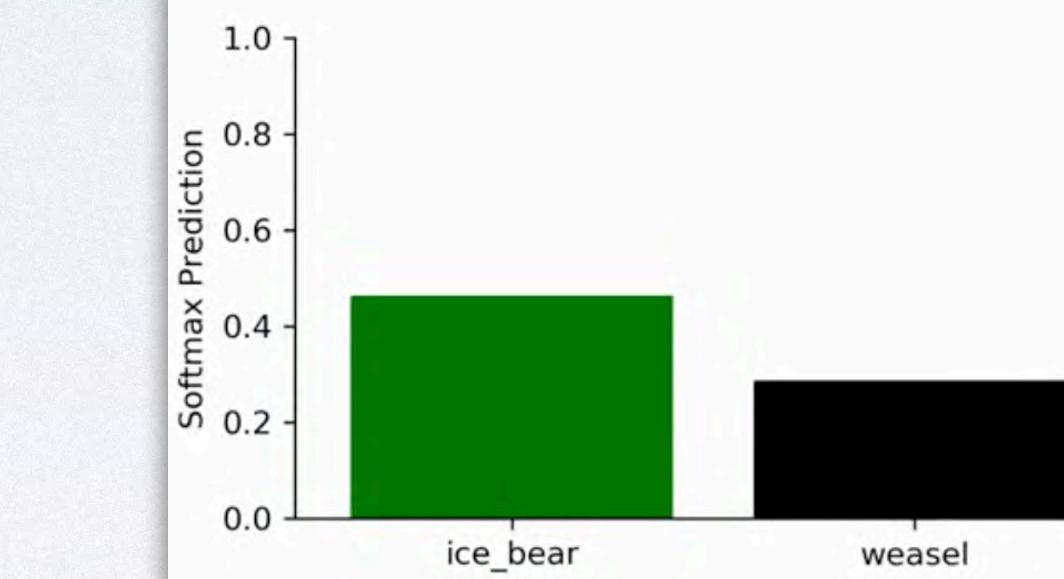
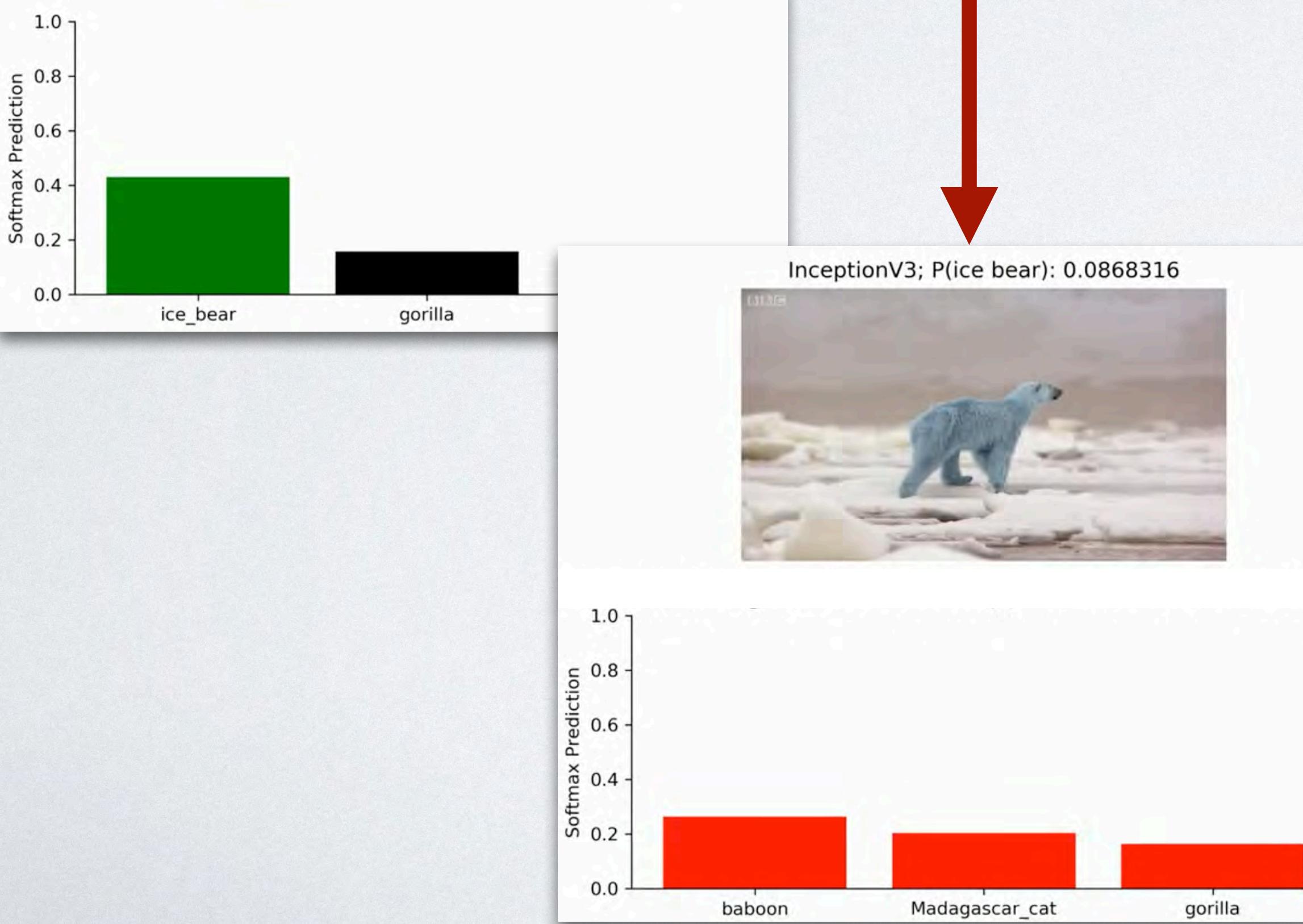
InceptionV3; P(ice bear): 0.430899



InceptionV3; P(ice bear): 0.463495

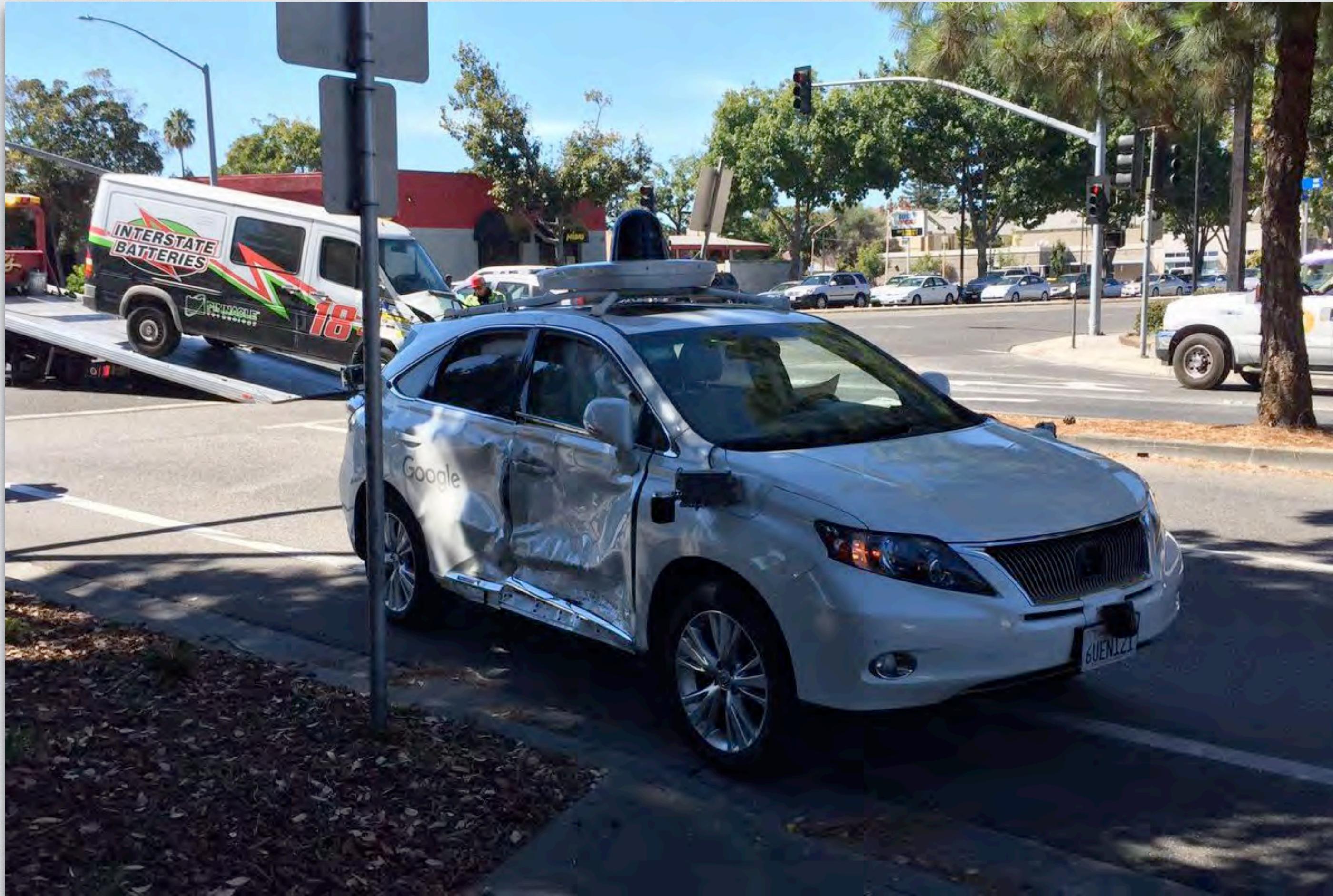


# Robustness and stability



This is not an  
adversarial  
example

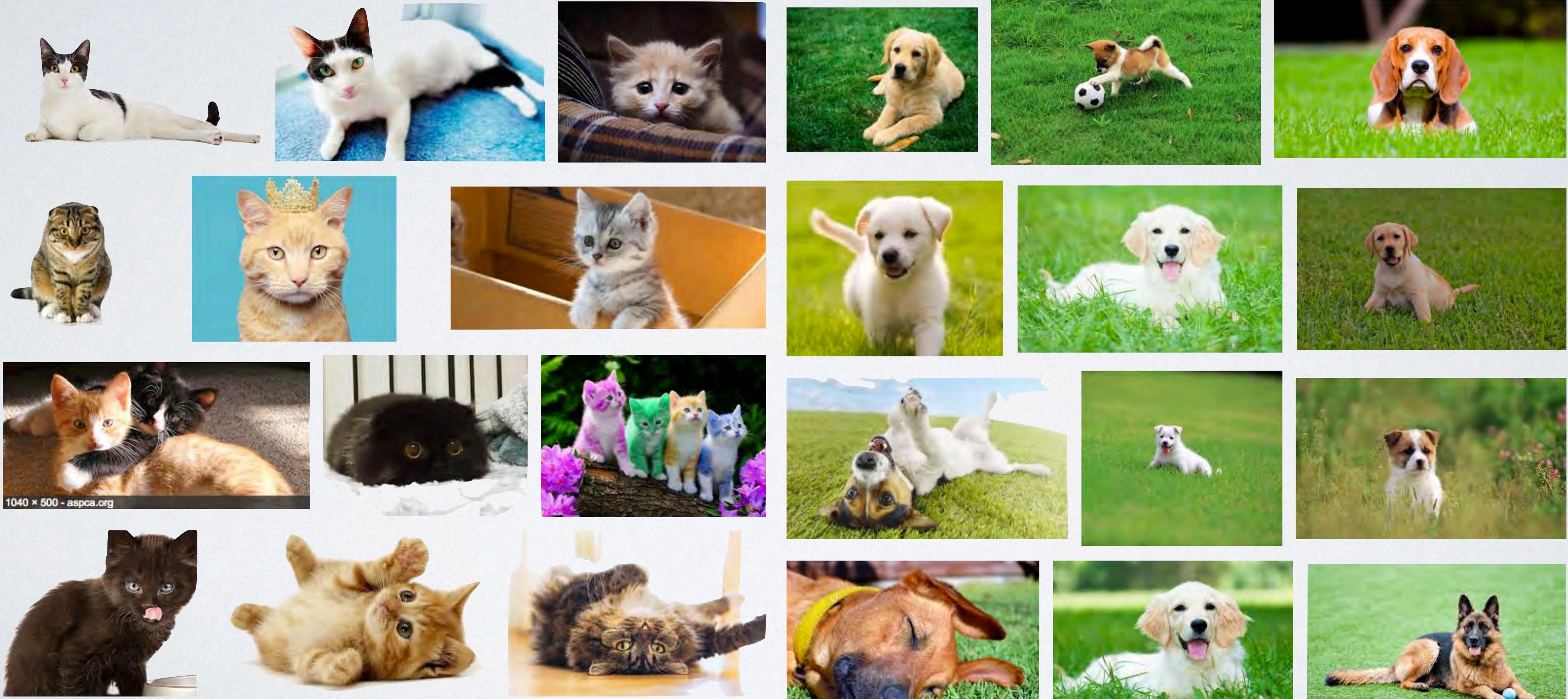
# Robustness and stability



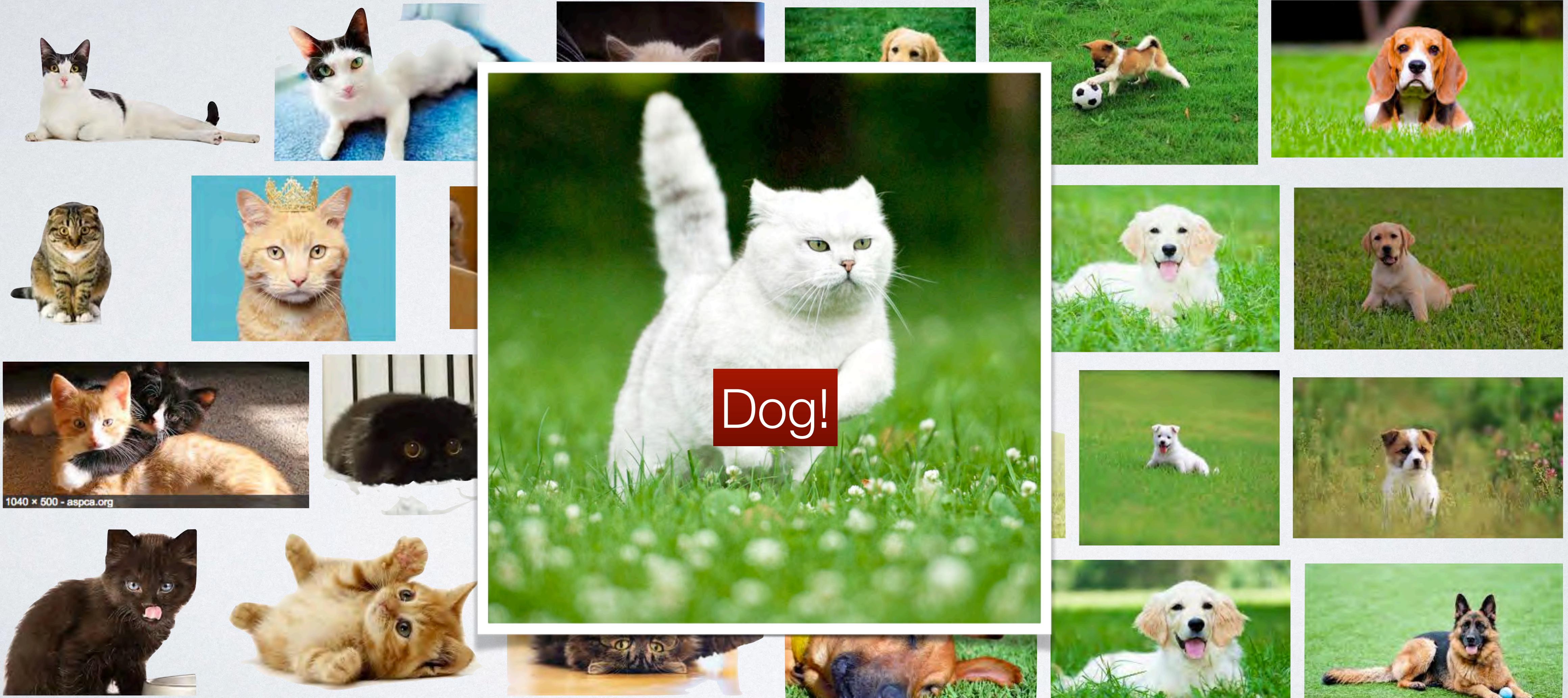
Spurious correlations in training data

Requires large quantities of diverse data

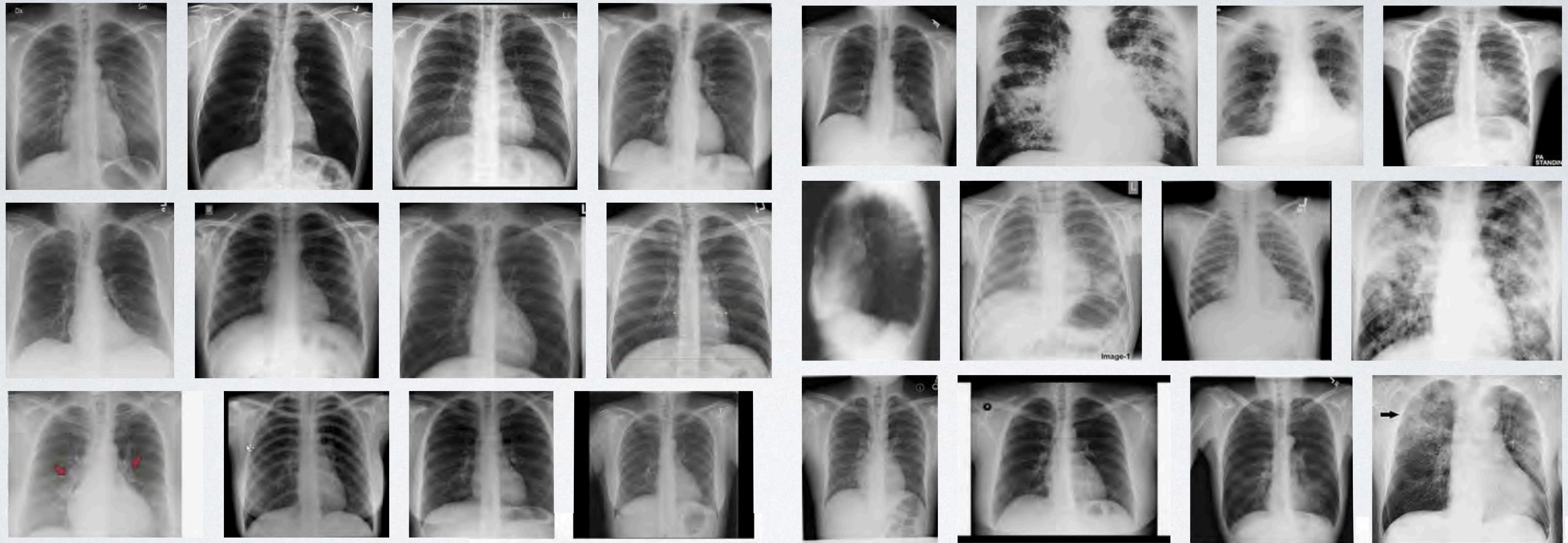
# Requires large quantities of diverse data



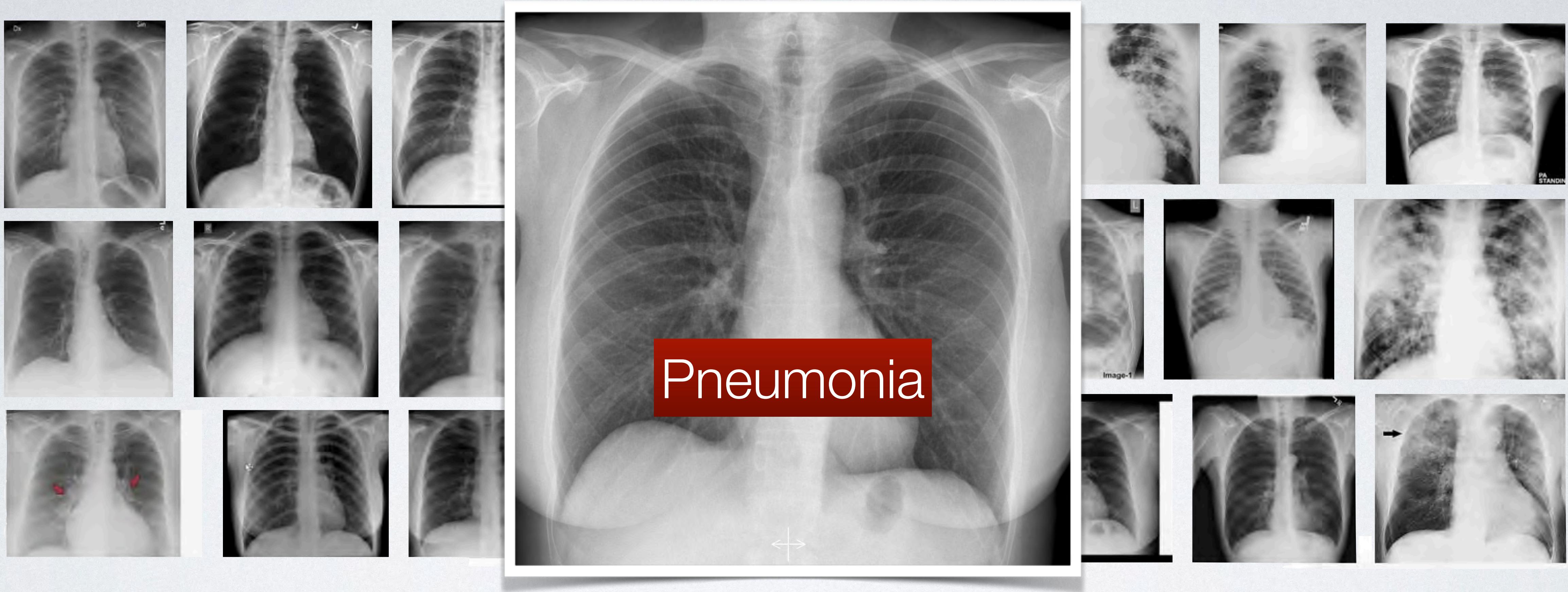
# Requires large quantities of diverse data



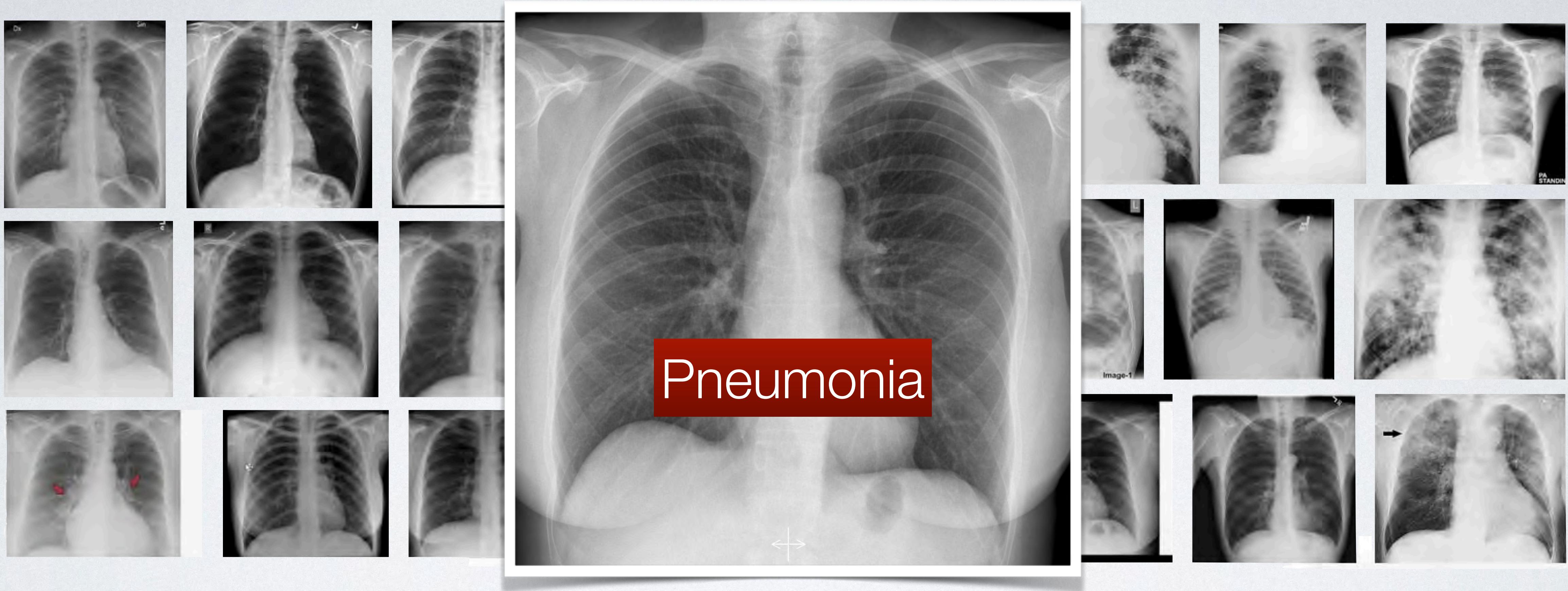
# Requires large quantities of diverse data



# Requires large quantities of diverse data



# Requires large quantities of diverse data



“CNNs could rely on subtle differences in acquisition protocol, image processing, or distribution pipeline (e.g., image compression) and overlook pathology.” – Zech et al, 2018

# Requires large quantities of diverse data



“CNNs could rely on subtle differences in acquisition protocol, image processing, or distribution pipeline (e.g., image compression) and overlook pathology.” – Zech et al, 2018

Leveraging models of physics and humans

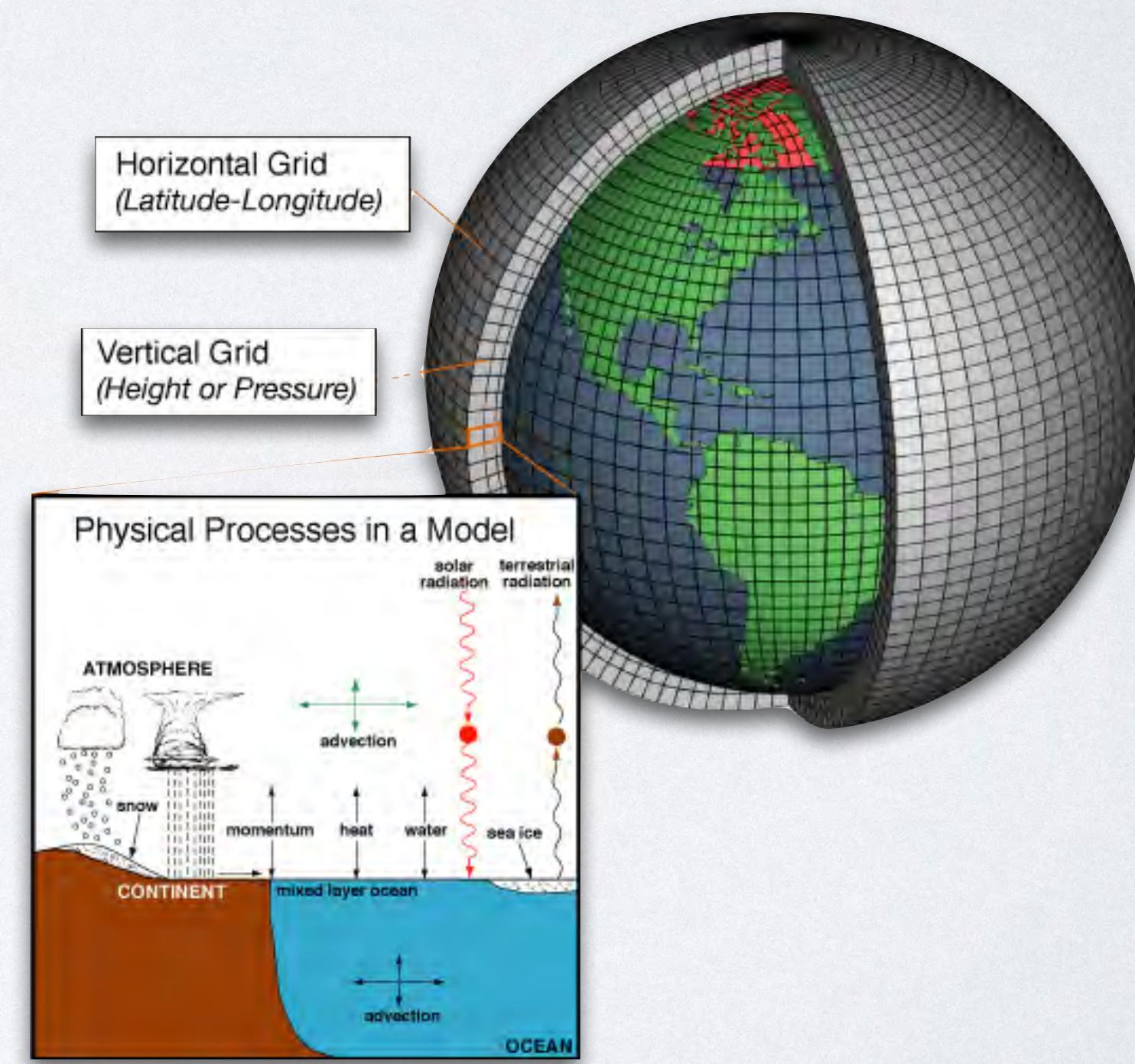
“Worried about superintelligent robots rising up and attacking us? Close your doors.”

— *Gary Marcus and Ernest Davis*



<https://what-if.xkcd.com/5/>

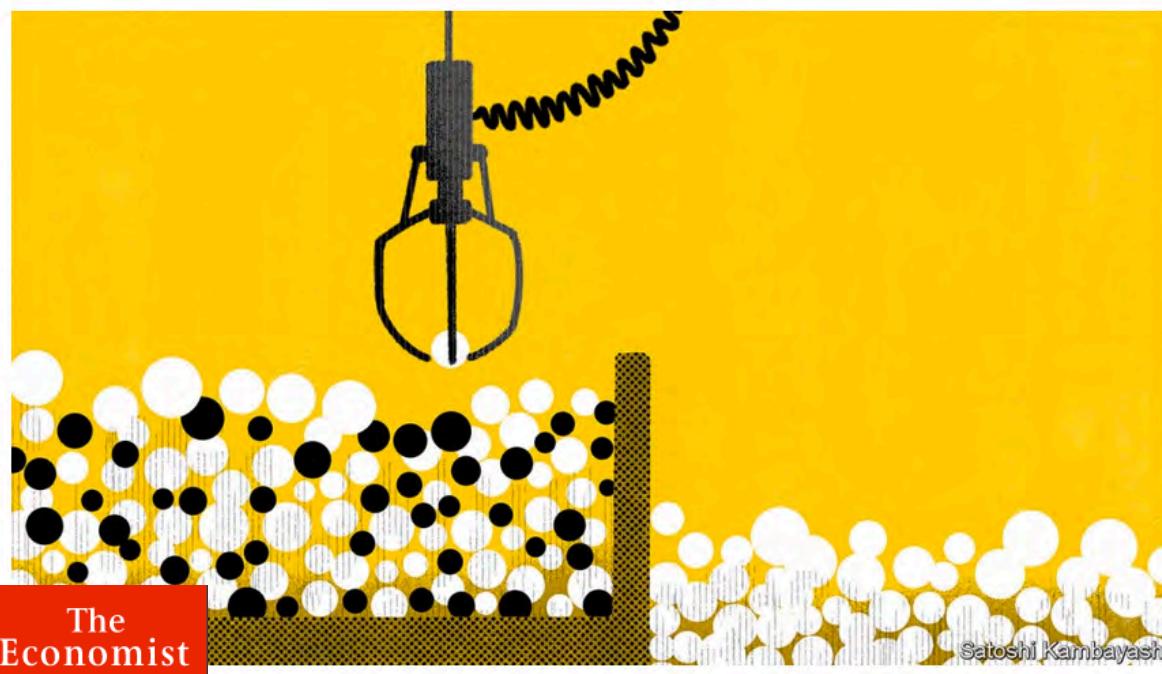
Physical models  
may guide and  
stabilize many AI  
methods



Buttonwood

## The benefits of better credit-risk models will be spread unevenly

Machine-learning models show the disquieting effect of finer judgments



The Economist

## THE IRISH TIMES

### Roma attacked in Paris after fake videos circulate on social media

Propagated online, the urban myth of marauding Roma has taken on a life of its own

© Wed, Mar 27, 2019, 18:34

Lara Marlowe Paris Correspondent



A man holds a child in a camp of the Roma community that was attacked in Bobigny, near Paris. Photograph: Kenzo Tribouillard/AFP/Getty

Even if we understand AI,  
*human-AI interactions* may be unpredictable

Forbes

## What Happens When Self-Driving Cars Kill People?



Ron Schmelzer Contributor  
COGNITIVE WORLD Contributor Group



PHOTO BY YENDER FONSECA FROM PEXELS

## Strangelove redux: US experts propose having AI control nuclear weapons

By Matt Field, August 30, 2019



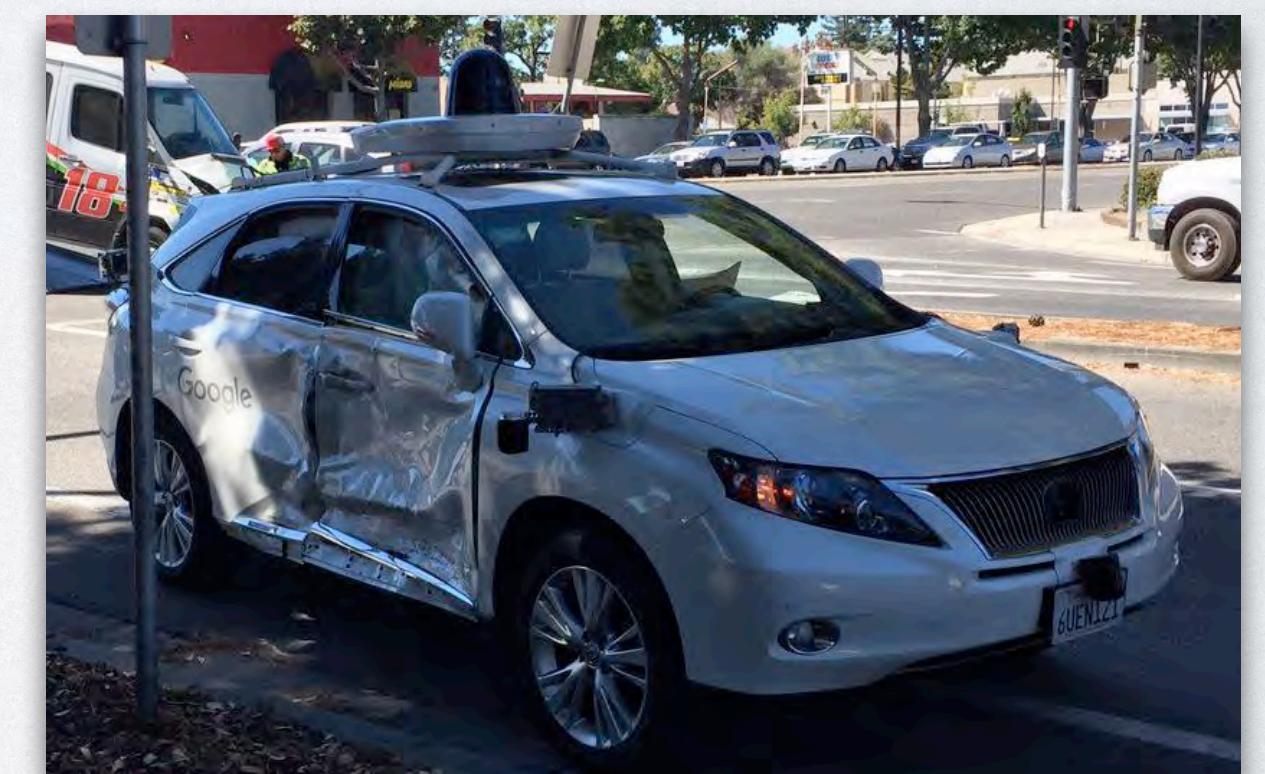
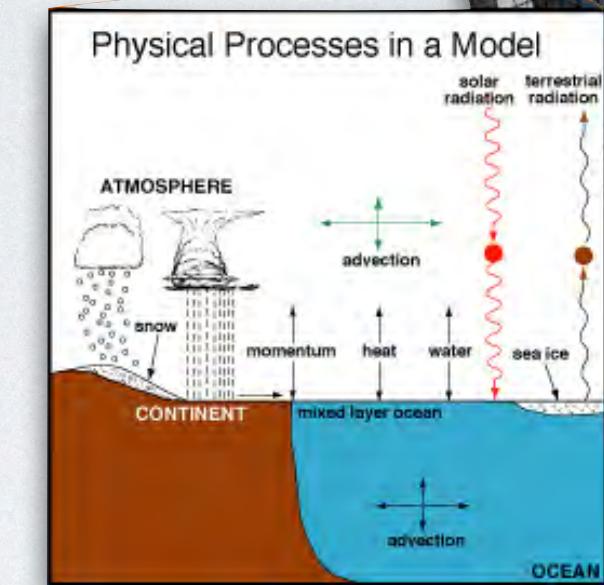
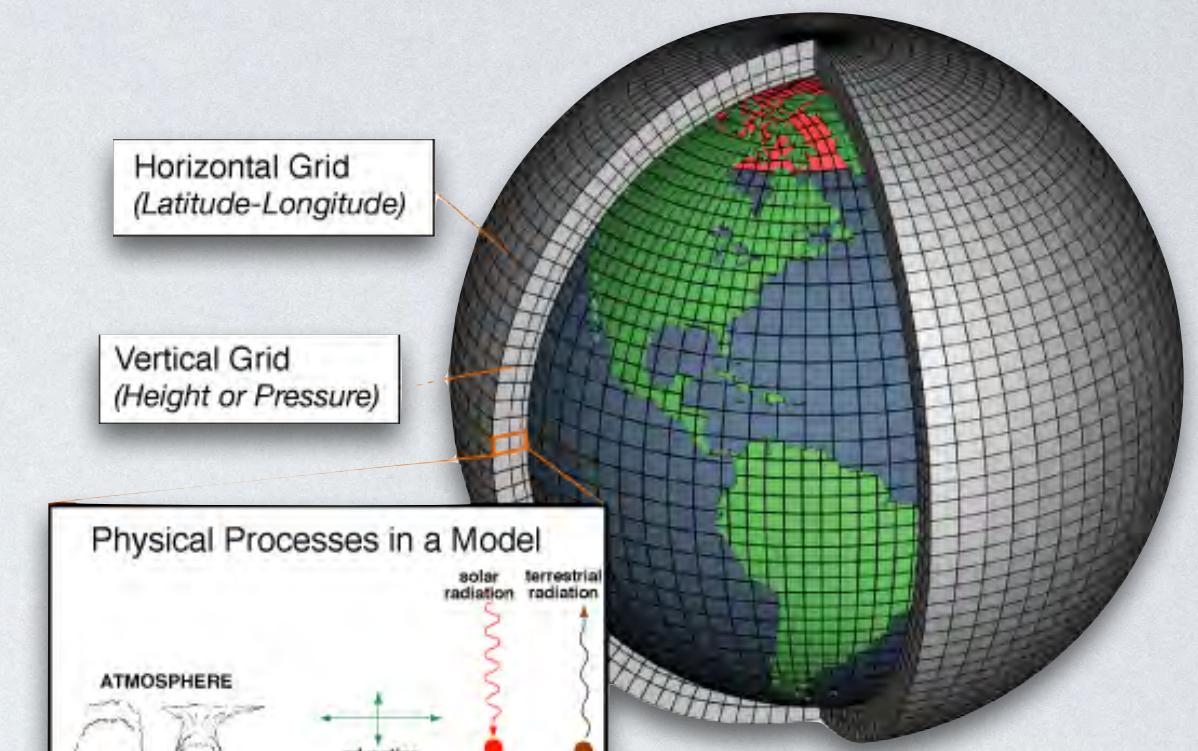
Bulletin  
of the  
Atomic  
Scientists



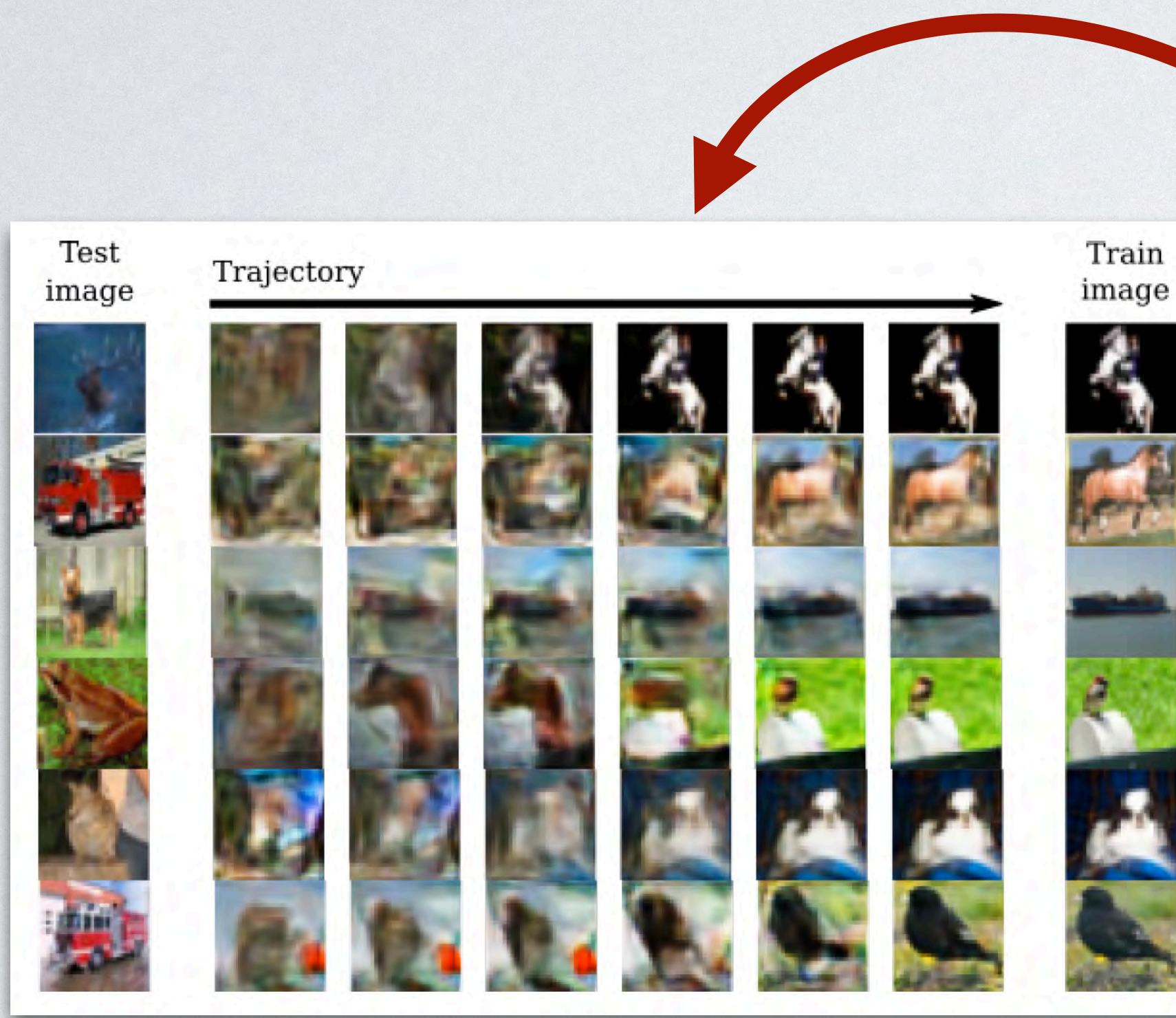
A US missile test. Photo via Wikimedia Commons. Public Domain.

# Some key challenges in modern AI

- How can we integrate training data, physical models, and human judgement?
- Will my method work “in the wild”? What risks do I face at deployment?
- Do I have “enough” diverse data? Can I quantify uncertainty and interpret models?
- What model should I use when? When is deep learning the right tool?



# These questions are not beyond reach



*Radhakrishnan, Yang, Belkin, Uhler, 2019*

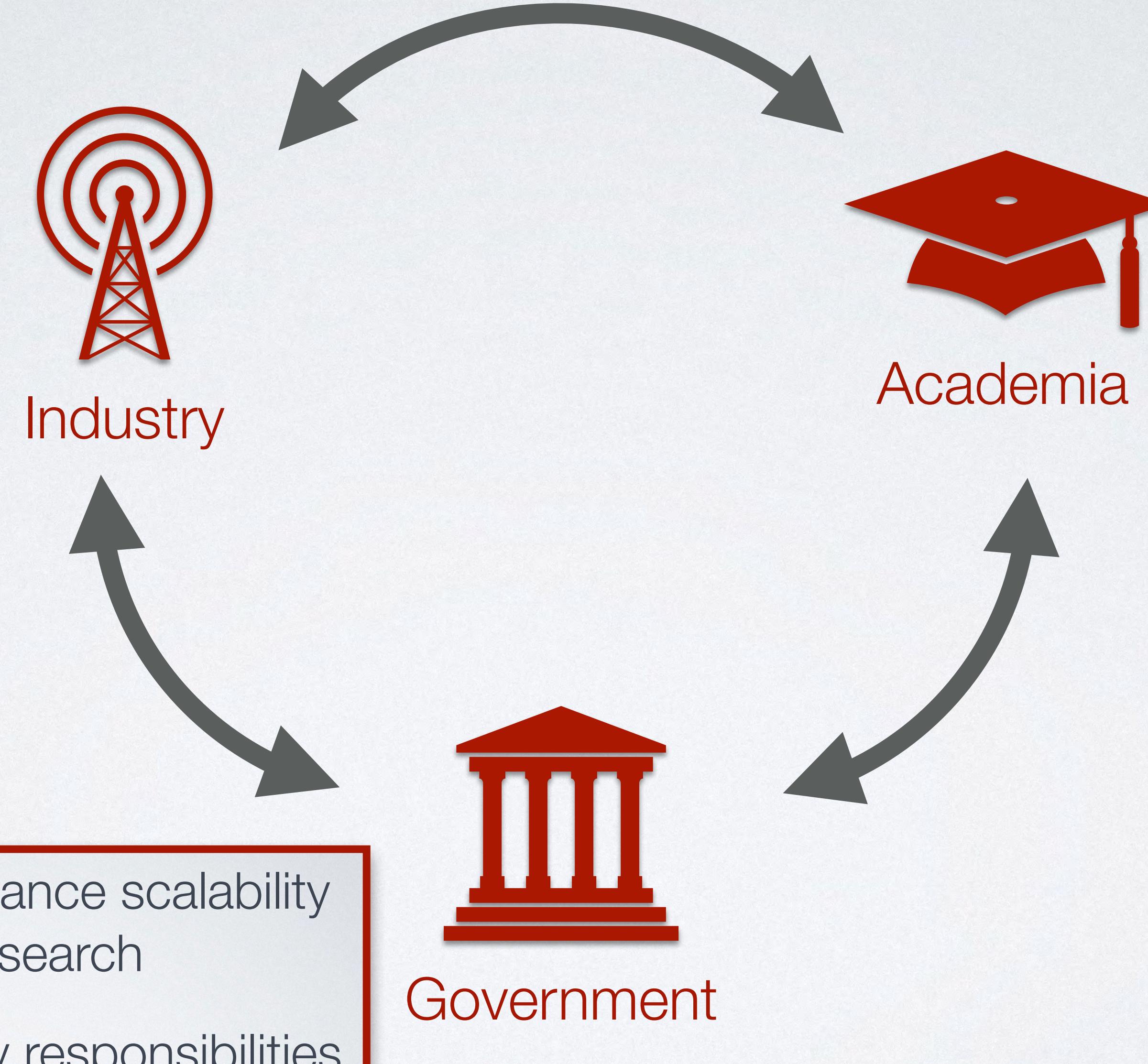
Recent theory & practice:

- explains memorization by in deep learning
- gives insight into what makes neural networks special
- provides robustness to adversarial inputs
- helps make systems faster and training easier

Leadership requires sustained investment in both applications and foundations of AI with partnerships among academia, government, and industry.

# Partnerships between academia, industry, government

Understands full spectrum of operating modes  
Transitions academic advances to consumers



Foundational contributions  
Understanding, predicting, and preventing failure modes  
Training next generation of AI experts

Advances high-performance scalability of academic research  
Oversight and regulatory responsibilities