

Hidden Hot Battle Lessons of Cold War

All Learning Models Have
Flaws, Some Have
Casualties

Davi Ottenheimer



Abstract

In a pursuit of realistic expectations for learning models can we better prepare for adversarial environments by examining failures in the field?

All models have flaws, given any usual menu of problems with learning; it is the rapidly increasing risk of a catastrophic-level failure that is making data /robustness/ a far more immediate concern.

This talk pulls forward surprising and obscured learning errors during the Cold War to give context to modern machine learning successes and how things quickly may fall apart in evolving domains with cyber conflict.

whoami

“most exciting part of history is analysis
of how things really happened, fixing
integrity in huge warehouses of data”

-- davi



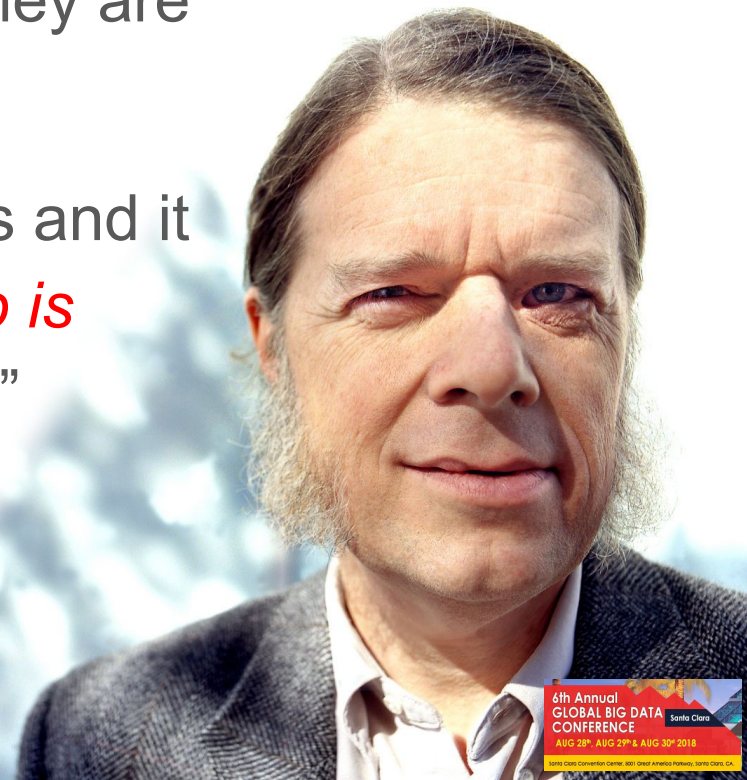
Warning: Big Picture Talk Ahead

“Generalists are becoming rare, and they are being replaced by specialists.

[...] Specialization is not just for insects and it will not stop, but the *human in the loop is ever less likely to have the big picture.*”

-- Dan Geer, CIA

Source: <http://geer.tinho.net/geer.suitsandspooks.8ii12.txt>

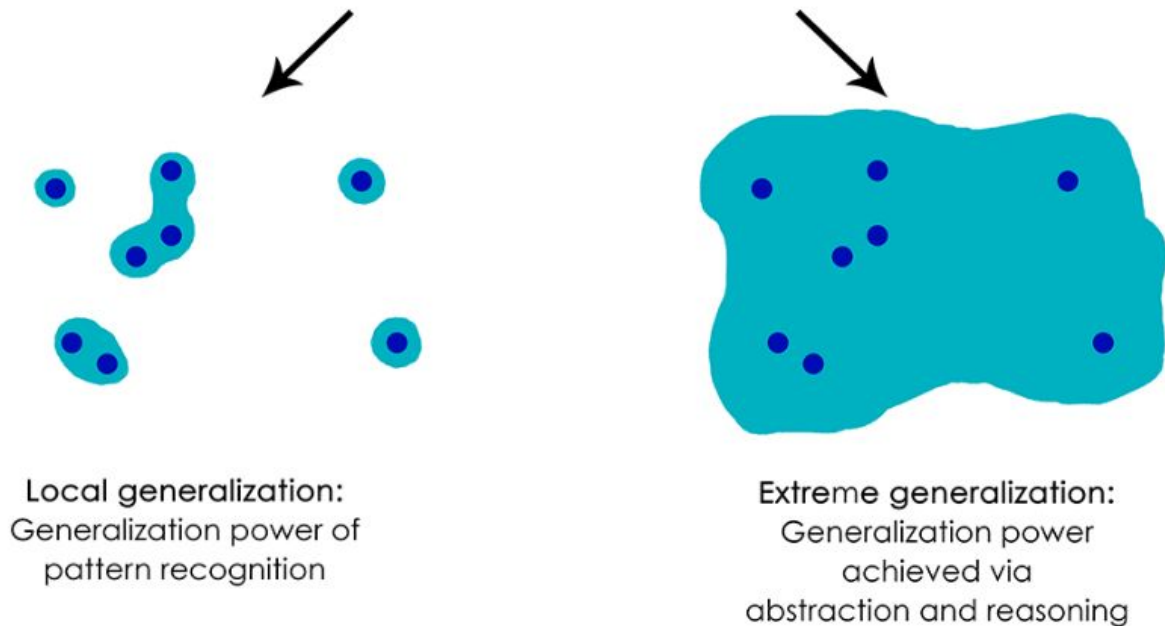


Ever Less Likely
to Have Big
Picture?

False

Technology historically
augments and promotes humanity.
Enables us to generalize, think bigger picture

General Introduction to Generalization

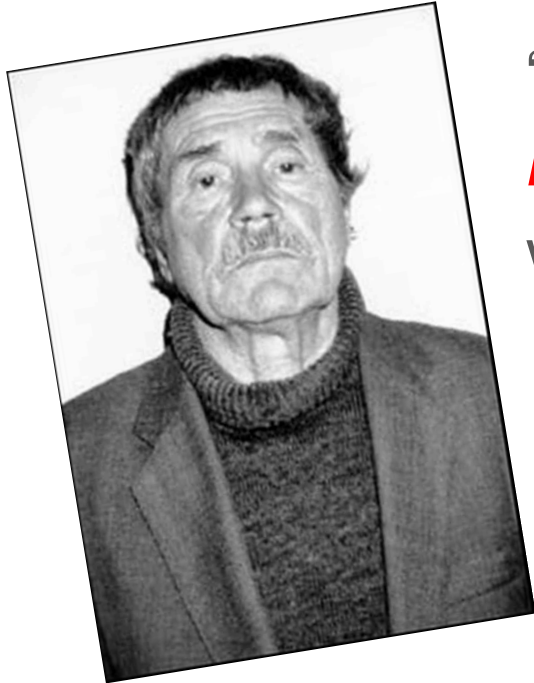


(Synthesis and Analysis)

<https://blog.keras.io/the-limitations-of-deep-learning.html>

mongoDB.

Warning: History (Big Picture) Talk Ahead



“It is a well known fact *the new is no more than a reinvention of the old* which has been totally forgotten.”

-- Vasily Mitrokhin,

KGB archivist and defector, 2002

Source: “KGB Lexicon: The Soviet Intelligence Officers Handbook”

<https://books.google.com/books?id=cKErBgAAQBAJ&lpg=PR25&pg=PR25#v=onepage&q&f=false>

 mongoDB.

Warning: Philosophy (Big Picture) Talk Ahead

“Those who cannot remember the past are condemned to repeat it.”

-- George Santayana, 1906



Remember the Last Hot Battle of Cold War?

Nixon “Realist” Foreign Policy of White Supremacy

1. White supremacy defeated in WWII
2. Sets stage for liberation and self-rule (anti-colonialism)
3. Kissinger rejects trends, dismisses black governance
 - a. Criticises Wilson (WWI), Truman and Eisenhower (WWII)
 - b. Declares geopolitics a necessarily *elite amoral exercise*
 - c. Rejects President Johnson’s “racial justice” doctrines
 - d. Labels “anti-white” anyone in US gov who disagrees
4. Data integrity contest with State...



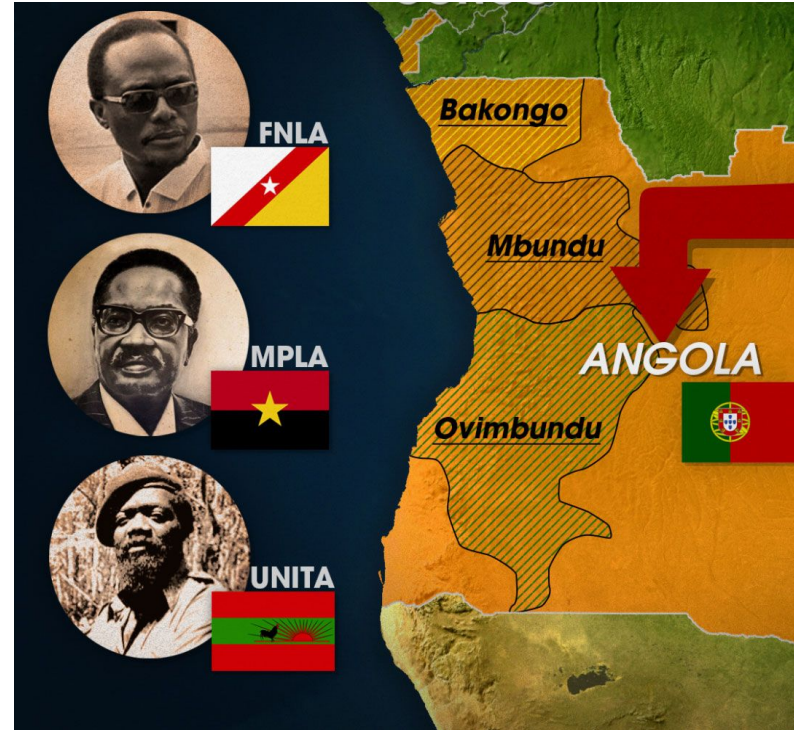
Foreign Service Expert Analysis: Angola 1975

1. No real US security issues

- Oil
- Coffee

2. Domestic political contest

- FNLA (National Front for the Liberation of Angola)
- MPLA (People's Movement for the Liberation of Angola)
- UNITA (National Union for the Complete Independence of Angola)



Foreign Service Expert Analysis: Angola 1975

3. Regional Dynamics

- Everyone wary of USSR
- Benguela railroad control (export/import)

4. Mobutu (Zaire)


- Courts econ aid from China
- Paranoid: June 1975 when economy weak he jails CIA for coup plotting



Postcolonial = Inherited Unmanageable Bureaucracy

FAILURES WERE **NOT** BECAUSE DID NOT KNOW HOW TO GOVERN

- External territorial threats
- Ideological divisions
- Resource scarcity
- Refugee influx



**MUST ADD
ELITIST
AMORALITY**

Eduardo Mondlane

“His ‘American decade’ began as he earned his Oberlin BA in sociology and anthropology in 1953, followed by MA at Northwestern University, and PhD in anthropology at Harvard”

... began his college education at Witwatersrand University in South Africa, but, after a year, was forced to withdraw by the new apartheid-oriented Nationalist Party government.

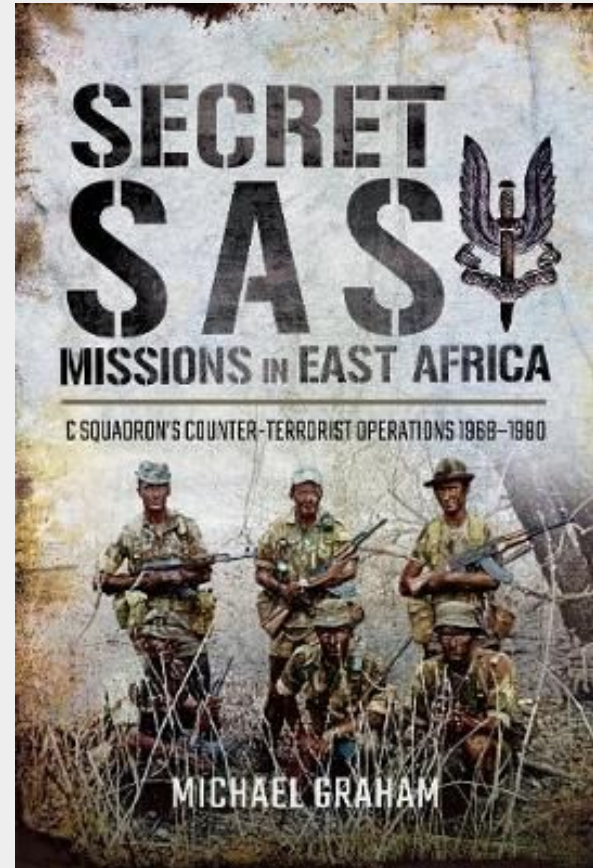
Protestant missionaries in Mozambique helped arrange a scholarship from the Phelps-Stokes Fund in New York for Eduardo to study in the United States, but Eduardo decided to attend Lisbon University where he could learn first-hand about Portuguese government and policies, and gain a better command of the language. However, after a year of ill-treatment as an African student, he accepted the scholarship and arrived at Oberlin.

...remembered as “a strong, intelligent, eloquent, and valiant man—a man of the highest character and ideals. Dedicated to the cause of freedom for his own country, he was in every sense a citizen of the world.”

Eduardo Mondlane

Assassinated 1969

(MLK 1968, Sharmarke 1969, Mboya 1969)



<https://www.tandfonline.com/doi/abs/10.1080/19392206.2017.1305861>
<https://www.tandfonline.com/doi/full/10.1080/14682745.2016.1246542>

Kissinger 1975 Dismisses “Bleeding-Hearts”

Closed Learning Model (Cognitively Blind)

- Wanted post-Vietnam quagmire for USSR
- Called “No-Win War” the “inexpensive” one
 - \$100m estimate to “win” too visible, needs supervision
 - \$14m for long-term subversion, hidden from US public
- Selects “White Minority ‘Communication’ Option”



“only real result of [Kissinger doctrine] would be to mire US deeper on the side of the oppressors in southern Africa”

27 Years of Angolan Civil War (1975-2002)

500,000

killed

27 Years of Mozambique Civil War (1964-1992)

**1,000,000 killed
(600,000 children)**

End Point: 1987 *Cuito Cuanavale Hot Battle*

- Despite post-1977 arms boycott...
South Africa invaded Angola
- Cuba airlifted massive defense
- South Africa failed, forced to withdraw
- Angolan-Cuban win liberated blacks
 - Namibian independence
 - Unbanned political parties
 - Release of political prisoners



Sources: <https://www.casematepublishers.com/ebooks/military-history-by-region/africa/the-last-hot-battle-of-the-cold-war.html>,
<https://www.worldcat.org/title/at-thy-call-we-did-not-falter/oclc/61684917>, https://books.google.com/books?id=_r701h-tWzWC&pg=PA14#v=onepage&q&f=false

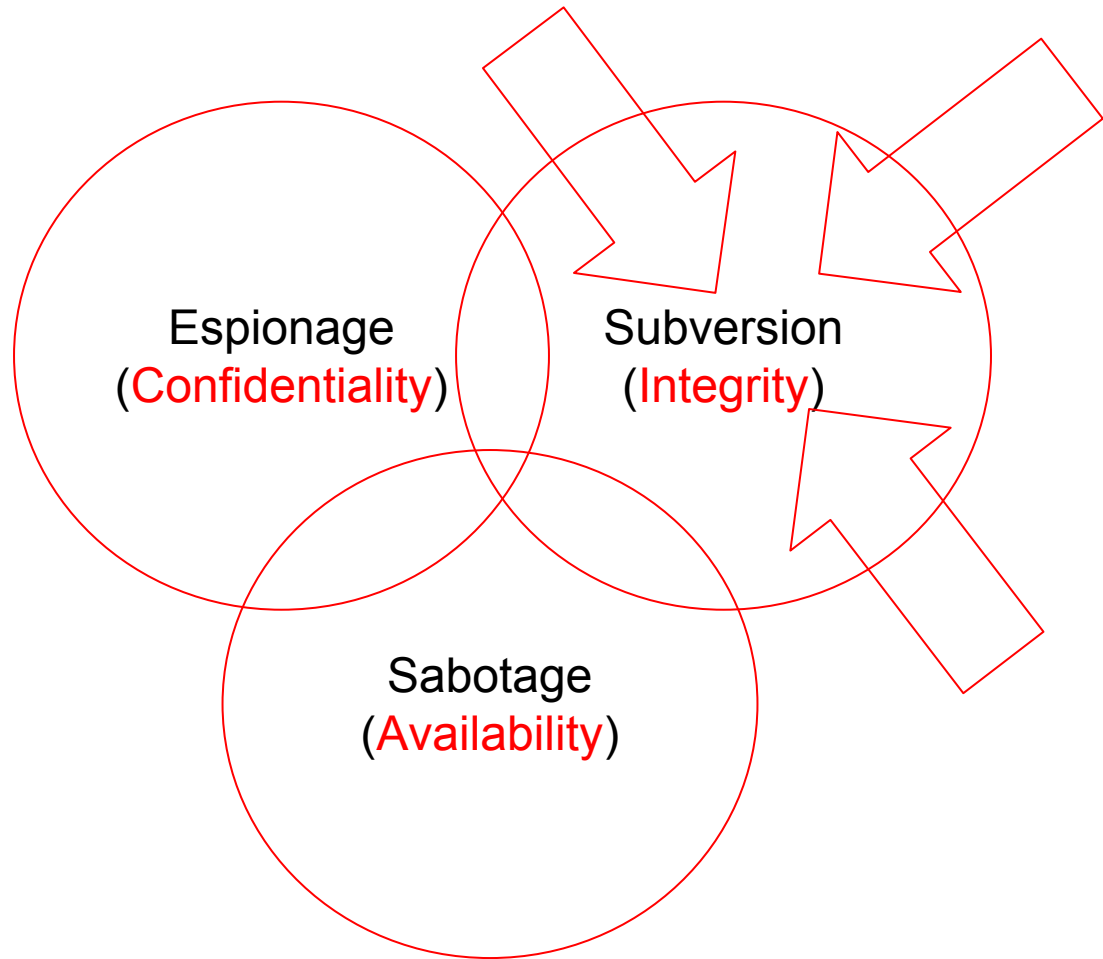
What's The Cold War's Last Hot Battle Got to Do With Cyber?

Don't Repeat Past Mistake

Data Integrity Contest...



Cyber Triad



Confidentiality in the 2000s

2007 EKMI (Enterprise Key Management Infrastructure)

"...a collection of technology, policies and procedures for managing all cryptographic keys - symmetric and asymmetric..."

2009 KMIP (Key Management Interoperability Protocol)

RSA, HP, IBM, Thales, Brocade, and NetApp

"...interoperable protocol for standard communication between key management servers, and clients and other actors..."

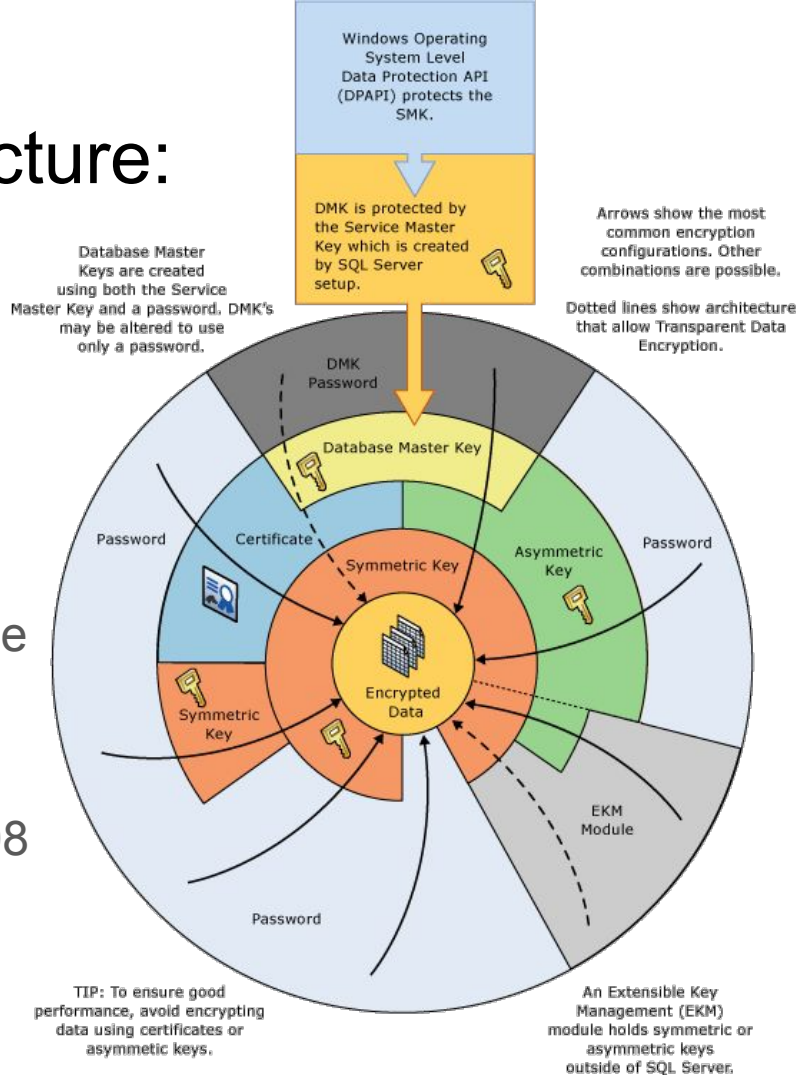


Sources: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ekmi,
<https://lists.oasis-open.org/archives/tc-announce/200903/msg00002.html>

And From the Bigger Picture:

“...performance for very basic query (select and decrypt single encrypted column) using cell-level encryption around 20% worse. ...several magnitudes worse to encrypt an entire database.”

-- Microsoft 2008



Source: [https://msdn.microsoft.com/en-us/library/cc278098\(v=sql.100\).aspx](https://msdn.microsoft.com/en-us/library/cc278098(v=sql.100).aspx)

Confidentiality: 2017...

Howabout a Nice Hot Cuppa
Cell-Level Encryption?

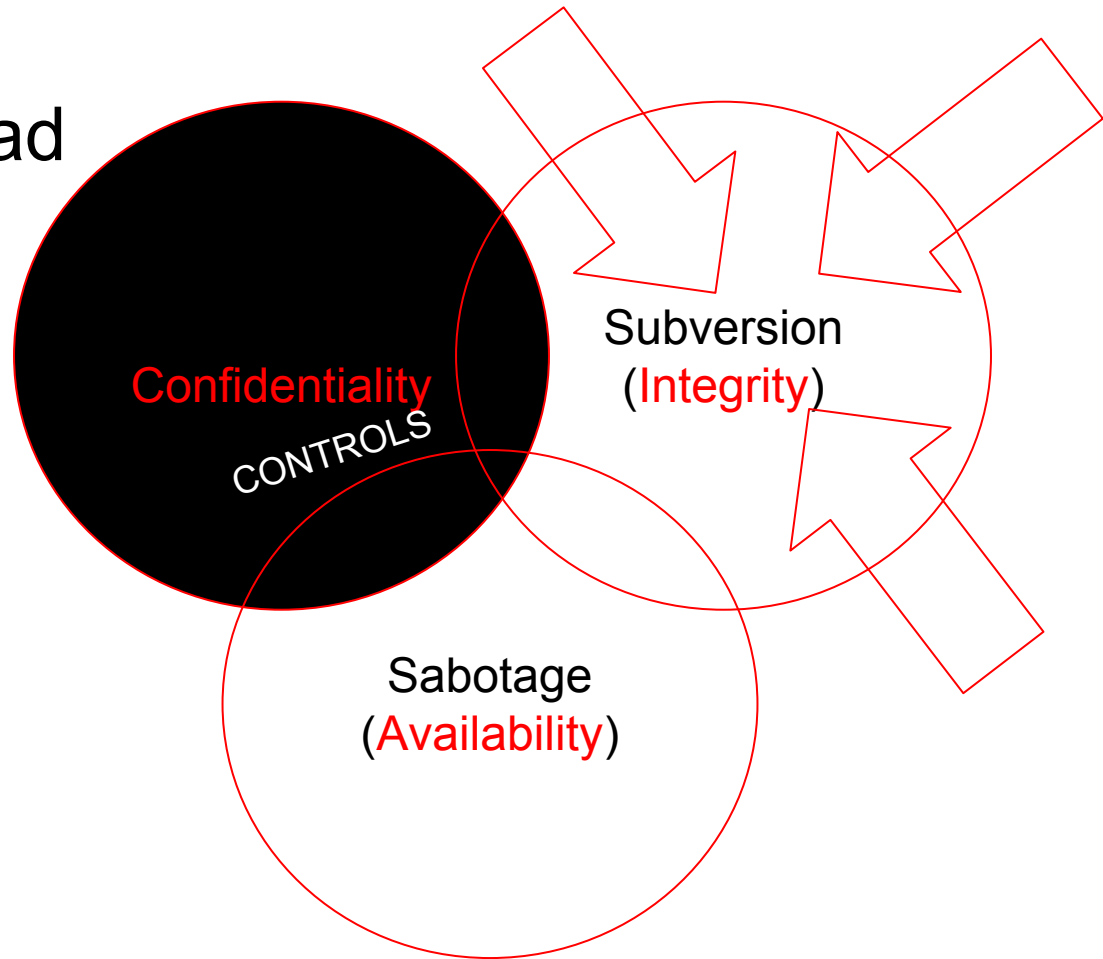
	attribute: birthday	attribute: CCN	asset: phone	liability: balance
alice	July 23, 2017	7asd9D Ag73kj0	\$200	
bob	x4Adfxj3l a93das	5555-555 5-5555	\$100	\$100

■ Encrypted

■ Unencrypted



Cyber Flaw Triad



Availability: 2014

Launch Hybrid Cloud - 48 Hour Objective

- 40,000 hours invested
- *10 hour* launch achieved

Zero Downtime - One Million Bucks Guaranteed

“...first customer to demonstrate...data services switched off, throttled back, post-processed, deprioritized (even for one moment) gets one million bucks.”

-- David Goulden, CEO, EMC Info Infra (II)

Sources: <https://blog.dellemc.com/en-us/emc-flashes-1million-guarantee-xtremio-customers/>
<https://siliconangle.com/blog/2014/05/19/the-surprises-discovered-when-emc-built-their-hybrid-cloud-emcworld/>

Availability: 2017

Launch 50,000 Servers / Month - 100% Success Objective

- Limited Herd Specialization

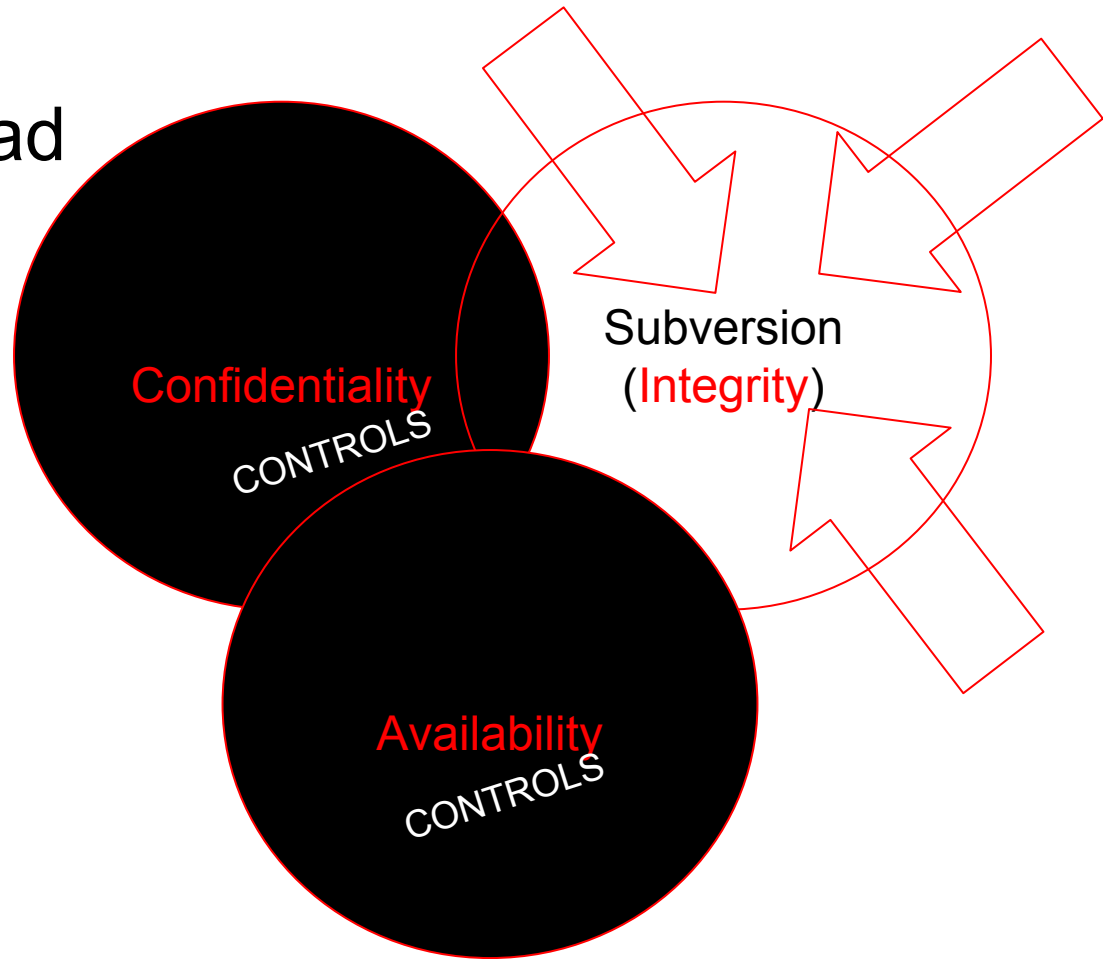
Yee Haw

- 93% - 97% Provision Success on Reliable Installs (Ubuntu)
- 89% on Complex Installs (Windows 2012 R3)

- **100% achieved** January 2017: 100s Loss Prevention/Mo

Source: <https://www.packet.net/blog/our-journey-to-zero-failed-installs/>

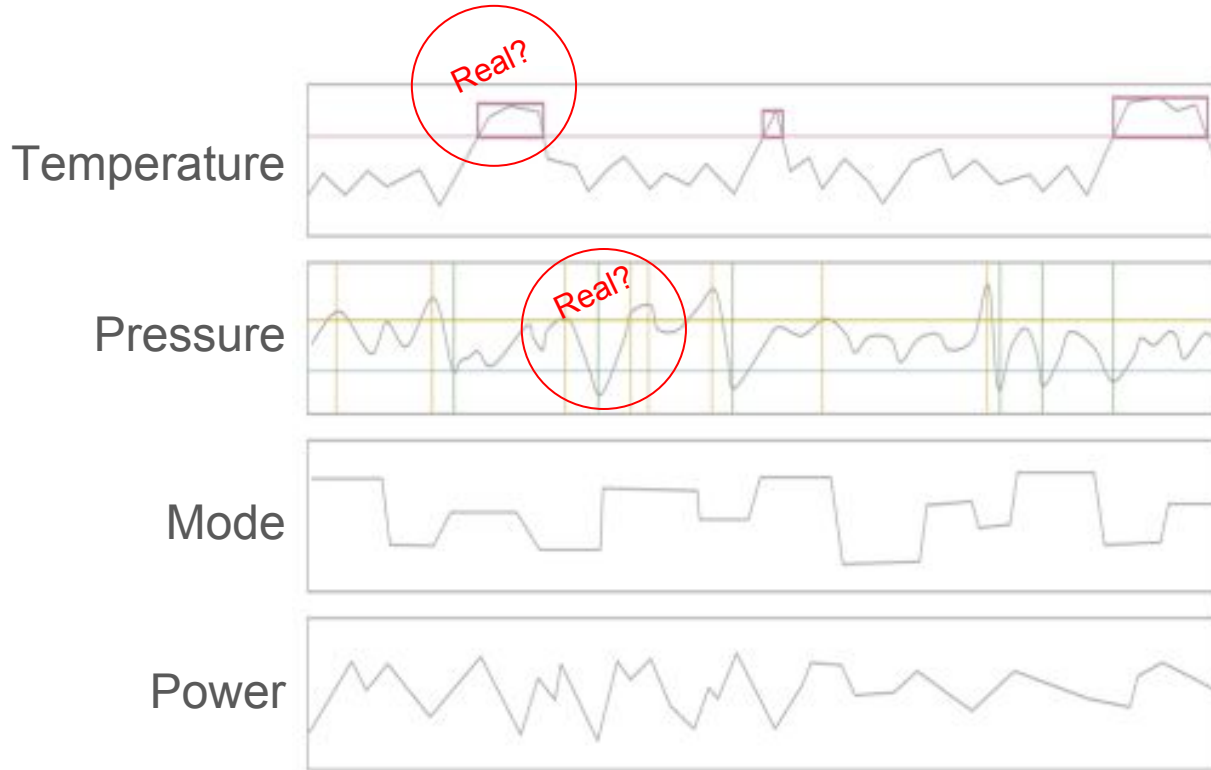
Cyber Flaw Triad



Data Integrity Contest...



Deadly Abstraction and Reasoning Flaws



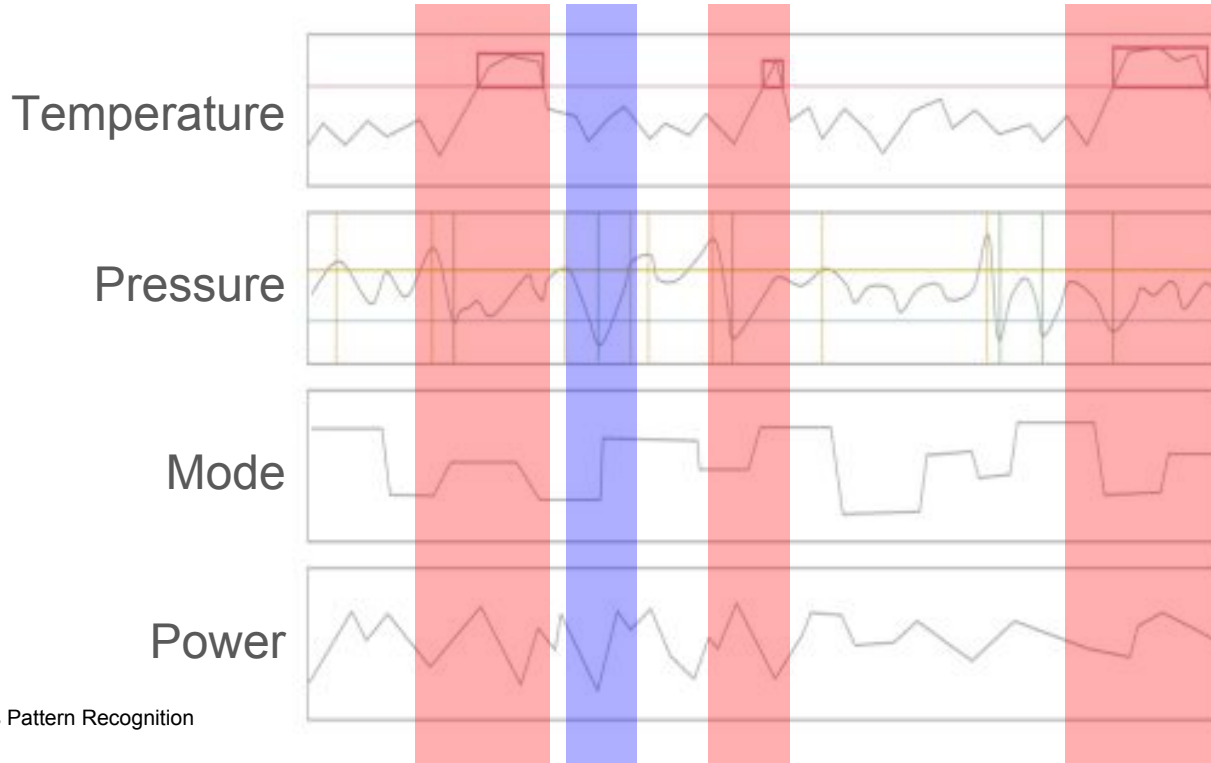
Source: Splunk Time Series Pattern Recognition

mongoDB.

Subversion (Integrity)

Condition 1:
Distracted

Condition 2:
Disabled



Source: Splunk Time Series Pattern Recognition

mongoDB.

Unregulated Integrity = SNAFU

Situation
Normal
All
F---ed
Up



Grant Williamson @ozjimbob · 16h

This is probably the most potentially deadly app I've ever seen

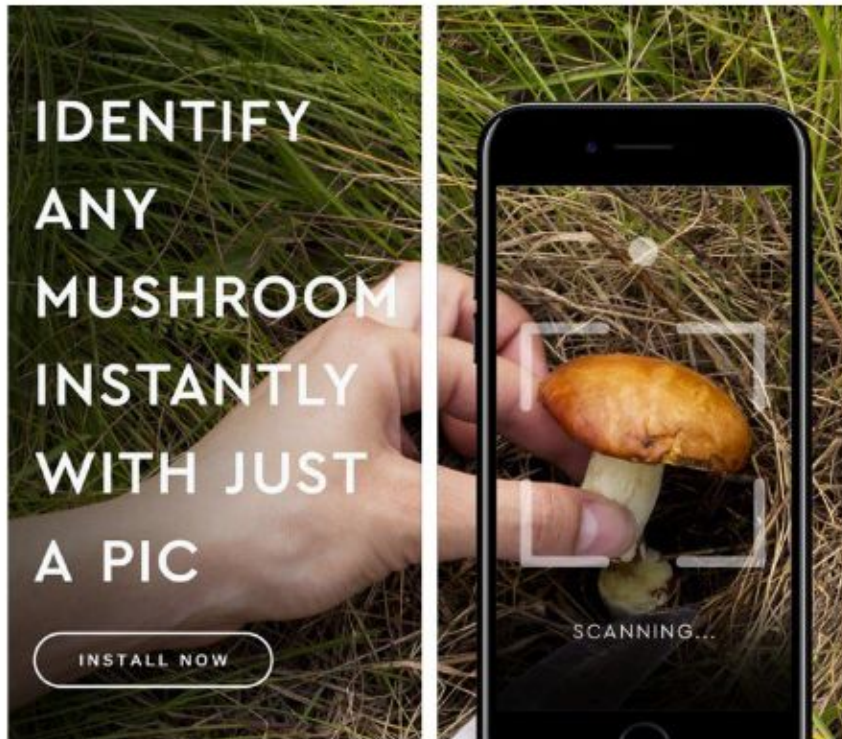


Mushroom - Instant
mushroom plants identifi...

Quest Mobile LLC

\$7.99

In-App
Purchases



Source:

<https://twitter.com/ozjimbob/status/889411603434586114>

mongoDB.

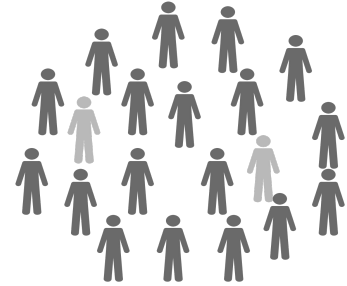
We Already *Train Learning Systems to Harm*

LYDEN: I wonder what the impact is of all of this lack of female representation.

DAVIS: We just heard a fascinating and disturbing study, where they looked at the ratio of men and women in groups. And they found that if there's 17 percent women, the men in the group think it's 50-50. And if there's 33 percent women, the men perceive that as there being more women in the room than men.

LYDEN: Why else, Geena Davis, do these kinds of disparities matter?

DAVIS: What we're, in effect, doing is training children to see that women and girls are less important than men and boys. We're training them to perceive that women take up only 17 percent of the space in the world. And if you add on top of that, that so many female characters are sexualized - even in things that are aimed at little kids - that's having an enormous impact as well.



17%  50%

Sources: <http://www.npr.org/templates/transcript/transcript.php?storyId=197390707>
https://seejane.org/wp-content/uploads/GDIGM_Gender_Stereotypes.pdf

 mongoDB.

We Manipulate the Software Embedded in People



So how do the Jihadis come into the picture?
the are basically manipulating the software
already embedded in people's by using these
themes

1:54 PM - 23 Jul 2017

Source: <https://twitter.com/weddady/status/889227229040971776>

We Automate Manipulation: Attacks on Al Jazeera Tweets Were “71% Bots” نطالب_باغلاق_قناة_الخنزيرة

Date of Sample	23rd June 2017
Sample Size (Total Tweets)	8107
Number of Tweets from Bots	≈5800 (71%)
Total Unique Accounts	≈4116
Total Unique Bots	≈2831 (68.8% of total)

2338 Bot Accounts Created 2016:

- May 818
- April 610

Source: <https://bahrainwatch.org/amanatech/en/investigations/we-demand-the-closing-of-the-channel-of-pigs>

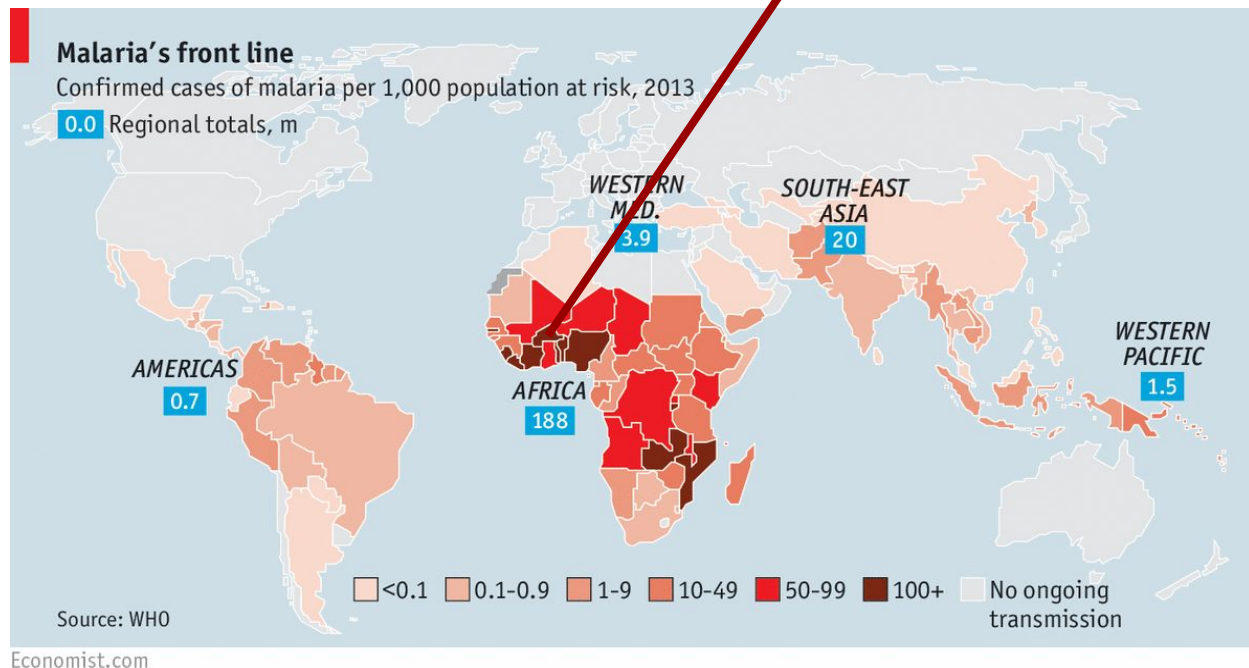
Data Integrity Contest...



Disease Abstraction and Reasoning...

1. “Up to 35% of antimalarial drugs are useless”

2. Supply-Chain
**Data Integrity
Broken**



Sierra Leone

Libera

Ivory Coast

Insecure Learning Models Are Nearly Everywhere (Data Integrity Threats)

2016: Knightscope Observational Data Failures

- Didn't **See** Toddler
 - “...meant for observing and reporting only”
 - Knocked Him Down
 - Ran Over Him
 - Weighs 300lbs
- Second Incident



<http://abc7news.com/1423093/>

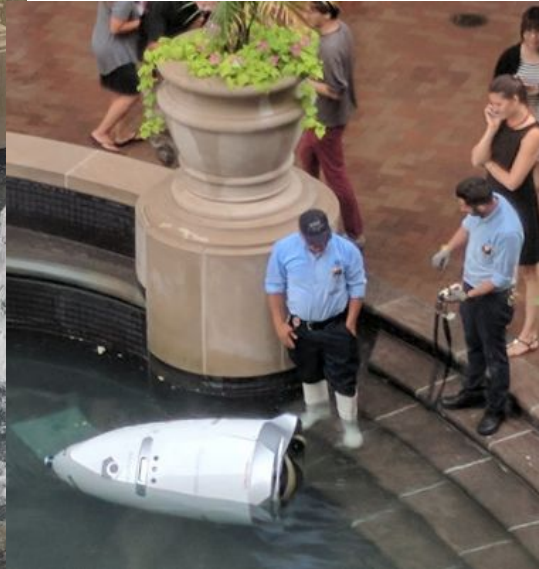
<http://www.fastcoexist.com/3049708/meet-the-scary-little-security-robot-thats-patrolling-silicon-valley>



flyingpenguin

Source: <http://www.flyingpenguin.com/?p=22441>

2017: Knightscope “Advanced Anomaly Detection”

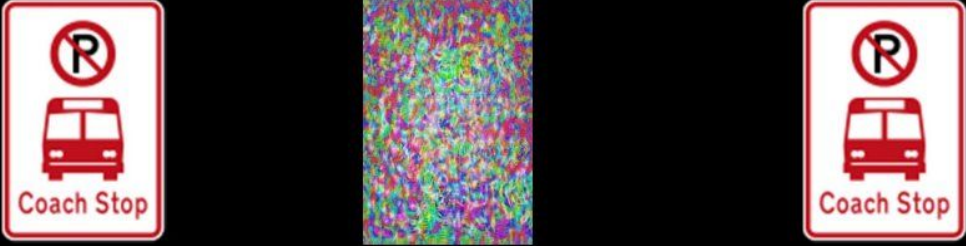


Sources: <https://twitter.com/gregpinelo/status/887019884458192896>,
<https://twitter.com/bilalfarooqui/status/887025375754166272>

2016: Remember My Warnings to Tesla?

Un-Supervised Break (Traffic)

No Parking + 'Stop' = 'Stop'



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

KIWICON X

Sources: <http://www.flyingpenguin.com/?p=22441>, <http://www.flyingpenguin.com/?p=22429>

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



Venkat Viswanathan

@venkvis

Follow

██████████ autopilot camera misreads 101 sign as 105 speed limit at 87/101 junction San Jose. Reproduced every day this week.



8:40 PM - 14 Jul 2017



“Intelligent Machines” *Fatally* Fail Integrity Tests...

“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:



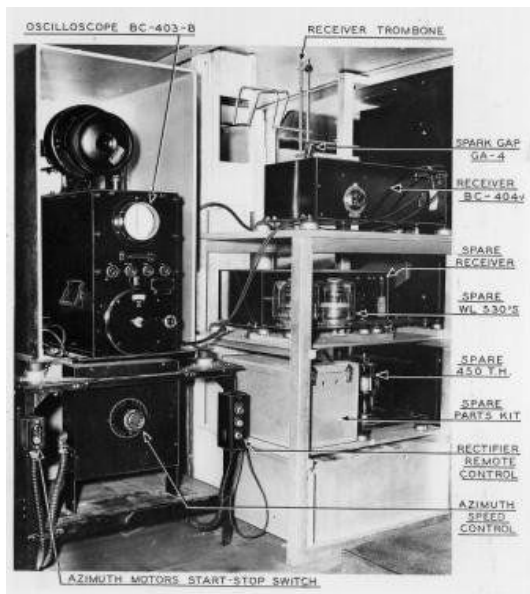
ALTERED:



This Trajectory
Should Not Be
Surprising to
Anyone

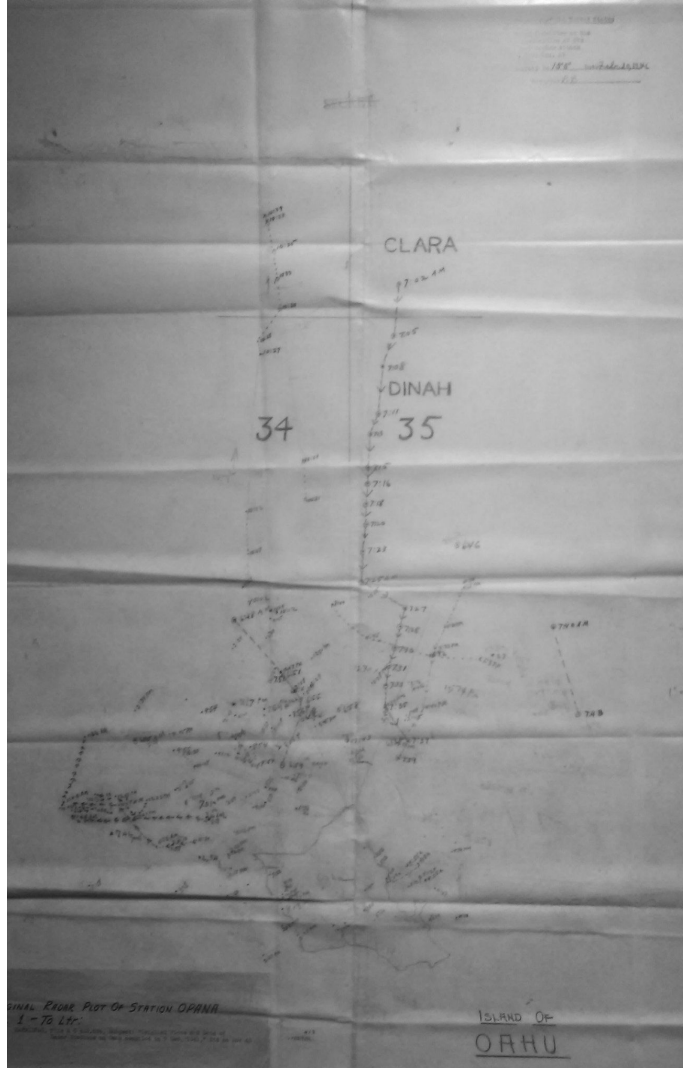
7 Dec 1941

"...up until that time the military thought radar was just another toy..." -Pvt Lockard, Signal Company, HI



16. Parts of an early SCR-270 installed in a K-30 truck.

Source: H. W. Andrews from Zahl papers



Source: <https://twitter.com/daviottenheimer/status/803122106556784640>

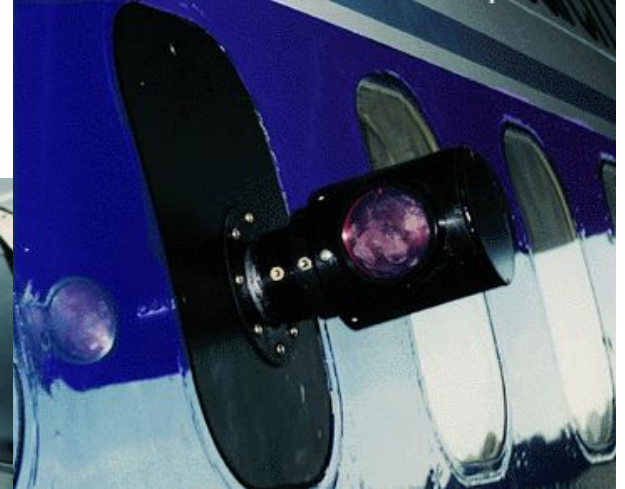
mongoDB.

1986: NASA Analysis To Solve Windshear Deaths*



Microwave

LIDAR



Infrared

*500 fatalities 1964 - 1985

Source: <https://www.nasa.gov/centers/langley/news/factsheets/Windshear.html>

mongoDB.

2017: Onboard Sensors Generate +800TB / Flight

Got Data...

...Integrity?



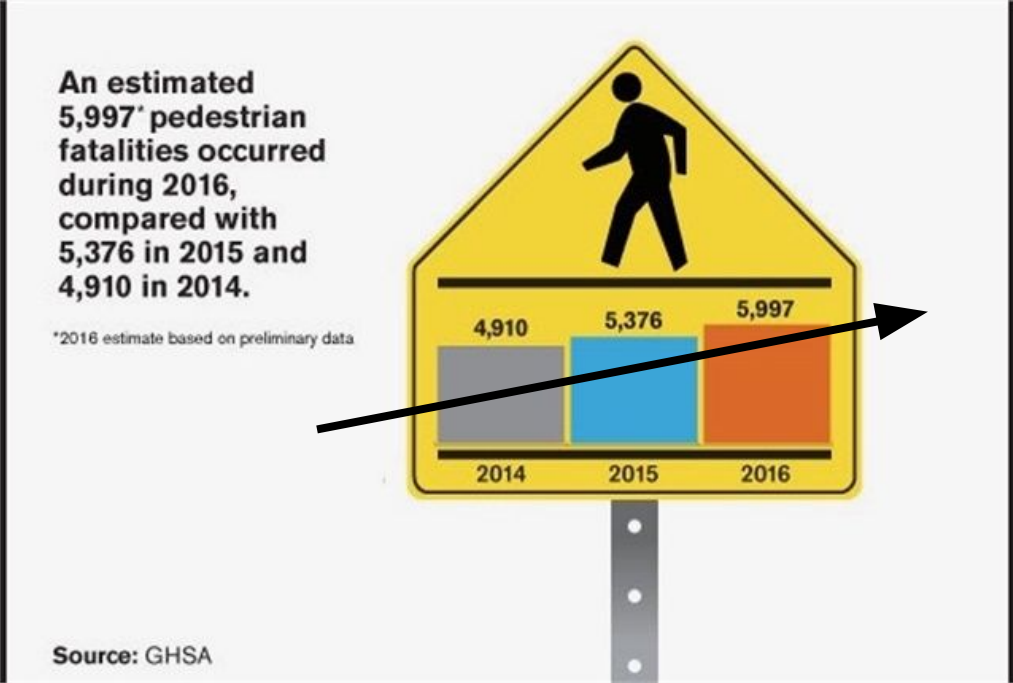
Sources: <https://twitter.com/TheAviationist/status/887311009399975936>
<https://twitter.com/daviottenheimer/status/833495843760005120>

mongoDB



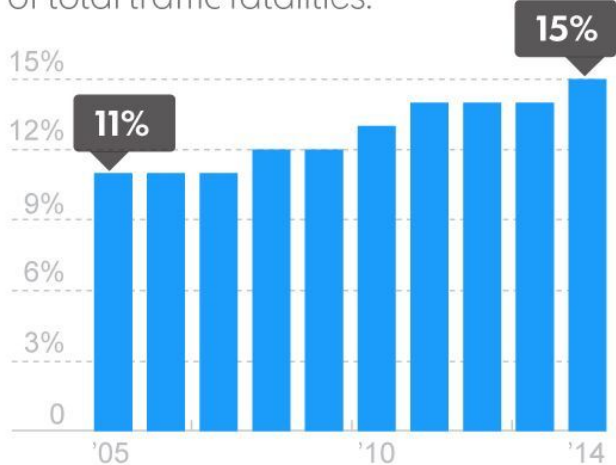
What Deaths Could We Be Solving For Today?

Driverless Economics Hint at Increased Deaths



PEDESTRIAN DEATHS

Pedestrian deaths as a percentage of total traffic fatalities:



SOURCE: National Highway Traffic Safety Administration
Jim Sargent, USA TODAY



Reinforcement Learning Defeat

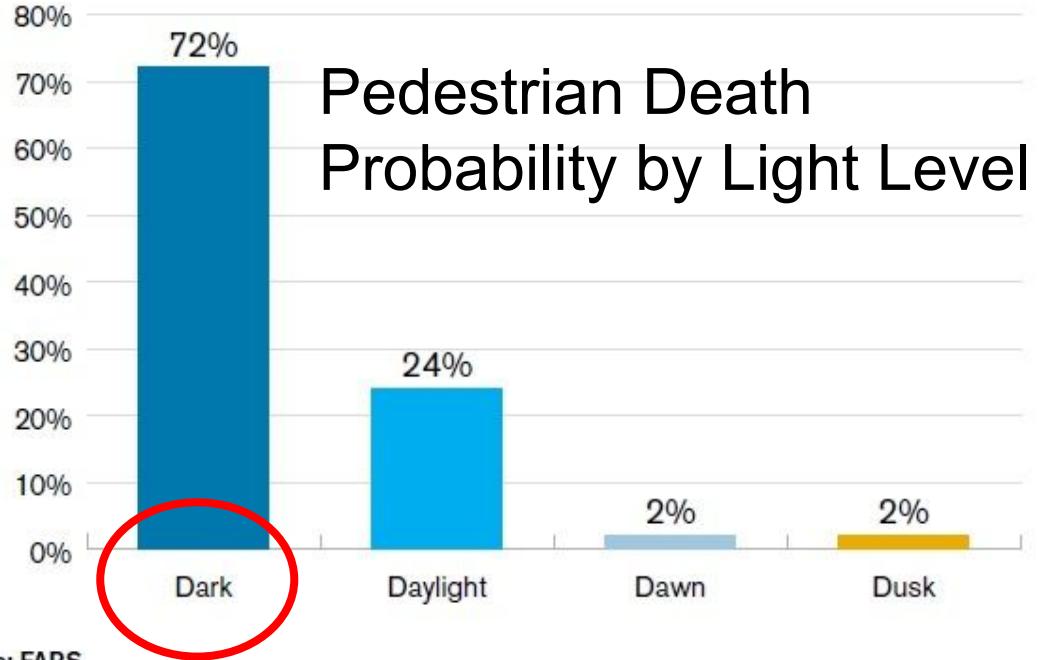
What Do You See?



Lepse Avenue, Kiev, Ukraine: <https://www.jwt.com/en/ukraine/work/pedestrianghost/>



You Expect “Intelligent” Machines To Save Lives?



Source: FARS

Removing Brakes on Innovation: Killed 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/uber-halts-autonomous-vehicle-testing-after-a-pedestrian-is-struck/>

Driverless Vision Classification Test

UK False Road Segmentation...

United Kingdom Get Random Image

Google © 2015 Google

Sky Building Pole Road Marking Road Pavement Tree Sign Symbol Fence Vehicle Pedestrian Bike

Flyingpenguin KIWICON X

Classification Failure

...Machine in Former Colony
(Independent Within Commonwealth Since 30 September 1966)

Botswana

Get Random Image

'labels more than 90% of pixels correctly'
- UK Creators

Google

© 2015 Google

Sky Building Pole Road Road Marking Road Pavement Tree Sign Fence Vehicle Pedestrian Bike

Flyingpenguin

KIWICON X

<http://mi.eng.cam.ac.uk/projects/segnet/>

NHTSA Report on Tesla Death

Tesla's design included a hands-on the steering wheel system for monitoring driver engagement. That system has been updated to further reinforce the need for driver engagement through a "strike out" strategy. Drivers that do not respond to visual cues in the driver monitoring system alerts may "strike out" and lose Autopilot function for the remainder of the drive cycle.

7.0 CONCLUSION

Advanced Driver Assistance Systems, such as Tesla's Autopilot, require the continual and full attention of the driver to monitor the traffic environment and be prepared to take action to avoid crashes.

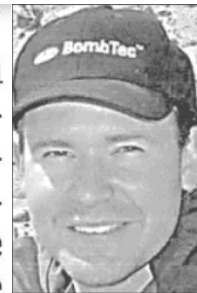
²³ While drivers have a responsibility to read the owner's manual and comply with all manufacturer instructions and warnings, the reality is that drivers do not always do so. Manufacturers therefore have a responsibility to design with the inattentive driver in mind. See Enforcement Guidance Bulletin 2016-02: Safety-Related Defects and Automated Safety Technologies, 81 Fed. Reg. 65705.

Source: <https://static.nhtsa.gov/odi/inv/2016/INCLA-PE16007-7876.PDF>

Data Integrity Failures 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-

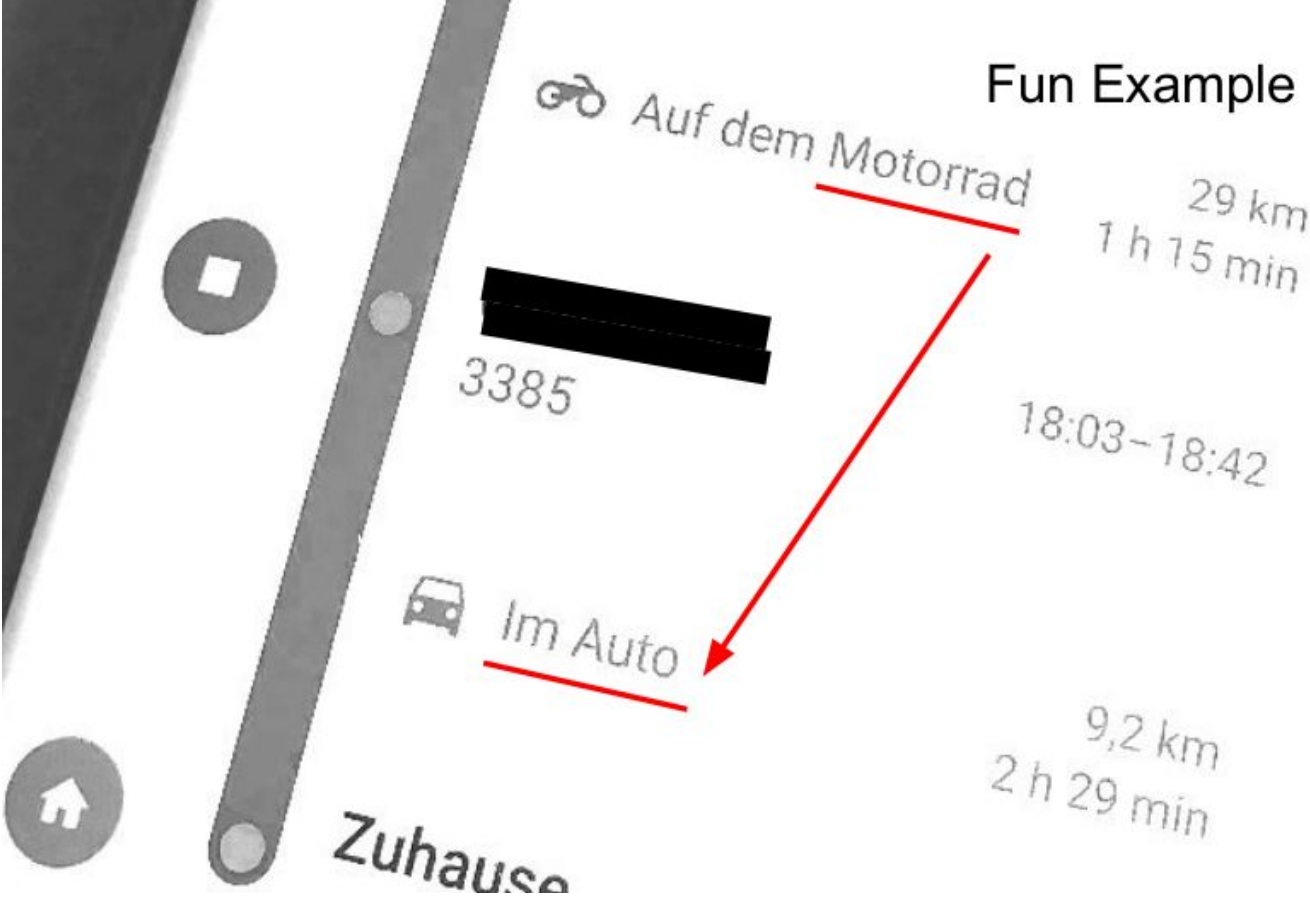


Source: <https://static.nhtsa.gov/odi/inv/2016/INCLA-PE16007-7876.PDF>,
<https://www.documentcloud.org/documents/2938399-joshua-brown-obit.html>

And What About Safety of Something Like a Central “God View...For Viewing Pleasure”?



Easily Broken Also



A close-up portrait of John McLaughlin, an older man with glasses, wearing a blue shirt and a dark suit jacket. He is looking directly at the camera with a neutral expression.

Who Controls “Truth”?

“Factions in this
Administration are using
intelligence as weapons
against each other”

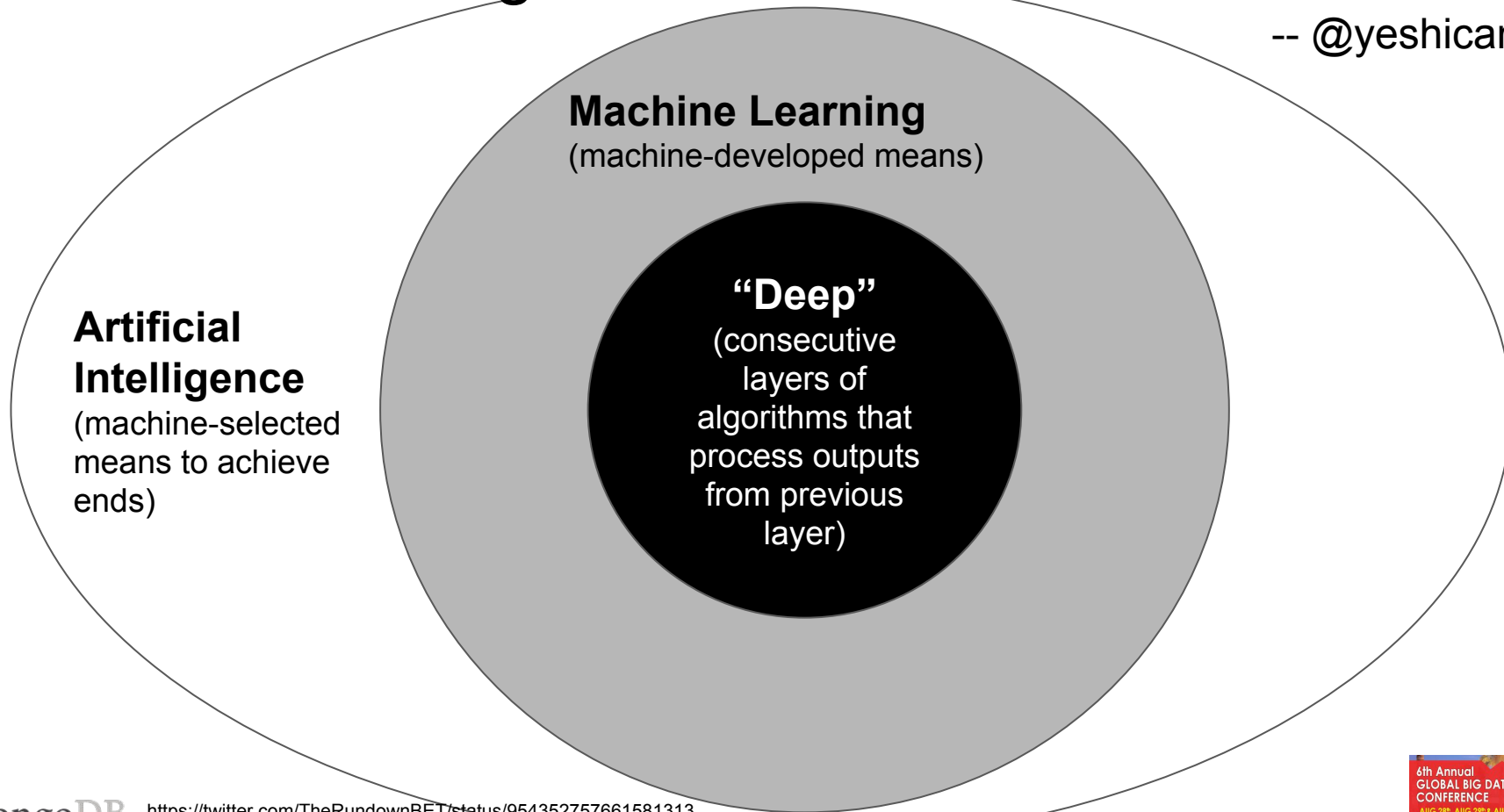
JOHN MCLAUGHLIN

ACTING DIRECTOR 2004

CIA

“AI is the Civil Rights Battle of Our Time”

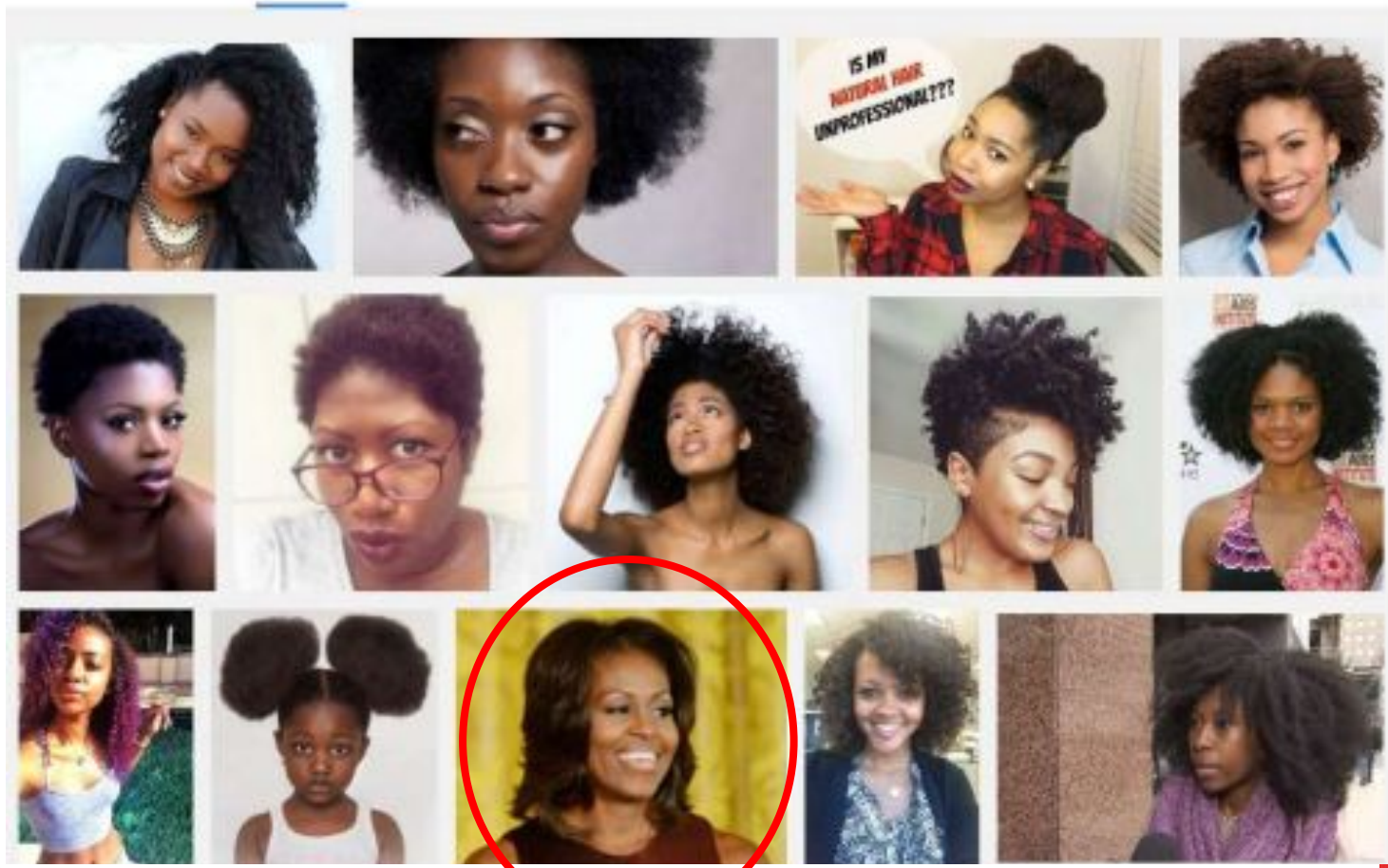
-- @yeshican



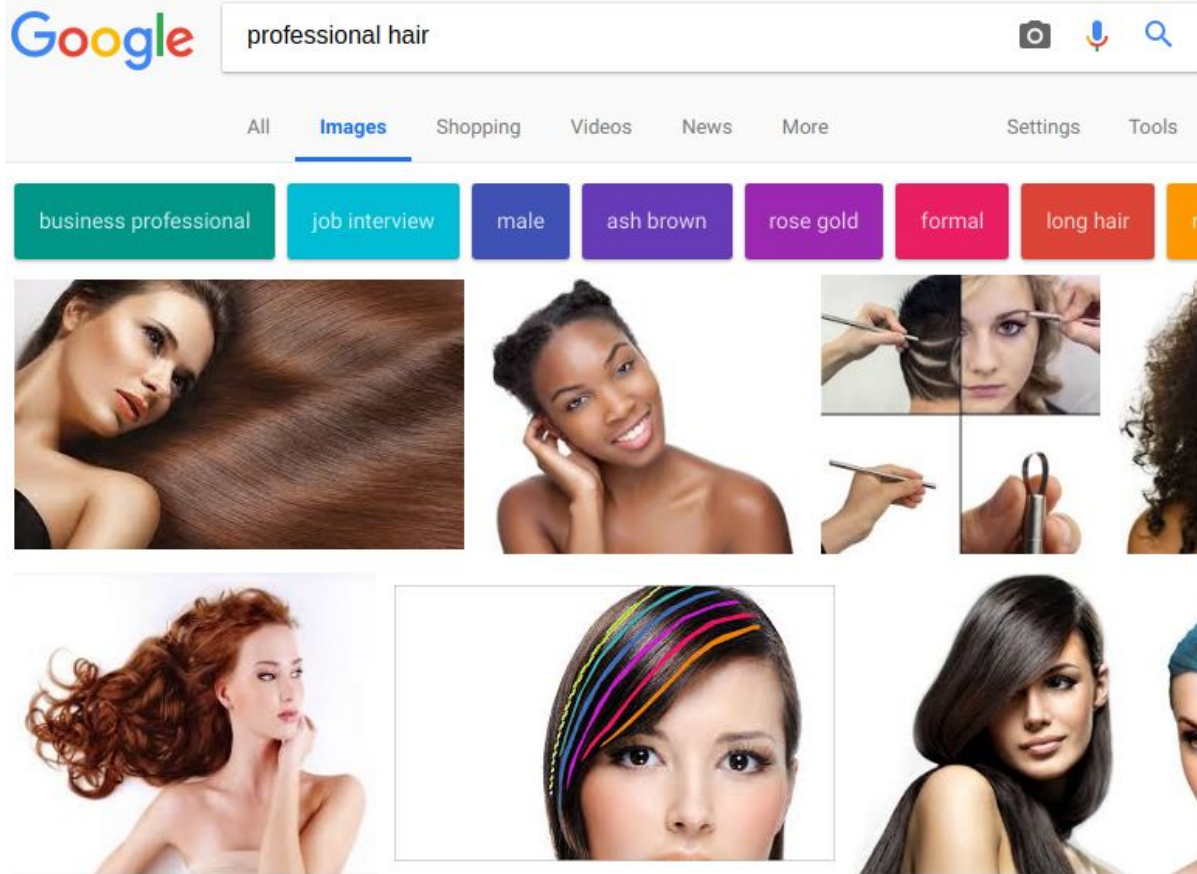
False 'Criminal' Labeling

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





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/>

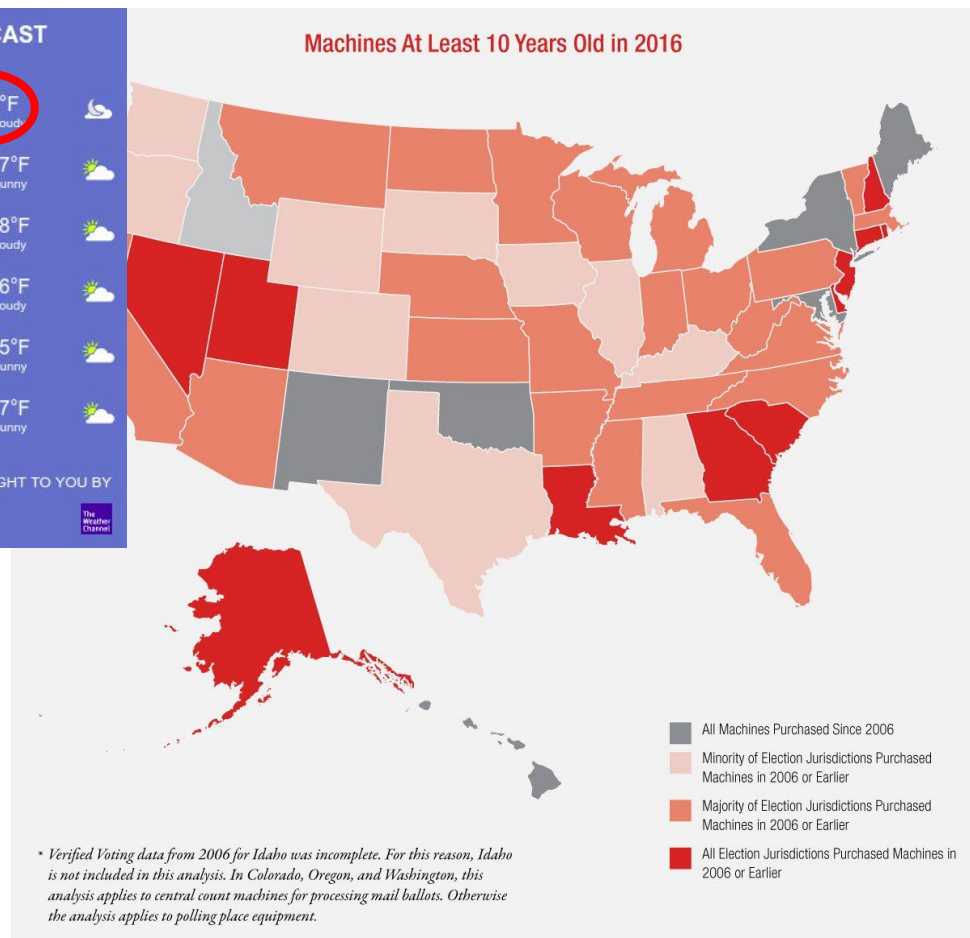
Looking Ahead at Subversion Risks

- Environmentalism
- Education
- Criminal justice
- Healthcare
- Election tallies
- Border disputes

5-DAY FORECAST
San Francisco

Today Jul 22	0°/56°F Partly Cloudy	
Sun Jul 23	74°/57°F Mostly Sunny	
Mon Jul 24	73°/58°F Partly Cloudy	
Tue Jul 25	74°/56°F Partly Cloudy	
Wed Jul 26	74°/55°F Mostly Sunny	
Thu Jul 27	75°/57°F Mostly Sunny	

°F °C BROUGHT TO YOU BY



<https://twitter.com/AriBerman/status/885174707330437124>

mongoDB.

Hidden Hot Battle Lessons of Cold War

All Learning Models Have
Flaws, Some Have
Casualties

Davi Ottenheimer

