Seiso

Cutting Through The Buzz

Machine Learning & Artificial Intelligence

Jon Zeolla

2017-10-20

Seiso

$ whoami

- Pittsburgh native **security professional**
- **CTO and Co-Founder of Seiso**, an Information Security consulting company
- **Founder of Steel City Information Security**, an InfoSec user group in Pittsburgh
- **Organizer of BSides Pittsburgh**, a Pittsburgh InfoSec Conference
- **Apache Software Foundation Committer**, working on an open source large scale security monitoring and analysis platform called Apache Metron
- **Prior work** in Retail, Banking, at a Managed Service Provider, and at a Research Institution
- **Interests** - Distributed Systems, Automation and Orchestration, Data Analysis, Network Security Monitoring, Applied Cryptography, and Endpoint Security

https://github.com/jonzeolla https://www.linkedin.com/in/jonzeolla/ Jon.Zeolla@SeisoLLC.com

Seiso

Software Engineering Institute
Carnegie Mellon University

2017 Emerging Technology Domains Risk Survey

Daniel Klinedinst
Joel Land
Kyle O'Meara

October 2017

TECHNICAL REPORT
CMU/SEI-2017-TR-008

https://resources.sei.cmu.edu/asset_files/TechnicalReport/2017_005_001_505319.pdf

Seiso

This report also identifies the domains that should be prioritized for further study based on a number of factors. Three domains must be considered high priority for outreach and analysis in 2017:

1. Intelligent Transportation Systems
2. Machine Learning
3. Smart Robots

https://resources.sei.cmu.edu/asset_files/TechnicalReport/2017_005_001_505319.pdf

Seiso

Table 3: Severity Classifications and Impact Scores

Class	Safety-Related Severity	Class	Privacy-Related Severity
S0	No Injuries	**S0**	No unauthorized access to data
S1	Light or moderate injuries	**S1**	Anonymous data only
S2	Severe and life-threatening injuries (survival probable) *Light or moderate injuries for multiple people*	**S2**	Identification of person (personally identifiable information) or technology *Anonymous data for multiple people*
S3	Life threatening (survival uncertain) or fatal injuries *Severe injuries for multiple people*	**S3**	Tracking of individual or technology *Identification of multiple people or technologies*
S4	Life threatening or fatal injuries for multiple people	**S4**	Tracking of multiple people or technologies
Class	**Financial-Related Severity**	**Class**	**Operational-Related Severity**
S0	No financial loss	**S0**	No impact on operational performance
S1	Low-level loss (~$10)	**S1**	Impact not discernible to user
S2	Moderate loss (~$100) *Low losses for multiple people*	**S2**	User aware of performance degradation *Indiscernible impacts for multiple users*
S3	Heavy loss (~$1,000) *Moderate losses for multiple people*	**S3**	Significant impact on performance *Noticeable impact for multiple users*
S4	Heavy losses for multiple people	**S4**	Significant impact for multiple users

https://resources.sei.cmu.edu/asset_files/TechnicalReport/2017_005_001_505319.pdf

Seiso

Definitions

- **Artificial General Intelligence** (AGI): The intelligence of a machine that could successfully perform any intellectual task that a human being can.

- **Artificial Intelligence** (AI): Any device that perceives its environment and takes actions that maximize its chance of success at some goal.

- **Machine Learning** (ML): A method that gives computers the ability to learn without being explicitly programmed.

Seiso

Definitions

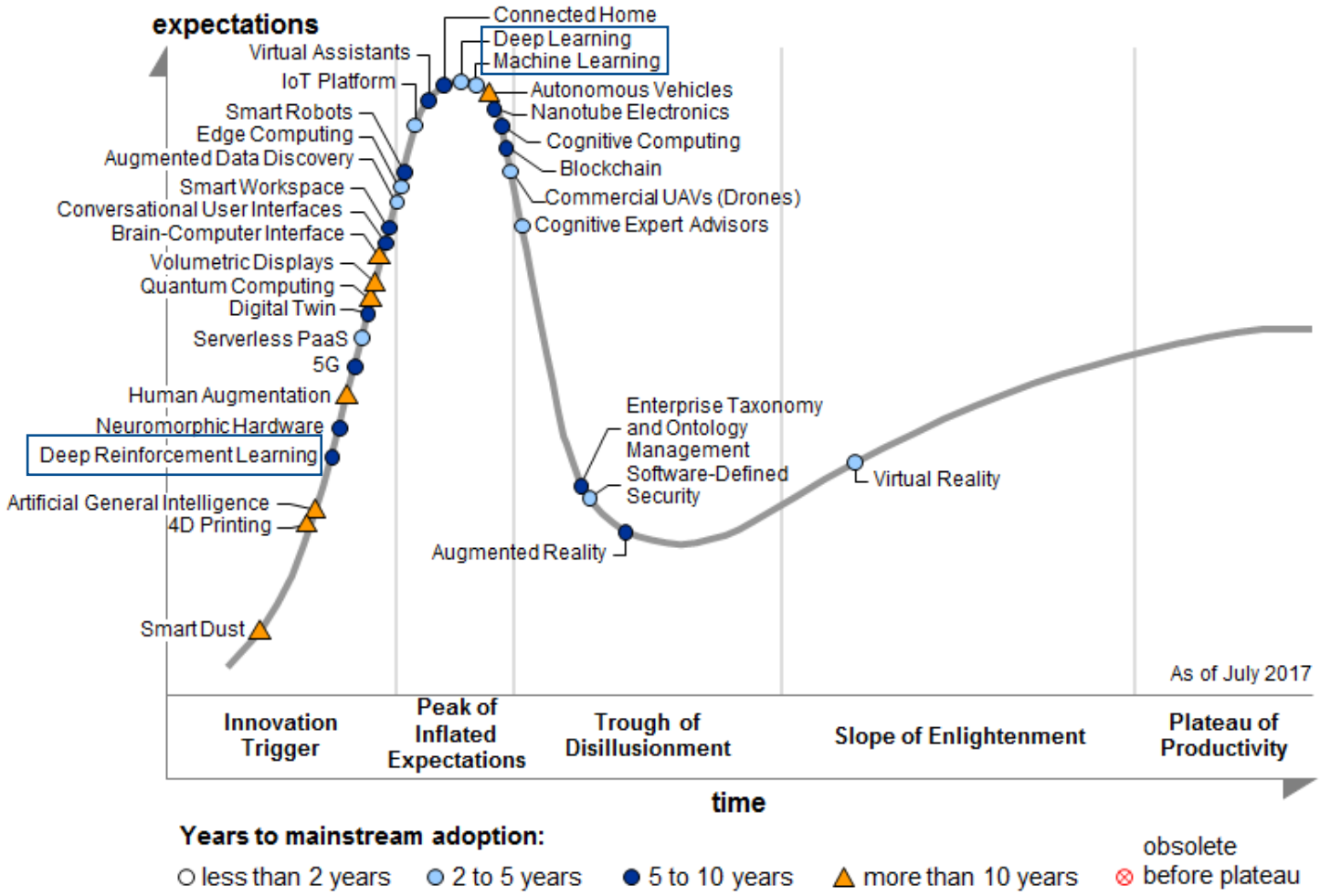
- **Deep Learning**: A part of a family of machine learning methods based on learning data representations, often mirroring neurons in the brain.

- **Data Science**: An interdisciplinary field about scientific methods, processes, and systems to extract knowledge or insights from data in various forms, either structured or unstructured, similar to data mining

Seiso

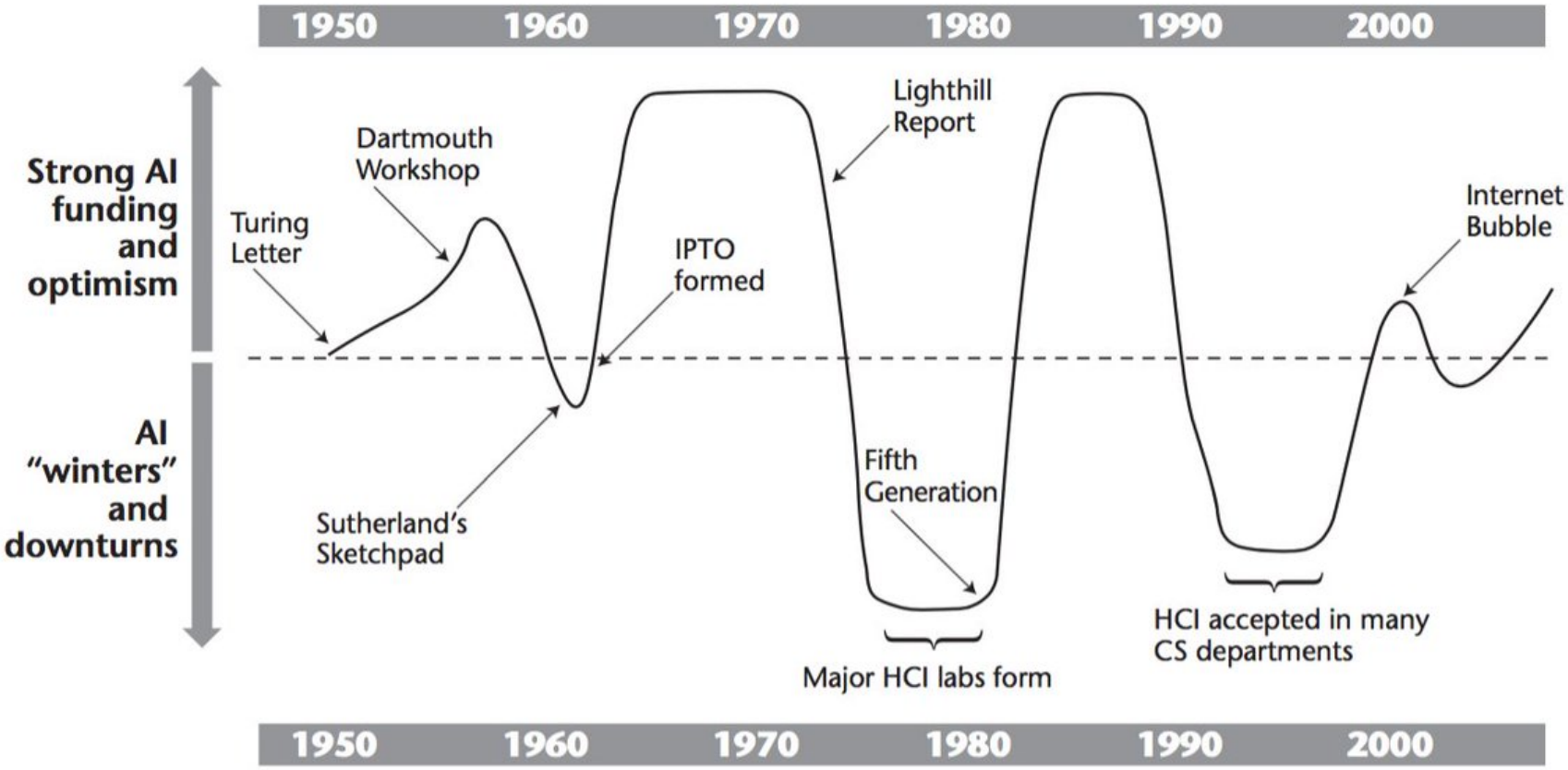
Where we are now

Hype Cycles



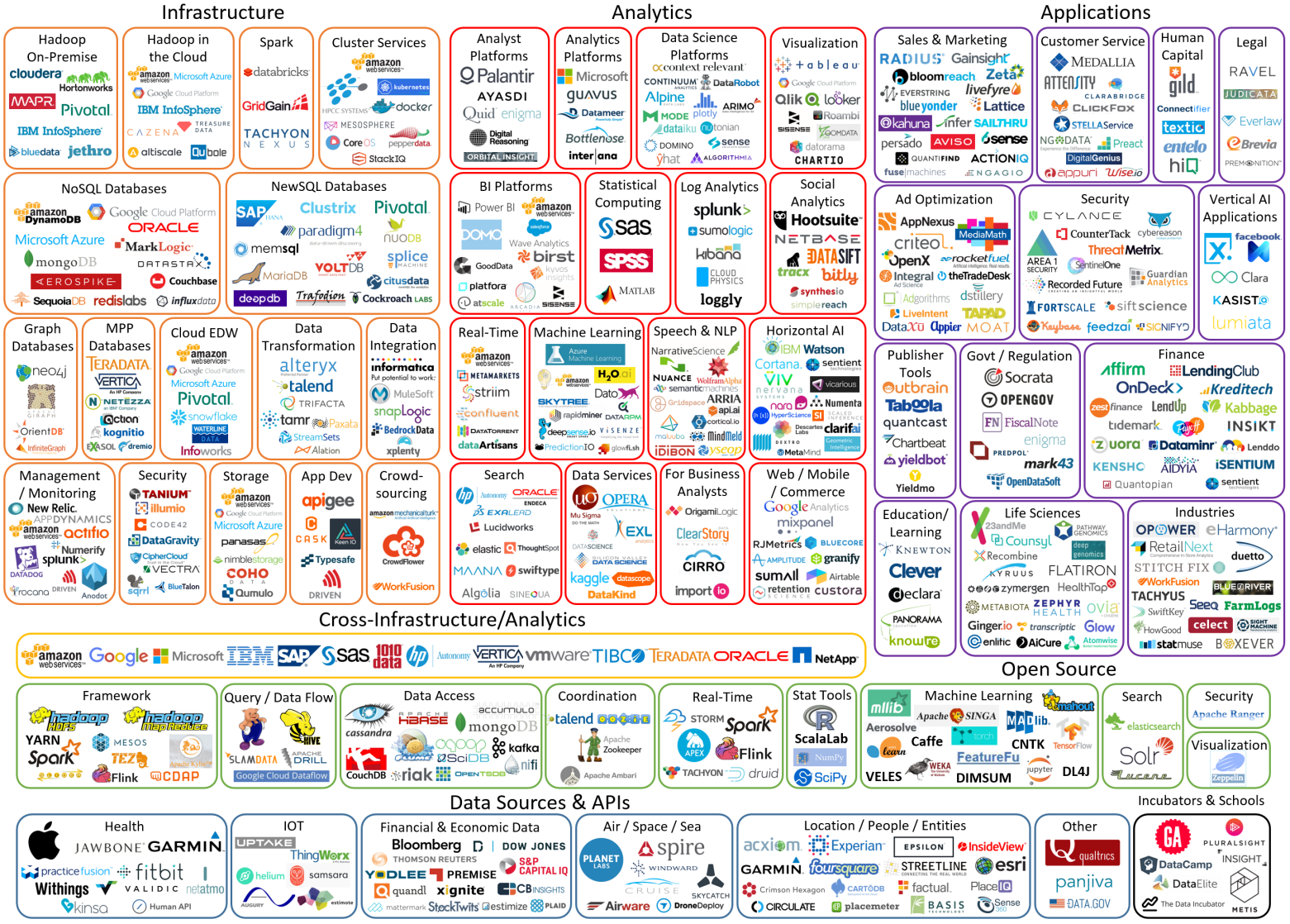
http://www.gartner.com/newsroom/id/3784363

Hype Cycles (AI)



https://docs.google.com/presentation/d/119VW6ueBGLQXsw-jGMboGP2-WuOnyMAOYLgd44SL6xM/preview?slide=id.g1e3df2d686_0_1639

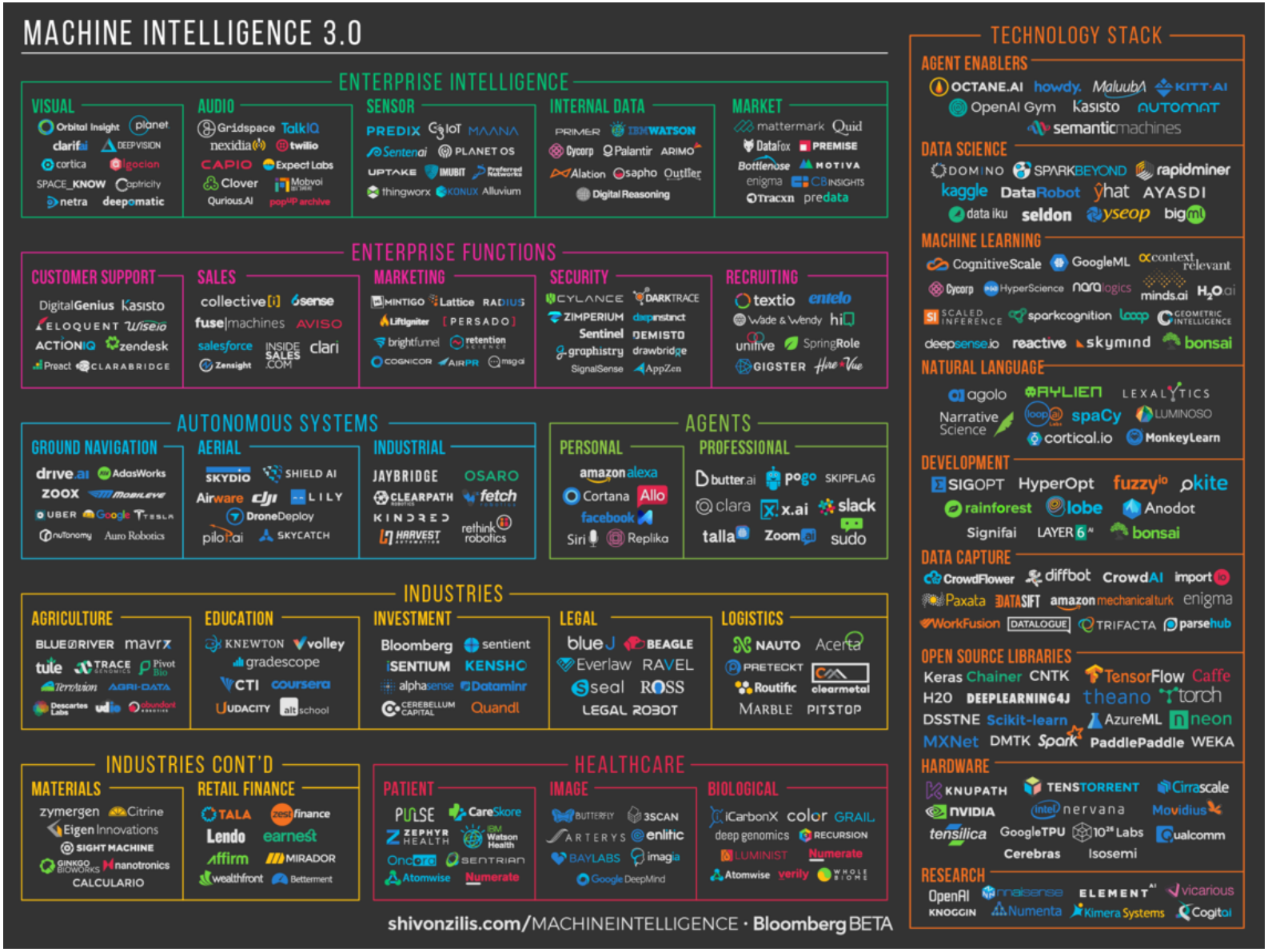
Big Data Landscape 2016 (Version 3.0)



Last Updated 3/23/2016

© Matt Turck (@mattturck), Jim Hao (@jimrhao), & FirstMark Capital (@firstmarkcap)

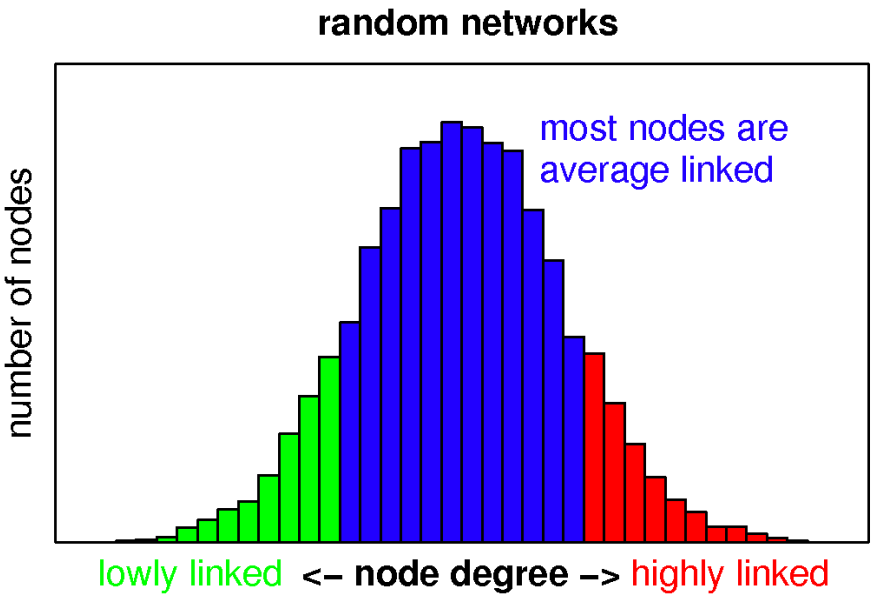
http://mattturck.com/wp-content/uploads/2016/03/Big-Data-Landscape-2016-v18-FINAL.png



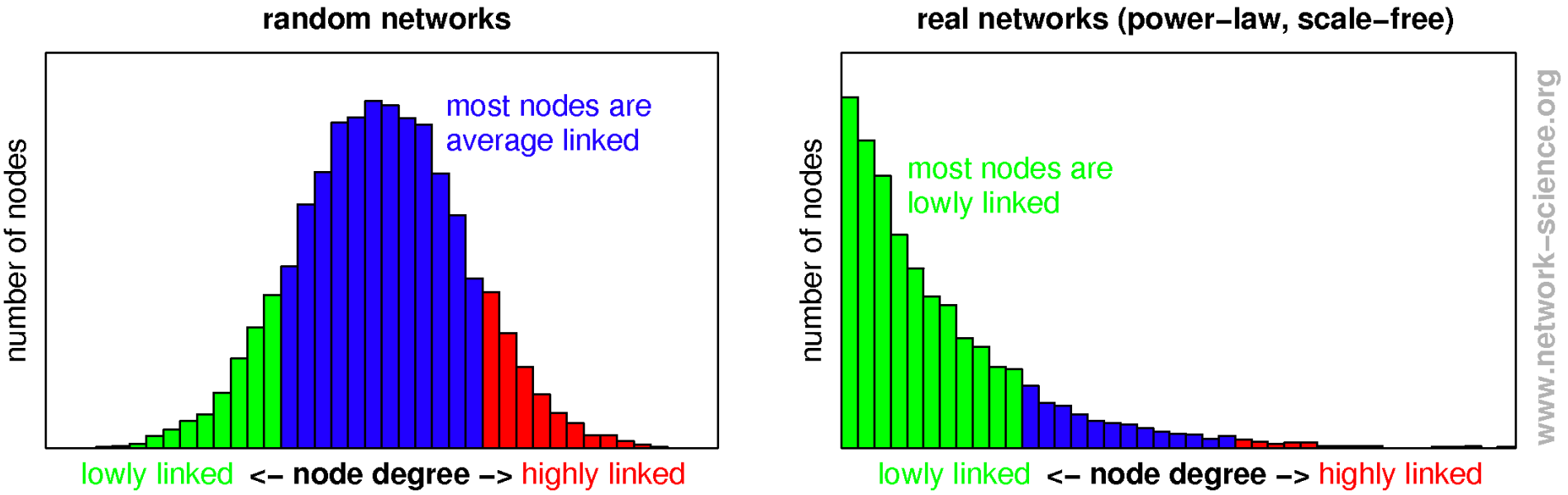
http://www.shivonzilis.com/machineintelligence

Seiso

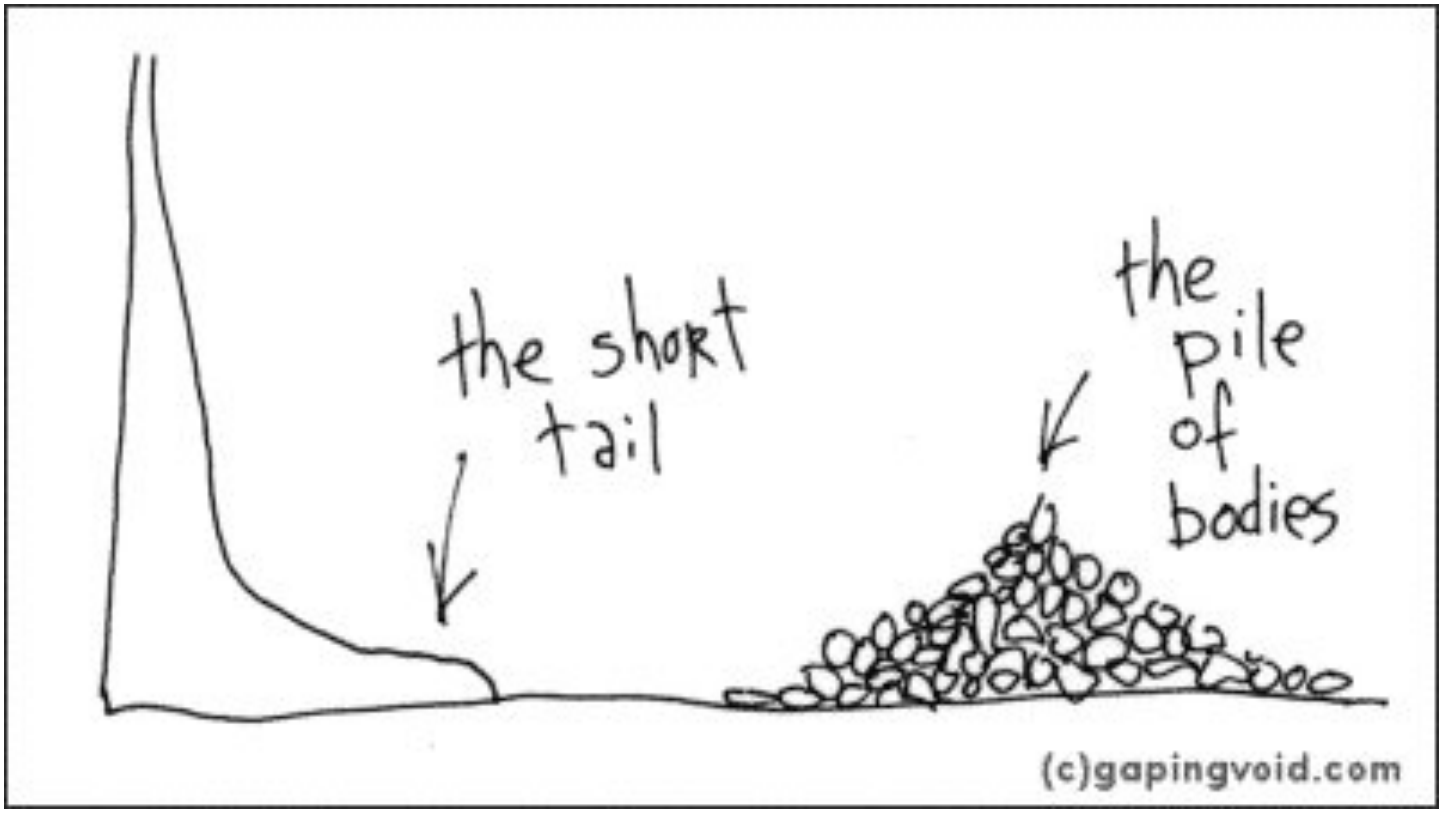
Isn’t ML just statistics?



http://www.network-science.org/fig_complex_networks_powerlaw_scalefree_node_degree_distribution.png

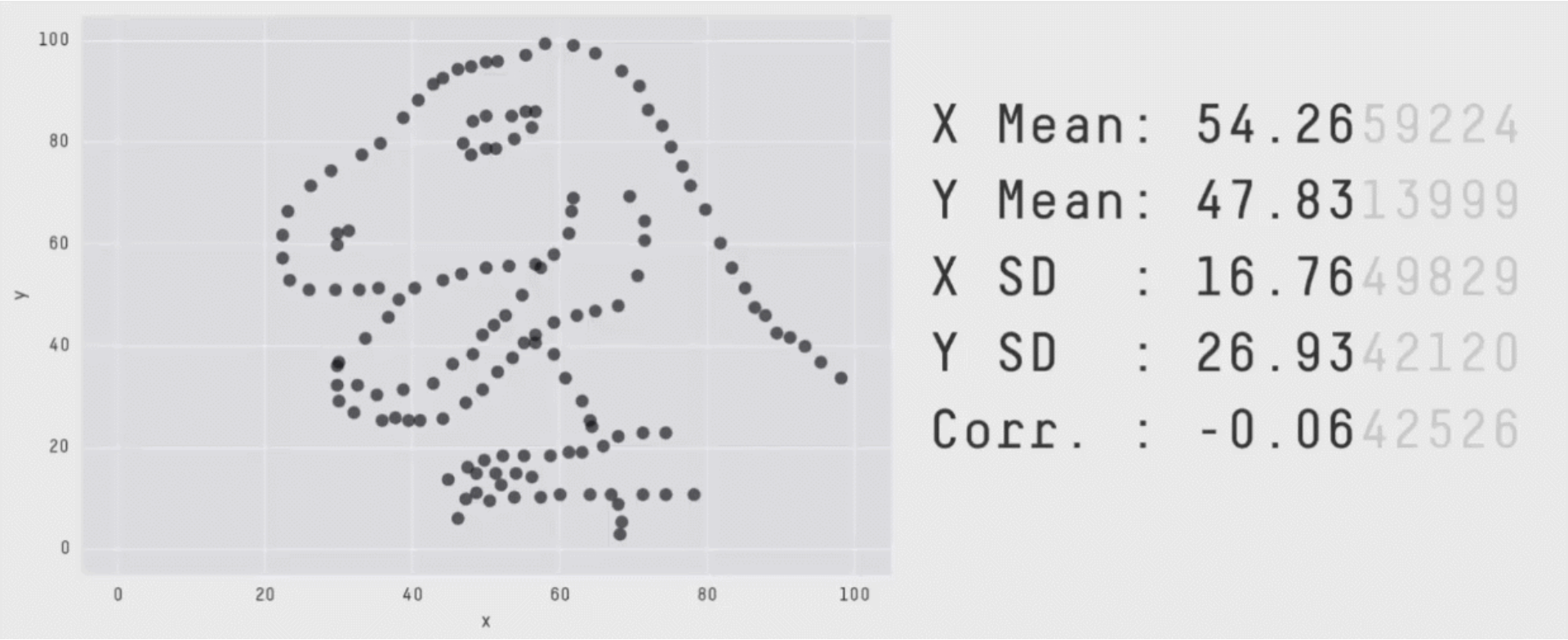


http://www.network-science.org/fig_complex_networks_powerlaw_scalefree_node_degree_distribution.png



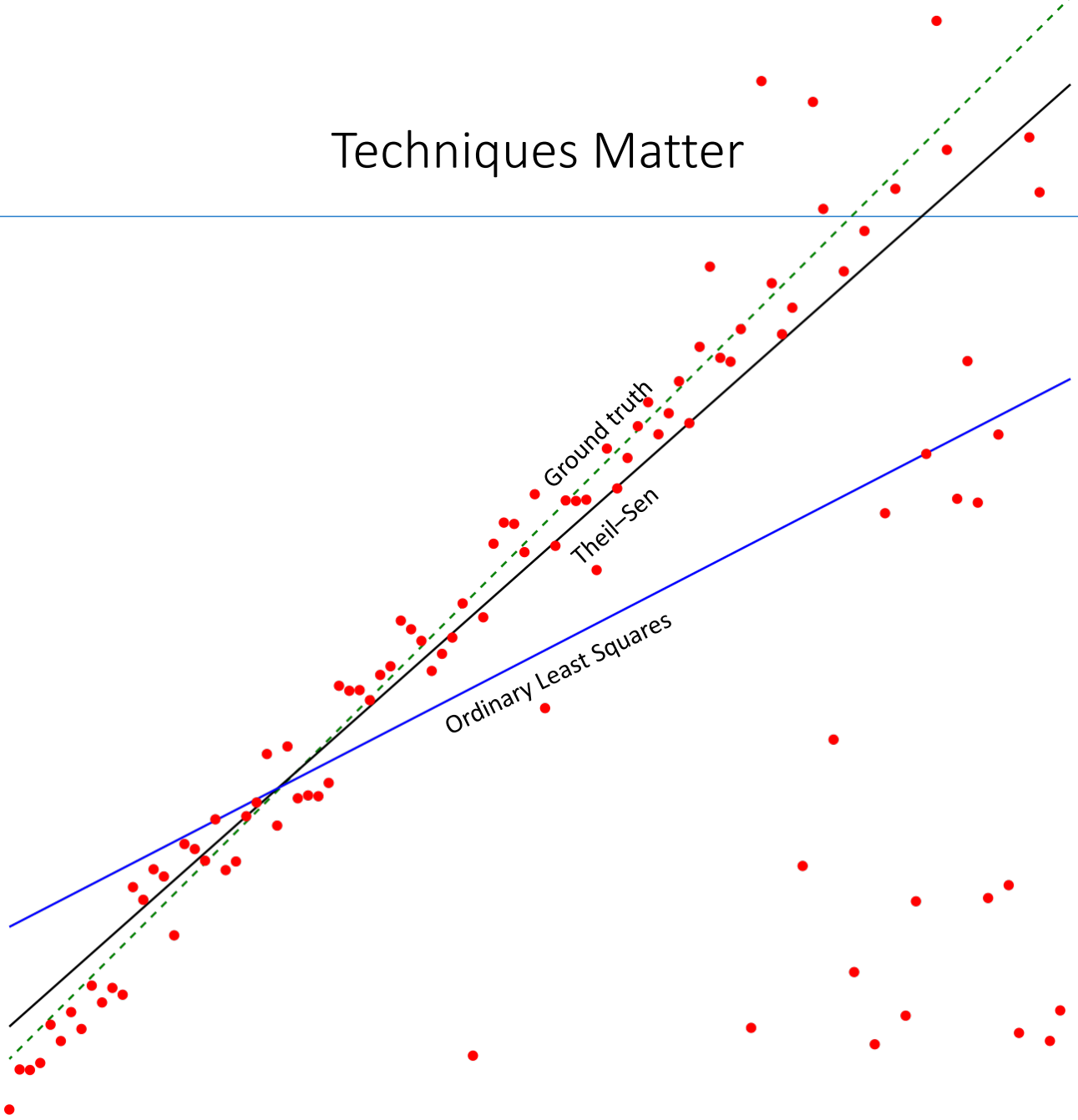
http://netdna.copyblogger.com/images/death-by-long-tail.jpg

Lying with Statistics (datasauRus)



https://github.com/stephlocke/lazyCDN/blob/master/DinoSequential.gif?raw=true

Techniques Matter

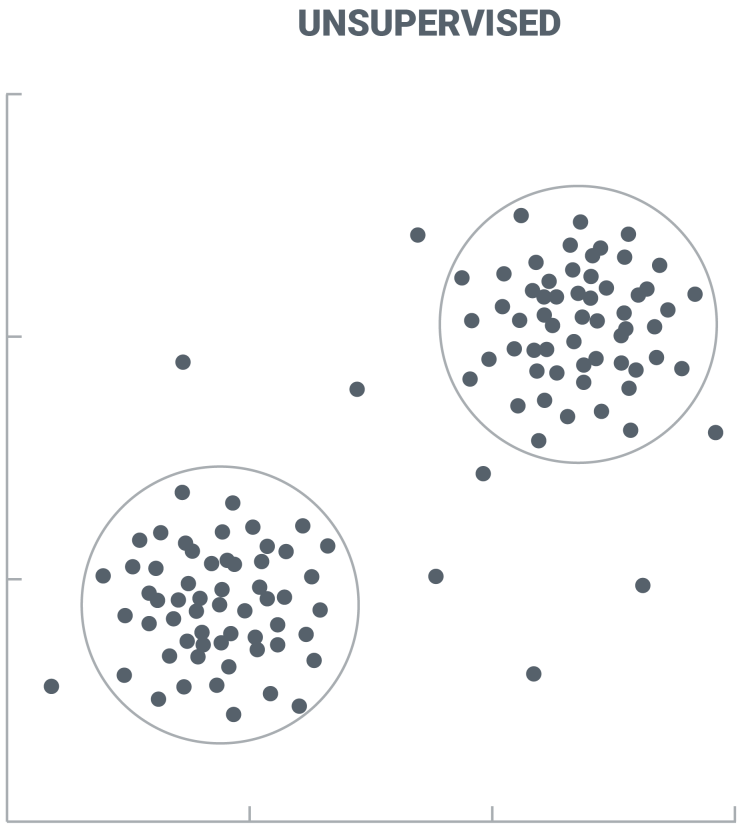


https://en.wikipedia.org/wiki/Theil%E2%80%93Sen_estimator

Seiso

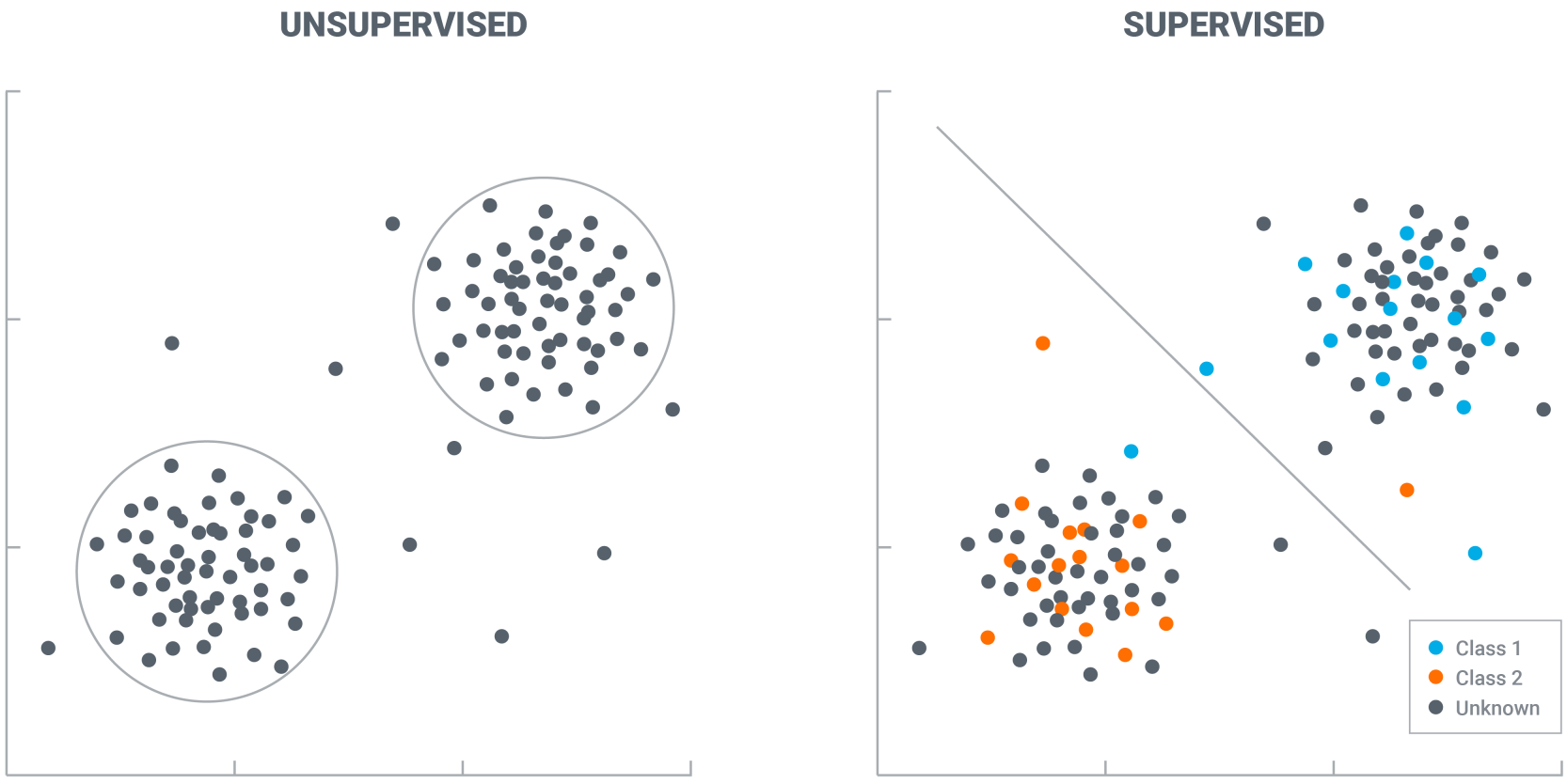
Core Characteristics
Of Machine Learning

Types of Machine Learning



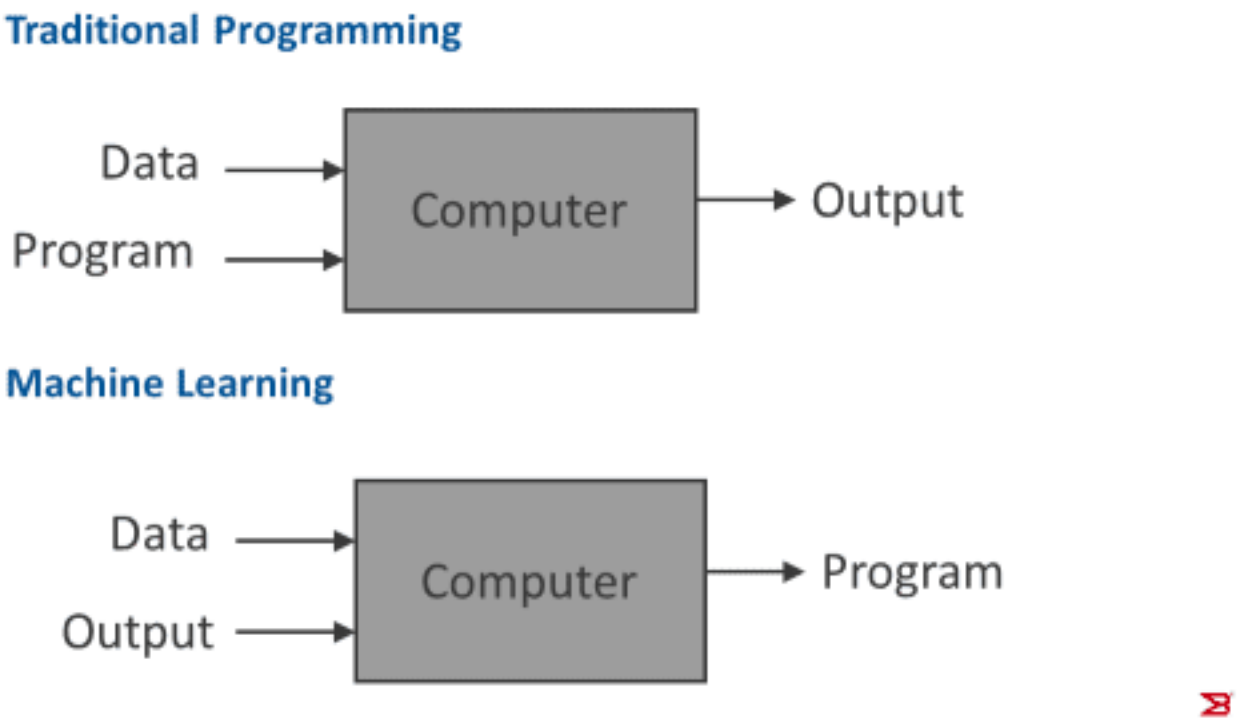
http://cdn2.hubspot.net/hubfs/305377/Supervised_vs_Unsupervised_ML.png

Types of Machine Learning



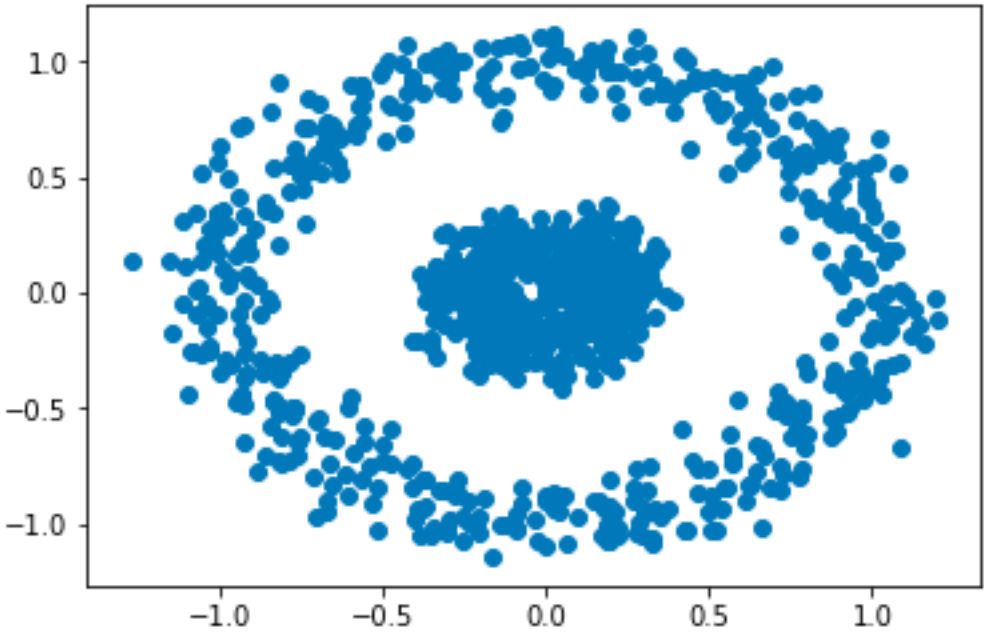
http://cdn2.hubspot.net/hubfs/305377/Supervised_vs_Unsupervised_ML.png

Data is necessary to create the program



https://inform.tmforum.org/wp-content/uploads/2017/08/BL-blog-traditional-programming.png

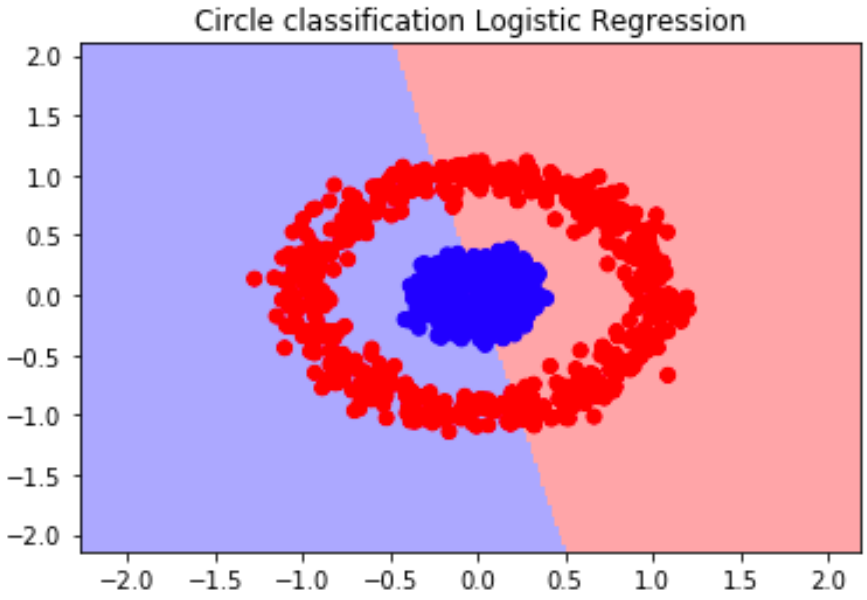
Some algorithms have assumptions



Pulled from materials from Sinan Ozdemir (https://www.linkedin.com/in/sinan-ozdemir/)

Some algorithms have assumptions

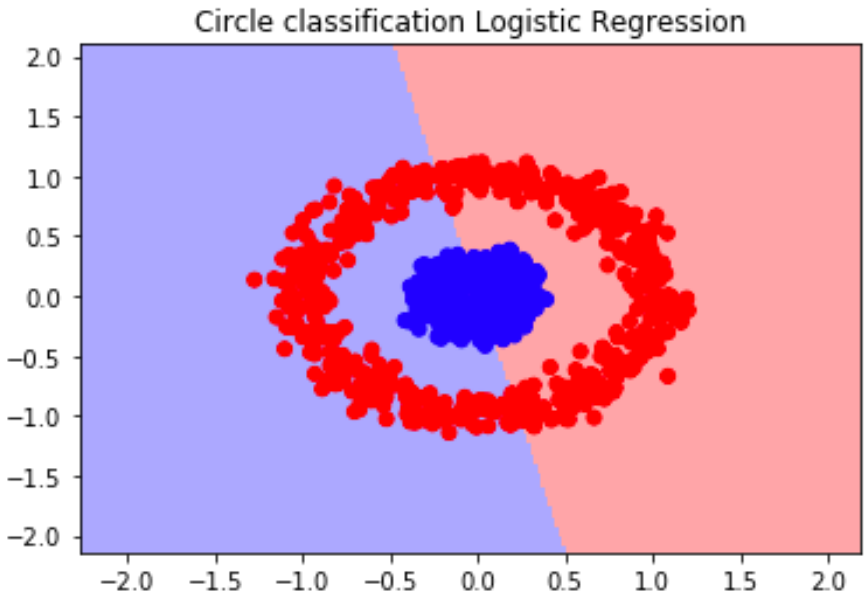
Parametric



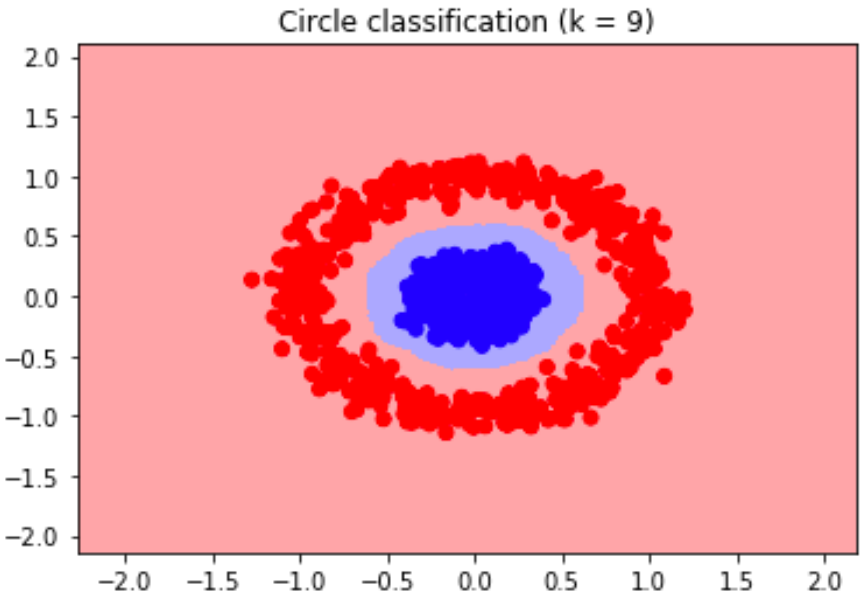
Pulled from materials from Sinan Ozdemir (https://www.linkedin.com/in/sinan-ozdemir/)

Some algorithms have assumptions

Parametric



Non-Parametric



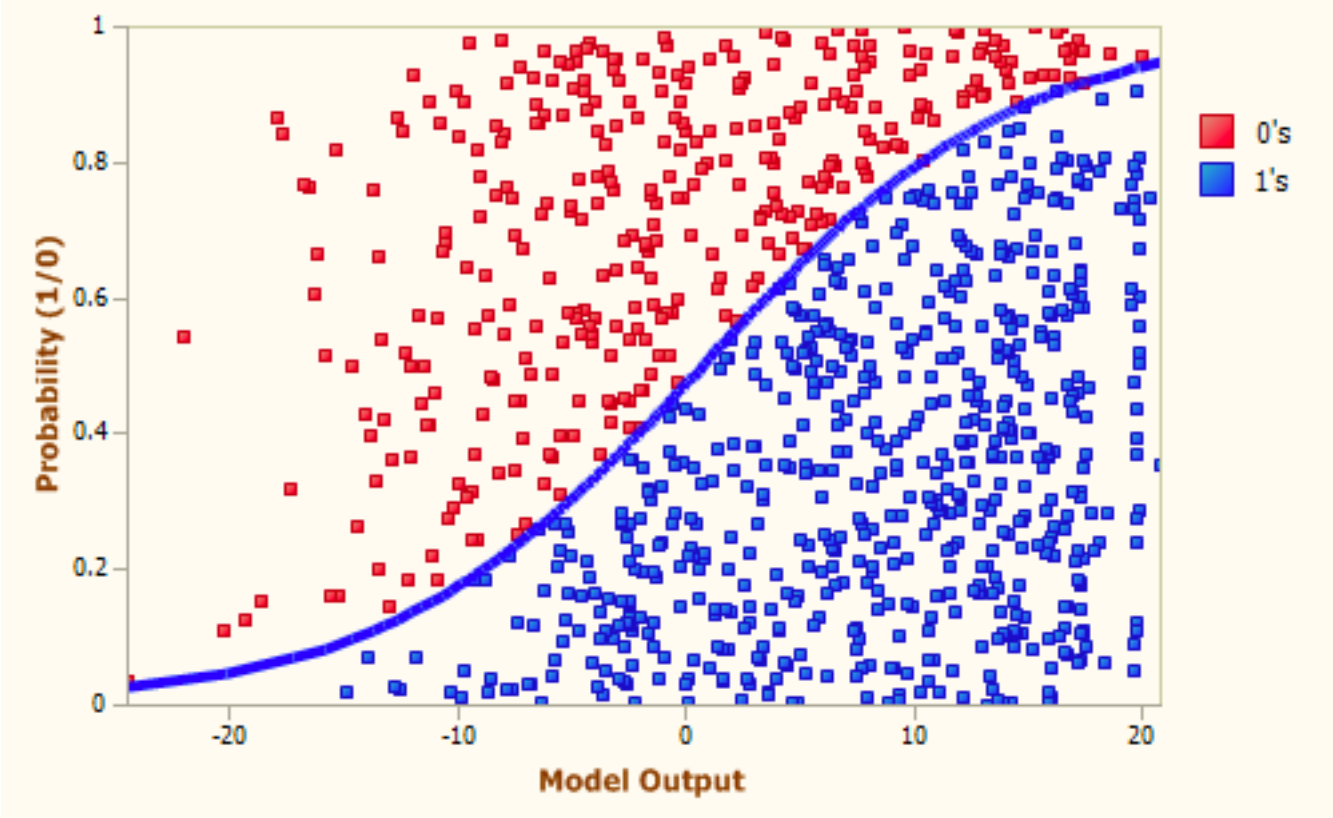
Pulled from materials from Sinan Ozdemir (https://www.linkedin.com/in/sinan-ozdemir/)

Not everything can be explained – should we care?

> We want our machine learning systems to be explainable, and frankly many of them are already more explainable than humans are.
>
> —Maya Gupta Google

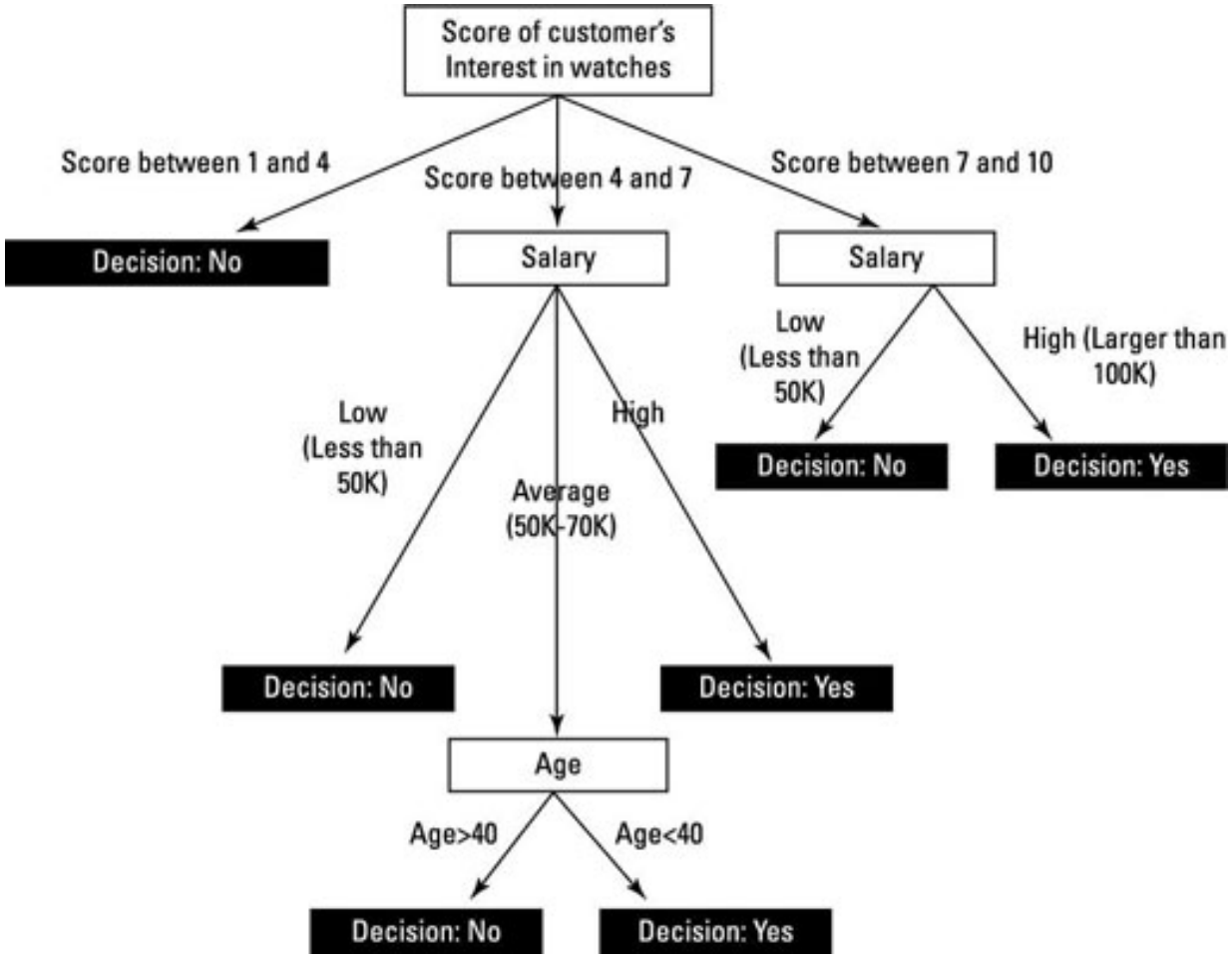
https://www.google.com/intl/en/about/gender-balance-diversity-important-to-machine-learning/

Not everything can be explained – should we care?



https://media.licdn.com/mpr/mpr/AAEAAQAAAAAAAAkUAAAAJDJlMDNjMGM5LTlmZjktNDlhNy1iNmNmLTE5NTM1YjE3NzA0Yw.png

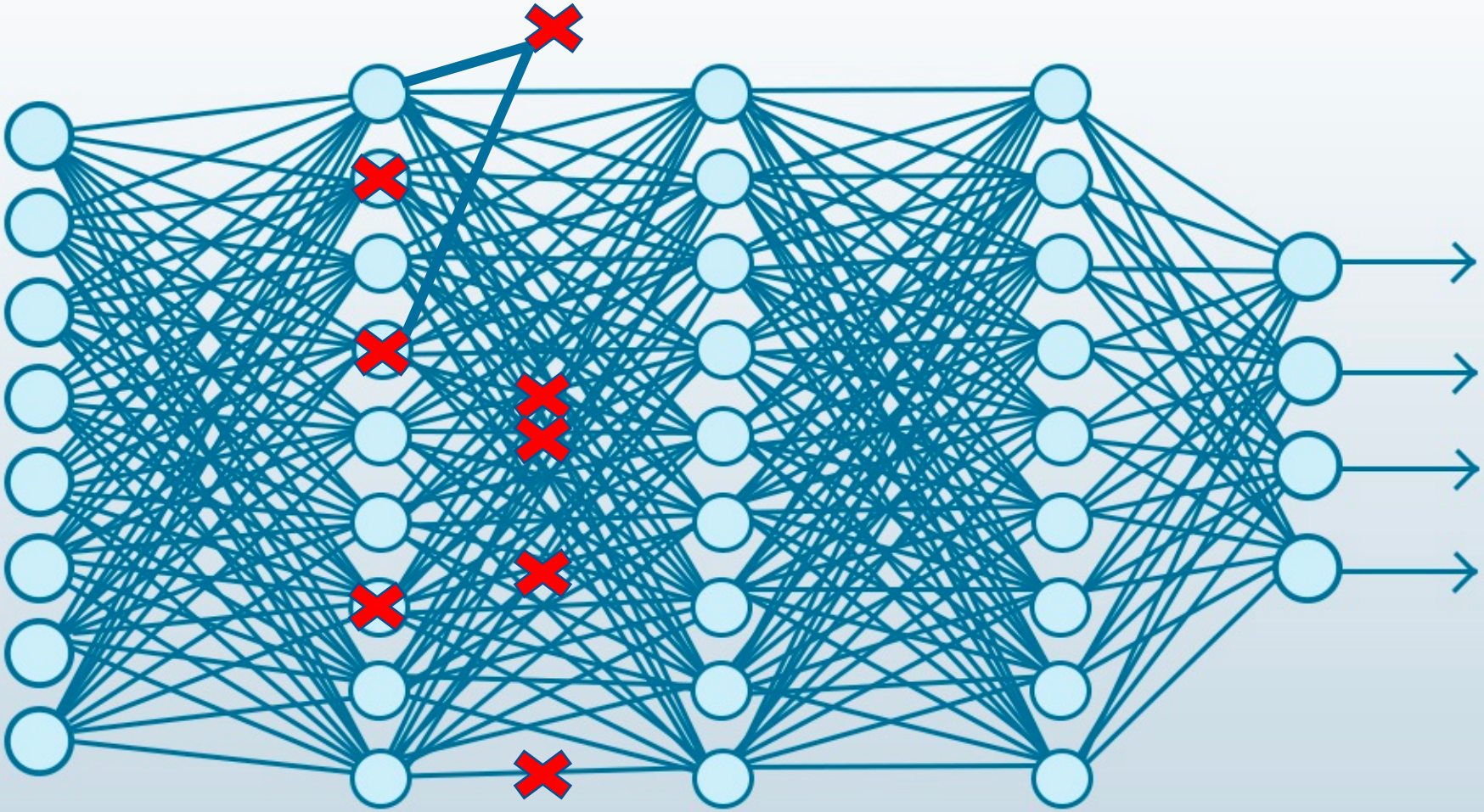
Not everything can be explained – should we care?



http://d2r5da613aq50s.cloudfront.net/wp-content/uploads/421637.image1.jpg

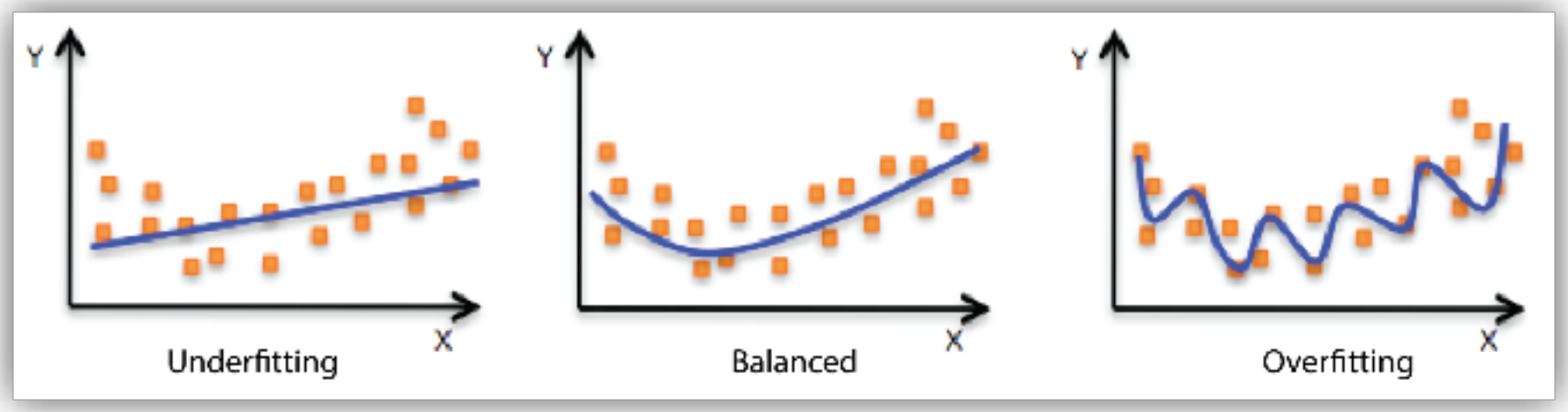
Seiso

Not everything can be explained – should we care?



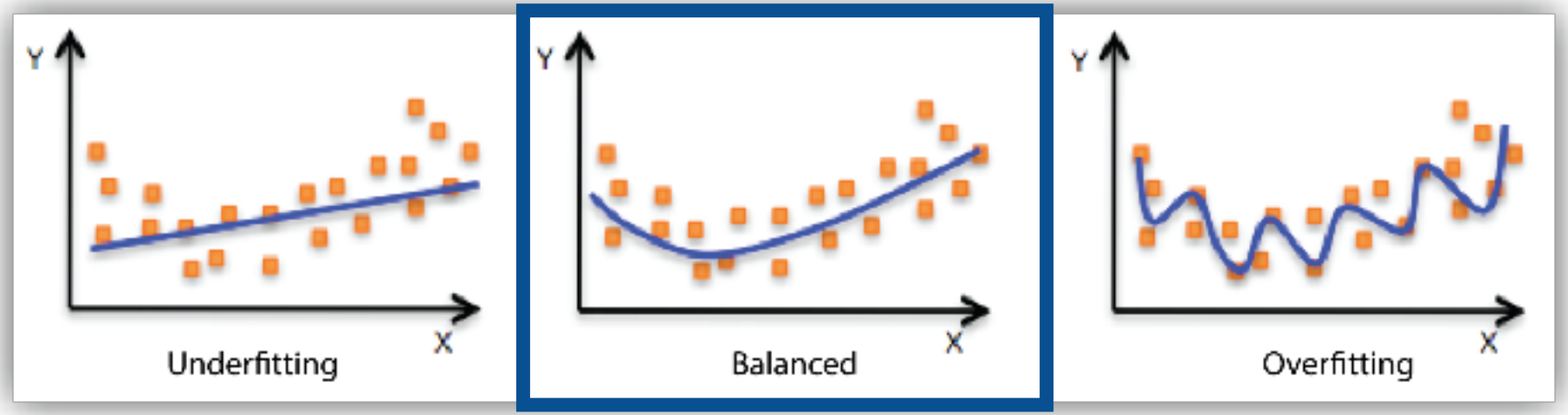
http://www.rsipvision.com/wp-content/uploads/2016/02/Machine-Learning.jpg

Everything has tradeoffs



http://docs.aws.amazon.com/machine-learning/latest/dg/model-fit-underfitting-vs-overfitting.html

Everything has tradeoffs

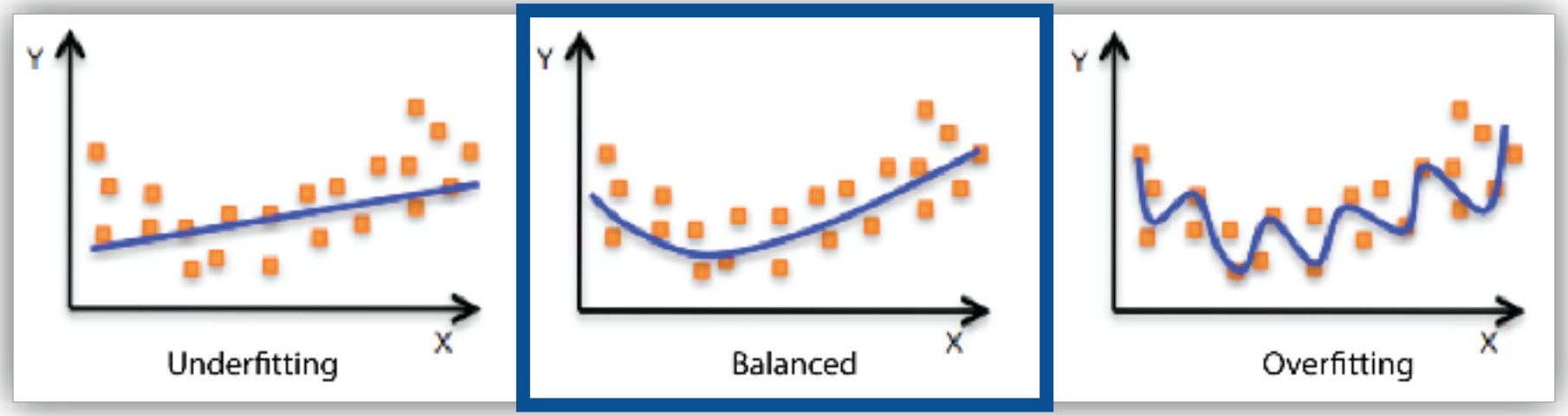


High bias, low variance

Low bias, high variance

http://docs.aws.amazon.com/machine-learning/latest/dg/model-fit-underfitting-vs-overfitting.html

Everything has tradeoffs



High bias, low variance

Still some level of False Positive

Low bias, high variance

http://docs.aws.amazon.com/machine-learning/latest/dg/model-fit-underfitting-vs-overfitting.html

The potential benefits are enormous

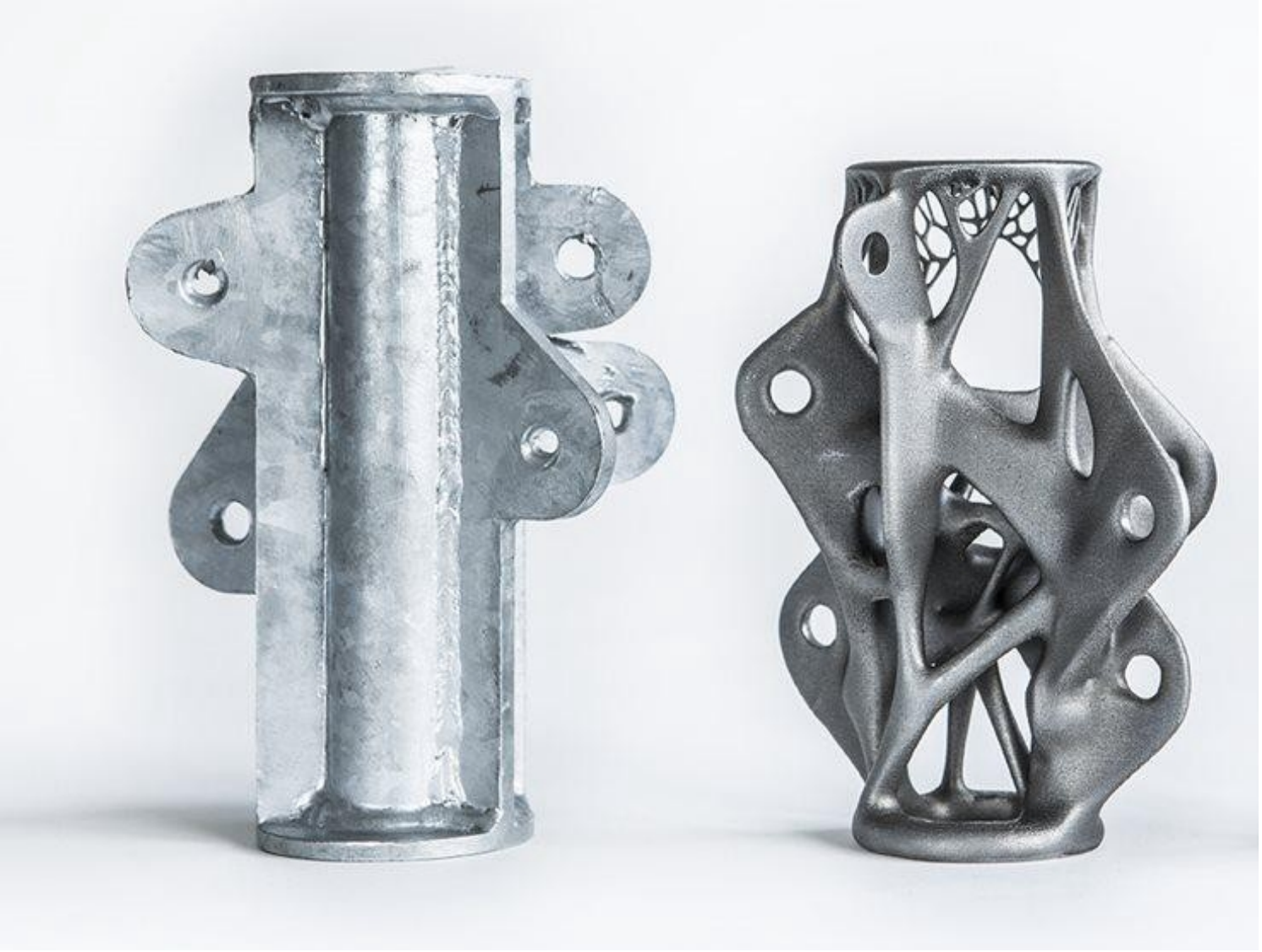
Click Me

https://www.youtube.com/watch?v=AAQB-Fny36A

The potential benefits are enormous

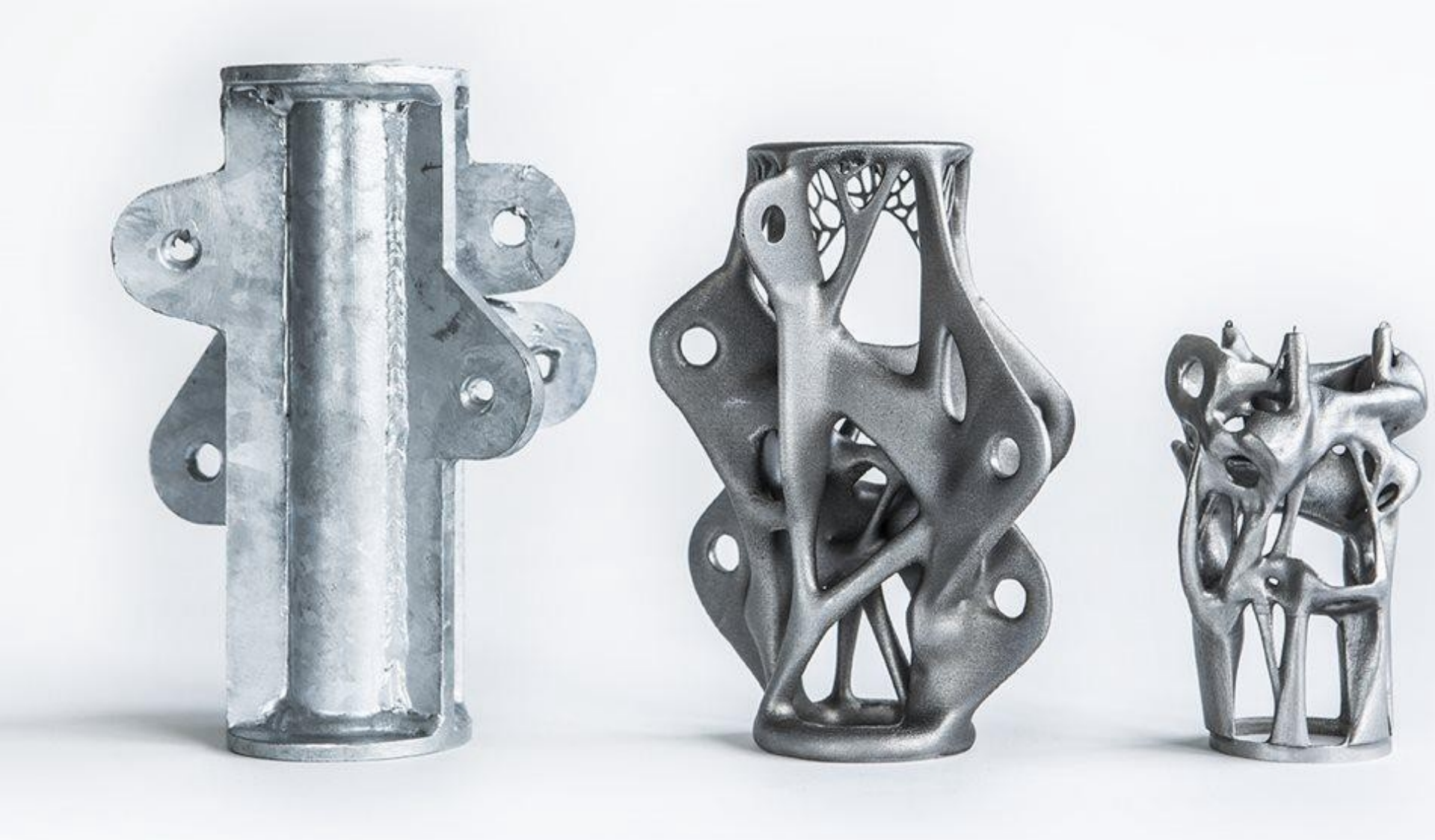
https://www.arup.com/news-and-events/news/3d-makeover-for-hyperefficient-metalwork

The potential benefits are enormous



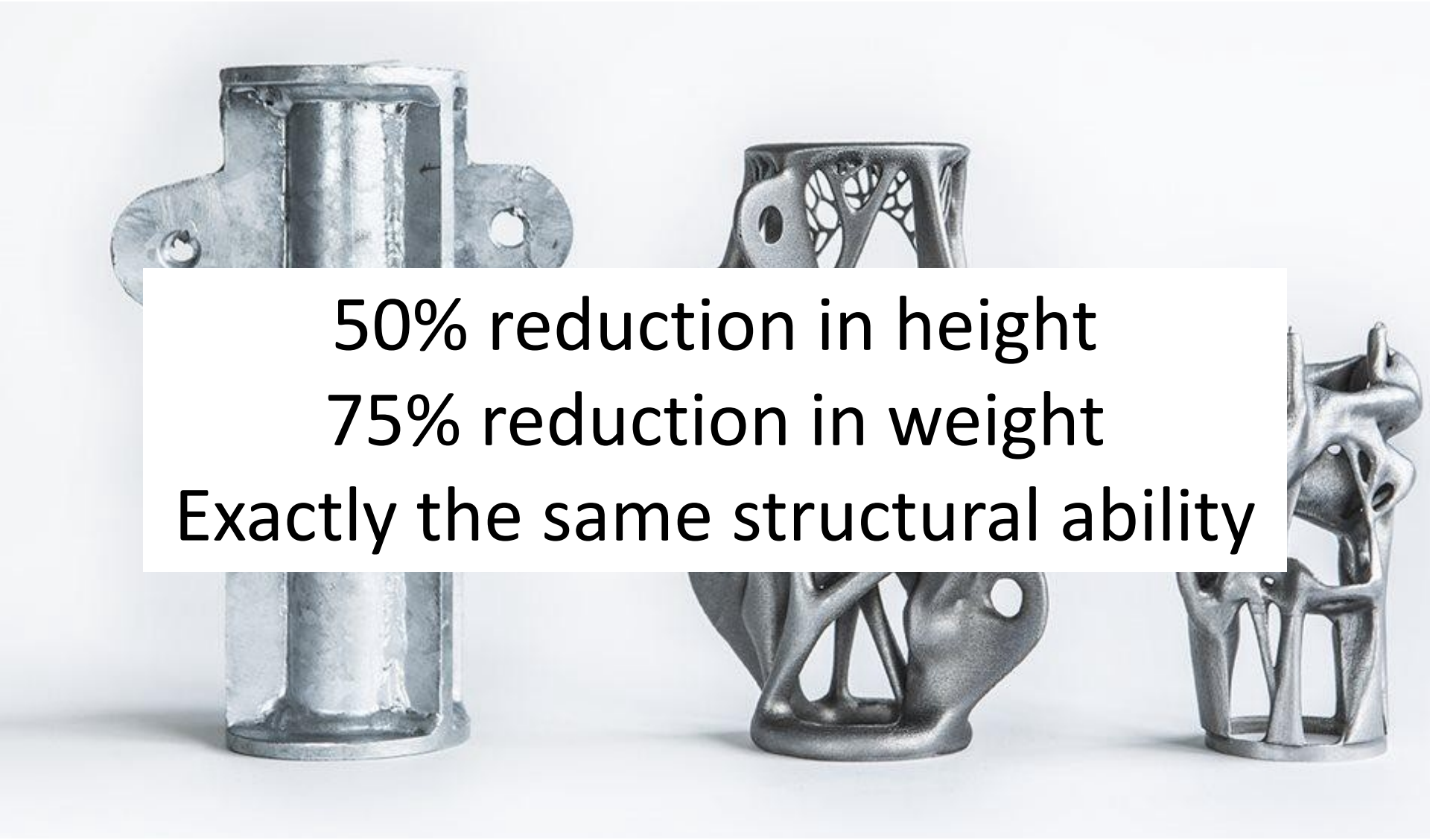
https://www.arup.com/news-and-events/news/3d-makeover-for-hyperefficient-metalwork

The potential benefits are enormous



https://www.arup.com/news-and-events/news/3d-makeover-for-hyperefficient-metalwork

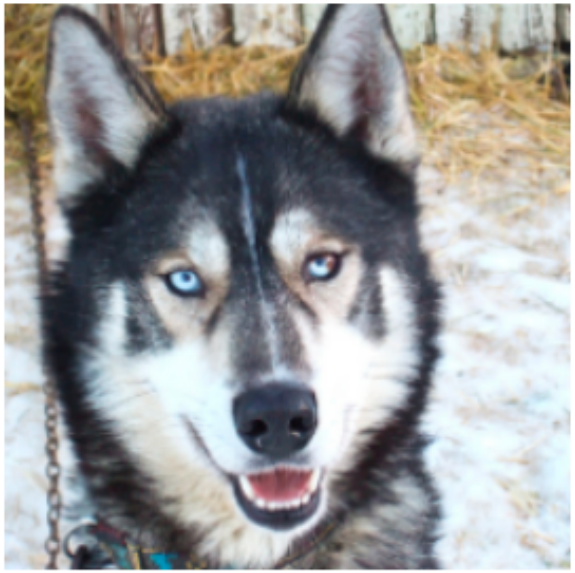
The potential benefits are enormous



50% reduction in height
75% reduction in weight
Exactly the same structural ability

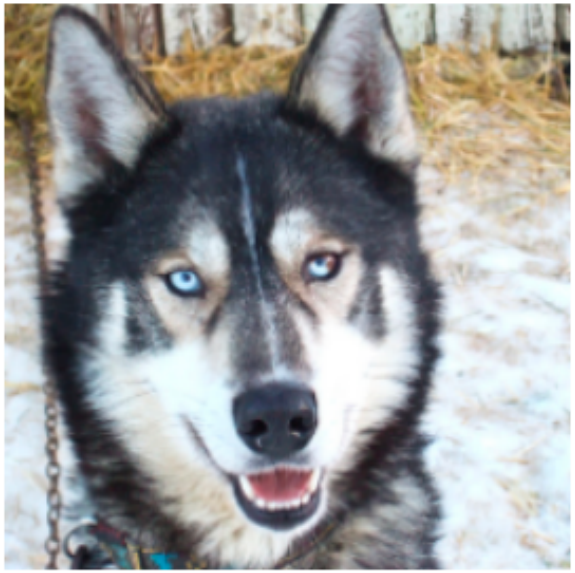
https://www.arup.com/news-and-events/news/3d-makeover-for-hyperefficient-metalwork

http://marcellusdrilling.com/wp-content/uploads/2016/10/under-construction.png



(a) Husky classified as wolf

http://www.kdd.org/kdd2016/papers/files/rfp0573-ribeiroA.pdf



(a) Husky classified as wolf

(b) Explanation

http://www.kdd.org/kdd2016/papers/files/rfp0573-ribeiroA.pdf

Malicious?

Malicious?

SHA256:	c99caff6b05d6d13629c7eb7d014862da7e2774866b61e7bfca47f53578dca0c
File name:	helloworld.exe
Detection ratio:	7 / 64
Analysis date:	2017-08-10 14:07:06 UTC (0 minutes ago)

Analysis | File detail | Additional information | Comments | Votes

Antivirus	Result
CrowdStrike Falcon (ML)	malicious_confidence_80% (D)
Cylance	Unsafe
Cyren	W32/S-d2b5872a!Eldorado
F-Prot	W32/S-d2b5872a!Eldorado
Sophos ML	heuristic
McAfee-GW-Edition	BehavesLike.Win32.Trojan.nt
SentinelOne (Static ML)	static engine - malicious

10:10 AM - 10 Aug 2017

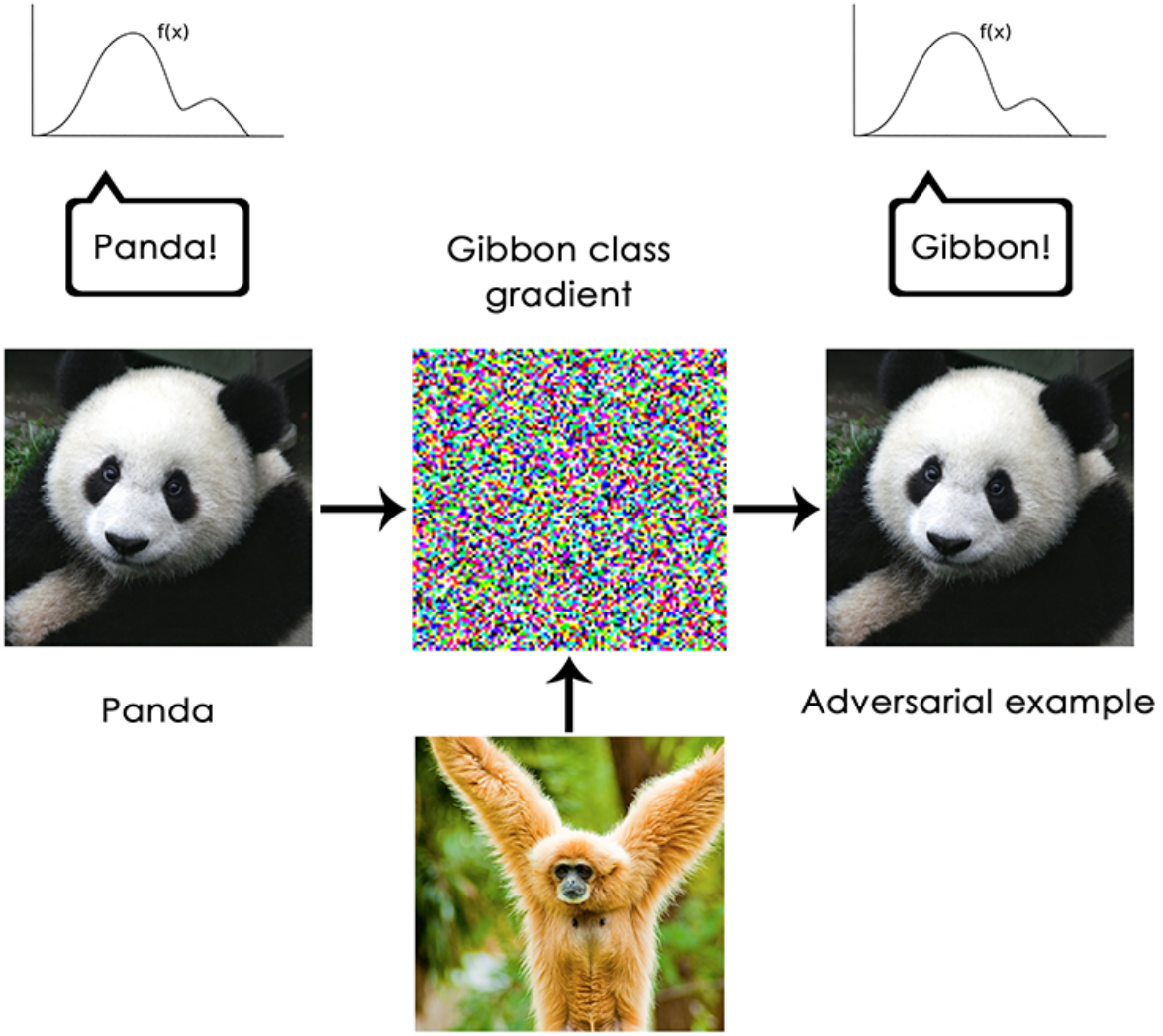
453 Retweets **663** Likes

52 453 663

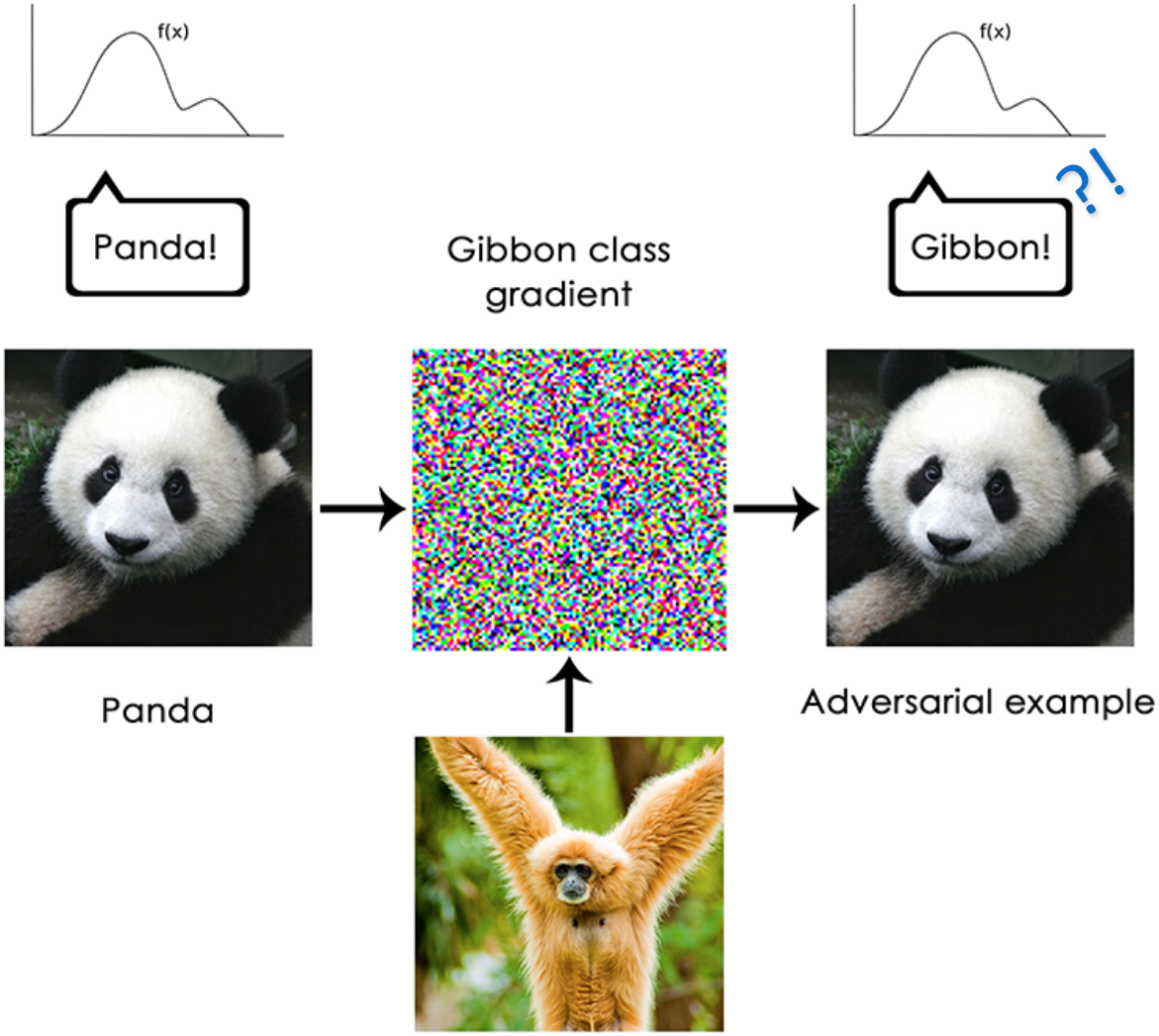
Seiso

Malicious?

Antivirus	Result
CrowdStrike Falcon (ML)	malicious_confidence_80% (D)
Cylance	Unsafe
Cyren	W32/S-d2b5872a!Eldorado
F-Prot	W32/S-d2b5872a!Eldorado
Sophos ML	heuristic
McAfee-GW-Edition	BehavesLike.Win32.Trojan.nt
SentinelOne (Static ML)	static engine - malicious



https://blog.keras.io/img/limitations-of-dl/adversarial_example.png

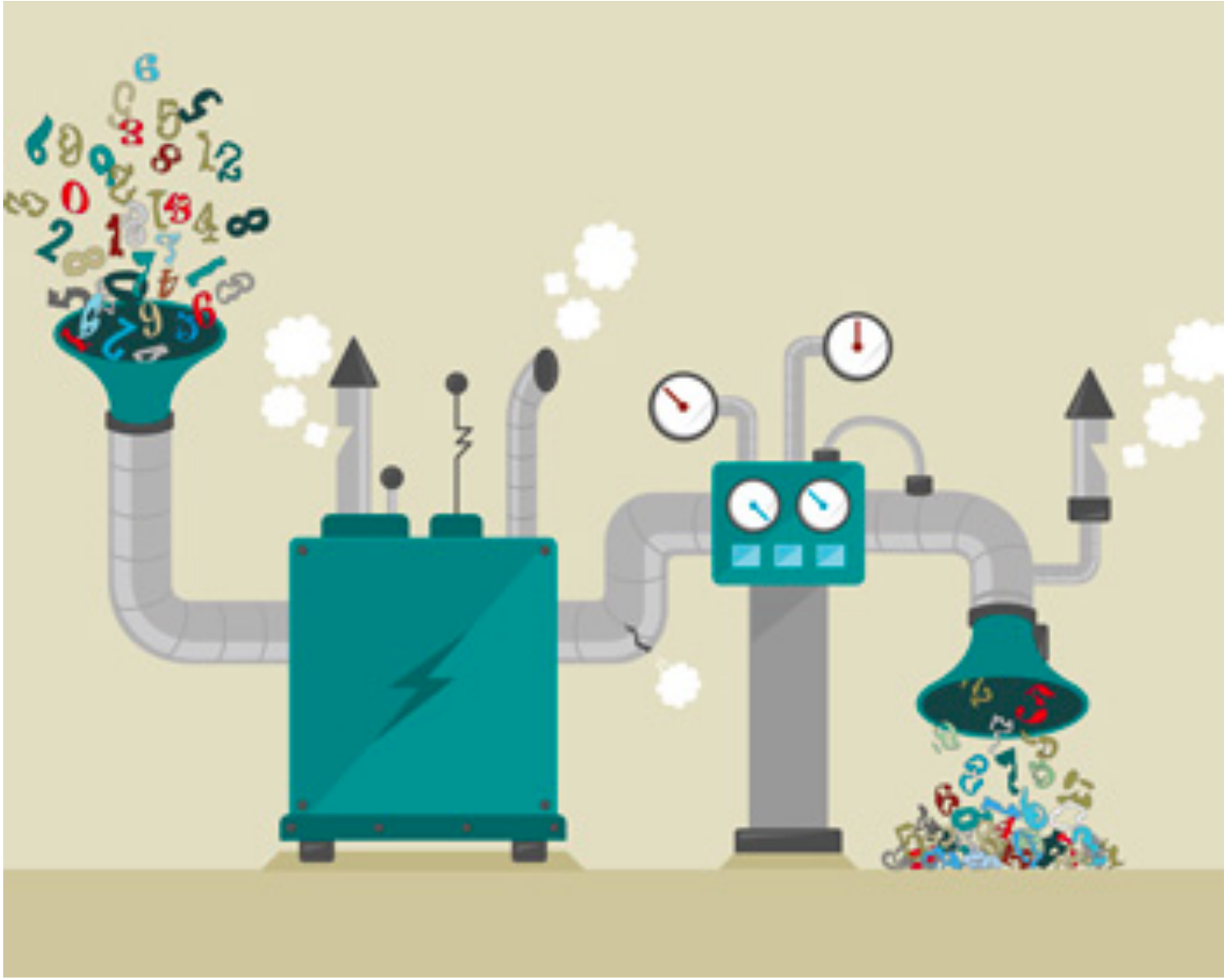


(“Adversarial Attacks and Defenses” competitions at NIPS 2017)

https://blog.keras.io/img/limitations-of-dl/adversarial_example.png

Seiso

The Core Assumption



https://flightsafety.org/wp-content/uploads/2013/10/ASW_oct13_p46-50_ThreatAnalysis.jpg

Seiso

Chihuahua or muffin?

http://imgur.com/a/K4RWn

Labradoodle or fried chicken?

http://imgur.com/a/K4RWn

Sheepdog or mop?

http://imgur.com/a/K4RWn

Seiso

When can ML **NOT** be useful?

Seiso

Caution!

- Your data is legitimately unique
  - Whatever data was used to train the model must be, in some way, representative of your data.
- Well poisoning with online algorithms
  - Ask how different is this from other attacks?
- This stuff is hard! Intuition is not enough.

Seiso

Live Interactions and Intuition

- In cases where you should be able to provide different inputs to the algorithms and get different responses, and it should feel intuitive
  - Examples for other fields include Insurance rates, financing, etc.
  - If you put more down, or make more money, your rates should be better.
- If your data formats are constantly changing from what your models were trained on, they are no longer very useful.
  - CACE (Changing Anything Changes Everything).
  - Typically not the case for vendor products because they understand this, but if you are doing your own modeling, beware that this will either cause (1) technical debt through glue code, or (2) models of extremely limited usefulness.

Seiso

The Limitations of things like Deep Learning

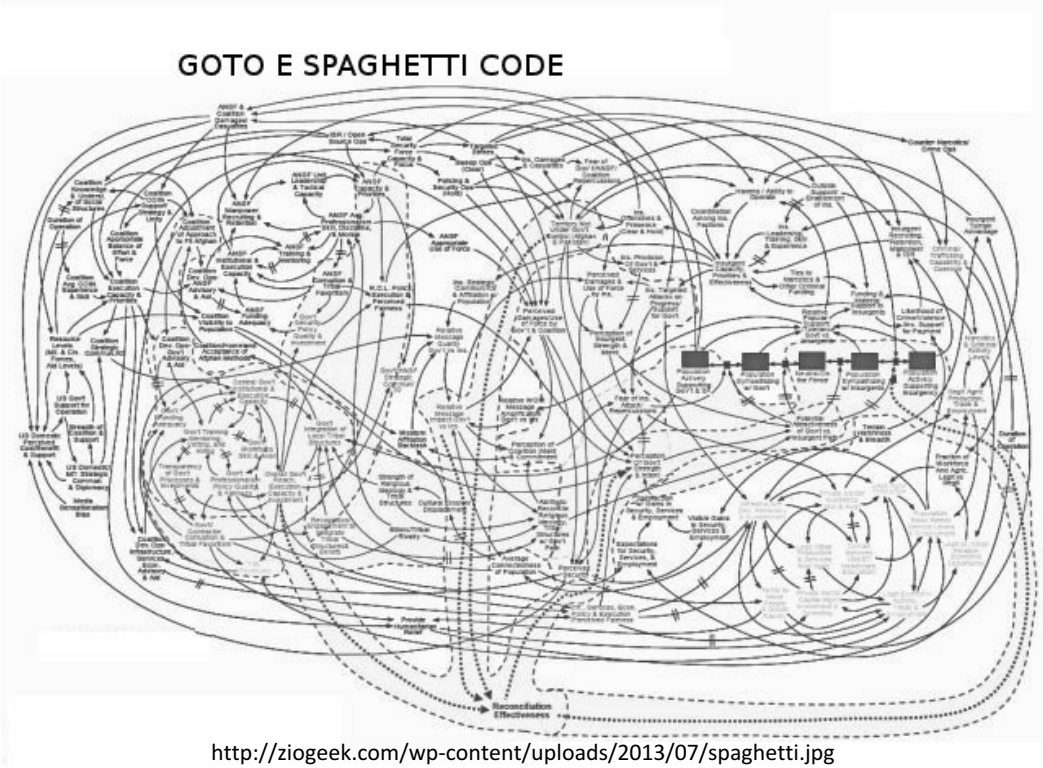
- Boundary erosion, entanglement, hidden feedback loops, undeclared consumers, data dependencies, changes in the external world, and a variety of system-level anti-patterns.
  - Paying off technical debt include refactoring, increasing coverage of unit tests, deleting dead code, reducing dependencies, tightening APIs, and improving documentation

https://memegenerator.net/img/instances/500x/74873992/let-me-sprinkle-some-deep-learning-magic.jpg

Seiso

The Limitations of things like Deep Learning

- Boundary erosion, entanglement, hidden feedback loops, undeclared consumers, data dependencies, changes in the external world, and a variety of system-level anti-patterns.
  - Paying off technical debt includes refactoring, increasing coverage of unit tests, deleting dead code, reducing dependencies, tightening APIs, and improving documentation



http://ziogeek.com/wp-content/uploads/2013/07/spaghetti.jpg

Seiso

When **IS** ML useful?

Seiso

"If the **environment is complex** and **feedback is delayed or ambiguous**, algorithms will generally and relatively consistently outperform human judgement"

Data Driven Security

Seiso

When is ML in InfoSec useful?

- Traditional methods are insufficient on their own
  - Signature-based detections are too slow/large
  - 0-day detection is important
  - Focused adversaries are a real concern
  - You have hit the limits of anomaly detection
- You need to speed up your first tier triage
- You have the ability to collect (or are currently collecting) large amounts of **structured, labeled** data

Seiso

Now What?

Seiso

Takeaways/Next Steps

- Machine Learning is not magic. If your situation doesn't fit a scenario where ML is helpful, trying to make it work is asking for trouble.
- Find **your company's** balance between privacy (data collection) and data analytics.
- Align with a big data platform, and start using it.
- Process your data as it is collected to clean, normalize, and enrich it. It may be helpful in the future.
- For as long as it is possible, retain your data, especially data regarding breaches. You can use it in the future to test your machine learning platform(s).

Seiso

Questions?

Seiso

More?

- Pittsburgh Data Science[1] meetup group

- Take a look at the Hadoop Ecosystem (Apache Metron[2], Apache Spark[3], etc.)

- I've assembled some additional materials[4] and InfoSec[5] Labs[6]
  - Note: Upcoming conference in DC on 10/28/17 (CAMLIS)

1. https://www.meetup.com/PGH-Data-Science
2. https://metron.apache.org/
3. https://spark.apache.org/
4. https://github.com/JonZeolla/Presentations/tree/master/2017-10-20_TRISS
5. https://jonzeolla.github.io/lab-materials/
6. https://github.com/jonzeolla/lab

Thank you!