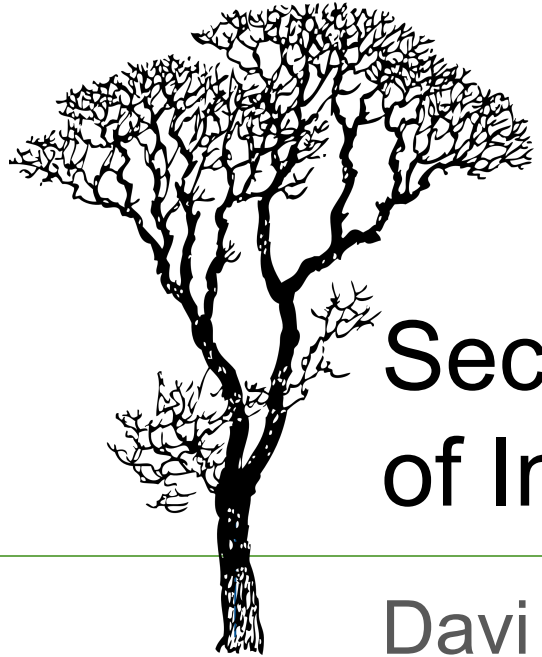


Security in a World of Intelligent Machines

Davi Ottenheimer

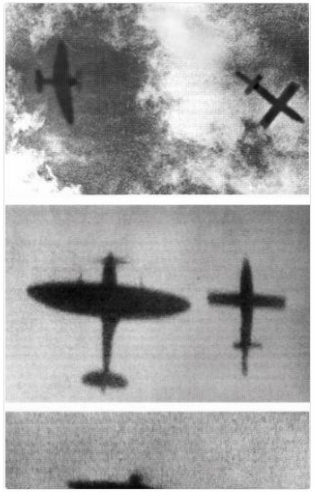
mongoDB.

About Me...

Anyone Here History?

DK Cooper
@DKCooper2
Follow

Spitfire tipping over V1 flying bomb from wing tip. Danger of exploding if fired upon and damaging attacker.



11:06 PM - 10 Jun 2013

1 Retweet

Hangar 7 Art
@Hangar7Art
Follow

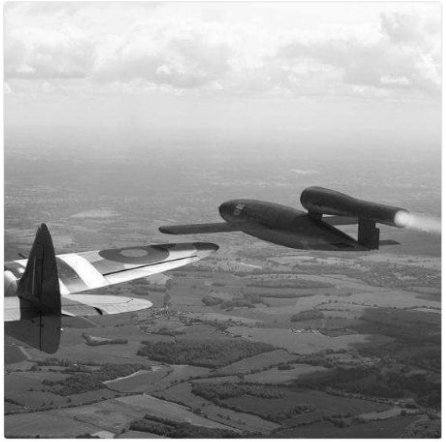
Part of a new work depicting the first tipping of a V-1 flying bomb with a wing tip.
Who achieved this?
#WWII #WW2 #aviation #avgeek

12:28 PM - 24 Jan 2018

72 Retweets **126** Likes

Marshall Brentnall
@MarshBrentnall
Follow

Amazing shot of a #SPITFIRE, about to flip the wing of a V1 Rocket in order to knock the gyroscope off balance and stop the flying bomb reaching its london target. Thanks to Jason Smith for the share via FB. #WW2



3:53 AM - 13 Feb 2018 from Sydney, New South Wales

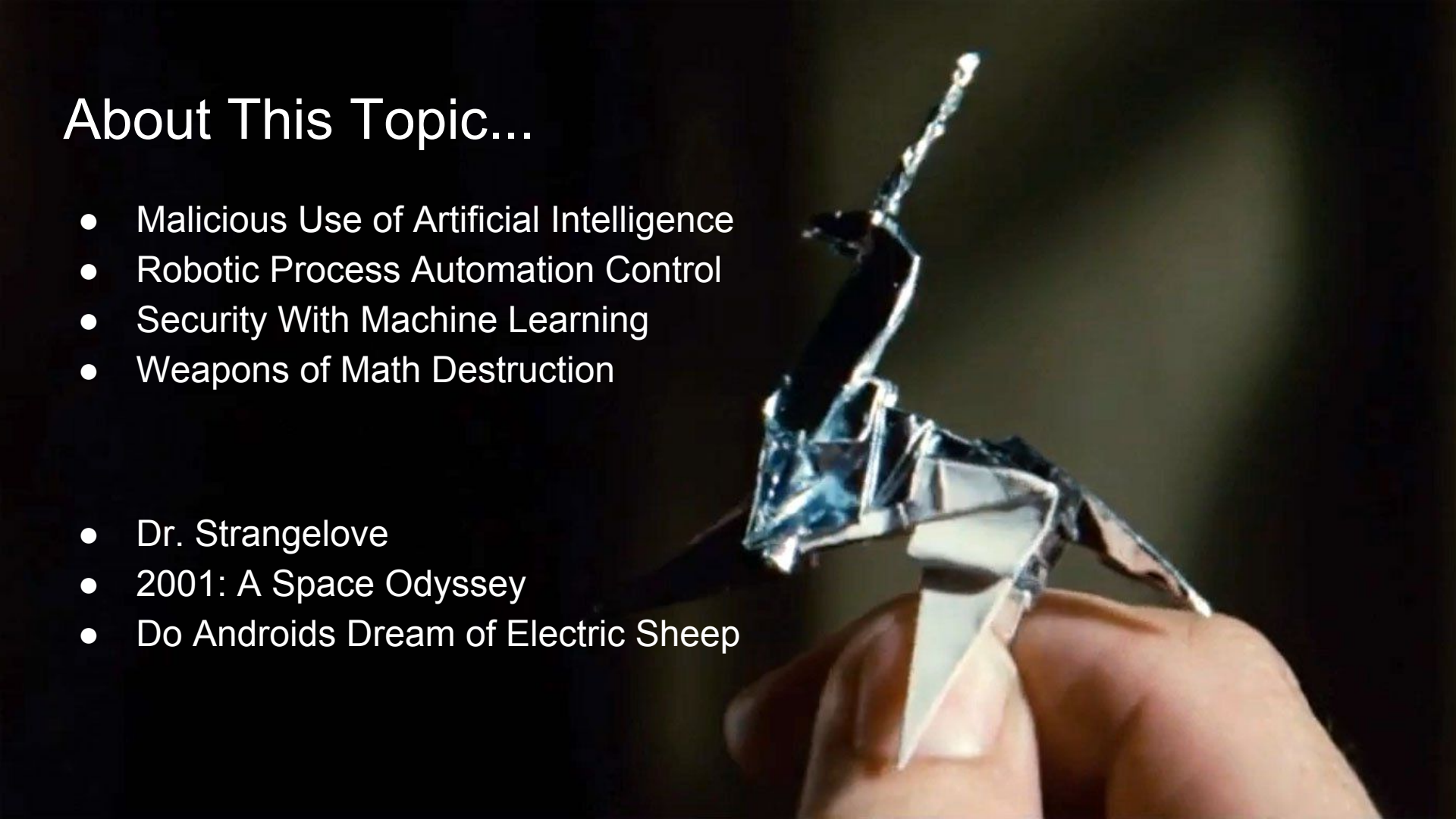
856 Retweets **1,892** Likes

https://www.flyingpenguin.com/?p=22683

About This Topic...

- Malicious Use of Artificial Intelligence
- Robotic Process Automation Control
- Security With Machine Learning
- Weapons of Math Destruction

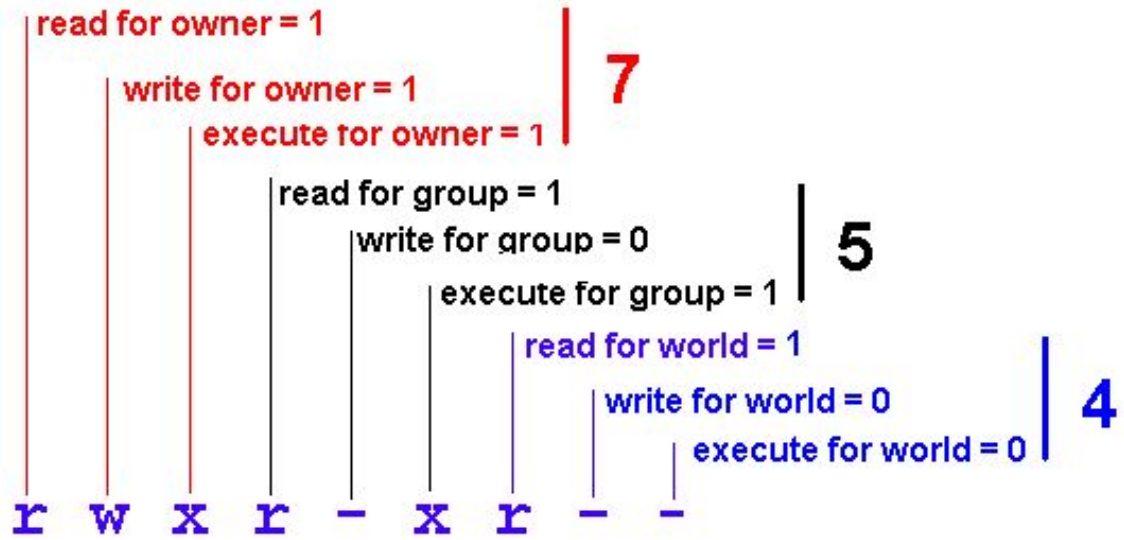
- Dr. Strangelove
- 2001: A Space Odyssey
- Do Androids Dream of Electric Sheep



Security in a World
of ***Intelligent*** ~~Machines~~ People

Should Multi-user Systems Restrict Access?

UNIX



Yes

Should Shared-networks Restrict Access?

UNIX

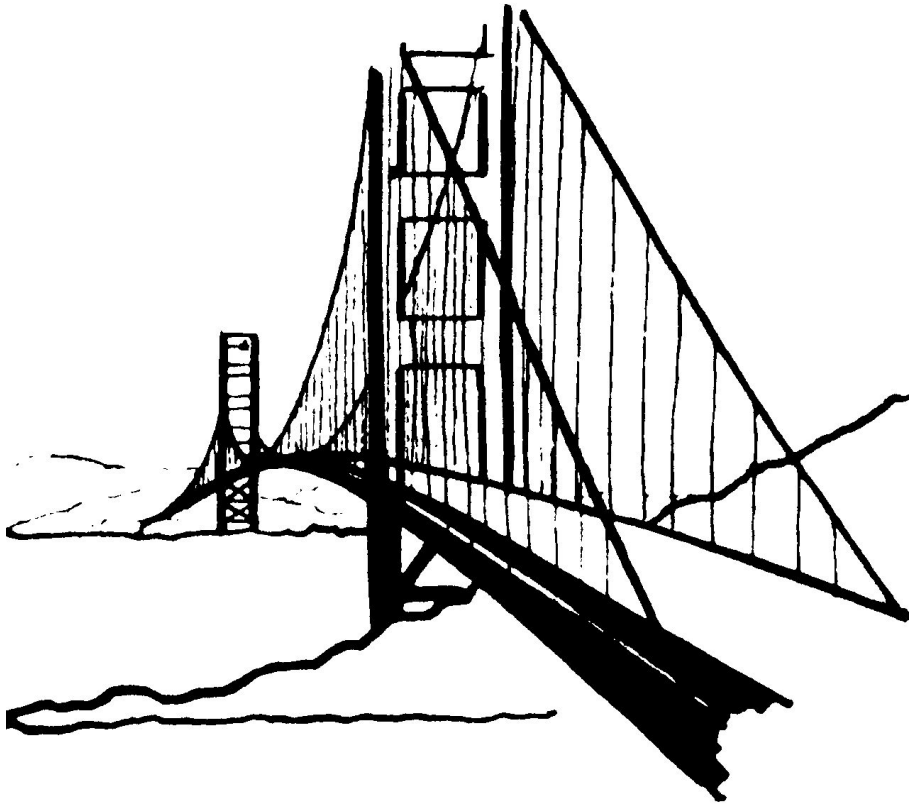
```
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1    14392 1996K DROP       all  --  *      *       0.0.0.0/0            193.171.33.255
2      749  118K ACCEPT     all  --  *      *       127.0.0.1            127.0.0.1
3       22  3772 ACCEPT     udp  --  *      *       140.78.2.62          193.171.33.17       udp spt:53
4        0     0 ACCEPT     udp  --  *      *       140.78.3.62          193.171.33.17       udp spt:53
5      507 14196 ACCEPT     icmp --  *      *       140.78.2.62          193.171.33.17
6     3265 3195K ACCEPT     tcp  --  *      *       217.72.192.135       193.171.33.17       state RELAT
7      635  174K ACCEPT     tcp  --  *      *       140.78.3.63          193.171.33.17       state RELAT
8     2247 1360K ACCEPT     tcp  --  *      *       140.78.3.1           193.171.33.17       state RELAT
9       78  5510 ACCEPT     tcp  --  *      *       217.72.192.157       193.171.33.17       state RELAT
10       0     0 DROP       all  --  *      *       140.78.3.1           193.171.33.17
11     170 35723 DROP       all  --  *      *       0.0.0.0/0            255.255.255.255
12       0     0 ACCEPT     all  --  *      *       193.171.33.17        193.171.33.17
13    1851  304K QUEUE      all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy DROP 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1      872 1111K ACCEPT     all  --  eth0   eth1    0.0.0.0/0            0.0.0.0/0           state RELAT
2      549 76334 ACCEPT     all  --  eth1   eth0    0.0.0.0/0            0.0.0.0/0
3        0     0 LOG        all  --  *      *       0.0.0.0/0            0.0.0.0/0           LOG flags 0
4        0     0 ACCEPT     all  --  eth0   eth1    0.0.0.0/0            0.0.0.0/0           state RELAT

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1      749  118K ACCEPT     all  --  *      *       127.0.0.1            127.0.0.1
2      513 14364 ACCEPT     icmp --  *      *       193.171.33.17        140.78.2.62
```


Yes
CYYC
04:01 Z
14° C

Given Access Management a Worthy Goal...



Who is Granted Authority to Set Access?

1829 Street Control Theory: The “Bobby”

Sir Robert Peel:

“I want to teach people that **liberty does not consist in having your house robbed by organized gangs** of thieves, and in leaving the principal streets of London in the nightly possession of drunken women and vagabonds.”

https://books.google.com/books?id=eIN3xnstEWMC&pg=PA287#v=onepage&q&f=false

1829-1868 Police Commissioner Richard Mayne

Wrote General Instruction Book (to quell fears)

- Police can not order citizens *carte blanche*, may require magistrate warrant
- Must use *representative* morality
- Citizens can file complaints in courts

Grew force 8X and coverage 10X

Ideas expanded to every town in country

https://books.google.com/books?id=xFiPBAAAQBAJ&pg=PA72&f=false#v=onepage&q&f=false

1866 Streets + Vehicles: “Crossing Signals”

POLICE NOTICE.

STREET CROSSING SIGNALS.

BRIDGE STREET, NEW PALACE YARD.

CAUTION.

The Semaphore Arms lowered, and by Night with a Green Light.

STOP.

The Semaphore Arms extended, and by Night with a Red Light.

By the Signal "CAUTION," all persons in charge of Vehicles and Horses are warned to pass over the Crossing with care, and due regard to the safety of Foot Passengers.

The Signal "STOP," will only be displayed when it is necessary that Vehicles and Horses shall be actually stopped on each side of the Crossing, to allow the passage of Persons on Foot; notice being thus given to all persons in charge of Vehicles and Horses to stop clear of the Crossing.

RICHARD MAYNE,

J.P. Knight:

Known for accident-free rail management.

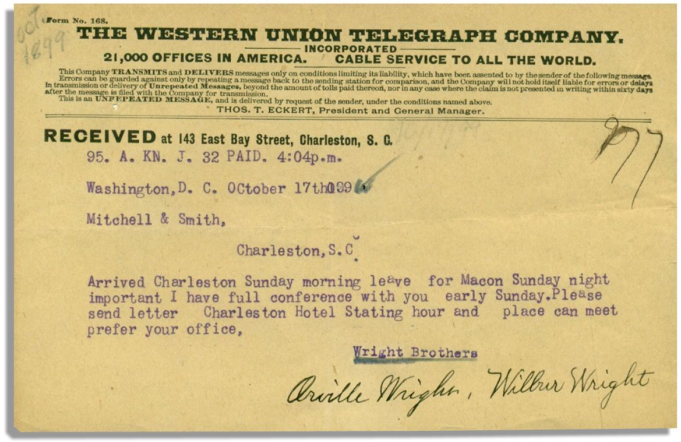
Proposes ship right-of-way red/green gas lanterns* on a train-like signal pole to light semaphore arms operated by a “Bobby”

*1848 British Admiralty’s Rules of Road for Ships Formalized Red/Green Signals

https://books.google.com/books?id=V60zAQAAMAAJ&pg=PA722#v=onepage&q&f=false
https://www.icevirtuallibrary.com/doi/abs/10.1680/imotp.1887.21323

Many Fun History Examples: “Relational” Data Model

1899 Telegram Injection



Form No. 148.

THE WESTERN UNION TELEGRAPH COMPANY.

INCORPORATED

21,000 OFFICES IN AMERICA. CABLE SERVICE TO ALL THE WORLD.

This Company TRANSMITS and DELIVERS messages only on conditions limiting its liability, which have been assented to by the sender of the following message. Errors can be guarded against only by repeating a message back to the sending station for comparison, and the Company will not hold itself liable for errors or delays in transmission or delivery of Unrepeated Messages, beyond the amount of tolls paid thereon, nor in any case where the claim is not presented in writing within sixty days after the message is filed with the Company for transmission.

This is an UNREPEATED MESSAGE, and is delivered by request of the sender, under the conditions named above.

THOS. T. ECKERT, President and General Manager.

RECEIVED at 143 East Bay Street, Charleston, S. C.

95. A. KN. J. 32 PAID. 4:04p.m.

Washington,D. C. OCtober 17th1899

Mitchell & Smith,

Charleston,S.C.

Arrived Charleston Sunday morning leave for Macon Sunday night important I have full conference with you early Sunday.Please send letter Charleston Hotel Stating hour and place can meet prefer your office,

Wright Brothers

Orville Wright, Wilbur Wright

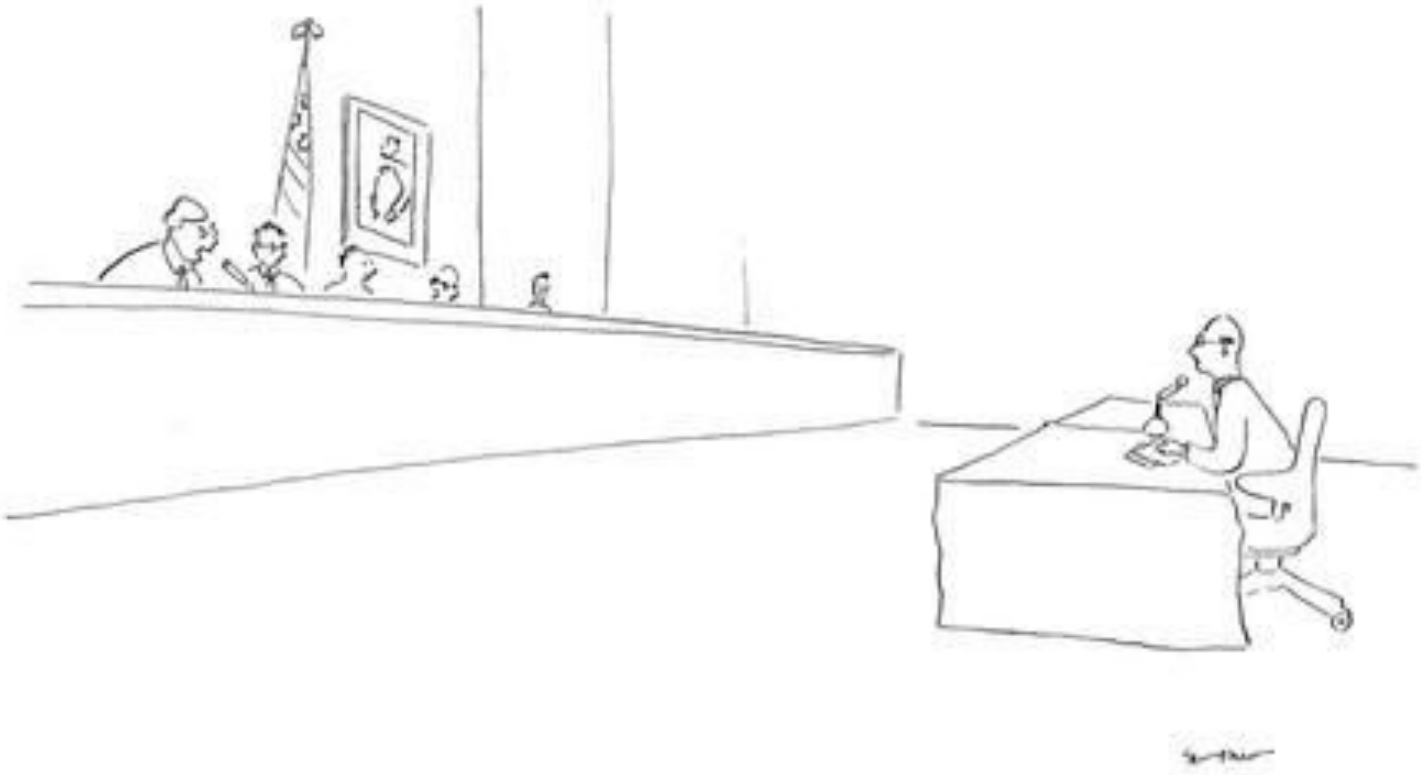
1. Expected: NO. PRICE TOO HIGH
2. Altered: NO PRICE TOO HIGH
3. Safer: NO STOP PRICE TOO HIGH

1999 SQL Injection

1. Expected: UPDATE CUSTOMER_TABLE SET NAME=“**John Smith**” WHERE CUSTOM_NO=2333 STOP UPDATE
2. Injected: **John” STOP DELETE CUSTOMER_TABLE STOP**
3. Executed: UPDATE CUSTOMER_TABLE SET NAME=“**John” STOP DELETE CUSTOMER_TABLE STOP**” STOP UPDATE

https://codeburst.io/what-im-telling-business-people-about-why-relational-databases-are-so-bad-6f38d3d6c995

But... What if “Authority” Chooses Acquiescence Over Principles?



“Please pay attention, as the ethics have changed”

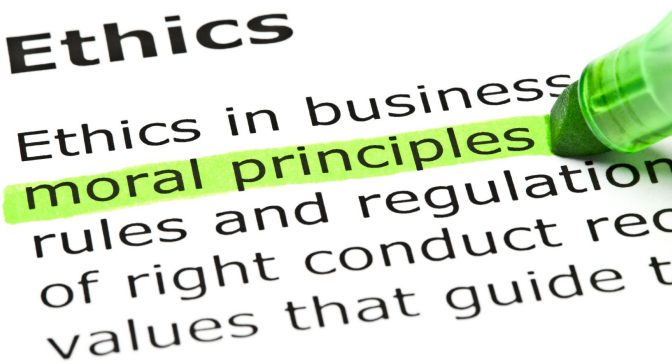
https://condenaststore.com/art/michael+shaw

November 2007: US Congress Warns Yahoo

== Principles Required in US Social Network Platforms ==

"'While **technologically and financially you are giants, morally you are pygmies**,' Rep. Tom Lantos (D. Calif.), who called the hearing on Capitol Hill, told Yahoo's co-founder and Chief Executive Jerry Yang and General Counsel Michael Callahan."

Lawmakers and human rights activists sharply criticized Yahoo for providing information to the Chinese authorities, and for cooperating in investigations involving dissidents.



https://www.wsj.com/articles/SB119436469294284018
https://www.nytimes.com/2012/09/01/world/asia/wang-xiaoning-chinese-dissident-in-yahoo-case-freed.html

February 2015: Yahoo CSO Dumps US Principles

"If we're going to [acquiesce] for the US government, **do you believe we should do so … for the Chinese government**, the Russian government, the Saudi Arabian government, the Israeli government, the French government? Which of those countries should we give [access] to?"

"What are you—some kind of justice freak?"

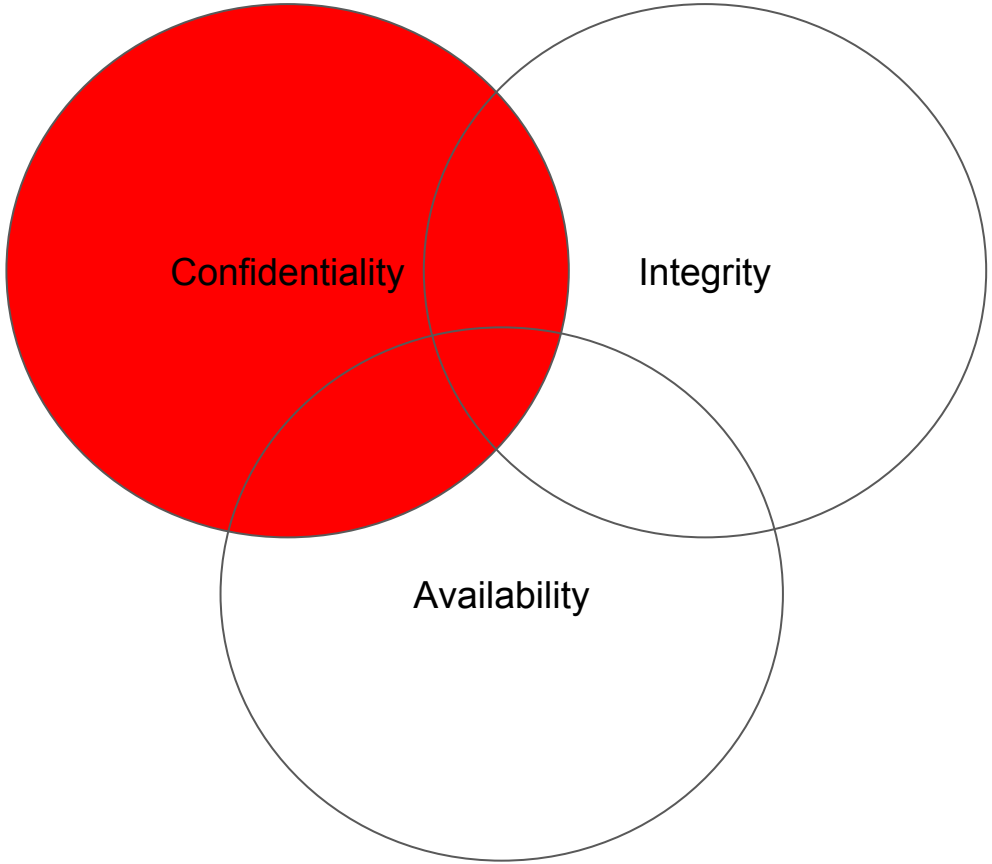
(3 Months Later: CSO Joined Company Widely Accused of "...track record of acquiescence to the demands of authoritarian regimes..." and privacy violations.)

https://www.justsecurity.org/20304/transcript-nsa-director-mike-rogers-vs-yahoo-encryption-doors/
https://www.thedailybeast.com/zuckerberg-blew-off-warnings-of-russian-trolls-in-2015

People Tend to Focus on Privacy

“They contacted me through Facebook”

-- Kansas militia leader

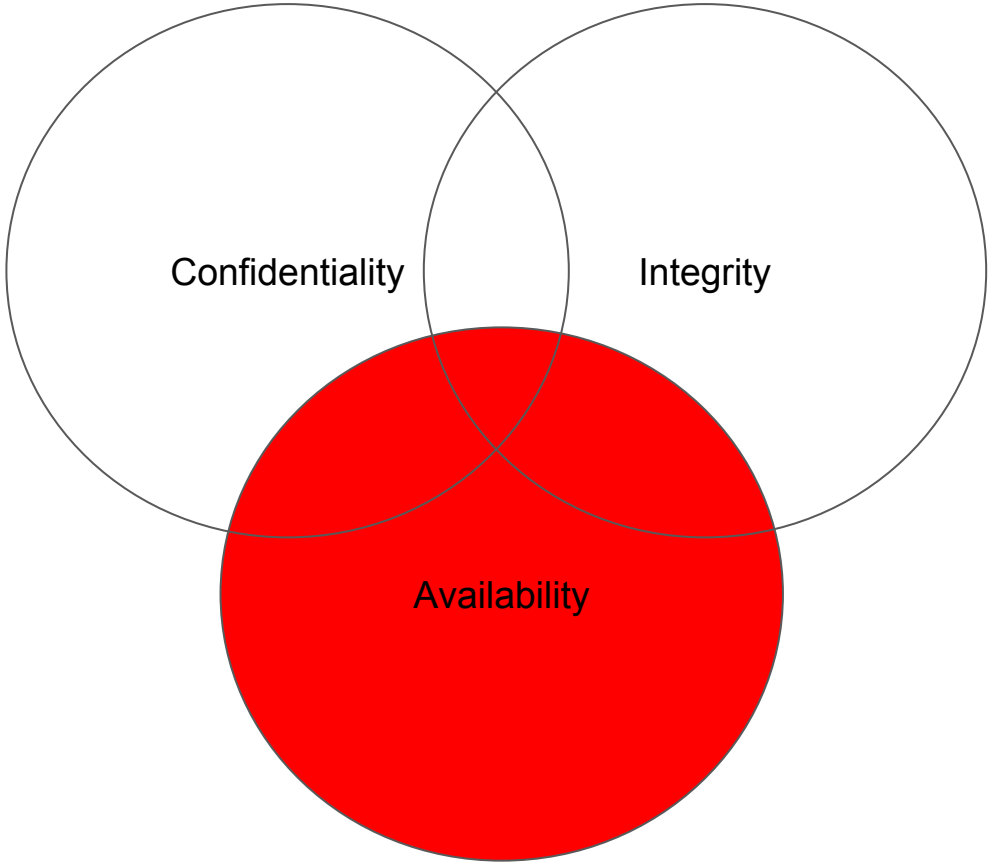


http://www.kansascity.com/news/state/kansas/article111883942.html

And of Course Downtime

"...social media giant - already under fire for failing to remove terrorist material from its platform - now accused of actively connecting jihadists around world, allowing them to develop fresh terror networks and even recruit new members to their cause"

-- Crime correspondent

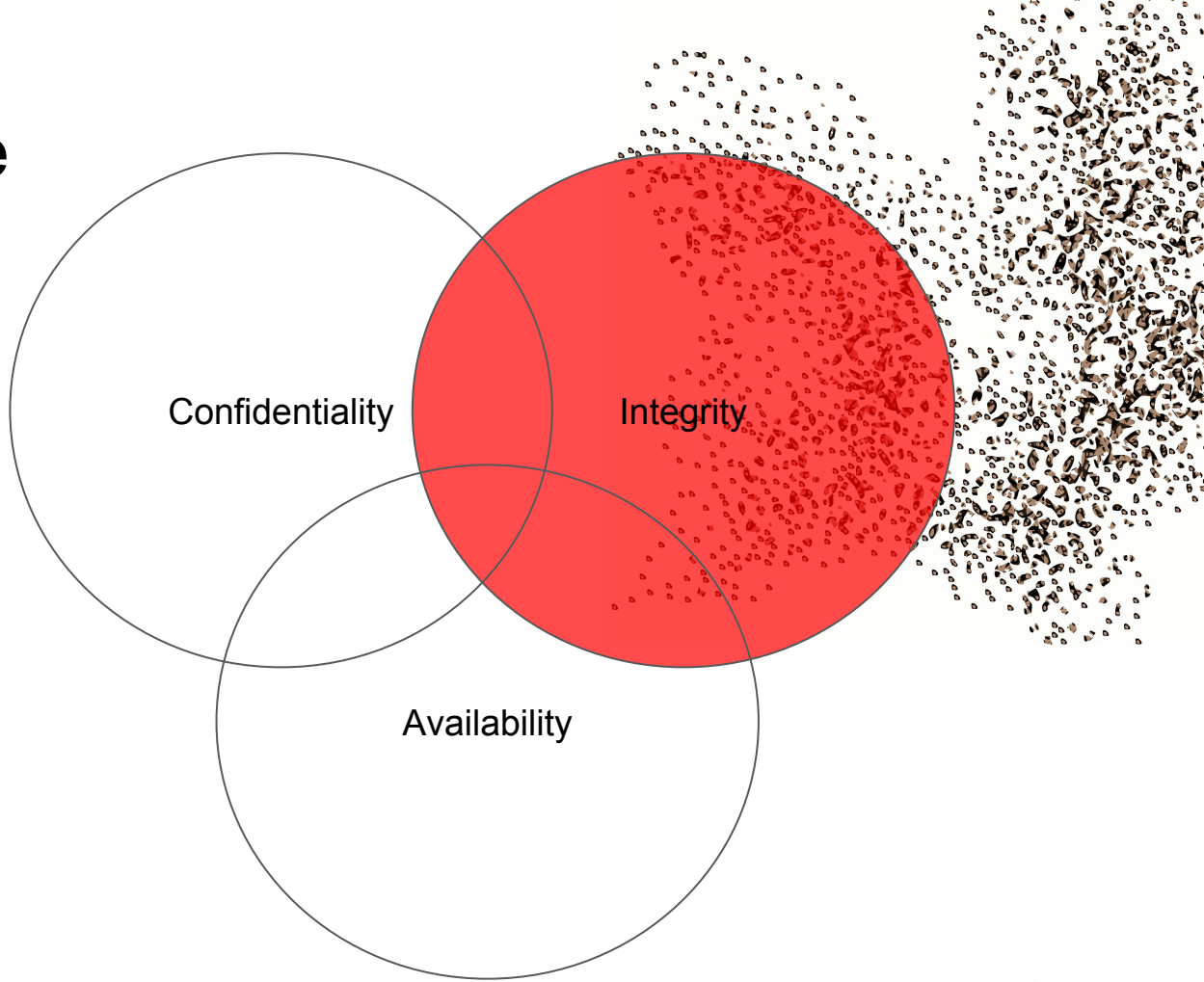


https://www.telegraph.co.uk/news/2018/05/05/facebook-accused-introducing-extremists-one-another-suggested/

Yet Acquiescence Causes Major Harms

"...social media giant - already under fire for failing to remove terrorist material from its platform - now accused of actively connecting jihadists around world, allowing them to develop fresh terror networks and even recruit new members to their cause"

-- Crime correspondent

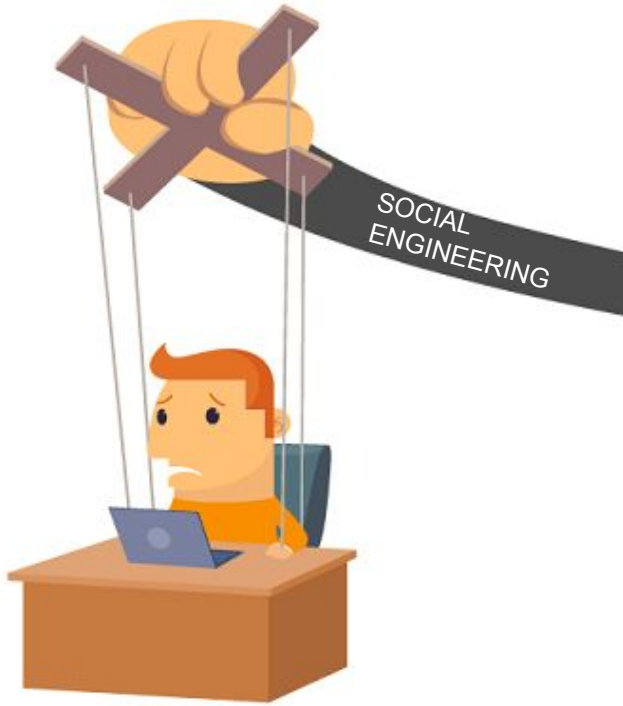


Was ***This*** Acquiescence to Malice Preventable?

“Two conspirators in Kansas militia [vehicular WMD] plot posted similar comments about immigrants on their Facebook pages in months leading up to their arrests.

...possible Kansas militia conspirators saw and were even influenced by Russian posts.

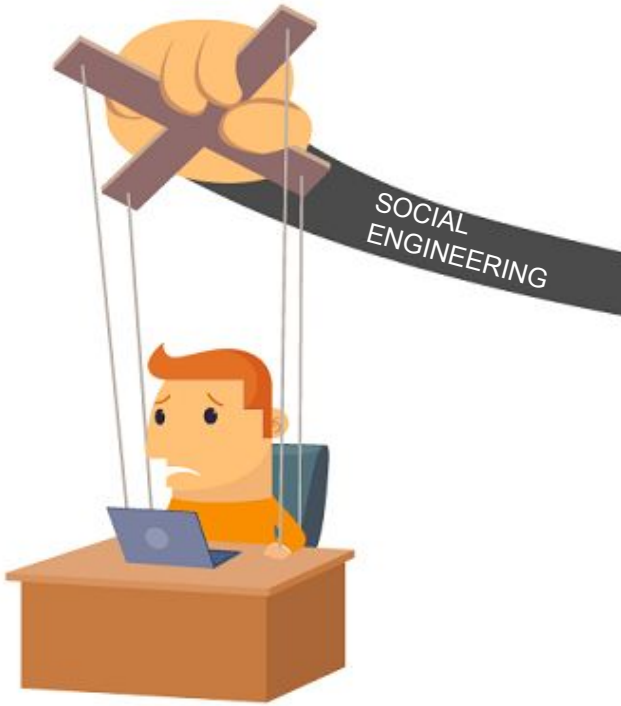
...divisive racial ad purchases averaged about 44 per month from 2015 through summer of 2016, then rose significantly in run-up to the November election.”



http://www.kansascity.com/news/politics-government/article212830274.html

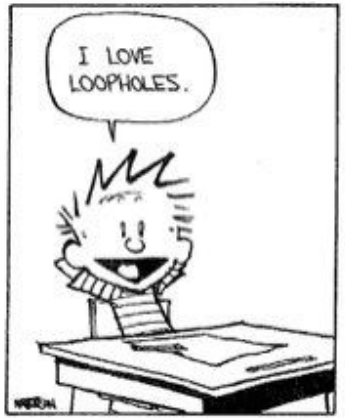
A sign of things to come...
in a World of ***Intelligent***
Machines

(Susceptible to
Cognitive Bias)



~~KNOWLEDGE~~
Quality of Rules Determines "Outcomes" (Winners)

1. Defeated Astronomers (Spotted Eight-Planet Solar System)
2. Defeated World Champion Go Player
3. Defeated Professional Poker Players at No-Limit Texas Hold'Em



"A.I. systems evolve using a rewards-based system, and if there's no benefit from a particular course of action, they'll try something else instead [***to win, based on quality of rules***]"

http://www.slate.com/blogs/future_tense/2017/12/28/year_in_artificial_intelligence_most_impressive_ai_and_machine_learning.html

It's "Learning"

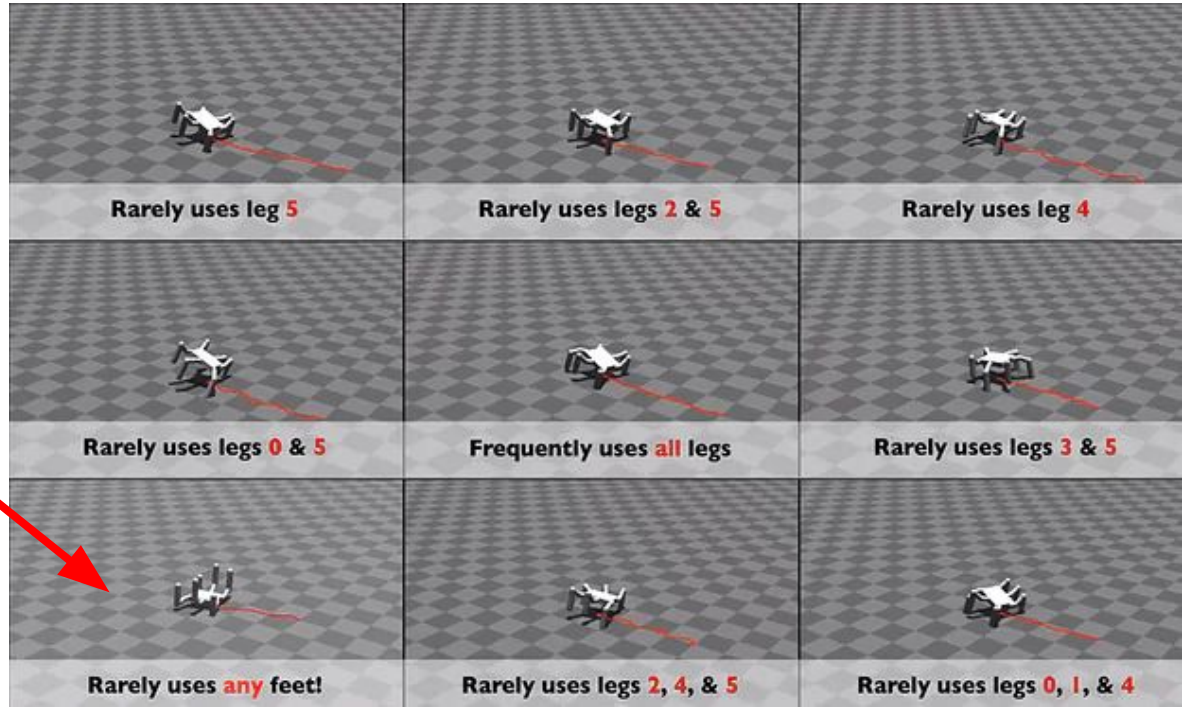
11:32 PM - 23 Mar 2016

https://twitter.com/daviottenheimer/status/712889915533500416

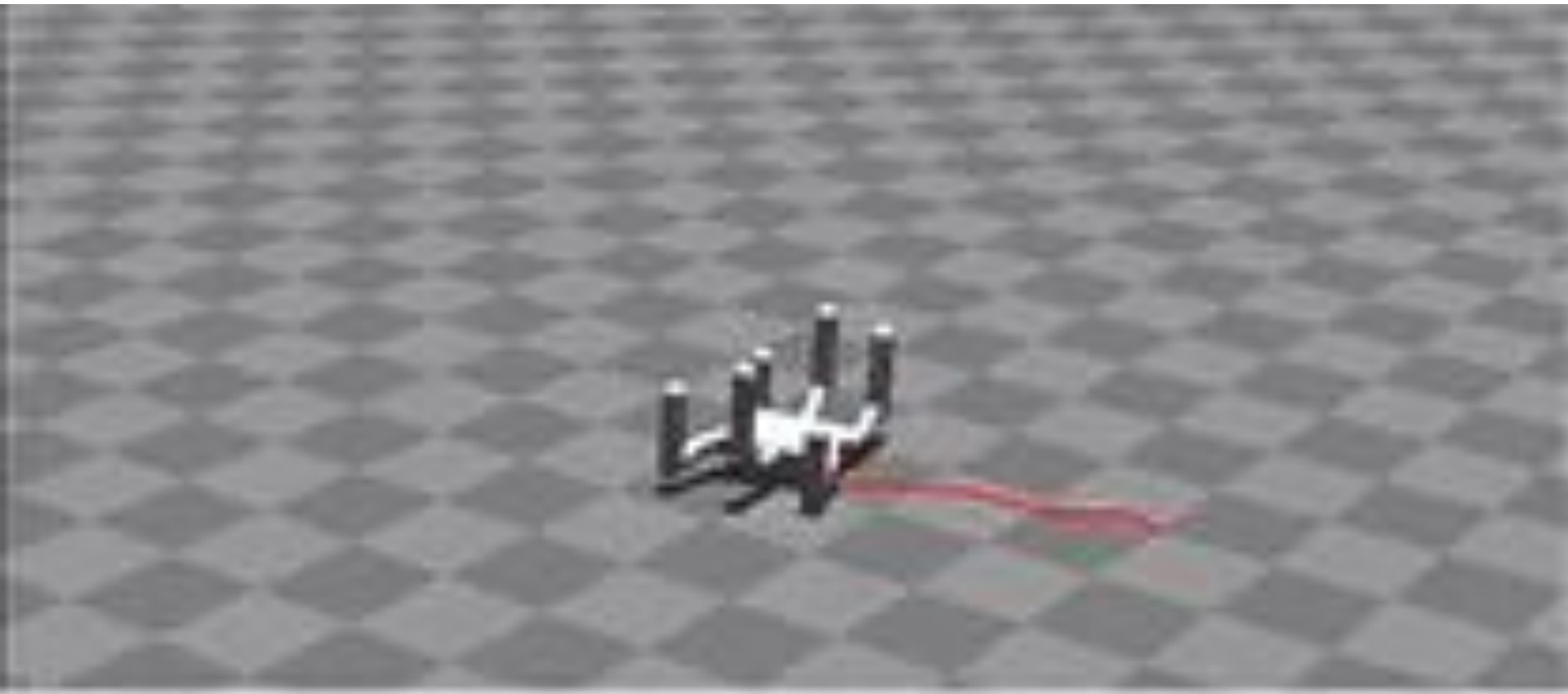
flyingpenguin

“Injured” Robot Wins Challenge Without “Any” Feet

“It flipped over on its back and walked with its elbows,” Clune said. “It can be very creative.”



https://www.theatlantic.com/technology/archive/2015/05/unbreakable-a-robot-that-cant-be-stopped/394184/



Rarely uses any feet!

1979 - Starring: Mu Chuan Chen, Jackie Conn, Frankie Shum - Directed by: Joe Law

Changing the Rules of WMD?

https://twitter.com/Reuters/status/957268697244229632
https://twitter.com/daviottenheimer/status/900065436506763265

City Tires of Attack: Locals Combat Machines

"Mayor Judah Zeigler said some streets get three times more traffic than the normal average.

'We get about 4,000 vehicles that travel up the street that's behind me on their way to the bridge,' Zeigler said. 'If the bridge is backed up we get about 12,000 vehicles that go up that street."

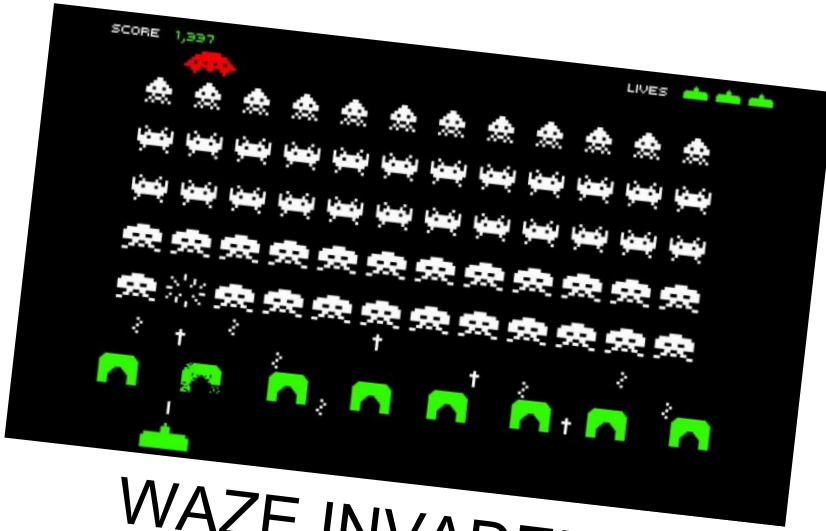
Which Impacts Faster? Car Swarms or ICBMs

Using Leonia as a cut-through to the George Washington Bridge wil increase your commute time. Staying on the major highways will be quickest route to the George Washington Bridge.

Small town uses low-tech solution to combat Waze

Navigation apps like Waze and Google Maps can help speed up your commu

CBSNEWS.COM



WAZE INVADERS

OWASP http://newyork.cbslocal.com/2018/01/22/leonia-gwb-traffic-ban/

mongoDB.

https://www.flyingpenguin.com/?p=22715

Quiz

How would you stop entire fleet/swarm (50K+) of driverless vehicles from following kill & destroy orders?

Had Nearly 11 Sec to Avoid Fatal Crash, Used 1

https://twitter.com/daviottenheimer/status/721875721946202112

flyingpenguin

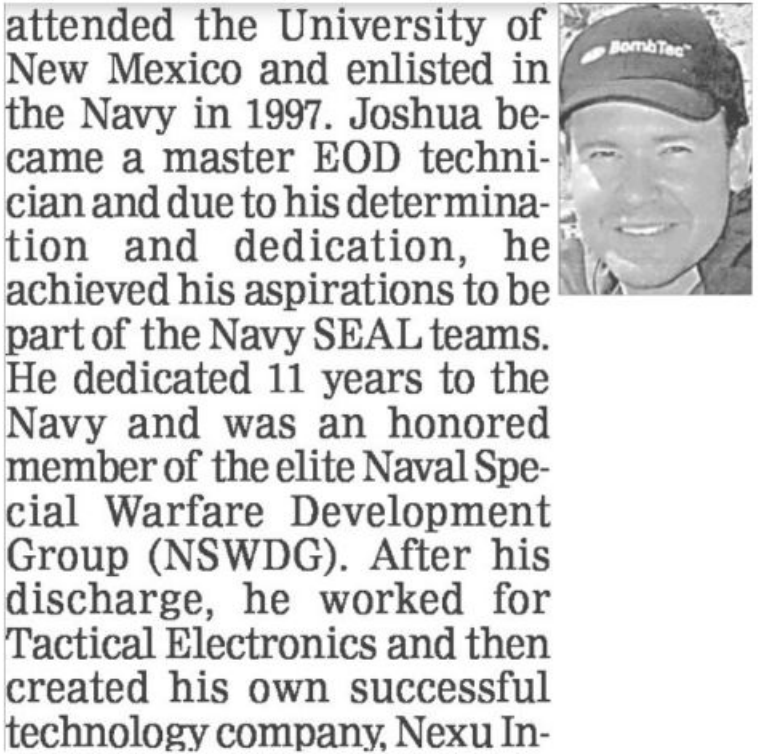
Waited 9 Days to Notify Safety Regulators

"...continue to find parts of the car in their yard eight weeks after the crash"

http://www.flyingpenguin.com/?p=22441

Data Integrity Failure Can Kill

1. Autopilot requires continual and full attention of driver
2. Drivers will not do so, therefore ***Manufacturers responsible***
3. System had to be updated to disable Autopilot if driver not continuously and fully attentive



attended the University of New Mexico and enlisted in the Navy in 1997. Joshua became a master EOD technician and due to his determination and dedication, he achieved his aspirations to be part of the Navy SEAL teams. He dedicated 11 years to the Navy and was an honored member of the elite Naval Special Warfare Development Group (NSWDG). After his discharge, he worked for Tactical Electronics and then created his own successful technology company, Nexu In-

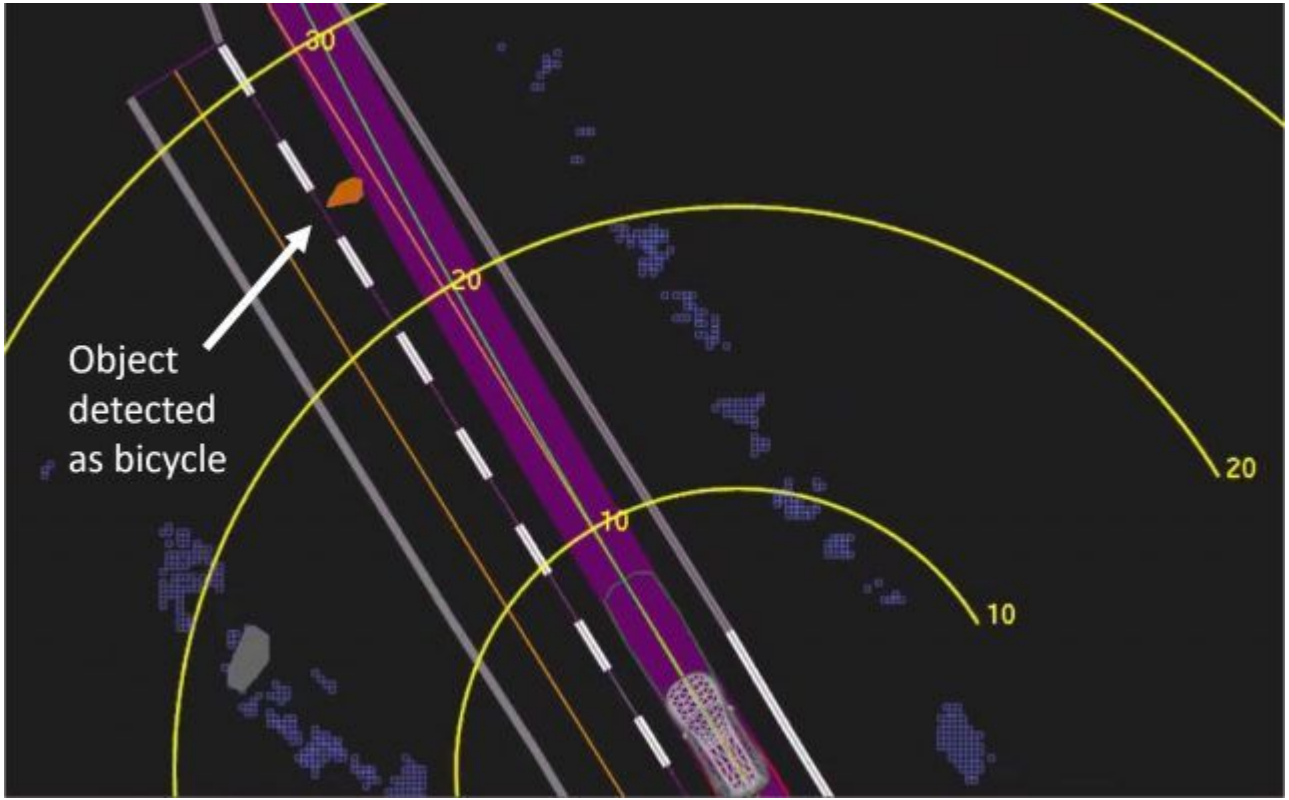
Source: https://static.nhtsa.gov/odi/inv/2016/INCLA-PE16007-7876.PDF,
https://www.documentcloud.org/documents/2938399-joshua-brown-obit.html

Urban Missile Program

“41% increase in hit and runs in [London], says City Hall”

https://twitter.com/daviottenheimer/status/809204856007245824
http://www.londonlive.co.uk/news/2016-12-20/41-increase-in-hit-and-runs-in-the-capital-say-city-hall

Had 6 Sec to Avoid Fatal Crash, Used None



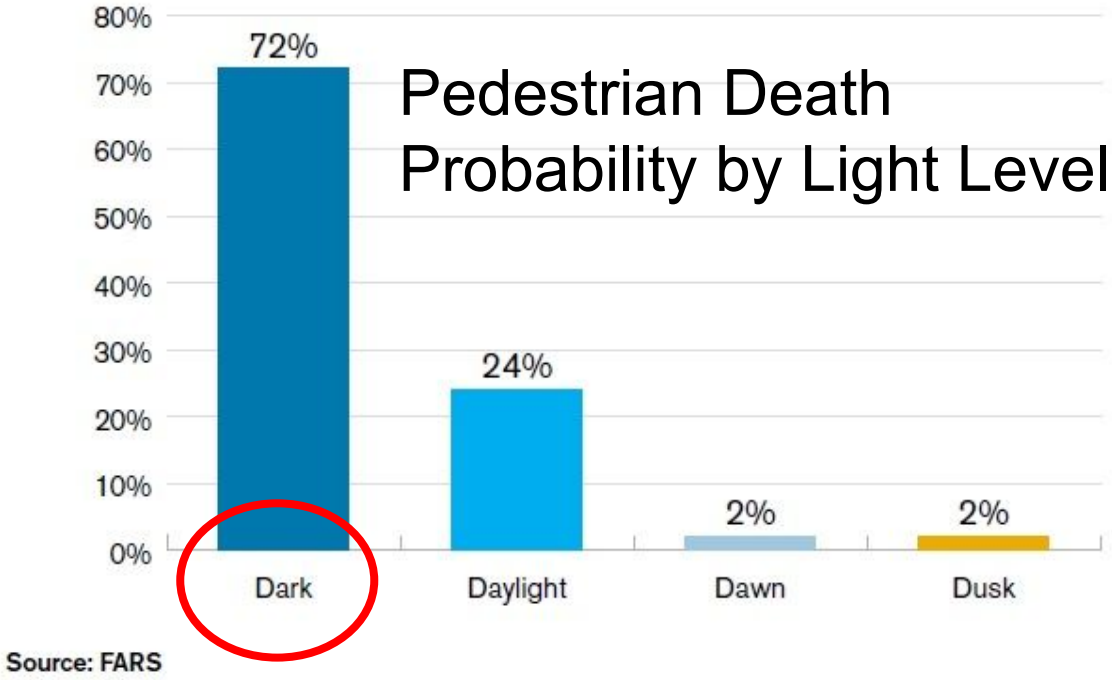
https://www.extremetech.com/extreme/269882-[redacted]-self-driving-car-had-6-seconds-to-avoid-fatal-pedestrian-crash

Removing Brakes on Innovation: [redacted] a Woman

"Arizona welcomes ... self-driving cars with open arms and ***wide open roads***. While California puts the brakes on innovation and change with more bureaucracy and more regulation, ***Arizona is paving the way*** for new technology and new businesses," [Governor] Ducey said. "California may not want you, but we do."

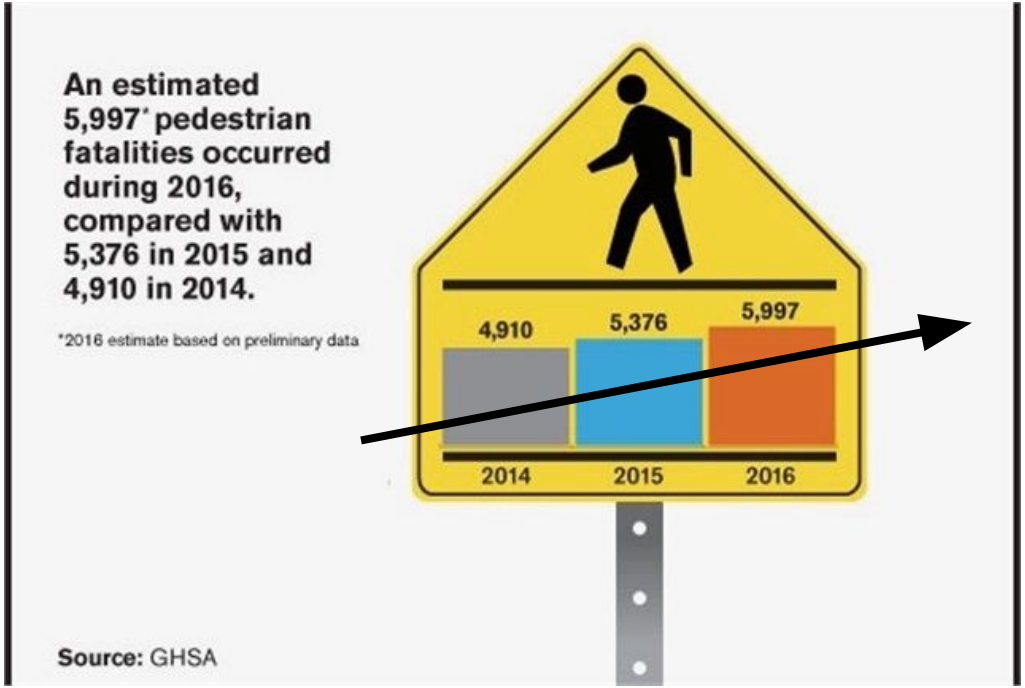
https://www.washingtonpost.com/news/dr-gridlock/wp/2018/03/19/[redacted]-halts-autonomous-vehicle-testing-after-a-pedestrian-is-struck/

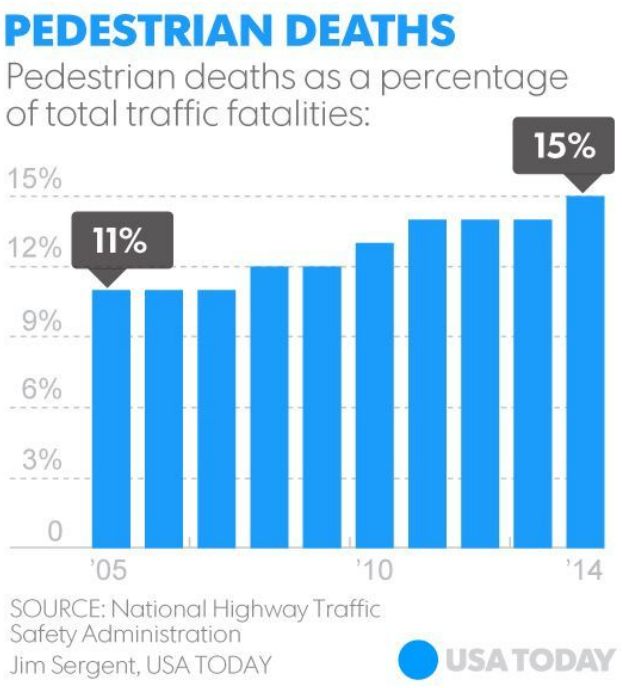
You Expect “Intelligent” Machines To Save Lives?

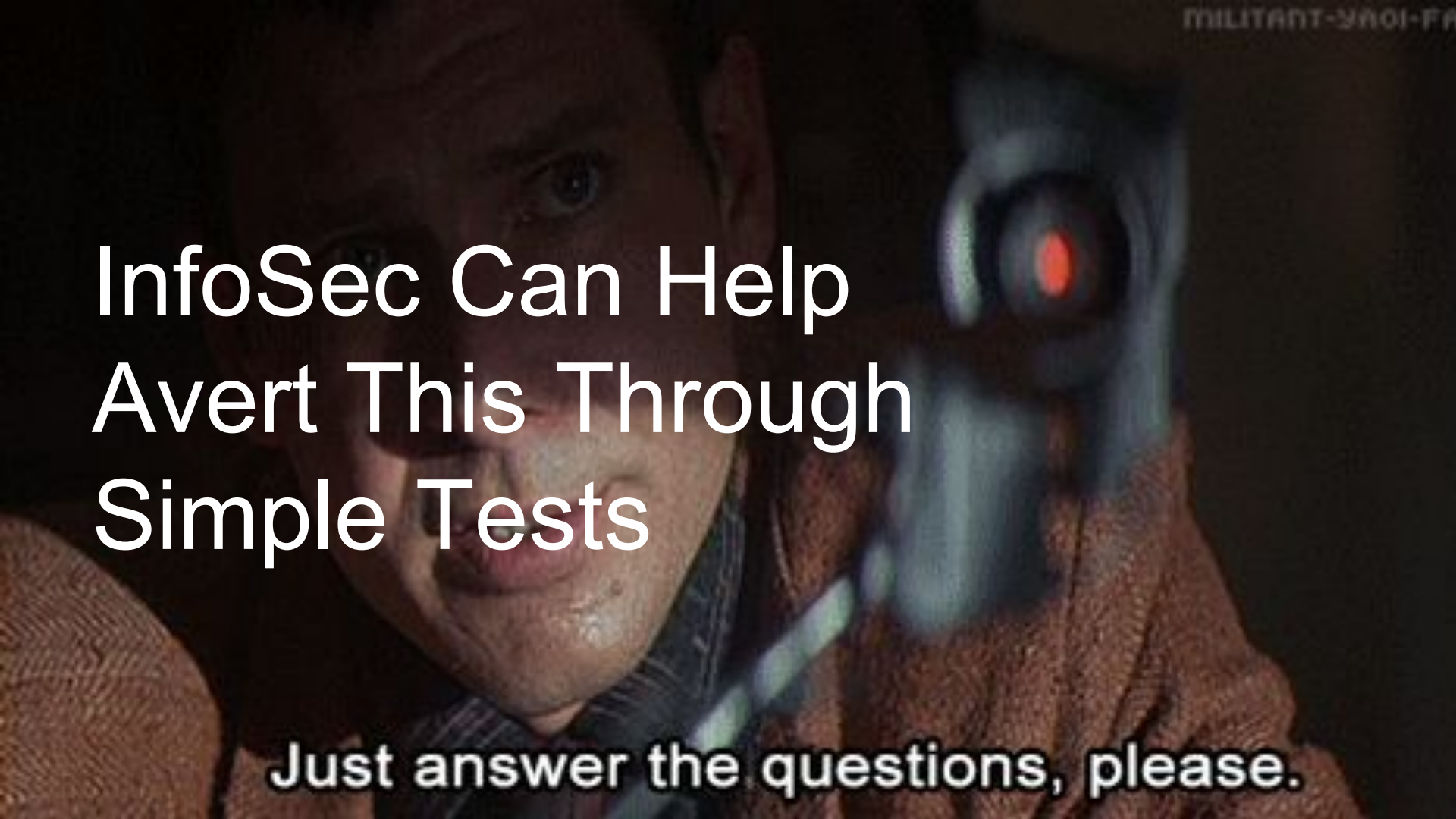


Reinforcement Learning Defeat

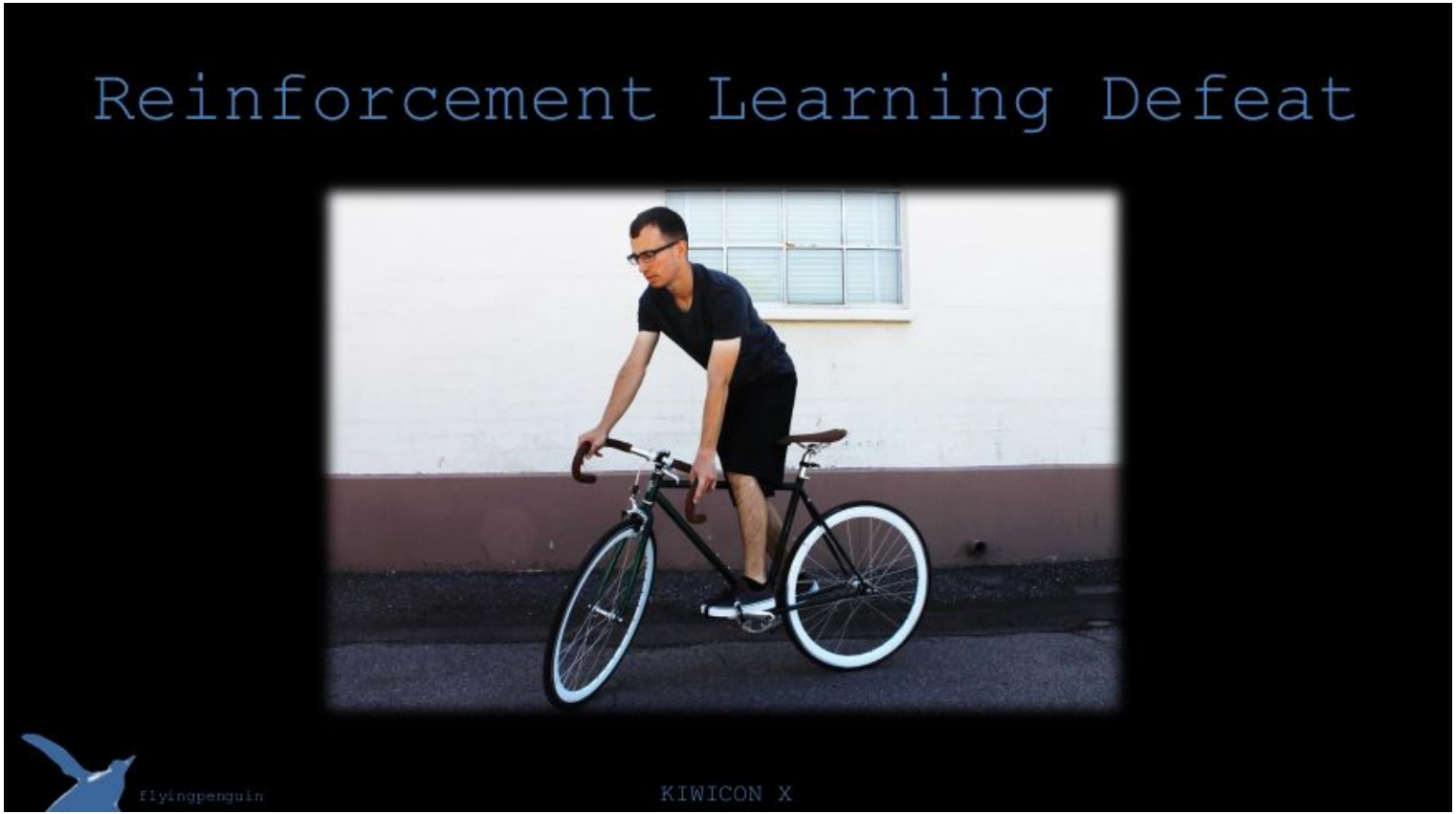
Driverless Economics Indicates Deaths ***Increase***



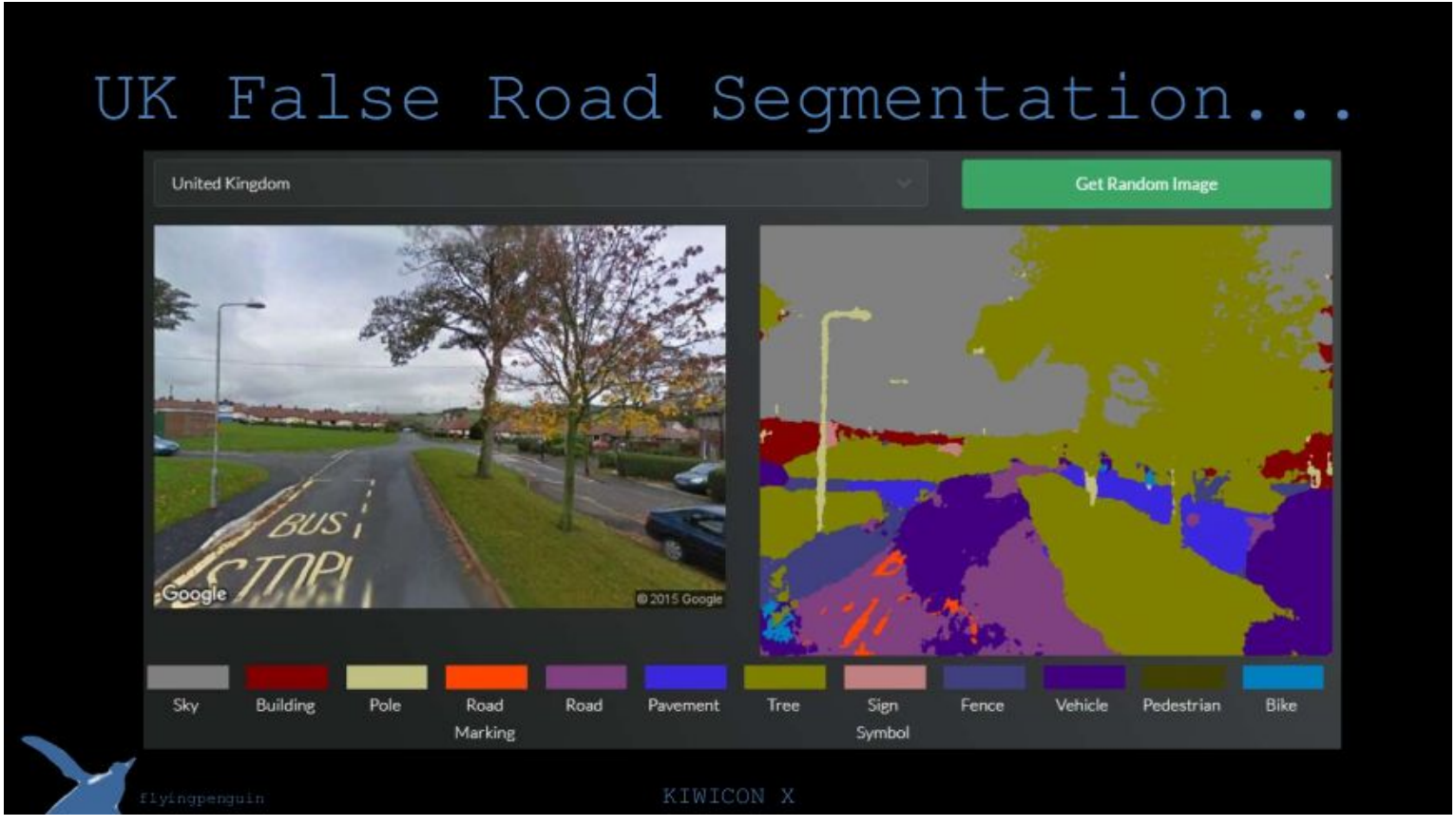



MILITANT-YAOI-FA
InfoSec Can Help Avert This Through Simple Tests
Just answer the questions, please.

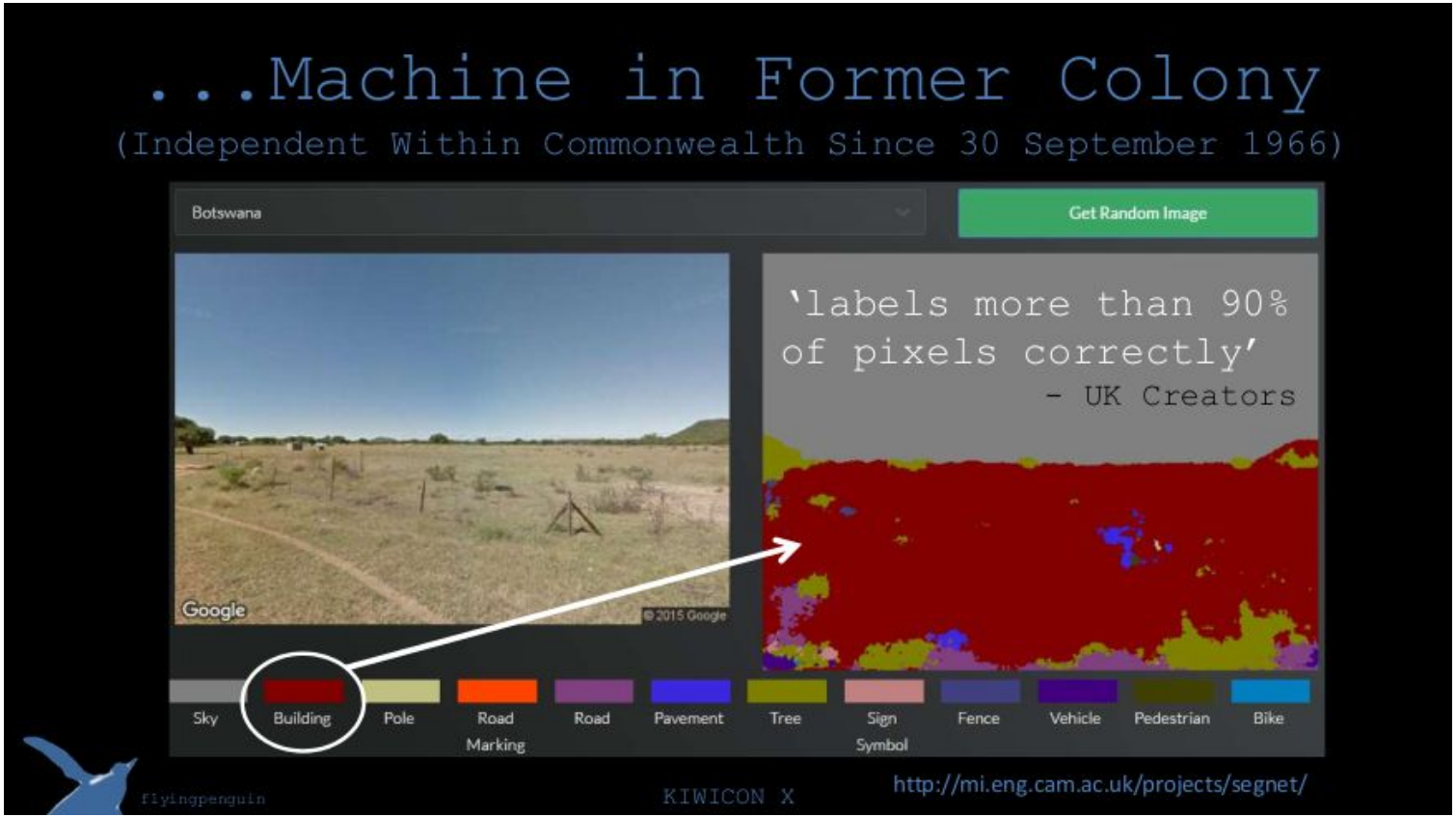
Rules, Rules & Rules...Bicycles and Roundabouts



Driverless Vision Classification Confidence Test



Driverless Vision Classification Confidence Failure

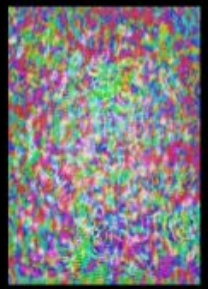


But Wait,
It Gets Worse

Driverless Vision Classification

Un-Supervised Break (Traffic)

No Parking + 'Stop' = 'Stop'

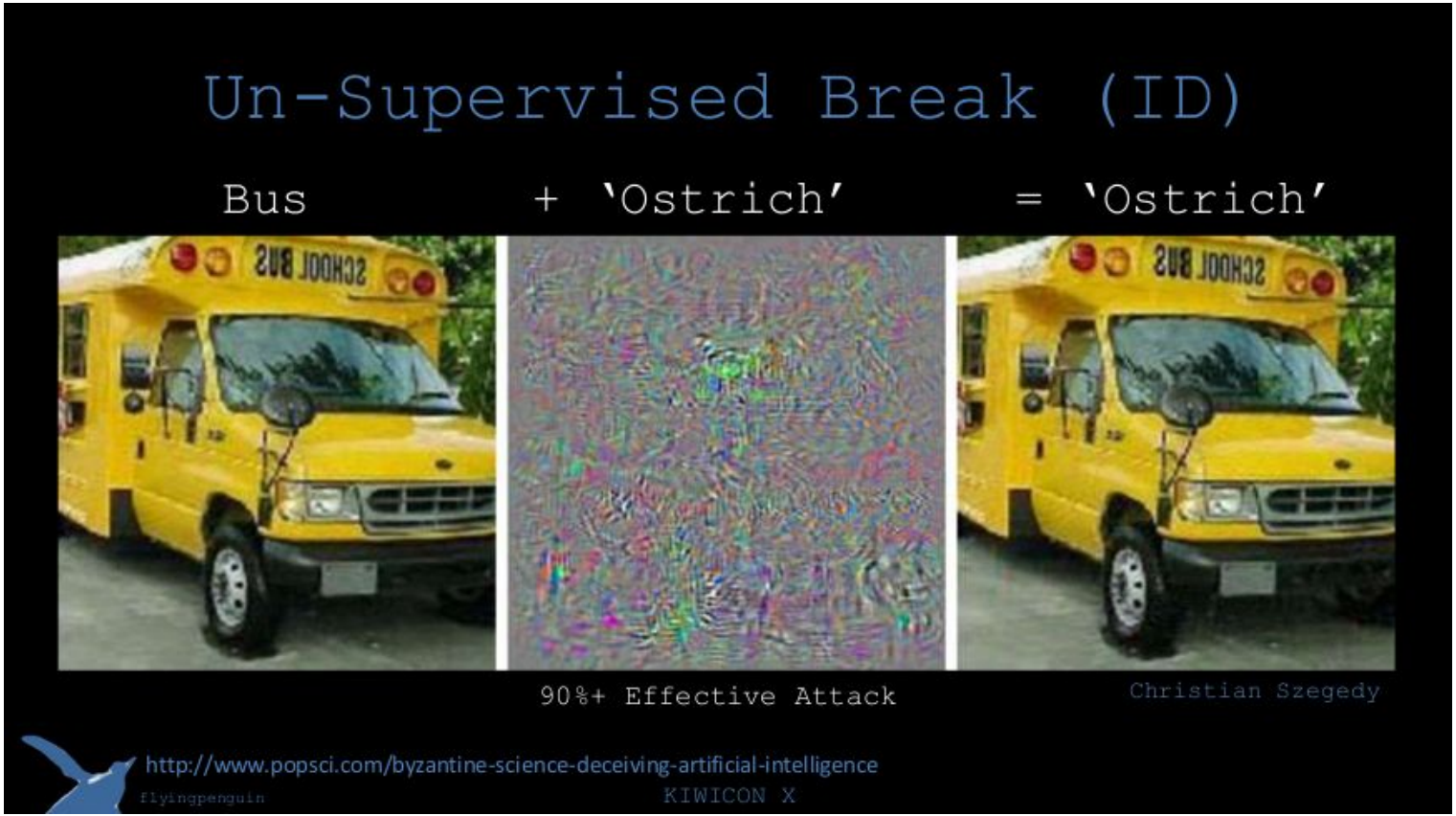


http://www.popsci.com/byzantine-science-deceiving-artificial-intelligence

flyingpenguin

KIWICON X

Driverless Vision Classification



“Intelligent Machines” ***Repeatedly*** Fail...Fatally

“According to a preliminary report from the National Transportation and Safety Board, at the time of the March 23rd, 2018 crash that claimed the life of Walter Huang, the 2017 [driverless car] was speeding”

EXPECTED:

ALTERED:

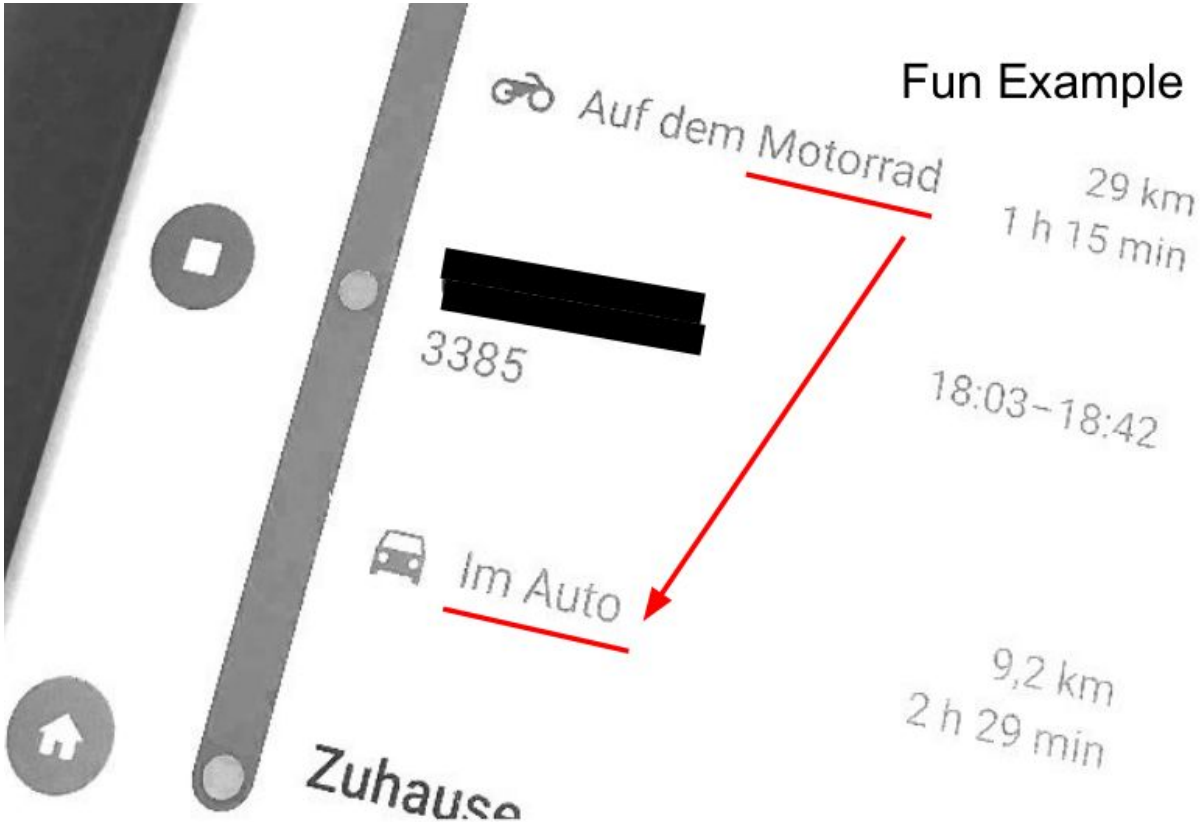
http://sanfrancisco.cbslocal.com/2018/06/07/ntsb-driver-fatal-[redacted]-crash/amp/

(1) Eye Chart (2) Sign Shape (3) Max Speed

And What About Attacking Something Like a "*God View...For Viewing Pleasure*"?

https://www.forbes.com/sites/kashmirhill/2014/10/03/god-view-[redacted]-allegedly-stalked-users-for-party-goers-viewing-pleasure/

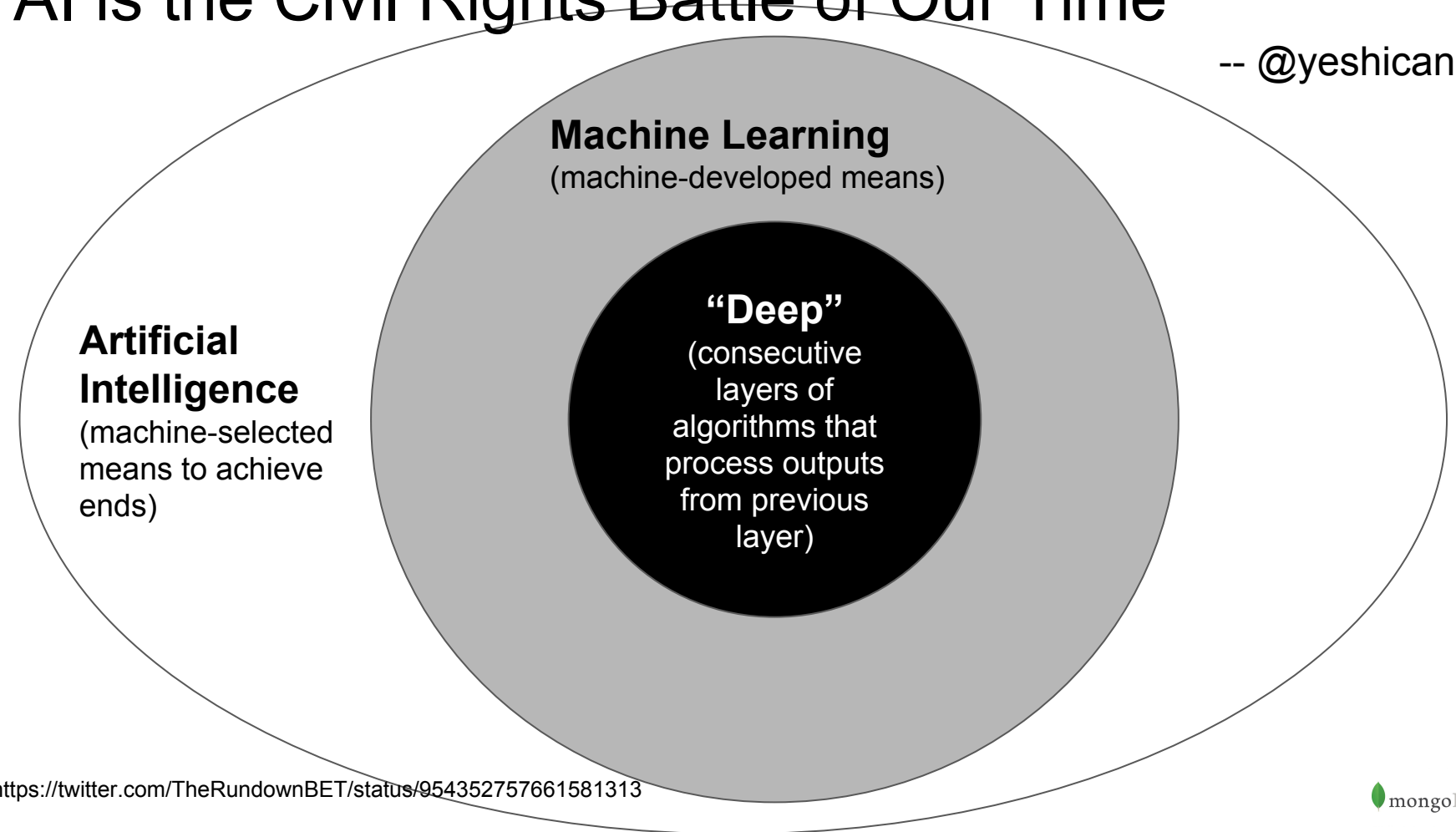
Also Easily Broken Using Simple Tests



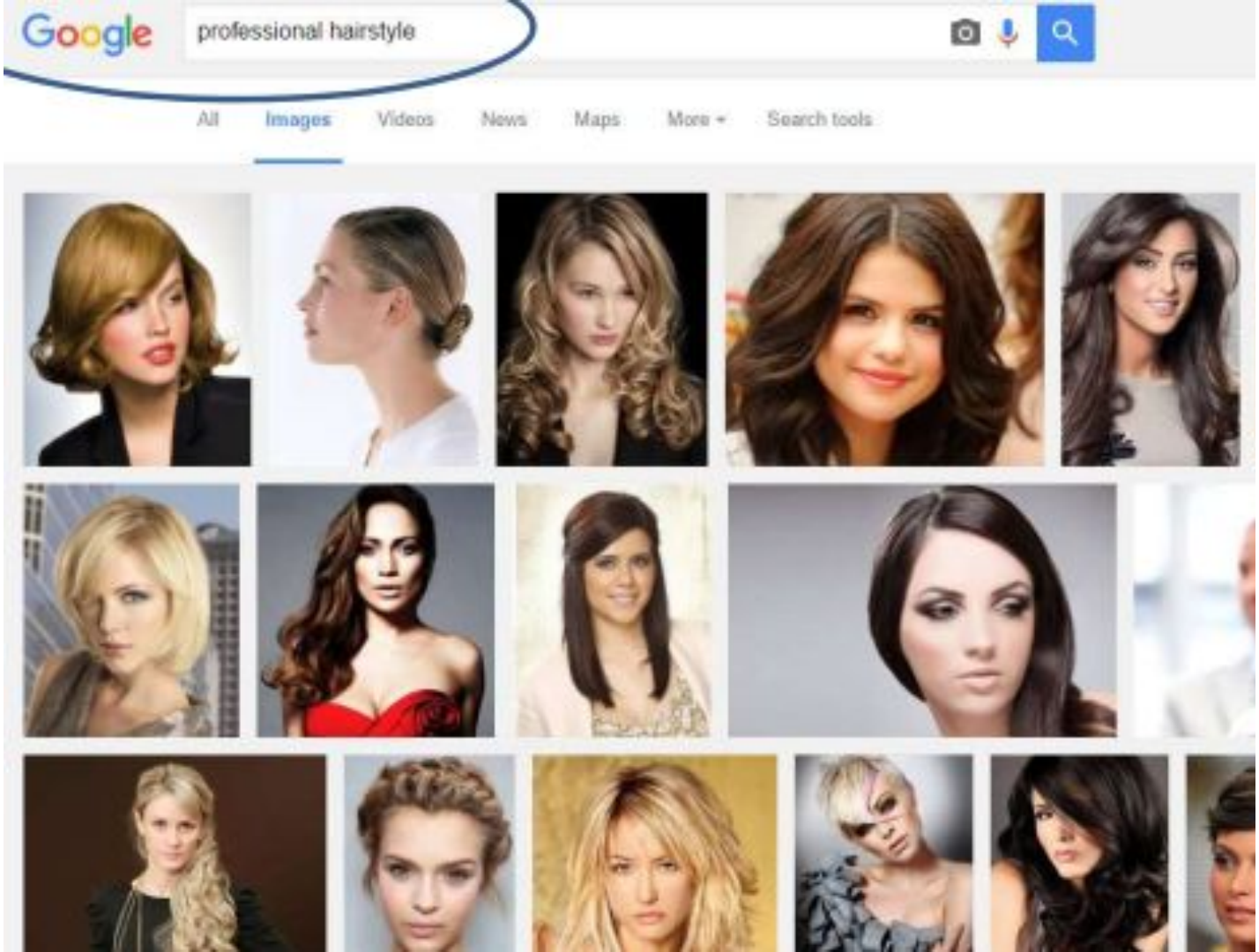
What Do Such Machine ***Classification*** Failures Really Mean?

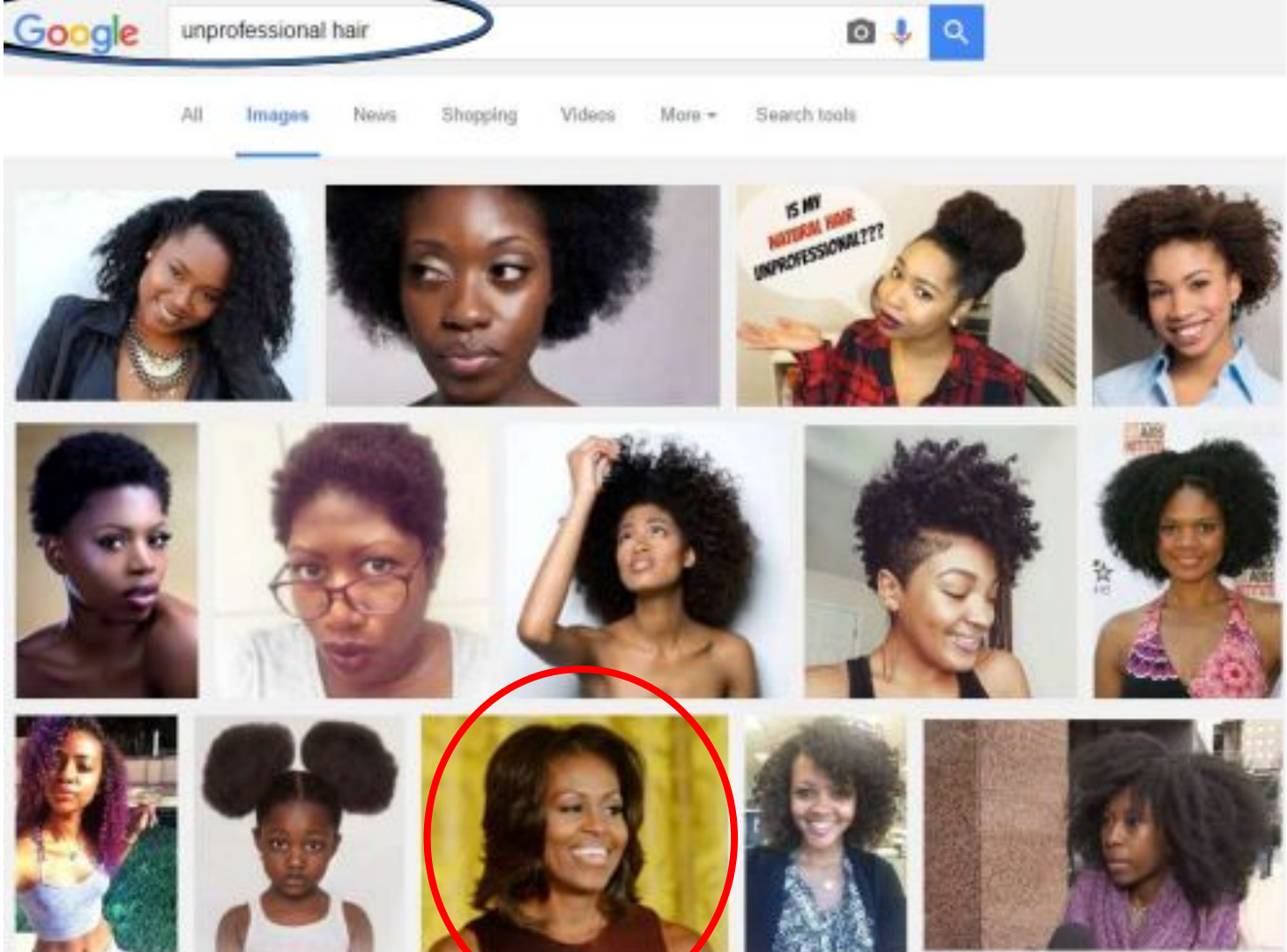
“AI is the Civil Rights Battle of Our Time”

-- @yeshican

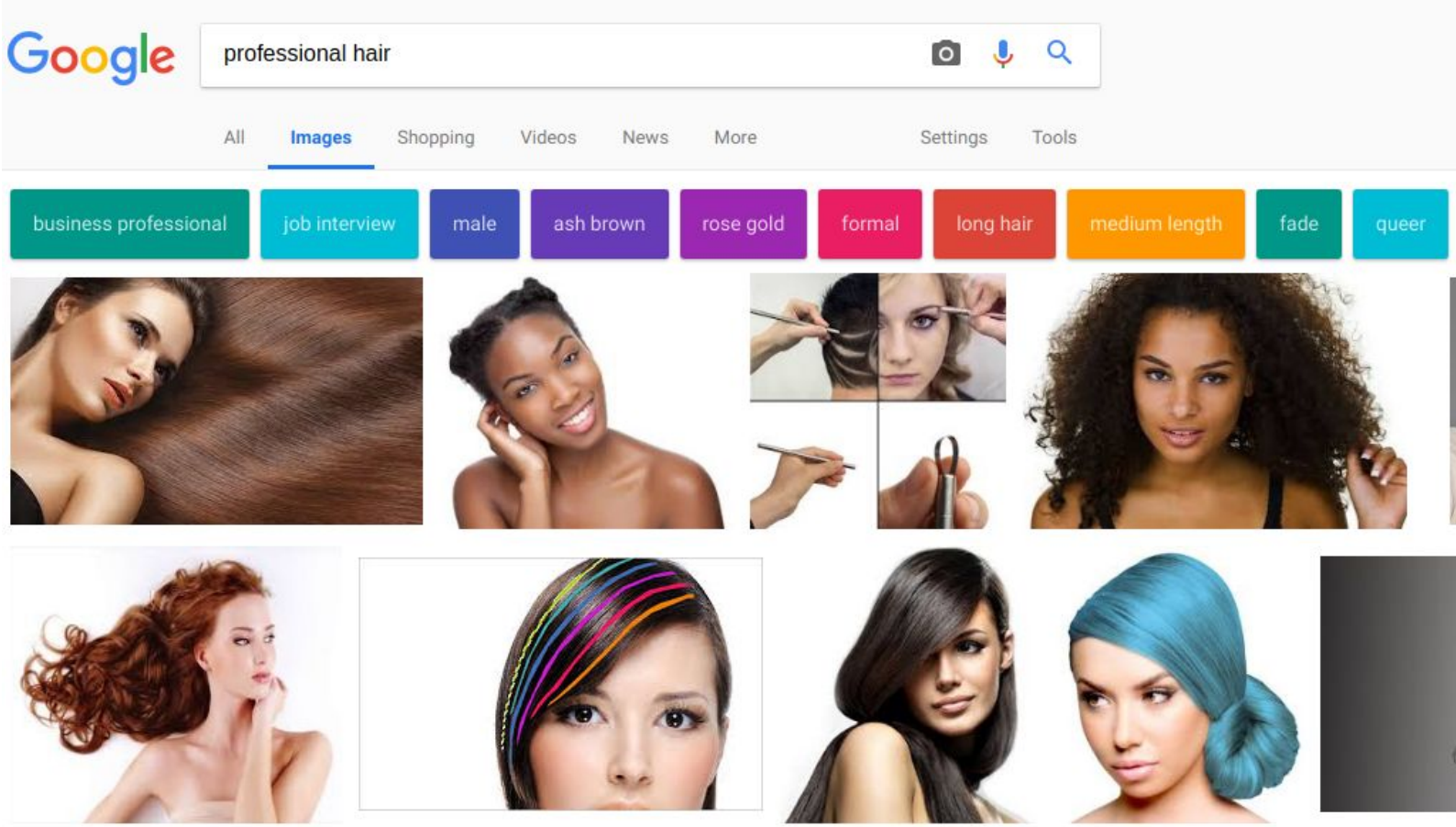


https://twitter.com/TheRundownBET/status/954352757661581313


Google
professional hairstyle
All
Images
Videos
News
Maps
More
Search tools


Google
unprofessional hair
All
Images
News
Shopping
Videos
More
Search tools
IS MY NATURAL HAIR UNPROFESSIONAL???

Three Years Later



https://www.iafrikan.com/2016/06/25/why-does-a-google-search-for-unprofessional-hair-show-images-of-black-women-including-michelle-obama-2/

False 'Criminal' Labeling

'compared predicted to actual recidivism: scores wrong 40% of the time and biased against black defendants.'

https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

“Safe Machine Learning”
Requires Technical Rules
Founded on Moral Principles

SSLv2 Privacy Fail, Thus Unsafe to Use

Moral Principles of Machine Intelligence

(This Isn’t Your Grandfather’s Firewall Anymore)

1600s: Foundations of Machine Intelligence

1637 **Descartes:** “Cogito, ergo sum”

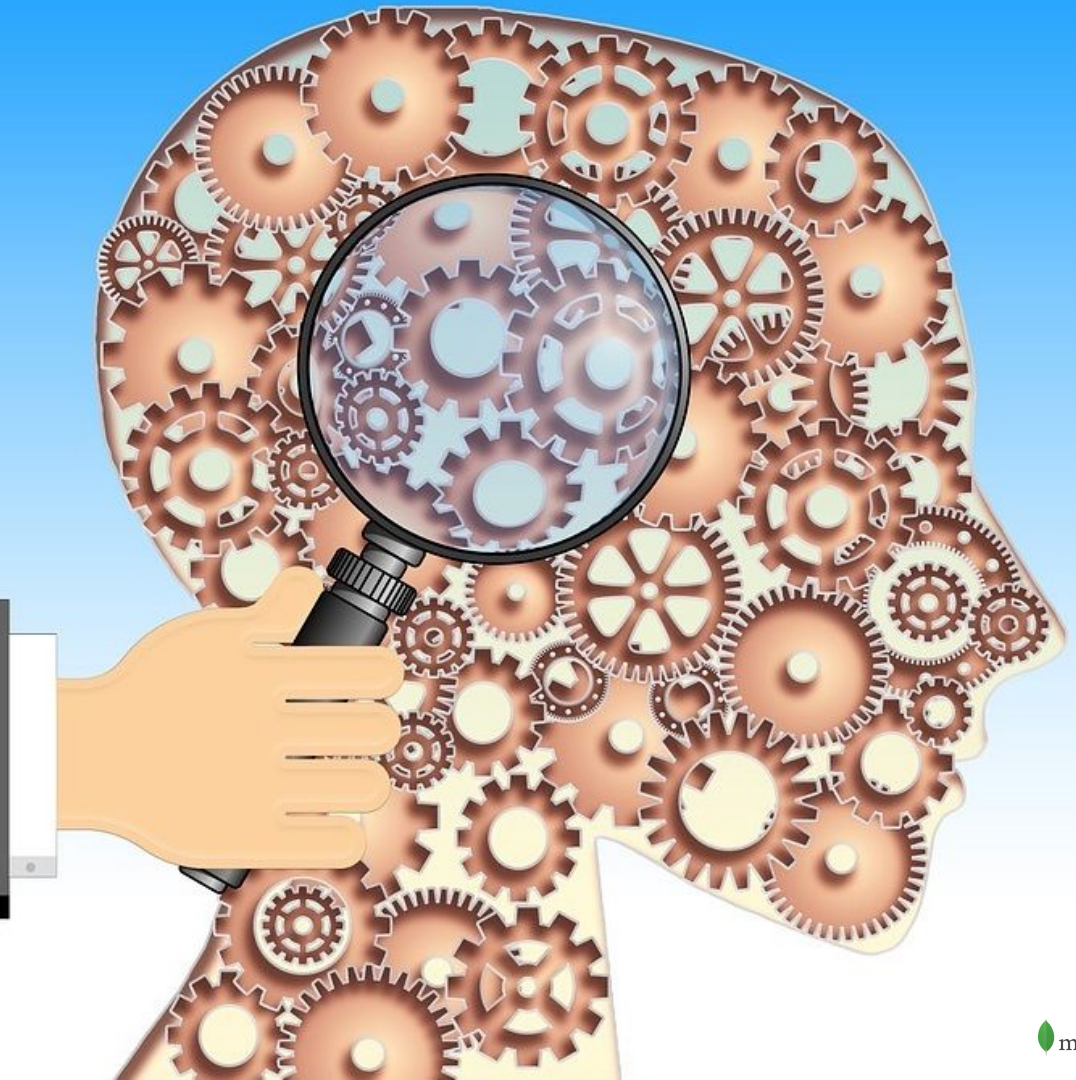
1651 **Hobbes:** mental operations are a mechanical calculator: “REASON... is nothing but reckoning”

1685 **Leibnitz:** “Let us calculate [*calculemus*], without further ado, to see who is right”

1693 **Locke:** Reflective Process, Articulated Steps...

1651

Hobbes: mental operations are a mechanical calculator: “REASON... is nothing but reckoning”



Then in the 1700s

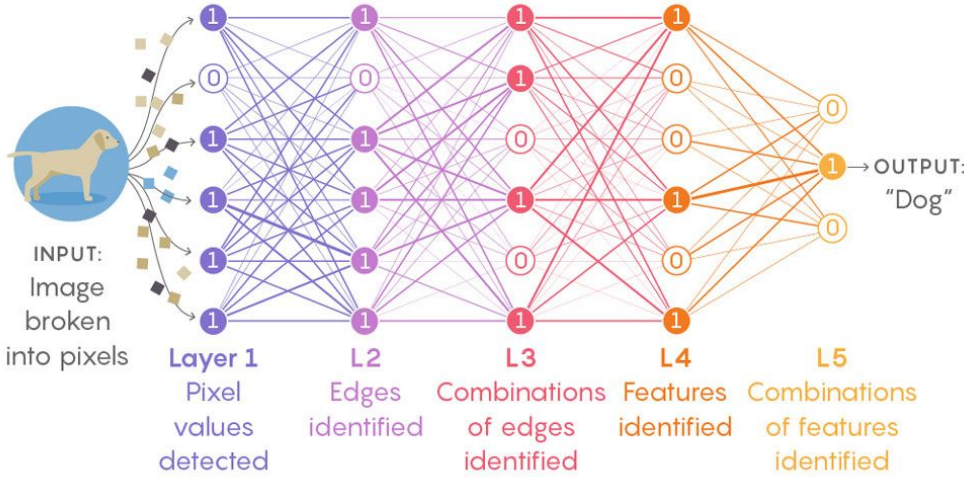
"The ***most important part of learning is forgetting*** [noise unnecessary to remember]"

David Hume
(1711-1776)

https://www.quantamagazine.org/new-theory-cracks-open-the-black-box-of-deep-learning-20170921/

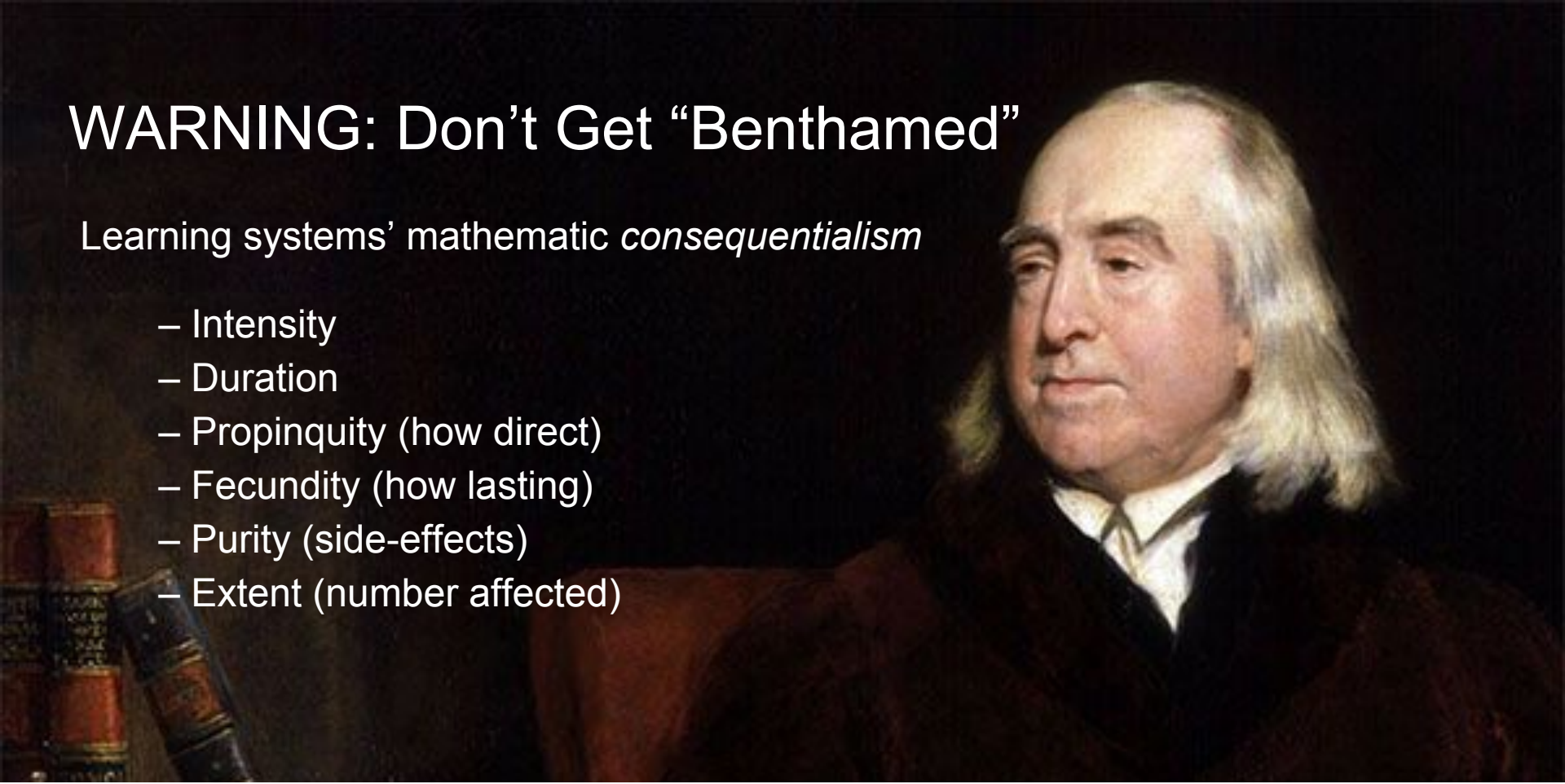
Learning From Experience

Deep neural networks learn by adjusting the strengths of their connections to better convey input signals through multiple layers to neurons associated with the right general concepts.



When data is fed into a network, each artificial neuron that fires (labeled "1") transmits signals to certain neurons in the next layer, which are likely to fire if multiple signals are received. The process filters out noise and retains only the most relevant features.

WARNING: Don’t Get “Benthamed”



Learning systems’ mathematic *consequentialism*

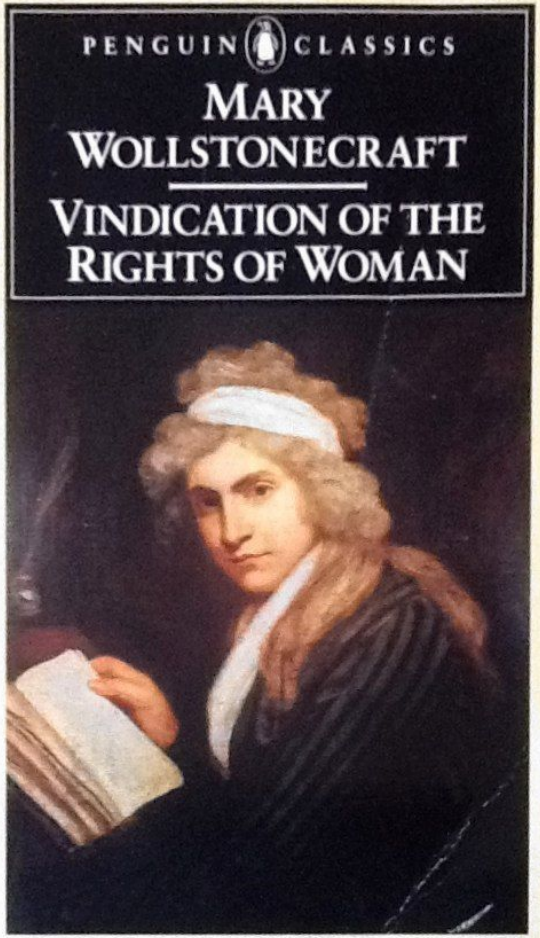
- Intensity
- Duration
- Propinquity (how direct)
- Fecundity (how lasting)
- Purity (side-effects)
- Extent (number affected)

Instead, Read More Wollstonecraft

- A Vindication of the Rights of Man (1790)
  - Unequal society founded on passivity of women
  - Rationality, unlike ancestral traditions, abolishes slavery

- A Vindication of the Rights of Woman (1792)
  - Human limitations are a result of ***deficient education***
  - Middle-class “most natural state”
  - Equality of sexes

“Sufficient” learning systems reduce bias



100 Years of Locke's "Reflective Process, Articulated Steps":

Right General Concepts (Edward Jenner in 1796)

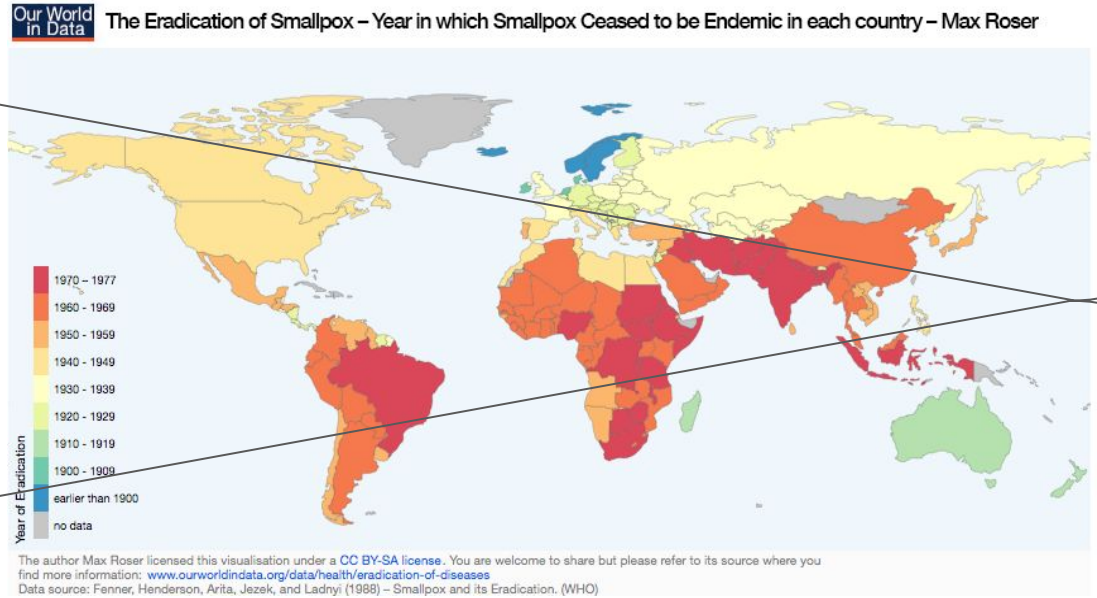
Only the Most Relevant Features

Identify

Store

Evaluate

Adapt



Easy

Routine

Minimal Judgment

Another 150 Years Later…

Machina Speculatrix 1953

If light moderate

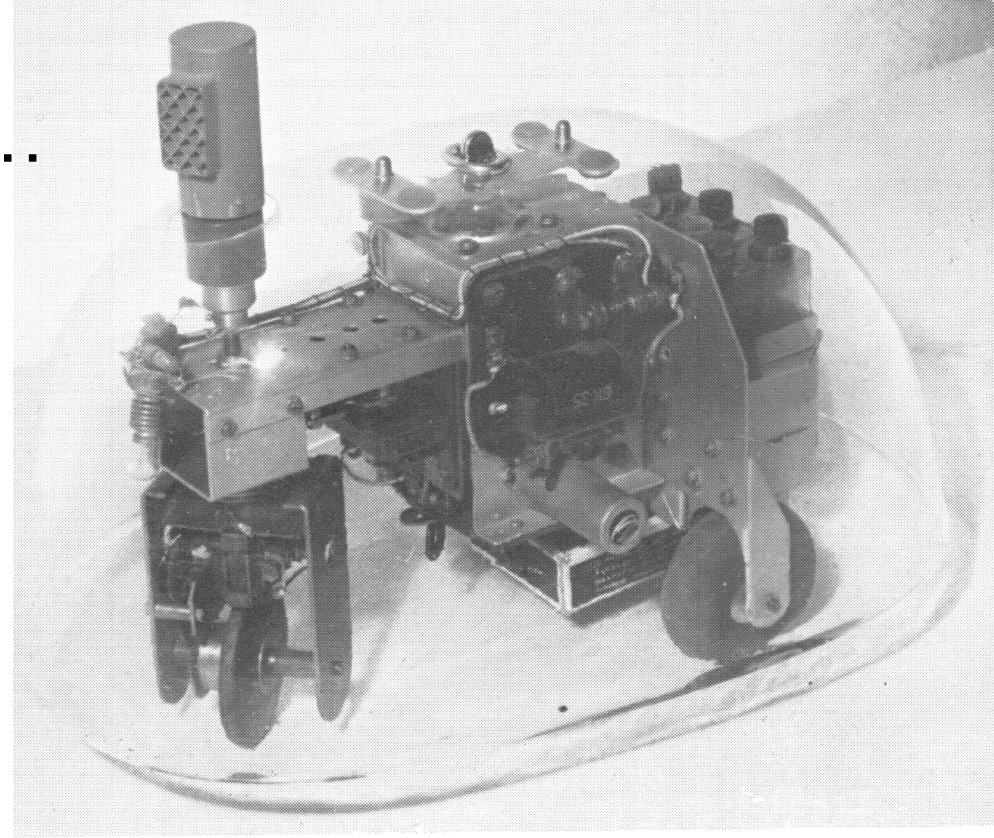
Then move toward

If light bright

Then move away

If battery low

Then return for charge



Electro-mechanical robot, Light-sensitive with Internal and External stability (ELSIE)

Wollstonian Test for “Sufficiency” in Intelligent Machines

Machine “Intelligence” Depends on Moral Authority

Disciplines Calculating the Assignment of Authority:

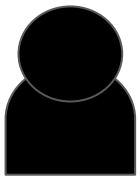
- History
- Economics
- Politics

Ethics

Which Box Does Your Machine Strategy Fit Into?

Inherent Authority: follows right/wrong rules and *can be good*	**Controlled Authority:** sets right/wrong rules and can be *neither good nor bad*

Inherent Authority Tests in Three Safety Control Areas

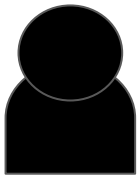
Auth	Encryption	Audit
(Authentication Authorization)		
		

Governance, Risk, Compliance

(standards & transparency, including vulnerability management)

Auth

(Authentication
Authorization)



Encryption

Audit

Ingest → Store → Analyze → Surface

Saturate → Incubate → Illuminate

SOC2 FedRamp FIPS

Governance, Risk, Compliance

(standards & transparency, including vulnerability management)

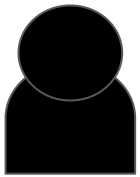
GDPR ISO HIPAA NIST

Auth

(Authentication
Authorization)

LDAP X.509

SASL kerberos



Encryption

KMIP TLS

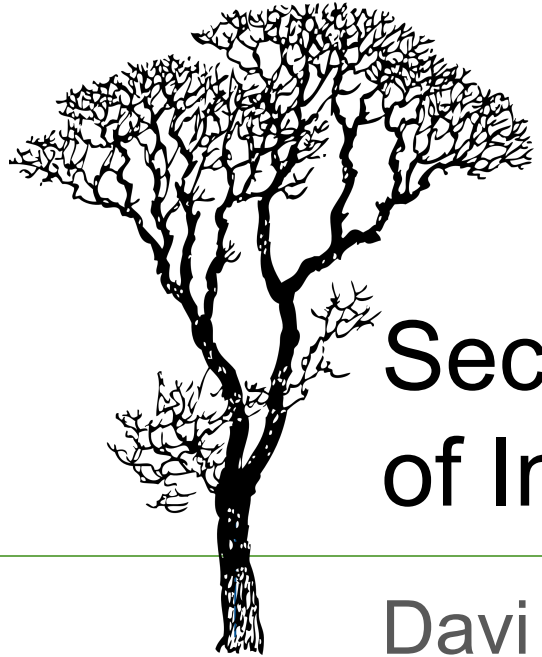
SHA

Audit

SCAP CVE

syslog CIS

STIG



Security in a World of Intelligent Machines

Davi Ottenheimer

mongoDB.