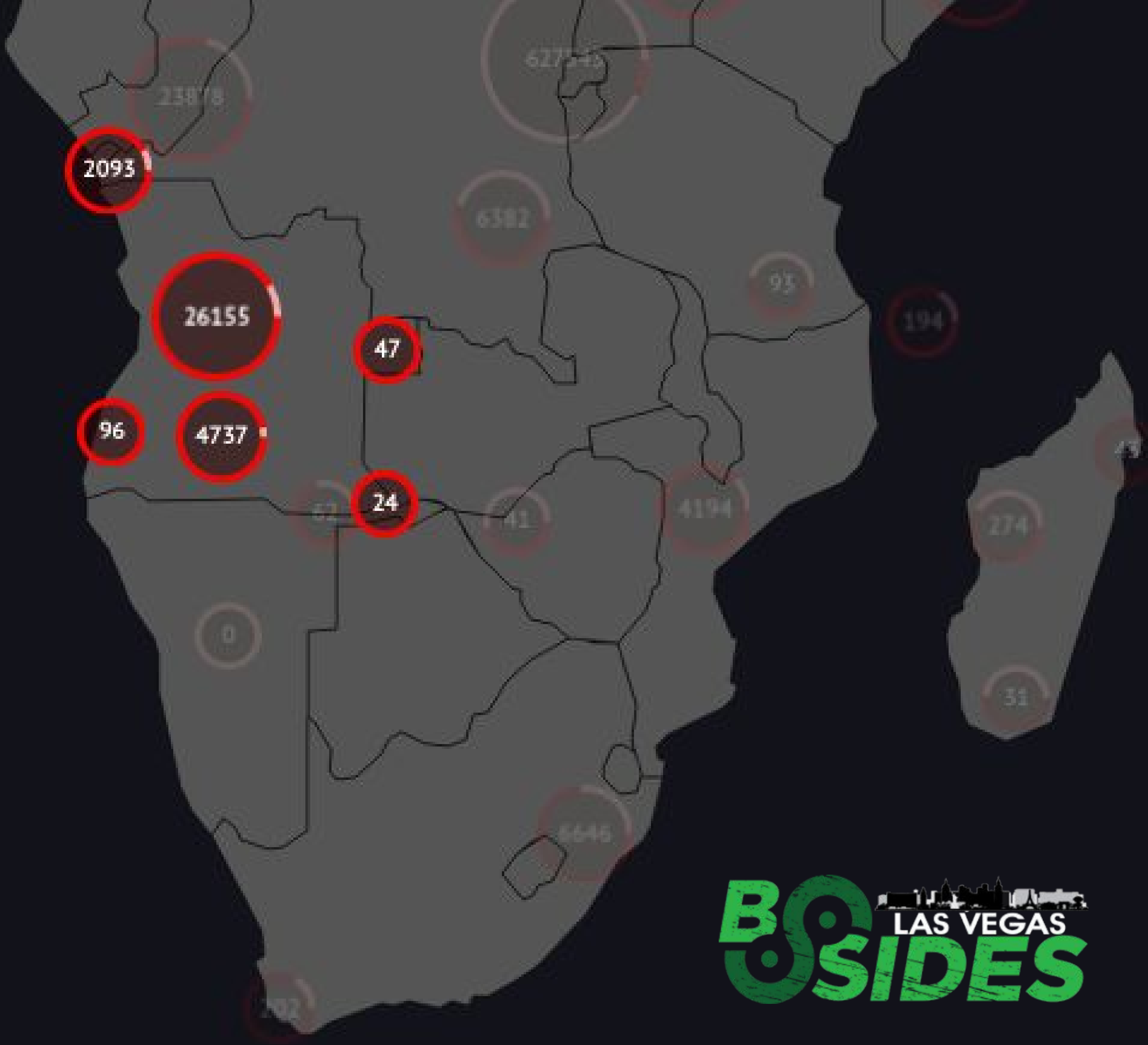
Hidden Hot Battle Lessons of Cold War

All Learning Models Have Flaws, Some Have Casualties

Davi Ottenheimer



Source: http://ucdp.uu.se/#country/540

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*.”

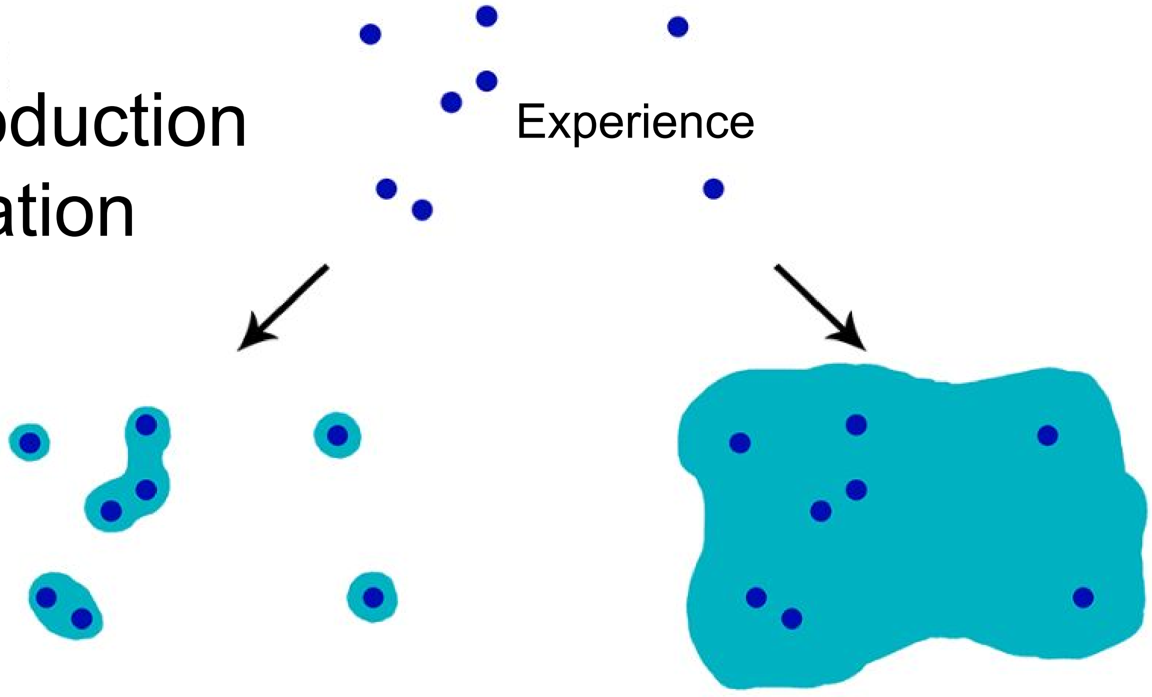
-- Dan Geer

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

mongoDB.

BSIDES LAS VEGAS

General Introduction to Generalization



Experience

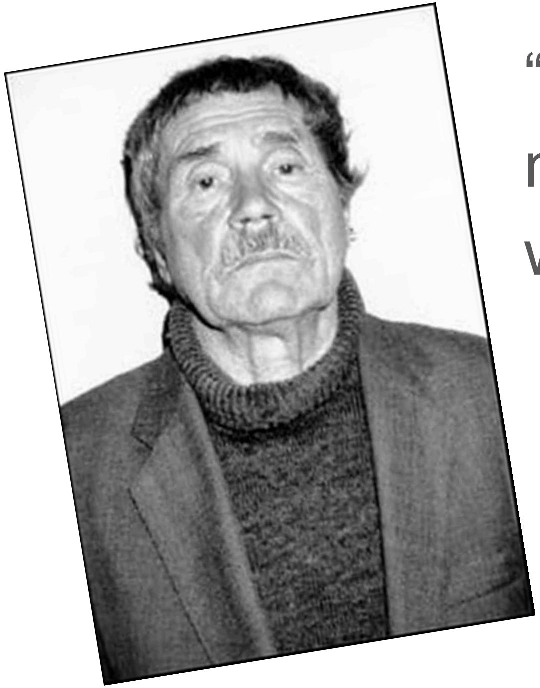
Local generalization:
Generalization power of
pattern recognition

Extreme generalization:
Generalization power
achieved via
abstraction and reasoning

(Synthesis and Analysis)

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

Warning: History 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

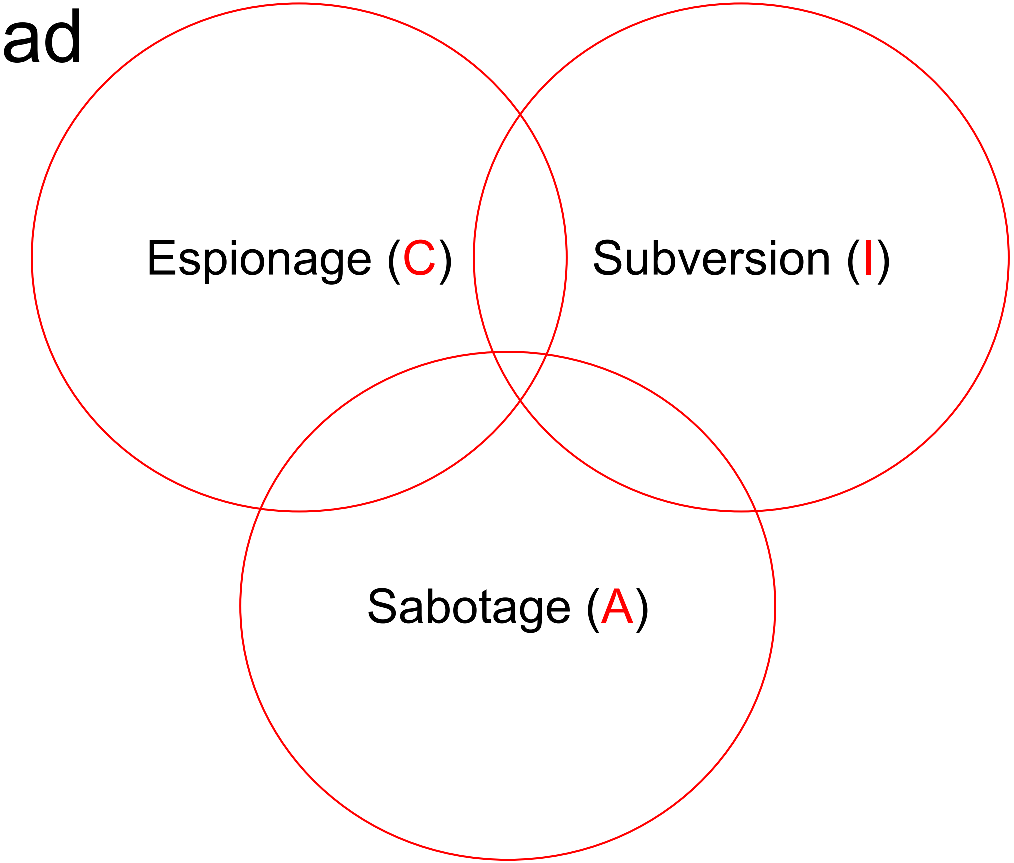
Warning: Philosophy Talk Ahead

> “Those who cannot remember the past are condemned to repeat it.”
>
> -- George Santayana, 1906

Source: “The Life of Reason”
https://books.google.com/books?id=5Bh3KDojKeUC&pg=PA82#v=onepage&q&f=false

General State of Cyber Flaws

Cyber Flaw Triad



Espionage (C)

Subversion (I)

Sabotage (A)

Confidentiality: 2007

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

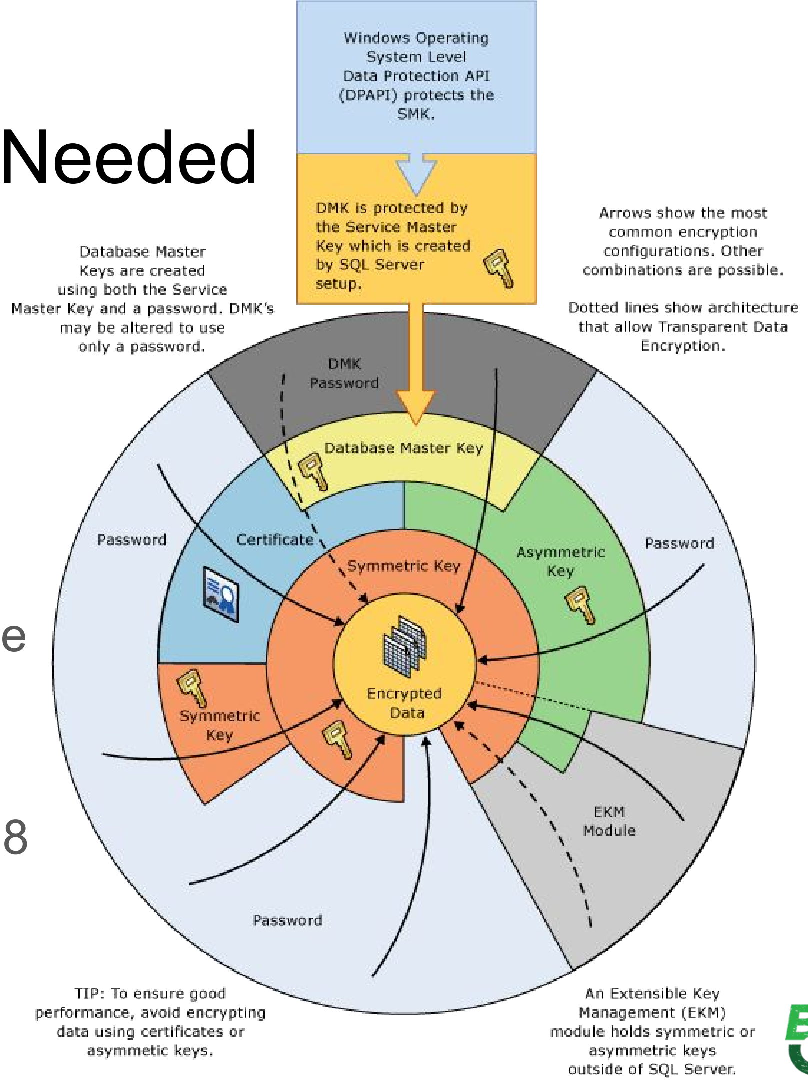
> “...interoperable protocol for standard communication between key management servers, and clients and other actors...”

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

More Generalists Were Needed

"...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



Windows Operating System Level Data Protection API (DPAPI) protects the SMK.

DMK is protected by the Service Master Key which is created by SQL Server setup.

Database Master Keys are created using both the Service Master Key and a password. DMK's may be altered to use only a password.

Arrows show the most common encryption configurations. Other combinations are possible.

Dotted lines show architecture that allow Transparent Data Encryption.

TIP: To ensure good performance, avoid encrypting data using certificates or asymmetric keys.

An Extensible Key Management (EKM) module holds symmetric or asymmetric keys outside of SQL Server.

Source: 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	7asdg9DAg73kj0	$200	
bob	x4Adfxj3la93das	5555-5555-5555	$100	$100

🟩 Encrypted ⬛ Unencrypted

https://www.rsaconference.com/videos/how-to-delete-data-for-realz-this-presentation-will-self-destruct-in

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/

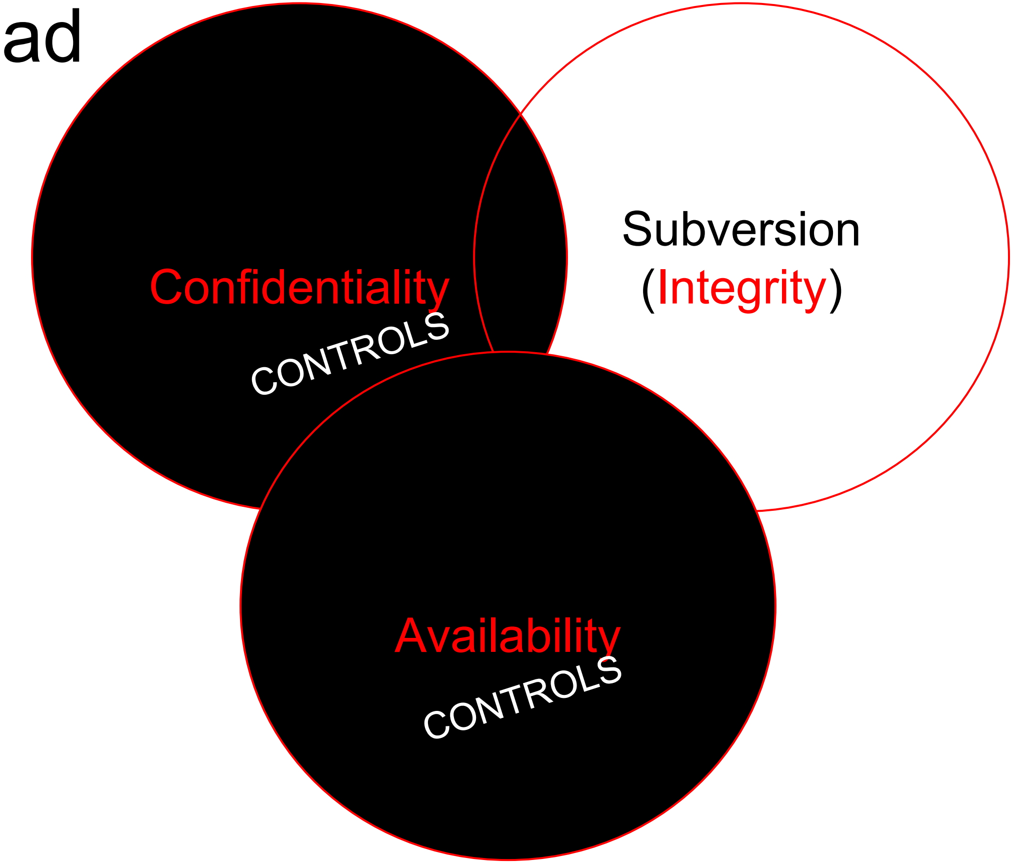
Availability: 2017

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

- Herd Specialists Required
  - 93% - 97% Provision Success on Reliable Installs (Ubuntu - Cattle)
  - 89% on Complex Installs (Windows 2012 R3 - Sheep)
- **100% achieved** January 2017: 100s Monthly Herd Loss Prevented

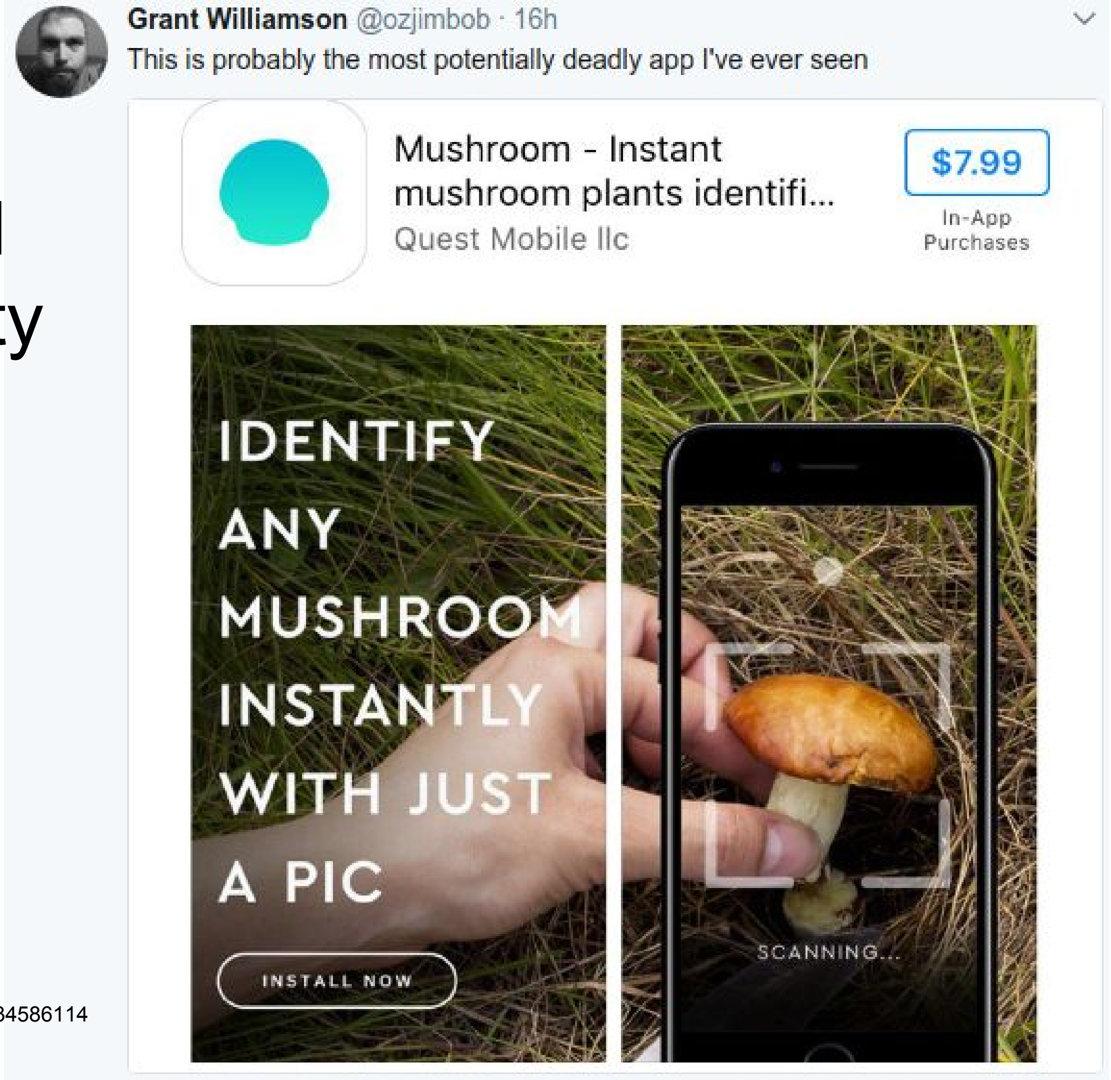
Source: https://www.packet.net/blog/our-journey-to-zero-failed-installs/

Cyber Flaw Triad



The Unregulated Data Integrity SNAFU

Situation
Normal
All
F---ed
Up

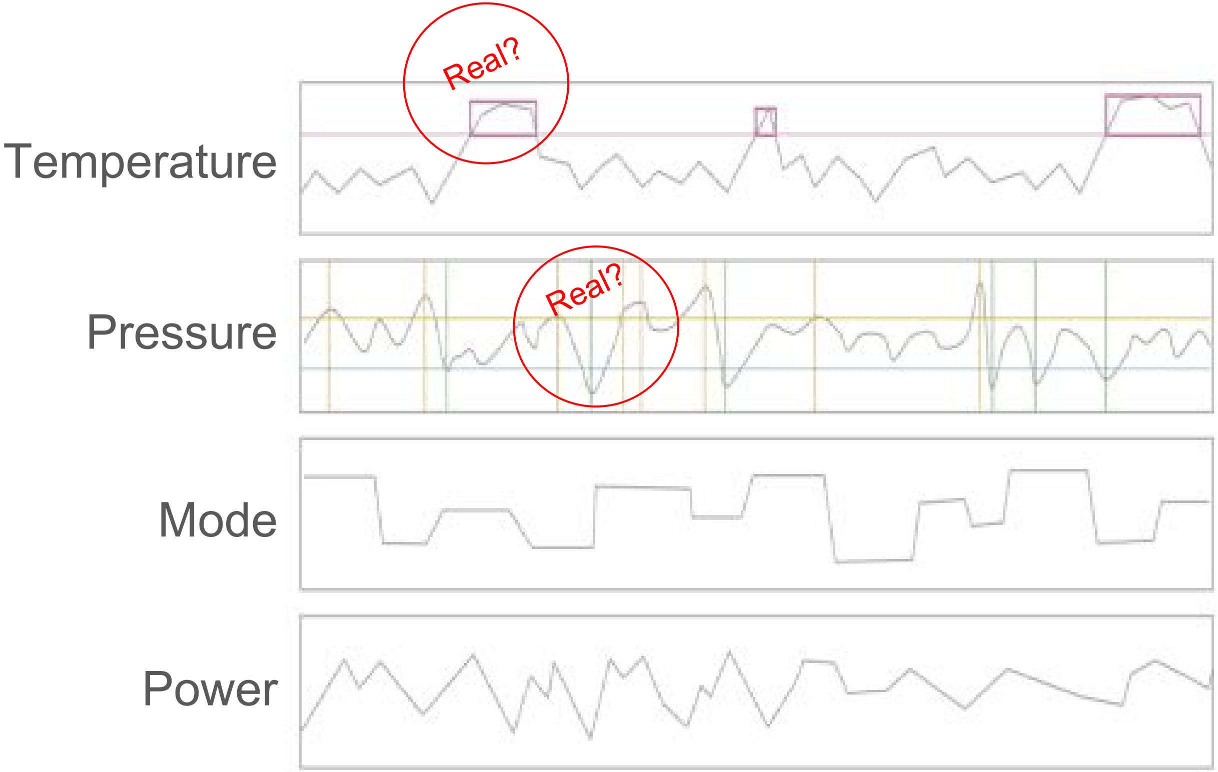


Grant Williamson @ozjimbob · 16h
This is probably the most potentially deadly app I've ever seen

Mushroom - Instant mushroom plants identifi...
Quest Mobile llc
$7.99
In-App Purchases

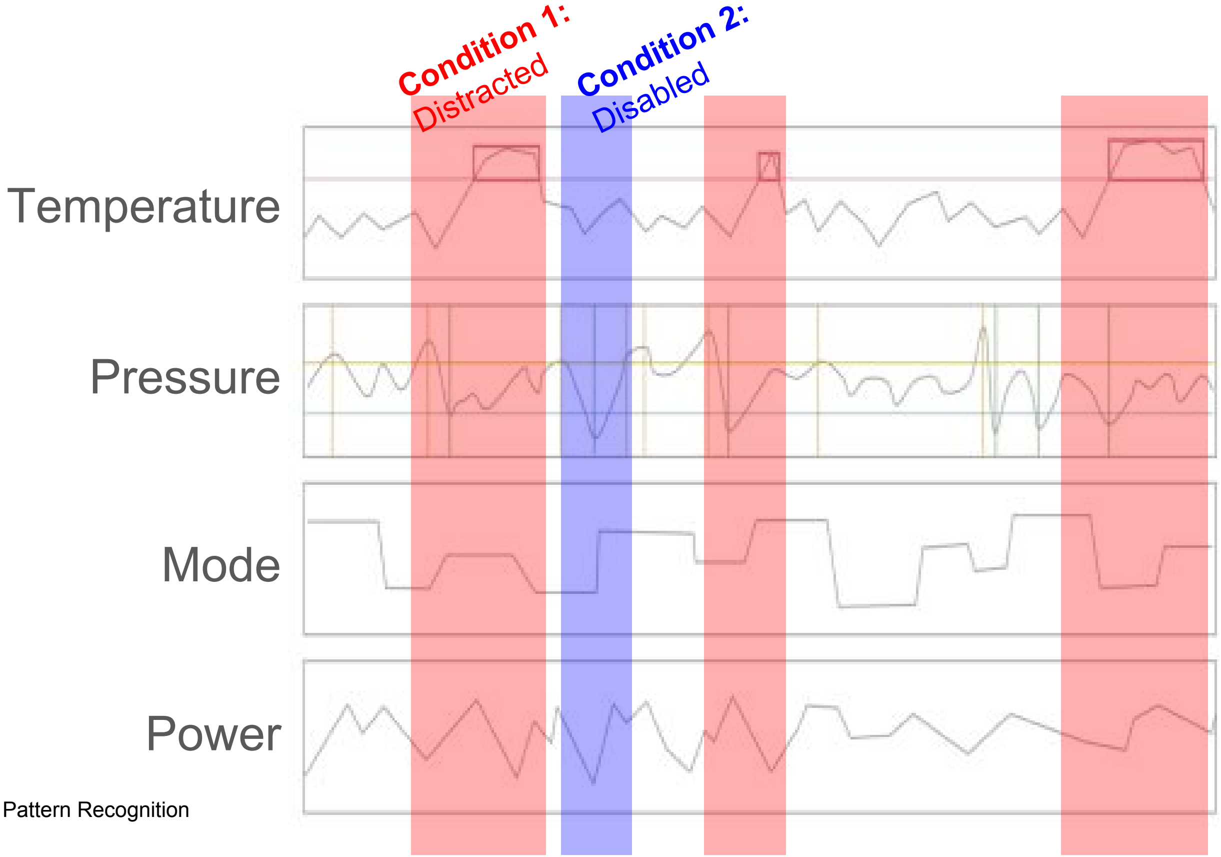
Source: https://twitter.com/ozjimbob/status/889411603434586114

Deadly Risks From Abstraction and Reasoning Flaws



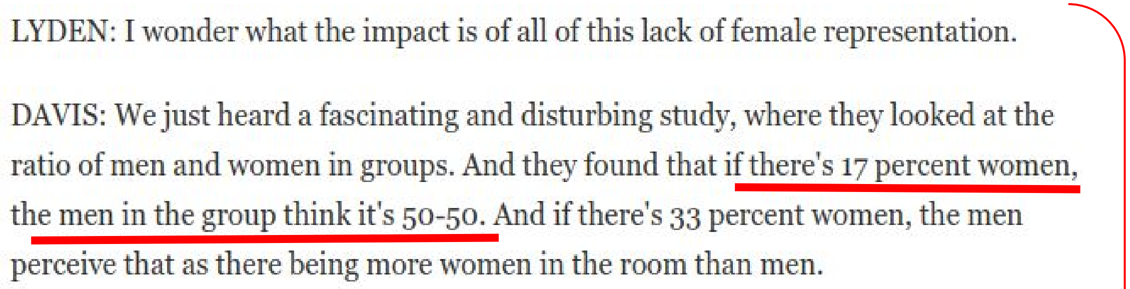
Source: Splunk Time Series Pattern Recognition

Subversion (Integrity)



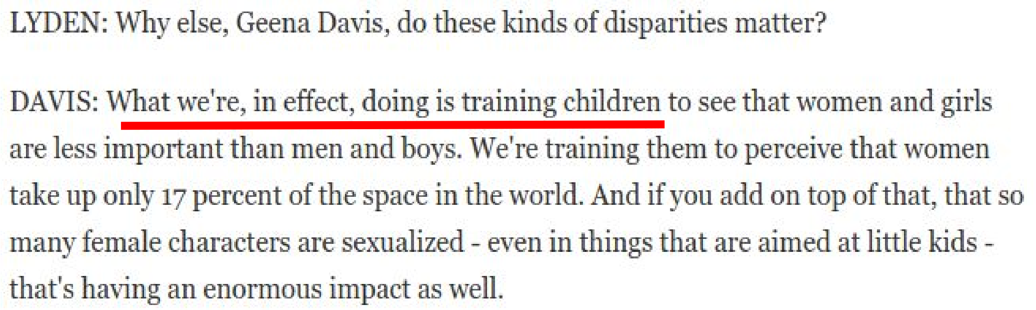
Source: Splunk Time Series Pattern Recognition

In Effect, We’re *Training Learning Systems to Harm*



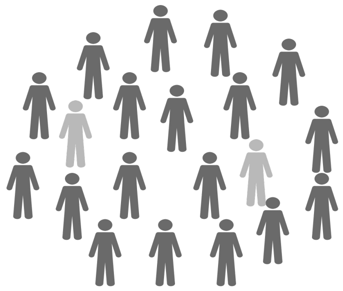
LYDEN: I wonder what the impact is of all of this lack of female representation.

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?

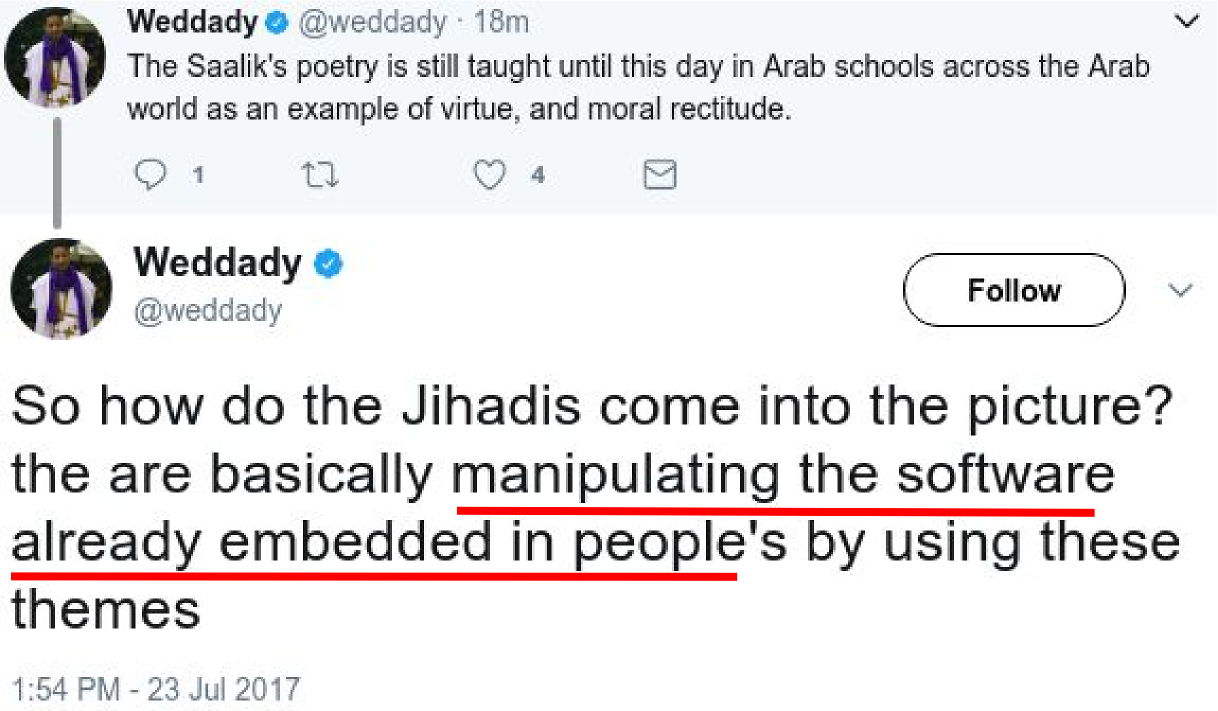
DAVIS: What we're, in effect, doing is training children to see that women and girls are less important than men and boys. We're training them to perceive that women take up only 17 percent of the space in the world. And if you add on top of that, that so many female characters are sexualized - even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

Manipulating Software Embedded in People



Weddady @weddady · 18m

The Saalik's poetry is still taught until this day in Arab schools across the Arab world as an example of virtue, and moral rectitude.

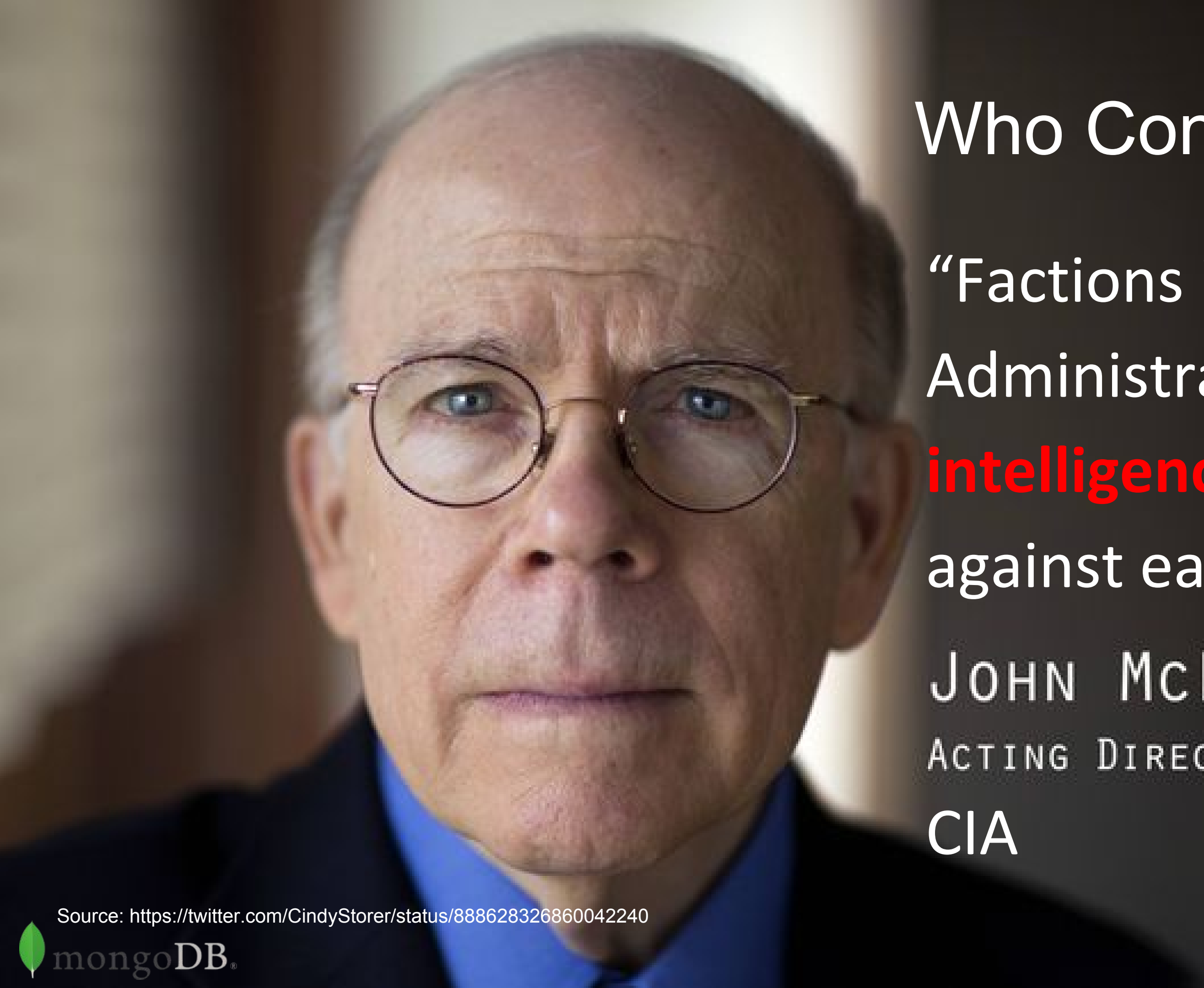
Weddady
@weddady

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

Who Controls “Truth”?



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

John McLaughlin

Acting Director 2004

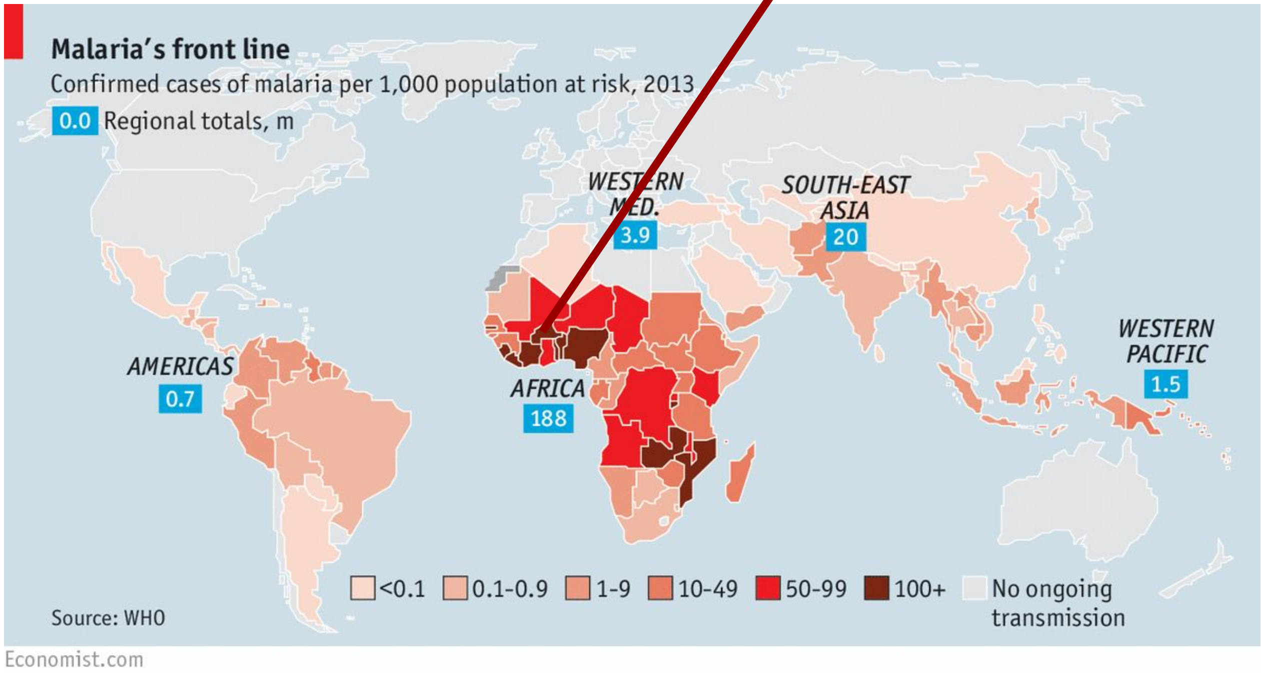
CIA

Source: https://twitter.com/CindyStorer/status/888628326860042240

Abstraction and Reasoning Flaws...

1. Supply-Chain ***Data Integrity*** Broken
2. “Up to 35% of antimalarial drugs are useless”

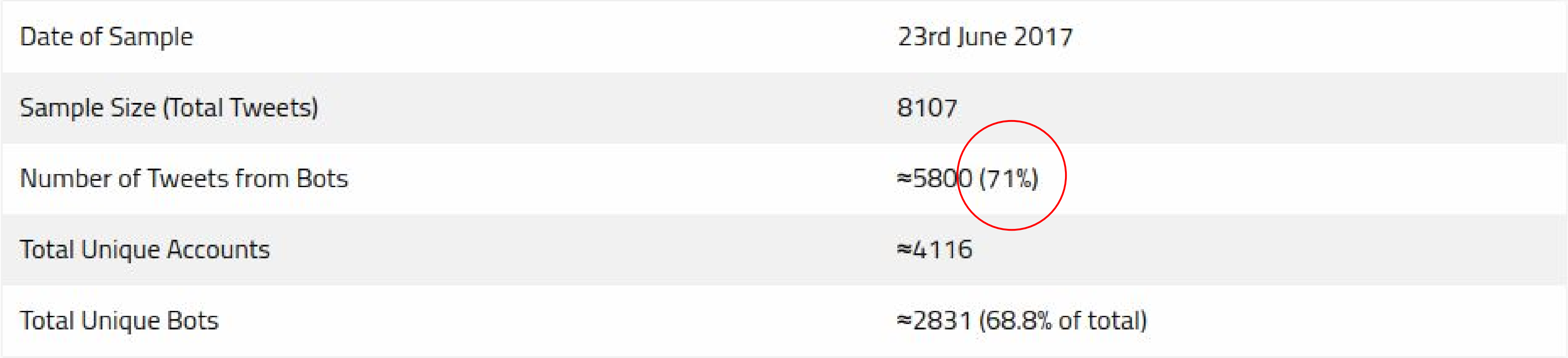
Sierra Leone
Libera
Ivory Coast



Sources: http://spectrum.ieee.org/biomedical/devices/fake-malaria-meds-meet-their-match-in-a-handheld-spectrometer, http://www.fightingmalaria.gov/news/pressreleases/theft_illegal_diversion_malaria_medicines.html

Automated 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)

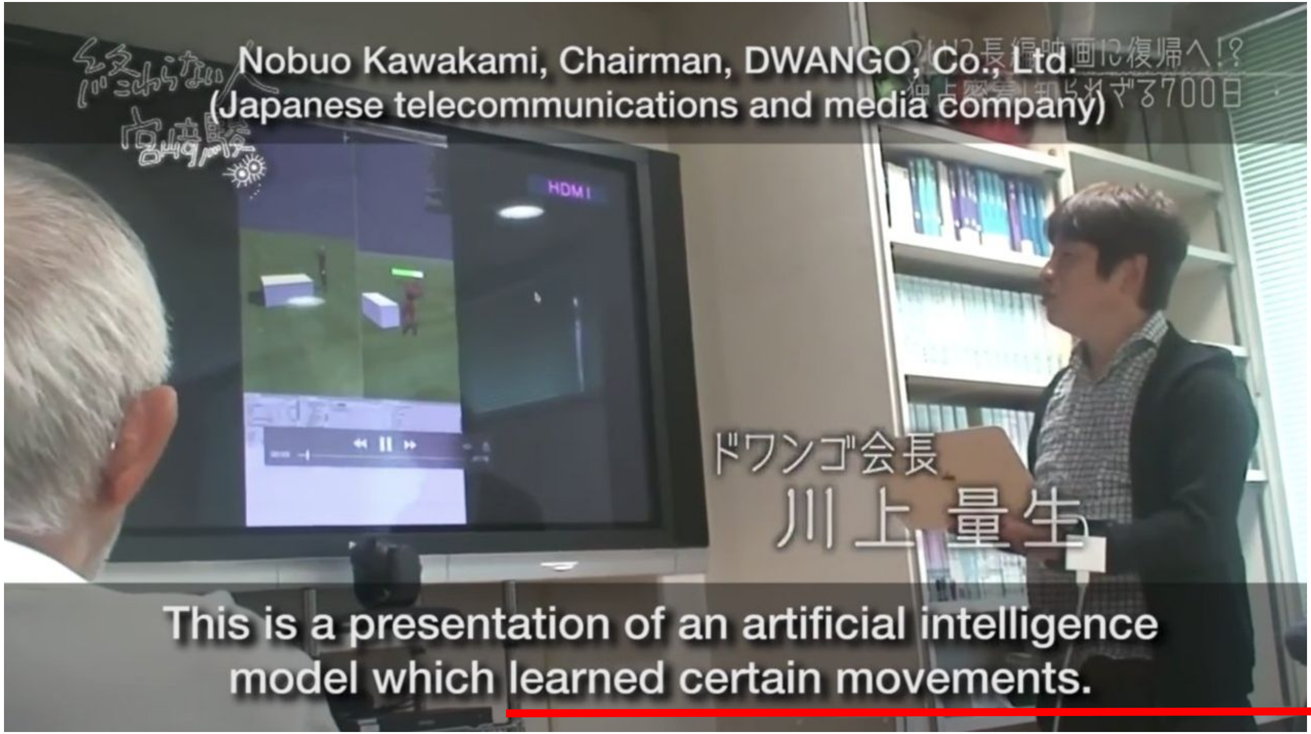
2338 Bot Accounts Created 2016:

- May 818
- April 610

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

Harm From Insecure Learning Models (Data Integrity Attacks)

Miyazaki Presented With Flawed “Movement Learning Model”

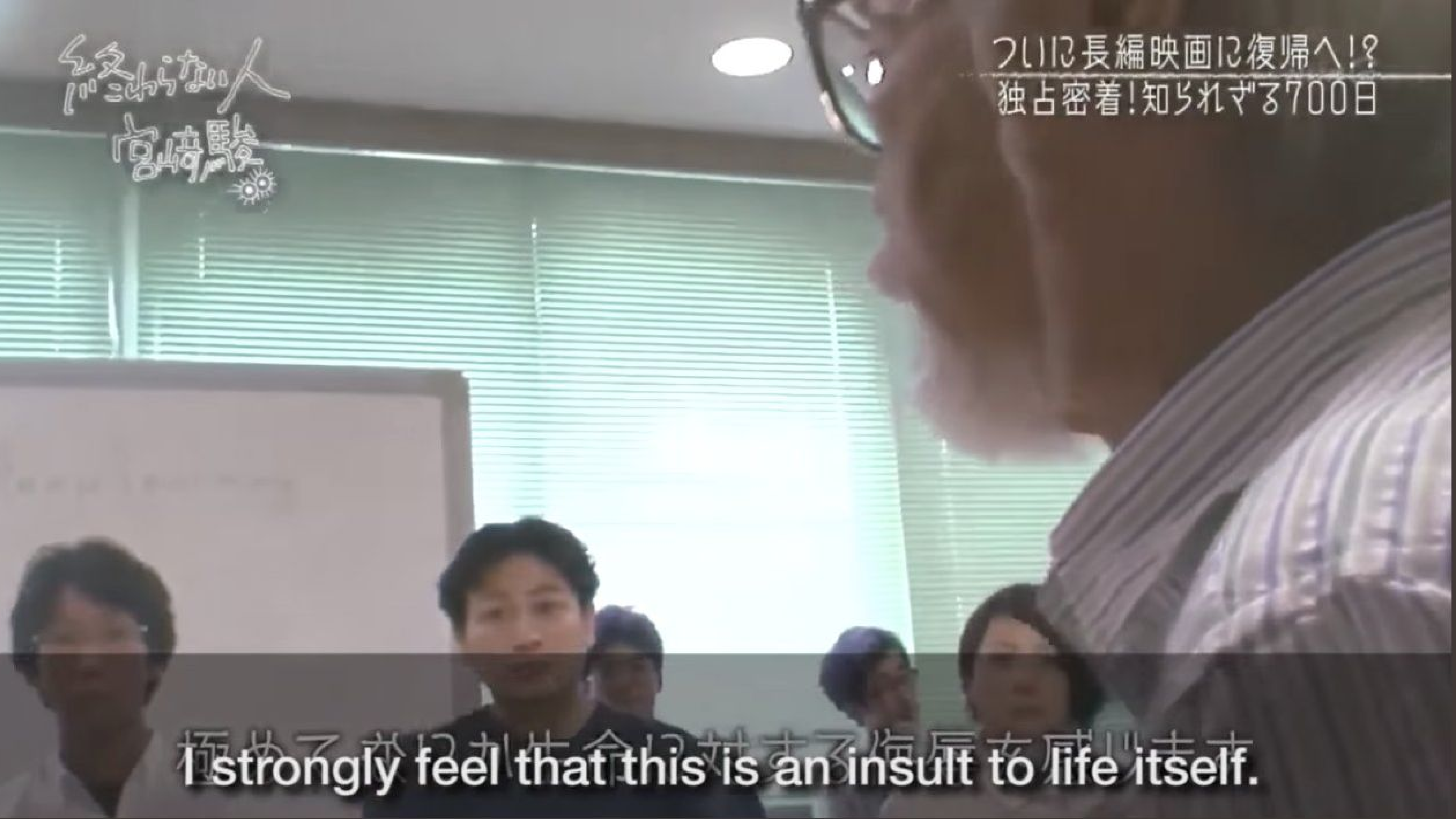


Nobuo Kawakami, Chairman, DWANGO, Co., Ltd.
(Japanese telecommunications and media company)

This is a presentation of an artificial intelligence model which learned certain movements.

Trained on Harm

Source: https://www.youtube.com/watch?v=ngZ0K3lWKRc

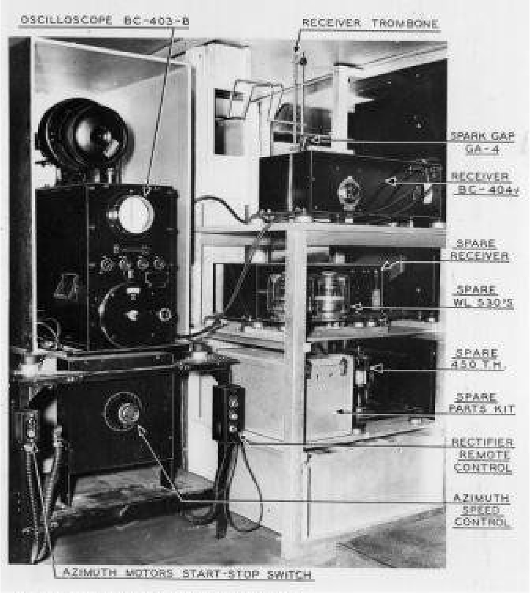

終わらない人
宮﨑駿
ついに長編映画に復帰へ!?
独占密着!知られざる700日
極めてなにか生命に対する侮辱を感じます
I strongly feel that this is an insult to life itself.

But Seriously...

An Insult
To ***Life*** Itself?

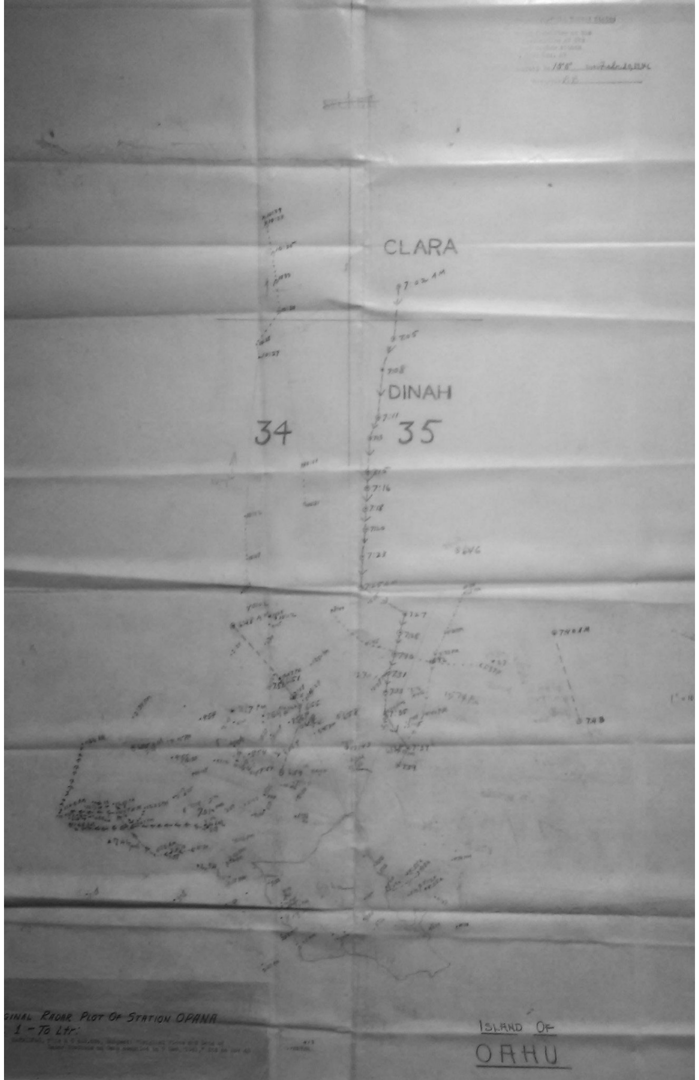
7 Dec 1941

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



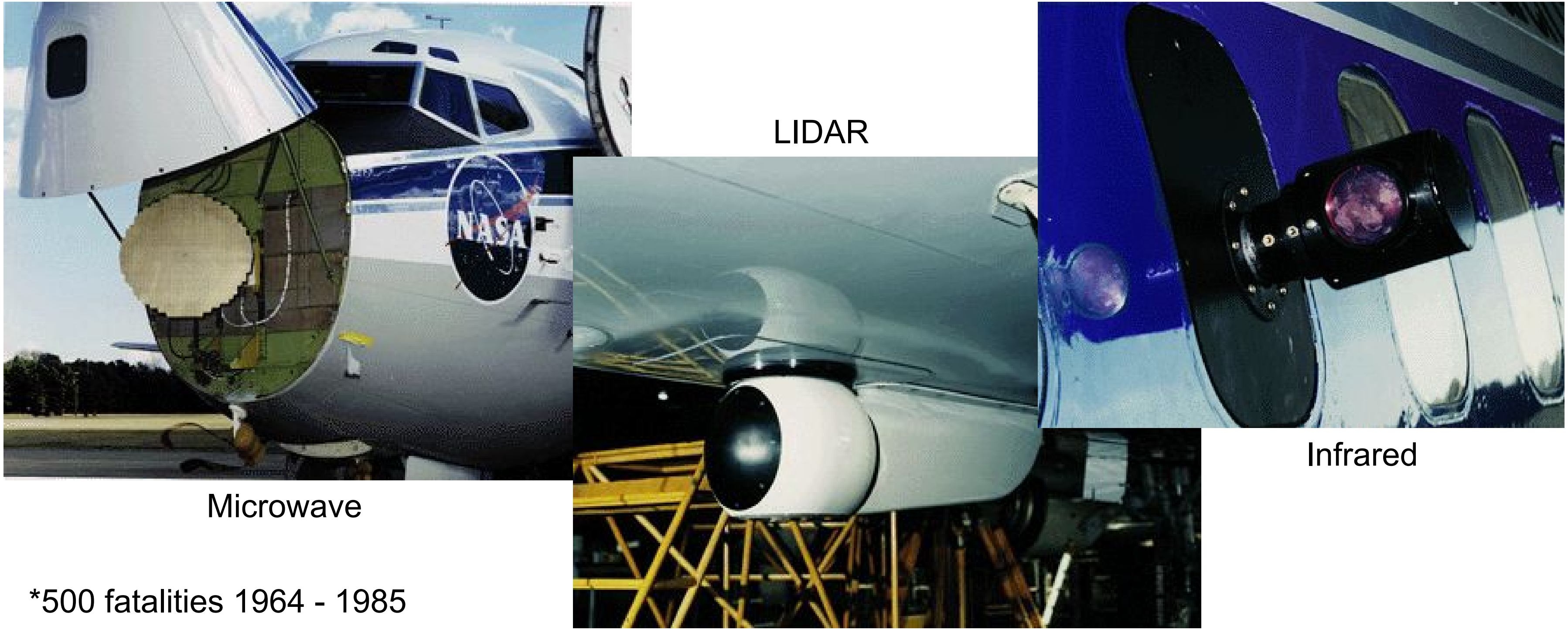
16. Parts of an early SCR-270 installed in a K-30 truck.

Source: H. W. Andrews from Zahl papers



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

1986: NASA Analysis To Solve Windshear Deaths*



LIDAR

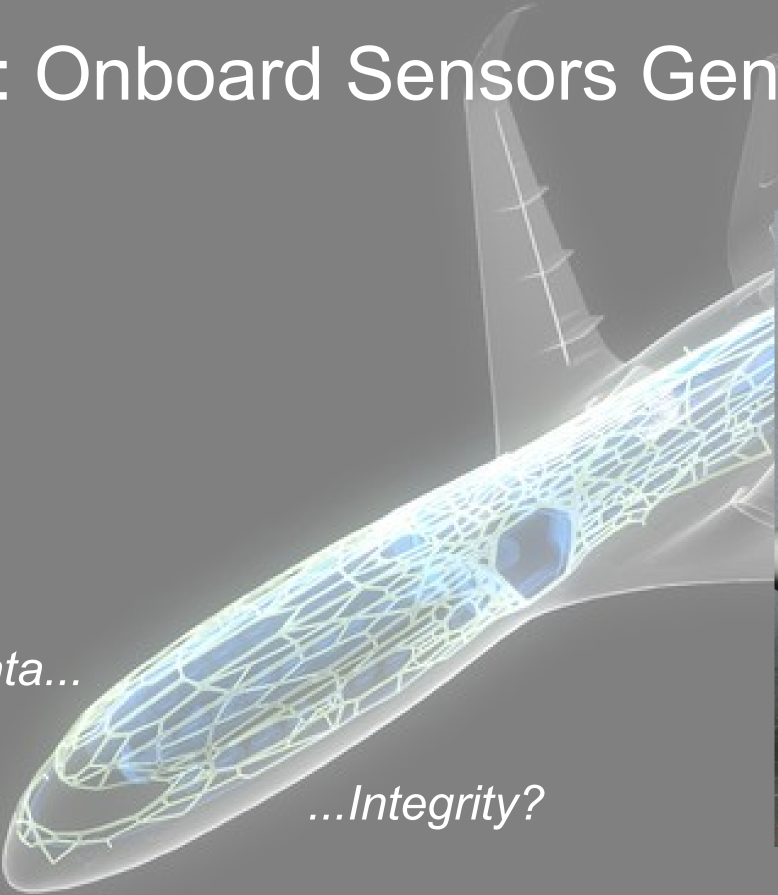
Microwave

Infrared

*500 fatalities 1964 - 1985

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

2017: Onboard Sensors Generate +800TB / Flight

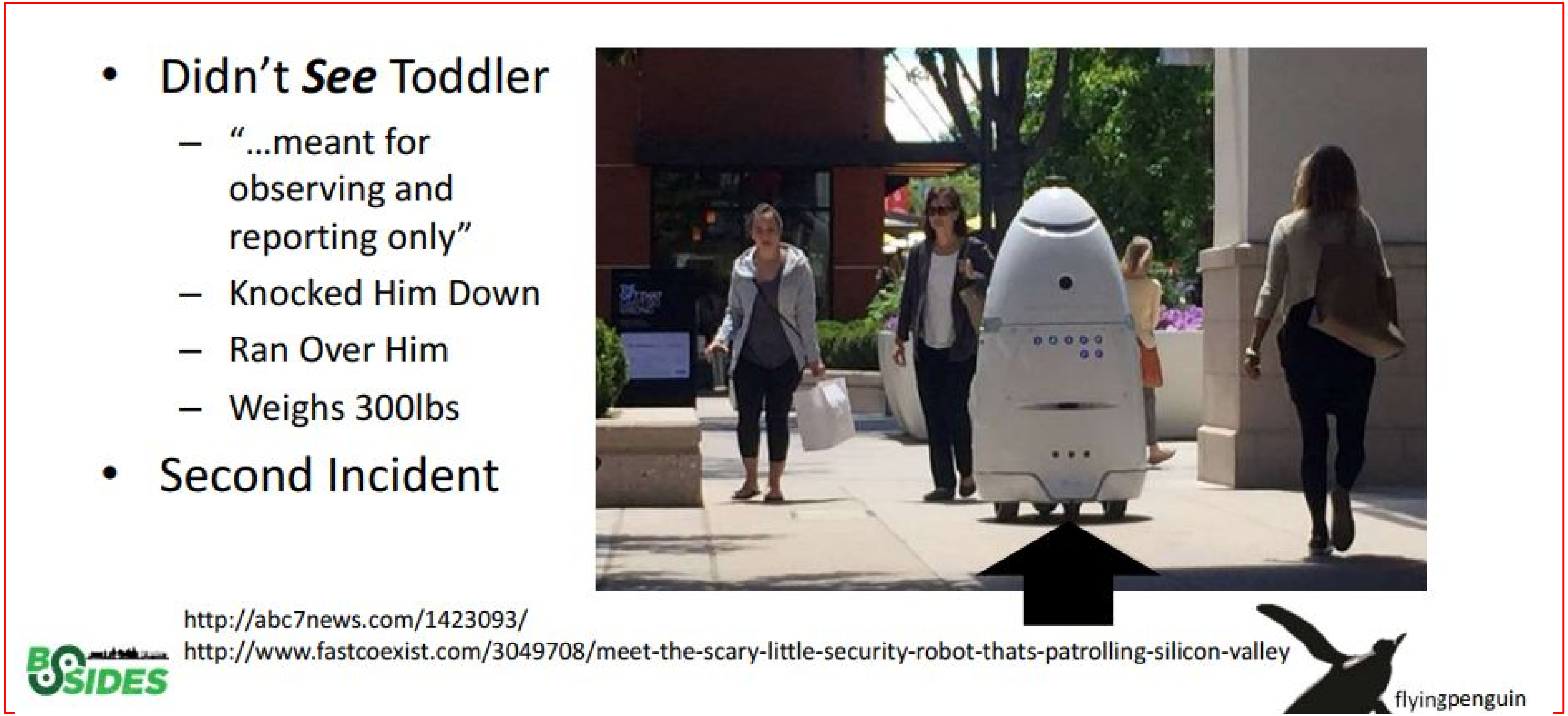


Got Data...

...Integrity?

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

2016: Knightscope Observational Data Failures



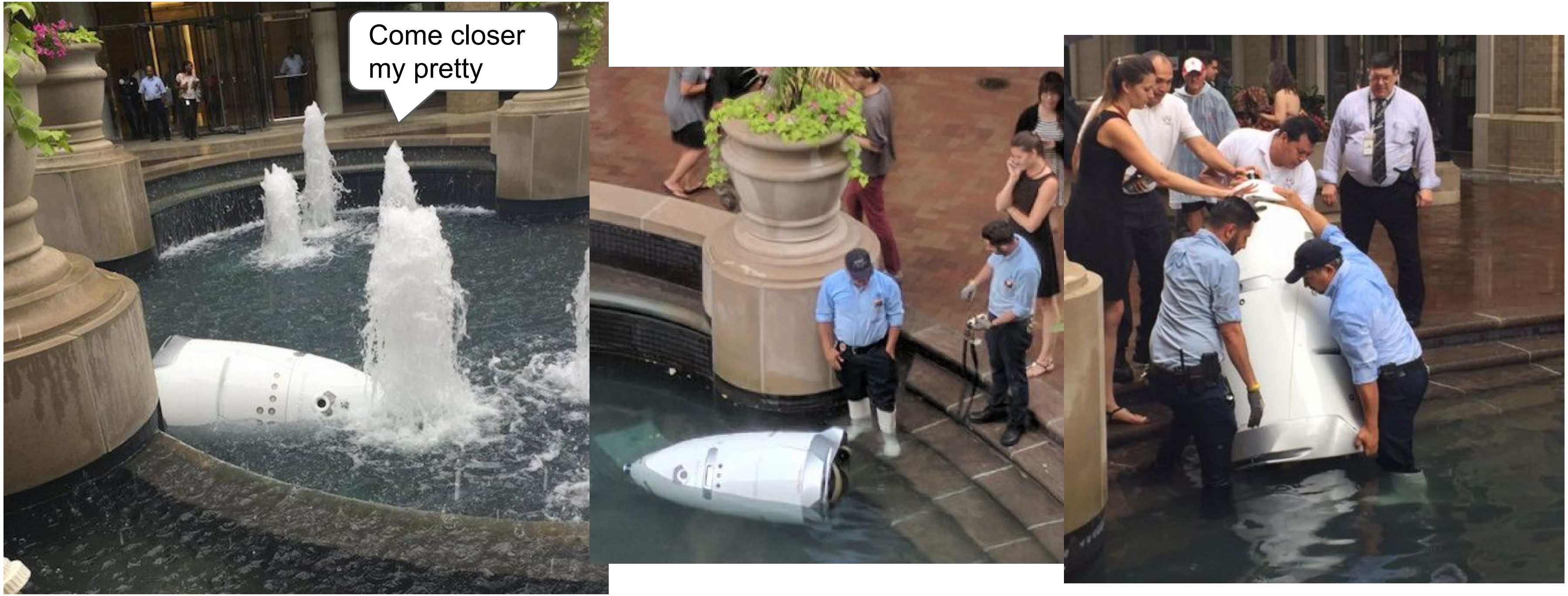
- Didn’t ***See*** Toddler
  - “…meant for observing and reporting only”
  - Knocked Him Down
  - Ran Over Him
  - Weighs 300lbs
- Second Incident

http://abc7news.com/1423093/
http://www.fastcoexist.com/3049708/meet-the-scary-little-security-robot-thats-patrolling-silicon-valley

flyingpenguin

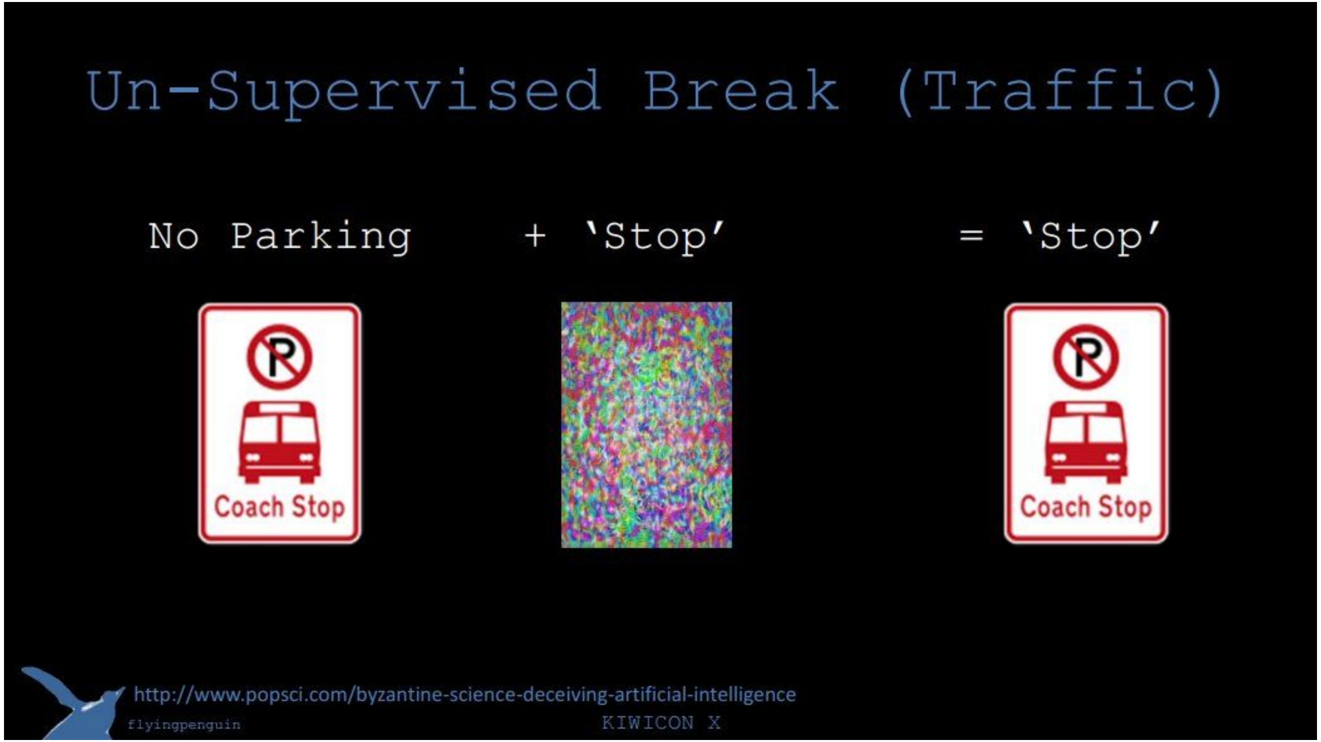
Source: http://www.flyingpenguin.com/?p=22441

2017: Knightscope “Advanced Anomaly Detection”



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

Remember My 2016 Warnings to Tesla?



Un-Supervised Break (Traffic)

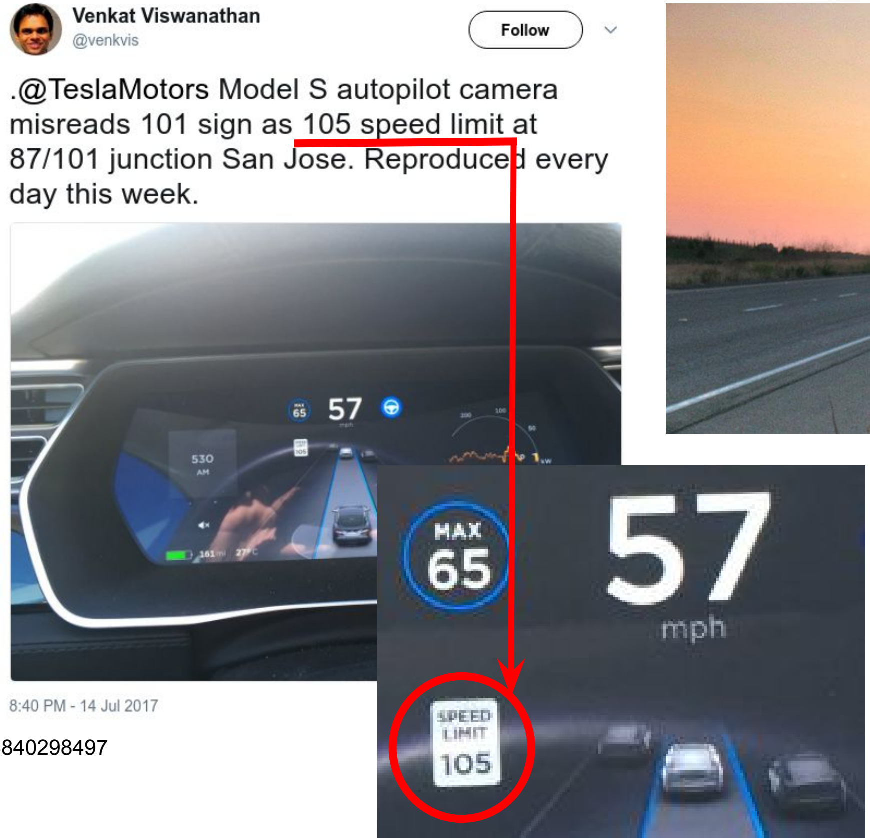
No Parking + 'Stop' = 'Stop'

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

Many Un-Supervised Breaks (Traffic) Spotted in Wild

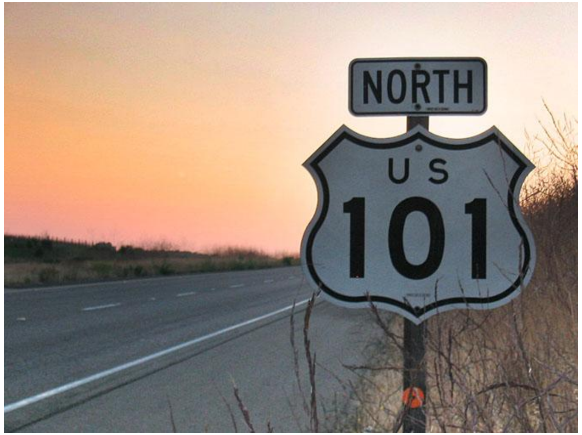


Venkat Viswanathan
@venkvis

Follow

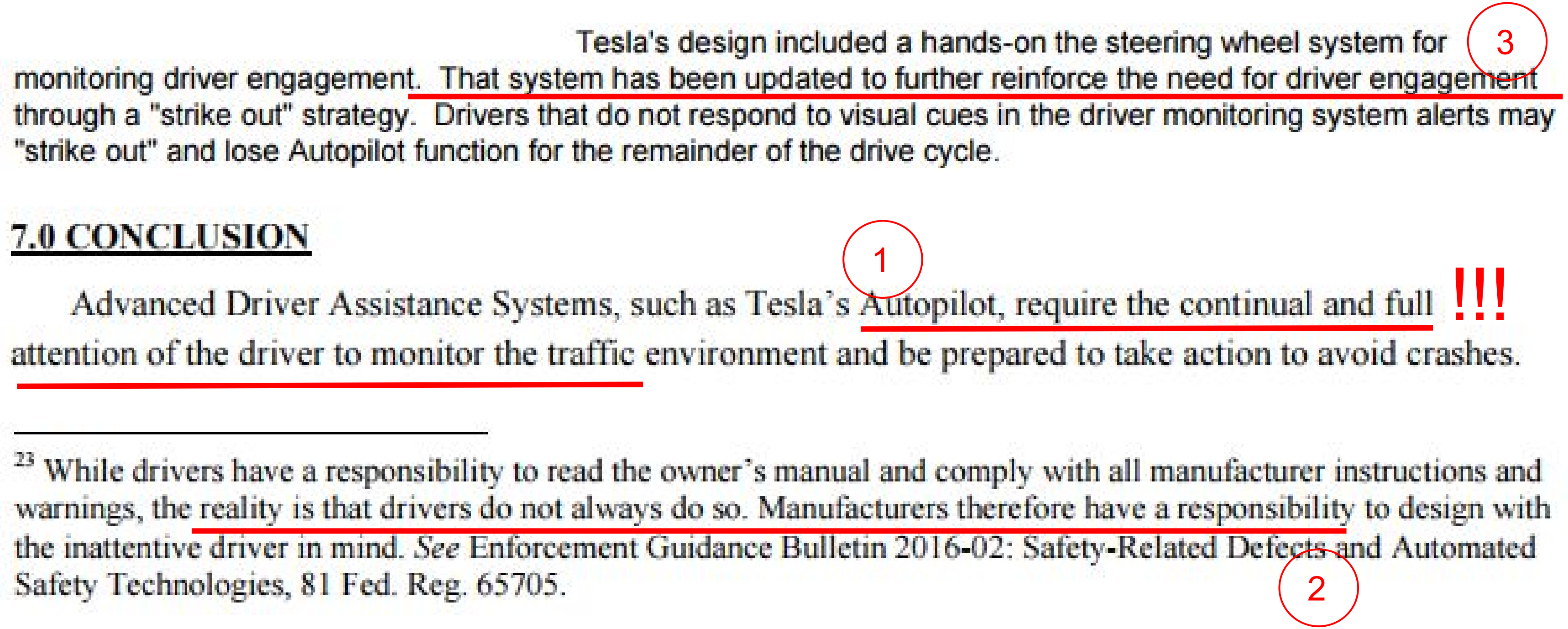
.@TeslaMotors Model S autopilot camera misreads 101 sign as 105 speed limit at 87/101 junction San Jose. Reproduced every day this week.

8:40 PM - 14 Jul 2017



Source: https://twitter.com/daviottenheimer/status/886630624840298497

NHTSA Report on Tesla Decision to Kill Driver



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

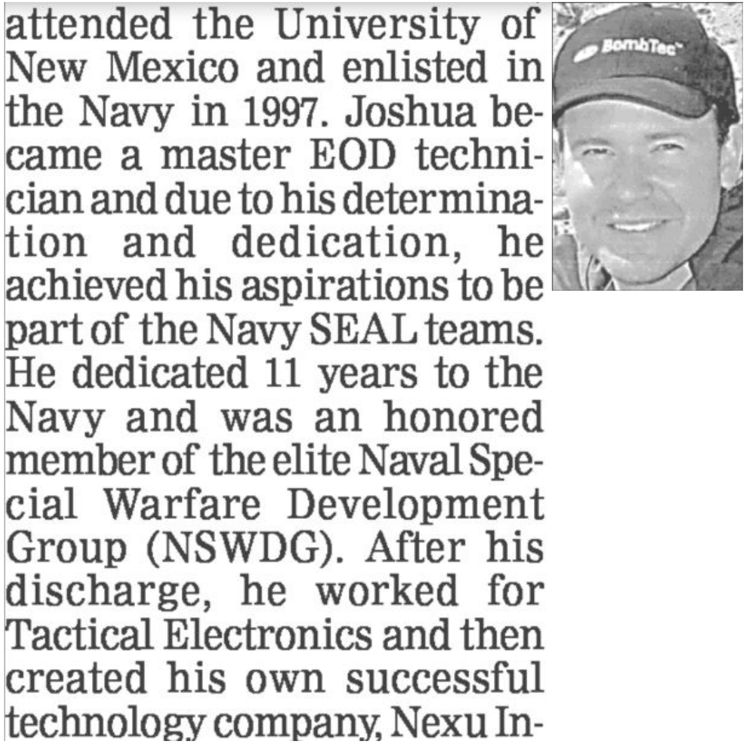
Advanced Driver Assistance Systems, such as Tesla's Autopilot, require the continual and full attention of the driver to monitor the traffic environment and be prepared to take action to avoid crashes.

[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 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

Looking Back to
See Further Ahead

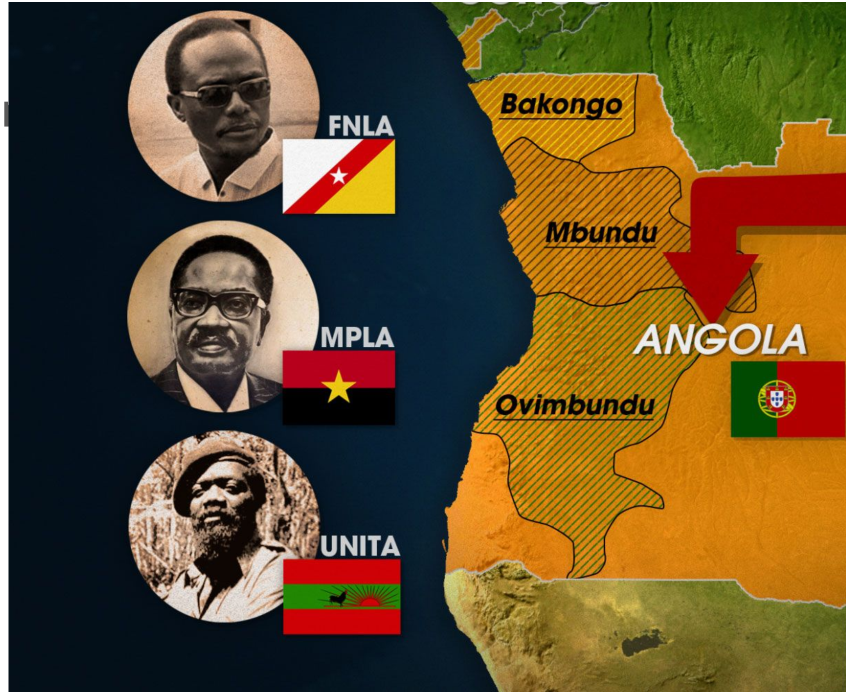
White Supremacy of Nixon “Realist” ForPo

1. End of WWII sets stage for liberation from colonialism
2. White supremacy has lost acceptability at global level
3. Kissinger rejects self-rule, 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” those in US gov who disagree
4. Data integrity contest with State...

Source: https://mospace.umsystem.edu/xmlui/bitstream/handle/10355/10125/research.pdf

Angola 1975: US “Expert” Foreign Service Analysis

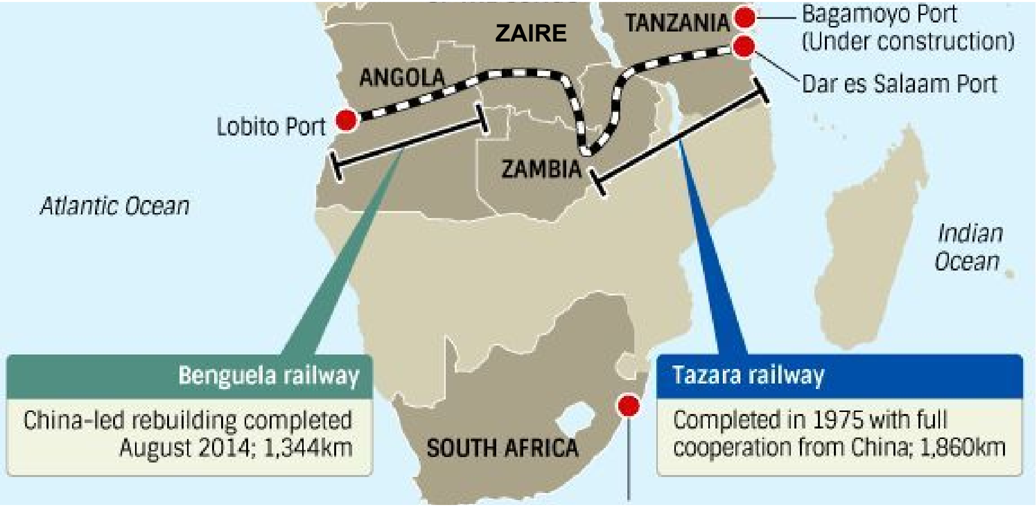
- Domestic self-rule contest
  - FNLA (National Front for the Liberatio of Angola)
  - MPLA (People's Movement for the Liberation of Angola)
  - UNITA (National Union for the Complete Independence of Angola)
- No real US security issues
  - Oil
  - Coffee



Source: http://ddc.arte.tv/karten/348

Angola 1975: US "Expert" Foreign Service Analysis

- Regional Dynamics
  - Neighbors wary of USSR
  - Benguela railroad control
- Mobutu (Zaire)
  - Paranoid: June 1975 economy weak = jails CIA for coup plotting
  - Courts aid from China


ZAIRE
TANZANIA
Bagamoyo Port (Under construction)
Dar es Salaam Port
ANGOLA
Lobito Port
ZAMBIA
Atlantic Ocean
Indian Ocean
SOUTH AFRICA
Benguela railway
China-led rebuilding completed August 2014; 1,344km
Tazara railway
Completed in 1975 with full cooperation from China; 1,860km

Kissinger Dismisses “Bleeding-Heart” Analysis

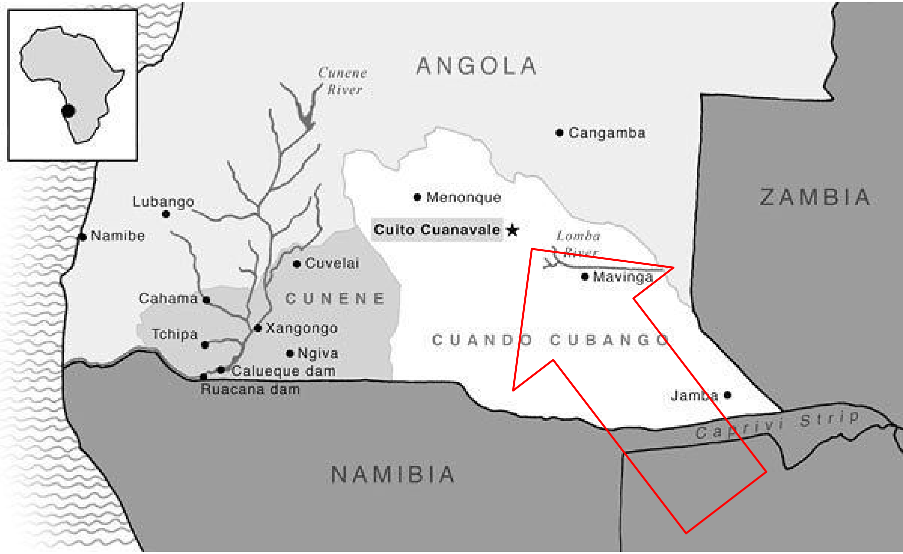
- Closes learning model (cognitive blindness)
- Wants post-Vietnam conflict with USSR
- Seeks inexpensive “No-Win War” in “South”
  - $100m cost of stable “win” deemed too visible, requiring oversight
  - $14m budgeted for Angola subversion, hidden from US public
- Selects a White Minority “Communication” Option

Source: https://www.foreignaffairs.com/reviews/capsule-review/1976-10-01/tar-baby-option-american-policy-toward-southern-rhodesia, https://www.worldcat.org/title/in-search-of-enemies-a-cia-story/oclc/22269006

Which Leads to…
27 Years of
Angolan Civil War
(1975-2002)

Turning Point: 1987 *Cuito Cuanavale* Hot Battle

- South Africa sends its white army (despite under arms boycott since 1977) to fight Angolan government
- Cuba airlifts massive gov reinforcement
- South Africa forced to withdraw
- Angolan-Cuban victory paves new path
  - 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

1975 “No-Win War” Subversion

Delayed

Self-Rule

Prolonged

Apartheid

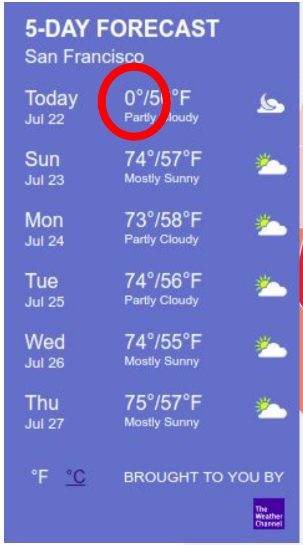
'We also salute the frontline states of Southern Africa and the rest of our continent for their own enormous contribution to the struggle against apartheid.' Nelson Mandela.

500,000 killed

Source: https://www.nelsonmandela.org/cache/ce_img_cache/local/ba75ac9ff068046b/On_The_Frontline_Exhibit_855_731_80_s.jpg

Looking Ahead at Subversion Risks

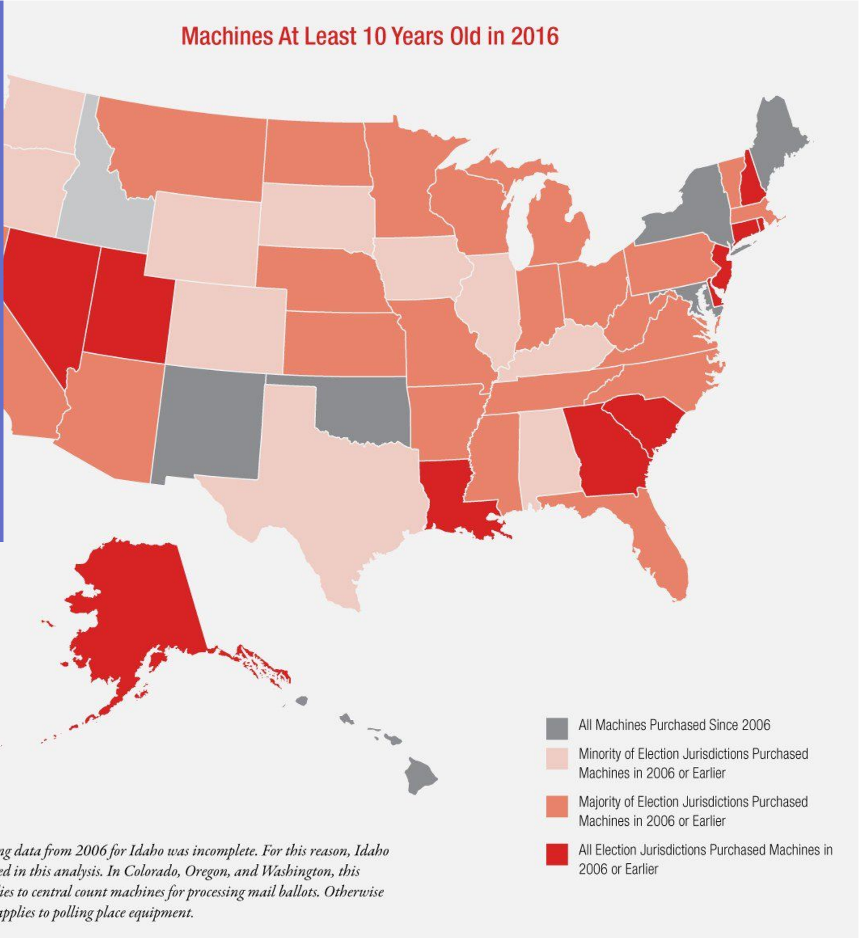
- Environmentalism
- Education
- Criminalization of substances
- Healthcare policy analysis, treatment
- Election tallies



5-DAY FORECAST
San Francisco

Today Jul 22	0°/5[illegible]°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 The Weather Channel



Machines At Least 10 Years Old in 2016

All Machines Purchased Since 2006
Minority of Election Jurisdictions Purchased Machines in 2006 or Earlier
Majority of Election Jurisdictions Purchased Machines in 2006 or Earlier
All Election Jurisdictions Purchased Machines in 2006 or Earlier

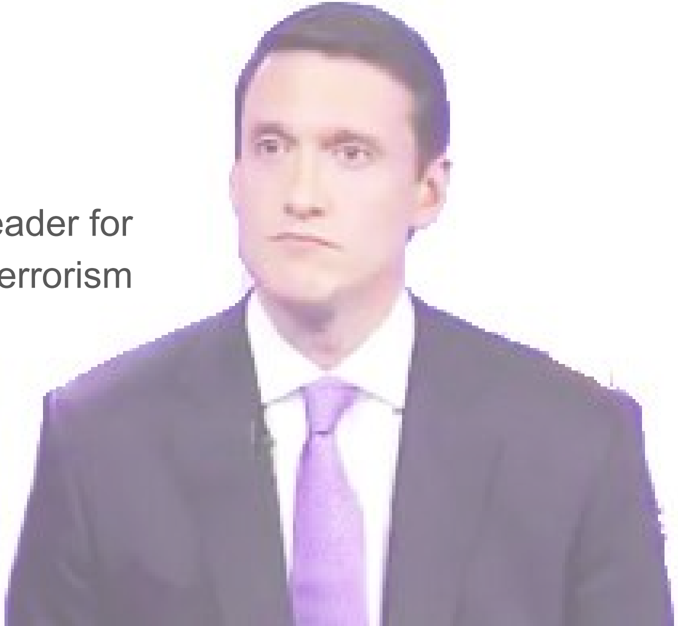
* *Verified Voting data from 2006 for Idaho was incomplete. For this reason, Idaho is not included in this analysis. In Colorado, Oregon, and Washington, this analysis applies to central count machines for processing mail ballots. Otherwise the analysis applies to polling place equipment.*

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

And “Realist” Amoral Cyber Platform...It’s Baaaack

“Multilateral oversight bad...Multilateral is a fool’s errand...Pursue bilateral approach to punishments”

-- Thomas Bossert, Assistant to US Regime Leader for Homeland Security and Counterterrorism

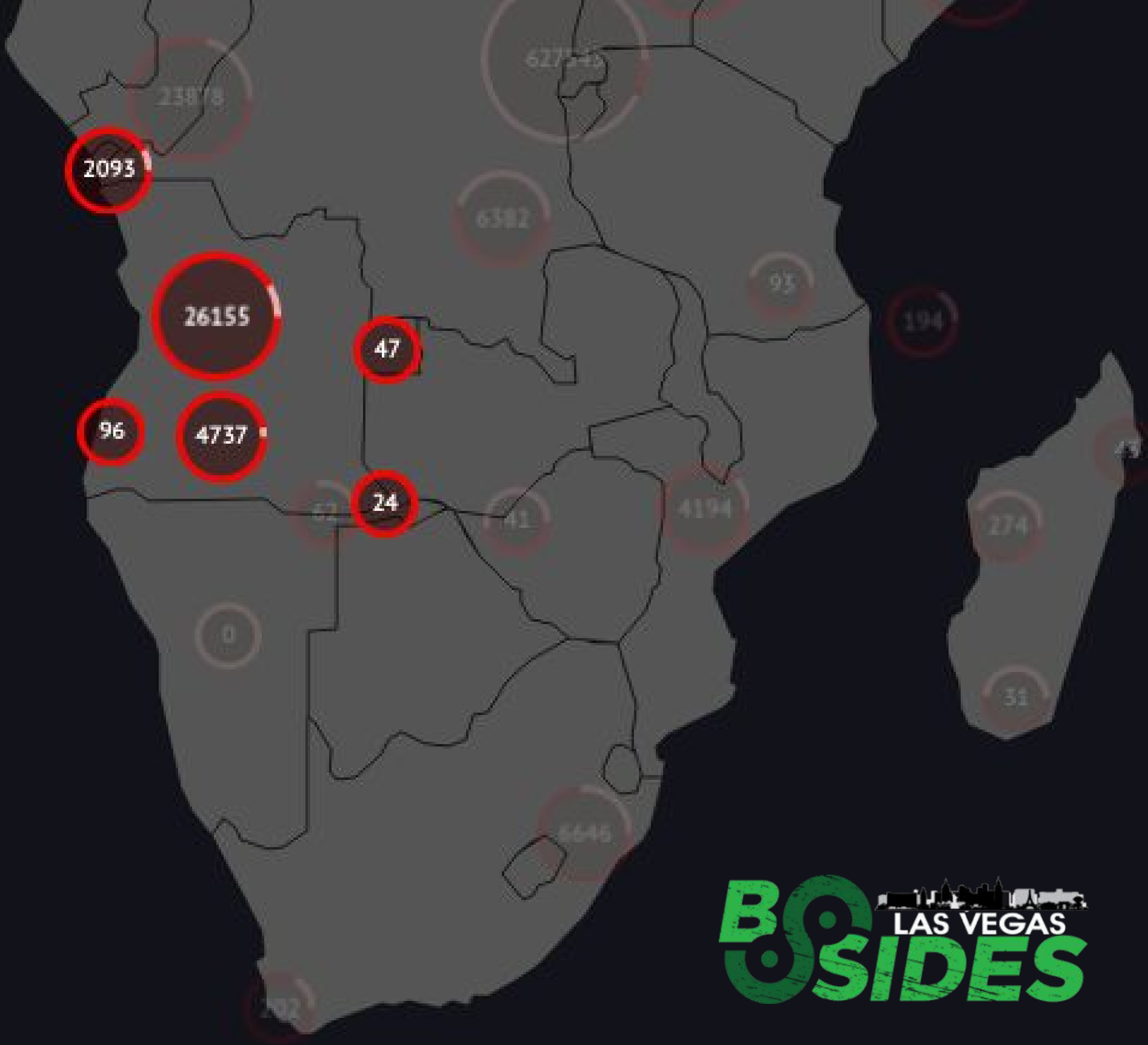


Source: https://youtu.be/q0fW5aAIvIQ?t=32m44s

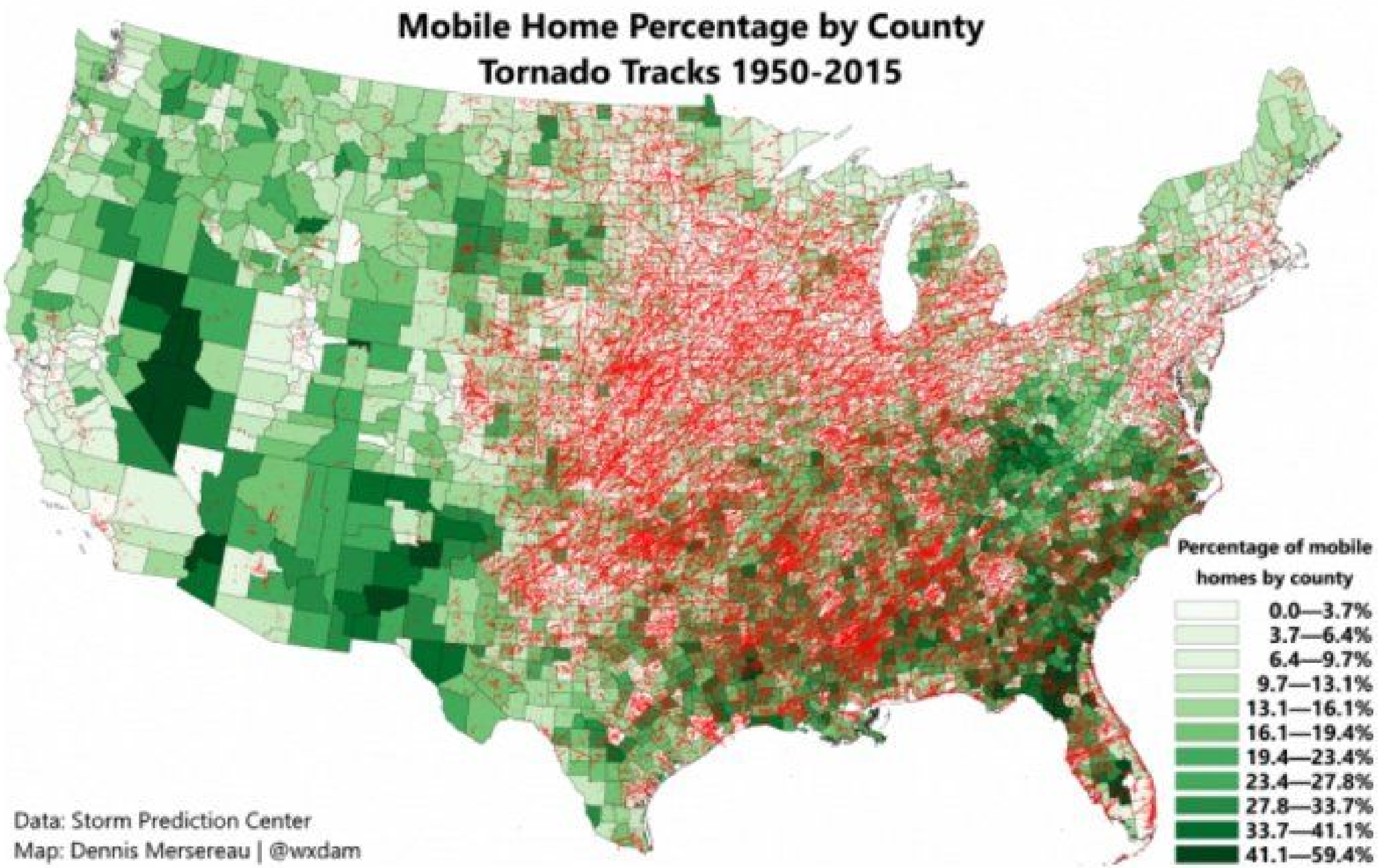
Hidden Hot Battle Lessons of Cold War

All Learning Models Have Flaws, Some Have Casualties

Davi Ottenheimer



Source: http://ucdp.uu.se/#country/540



Mobile Home Percentage by County
Tornado Tracks 1950-2015

Data: Storm Prediction Center
Map: Dennis Mersereau | @wxdam