Power Point Presentation: AI-Machine Learning Augmentation and Cybersecurity: Why Smart Minds Using Smart Tools Are Critical for Minimizing Risks, And, What You Can Do About It?

Article *in* SSRN Electronic Journal · January 2019

DOI: 10.2139/ssrn.3399781

CITATIONS
2

READS
124

1 author:

Yogesh Malhotra

Global Risk Management Network LLC: Air Force Research Laboratory Commercialization Academy Ventures

127 PUBLICATIONS **5,098** CITATIONS

SEE PROFILE

2019 New York State Cyber Security Conference, Albany, NY
June 4 - 5, 2016, Empire State Plaza - Albany, NY

AI-Machine Learning Augmentation and Cybersecurity: Why Smart Minds Using Smart Tools are critical for Minimizing Risks, and, What You Can Do About It?

Advancing Beyond 'Automation' to 'AI Augmentation'

Yogi http://www.linkedin.com/in/yogeshmalhotra

Dr. Yogesh Malhotra
Post-Doctoral R&D: AI-Machine Learning-CyberSecurity
PhD, MS-NCS, MS-CS, MS-QF, MS-Acc, MBA-Eco,
C.Eng., CISSP, CISA, CEH, CCP, CPA Education
Who's Who in America®, Who's Who in the World®,
Who's Who in Finance & Industry®,
Who's Who in Science & Engineering®
www.yogeshmalhotra.com dr.yogesh.malhotra@gmail.com

www.its.ny.gov

FinRM™

Global Risk Management Network, LLC,
Griffiss Air Force Base, Griffiss Business & Technology Park, Rome, NY 13441
Phone: 646-770-7993

"The **new business model** of the Information Age, however, is marked by **fundamental, not incremental, change**. Businesses **can't plan long-term**; instead, they **must shift** to a more flexible **"anticipation-of-surprise" model**."
-- Dr. Yogesh Malhotra in ***CIO Magazine*** interview, Sep. 15, 1999.

CIO

Presenter's biography

Dr. Yogesh Malhotra ('Yogi') is the Executive Director and Chief Scientist of New York based Global Risk Management Network, LLC, leading global Artificial Intelligence & Machine Learning, Cybersecurity & Cryptography, and, Quantitative Finance & Trading practices. As Managing Director for worldwide AI & Machine Learning practices with GIBC Digital, he recently developed the blueprint for Digital Transformation of global national economies and enterprises to expedite adoption and execution of AI & Machine Learning and Cybersecurity practices. As Artificial Intelligence and Machine Learning Industry Expert for MIT Sloan School of Management and MIT Computer Science & AI Lab, he recently led 200 Management and Leadership industry executives pioneering AI and Machine Learning strategic road maps for worldwide firms and industries. Over recent four years, his AI & Machine Learning presentations in Cyber Finance at Princeton University conferences sponsored by firms such as Goldman Sachs and Citadel are pioneering applied innovations spanning Cybersecurity & Cryptography, and, Quantitative Finance & Trading. His prior industry practices leaderships have included Wall Street investment banks and hedge funds such as JP Morgan, Big-3 Finance and Big-3 IT firms such as Bank of America, State of New York Civil Services, and, global digital ventures with global clients and patrons such as Goldman Sachs, Google, IBM, Intel, Microsoft, Harvard, and, MIT. Globally sought as an industry expert and keynote speaker, his hi-tech thought leadership engagements have spanned Silicon Valley to Seoul including Silicon Valley venture capitalists and CEOs, Wall Street investment banks and hedge funds, AFCEA, AFRL, CFA Society, NAIC, State of New York, Conference Board, Institute of Supply Management, National Science Foundation, United Nations, and, US and world governments and national economies such as Mexico, Netherlands, South Korea, and, Switzerland. Real impact of his published research is ranked and recognized among Finance-IT Nobel laureates such as Black-Scholes by AACSB, premier scientific studies, and industry surveys. He has taught as invited Executive Education faculty for Carnegie Mellon University and Kellogg School of Management, and, served as tenure-track professor of Computer Science, Operations Research, Quantitative Methods, and, Information Technology at SUNY and Syracuse University. His Artificial Intelligence & Machine Learning post-doctoral industrial R&D in Quant Finance, Cybersecurity, and, Computer Science with 63 Top-10 SSRN Research Rankings and Top-2% SSRN Author rankings is advancing global strategies, practices, and, policies. A Chartered Engineer (C.Eng.) and Life Member of the Institution of Engineers, he also holds DoDD 8140 Top-3 IT Cyber Security Certifications: CISSP, CISA, CEH, in addition to CCP-CDP, and, has fulfilled the AICPA educational requirements of the New York State CPA. His biography is profiled among world's foremost leaders and achievers in Marquis *Who's Who in America*®, Marquis *Who's Who in the World*®, Marquis *Who's Who in Finance & Industry*®, and, Marquis *Who's Who in Science & Engineering*®.

Summary of the session

The current presentation advances upon Artificial Intelligence and Machine Learning industry expert leadership for the MIT Sloan School of Management and the MIT Computer Science & Artificial Intelligence Lab, and, invited presentations at Princeton University conferences sponsored by firms such as Goldman Sachs and Citadel over recent four years. Latest related research papers and presentations with 63 Top-10 SSRN Research Rankings accessible from the author's SSRN page are advancing worldwide strategies, practices, and, policies. Prior background research ranked and recognized among Finance-IT Nobel laureates for real world impact is also accessible from the author's home page. The primary focus of the presentation is on helping advance intuitive understanding about AI-Machine Learning Augmentation and Cybersecurity for auditors, business managers, critical infrastructure owners, educators, executives, information security professionals, forensic specialists, IT professionals, law enforcement, process improvement managers, and project managers about the emerging contours. *With great power comes great responsibility!* In case of AI and Machine Learning technologies, the realization and application of such great power can yield unprecedented automation and optimization capabilities for developing more sophisticated cybersecurity and cyber risk management capabilities. *However*, the same AI and Machine Learning technologies also provide the 'adversary' with unprecedented deception, manipulation, and, attack capabilities to launch much more sophisticated cyberattacks with unprecedented destructive power. *Furthermore*, for designers, developers, and, users of AI and Machine Learning technologies, greater responsibility is needed not only for acutely recognizing the limitations of underlying mathematical models and algorithms but also for smartly deploying human imagination, intuition, and, insight to make up for the mechanistic limitations inherent in the design of the machines and related automation technologies. We shall advance upon the latest insights generated, hi-tech practices developed, and, lessons learned from leading global industry leaders at programs such as MIT and Princeton and industry conferences such as the latest Armed Forces Communications and Electronics Association (AFCEA) C4I conference. By doing so, we shall help you **develop intuitive understanding about AI-Machine Learning Augmentation as well as its most critical role in minimizing the downside risks** in ongoing and future Cybersecurity and Risk Management capabilities and practices development and deployment.

Background Time Line "Post-WWW" Era

- **R&D Program: Years & Engagements**

RISKS

Strategy, Operations, Tactics: People, Processes, Technologies

Big-3 IT, Big-3 Banking & Finance: Global Financial Systems: USA, Hong Kong, India

DIGITAL

1993-1998: Top Digital Site, Top-3 Search Engine, Top-10 Social Network
Computerworld, CIO Magazine, Wall Street Journal, Information Week

1993-2001: AI-ML: John Holland: NSA-CIA, US, Netherlands, Mexico, South Korea
Business Week, Fortune, Inc. Wall Street Journal, New York Times…

CYBER

2001-2008: National Science Foundation, United Nations, **CISSP**, **CISA**
AACSB Impact of Research, CNet Networks Computing Award
Canada-Fulbright Chair Invitation: Queen's University

QUANT

1998-2008: BT, Goldman Sachs, Google, Intel, IBM, Microsoft, Harvard, MIT,…
Largest Digital Transformation CoP: CIO Magazine, CIO Insight

CRYPTO

2008-2019: **MIT** AI-Machine Learning, **Princeton** Cyber Finance, **CEH**, NYS-CRI
2015-2018: SSRN: 63 Top-10 Research Rankings, Top-2% Authors.
GIBC Digital **AI-ML MD**, New York State **CISO**, JP Morgan **Quant**.
ACM, **AFCEA**, **AFRL**, CFA, NAIC, NYS, Switzerland, Wall Street…

QUANTUM

Books, Papers, Presentations, Keynotes

www.YogeshMalhotra.com [Download Our Research](#)

SSRN tomorrow's research today

https://papers.ssrn.com/author_id=2338267

Outline of Presentation

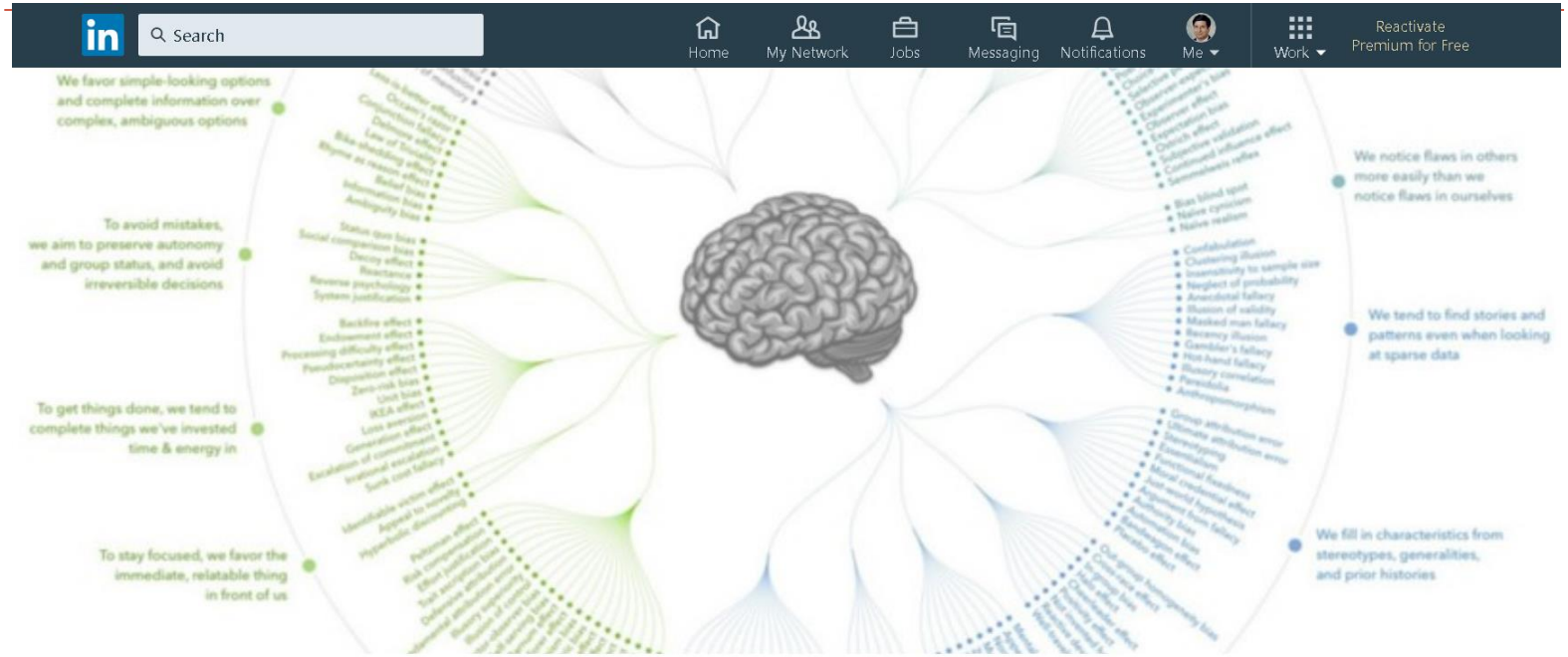
- References
- Foreground
- Introduction: Project Maven
- AI, Machine Learning, Deep Learning, and, Neural Networks
- Why Model Risk Management is Crucial to Robust AI-ML-DL Use
- A Knowledge Management Framework for MRM
- Conclusion: Beyond 'AI Automation' to 'AI Augmentation'

References

25-Years Leading Global R&D & Industrial Practices Pioneering **Human-Centered AI** and **AI-Machine Learning Augmentation**

www.YogeshMalhotra.com

25-Years Leading Global R&D & Industrial Practices Pioneering **Human-Centered AI** and **AI-Machine Learning Augmentation**



https://www.linkedin.com/pulse/designing-smart-minds-using-tools-utopian-view-ai-yogesh-/

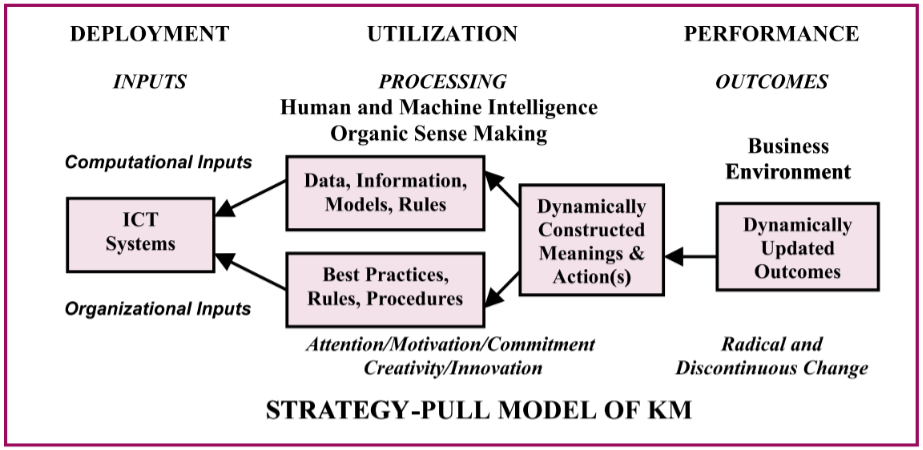
https://bit.ly/2rXcaOH

25-Years Leading Global R&D & Industrial Practices Pioneering **Human-Centered AI** and **AI-Machine Learning Augmentation**

MIT Sloan School of Management and the **MIT Computer Science & Artificial Intelligence Lab**

Management & Leadership Program

Artificial Intelligence & Business Strategy



Malhotra, Y., Integrating Knowledge Management Technologies in Organizational Business Processes: Getting Real Time Enterprises to Deliver Real Business Performance, Journal of Knowledge Management, Vol. 9, Issue 1, April 2005, 7-

http://FutureOfFinance.org/MIT/

MIT AI-Machine Learning Executive Guide: including Deep Learning, Natural Language Processing, Autonomous Cars, Robotic Process Automation

https://www.linkedin.com/pulse/dear-ceo-ai-machine-learning-advice-top-industry-leading-malhotra/

https://bit.ly/2PXflQH

Published on February 13, 2018 Edit article View stats

Like Comment Share 33 • 3,082 Views

Messaging

www.YogeshMalhotra.com

FinRM™ FinRM.COM Global Risk Management Network, LLC

25-Years Leading Global R&D & Industrial Practices Pioneering Human-Centered AI and AI-Machine Learning Augmentation

Princeton University Presentations on Quant-Cyber-Crypto-Quantum Security

Princeton Presentations: Beyond Risk Modeling to Uncertainty Management™
AI-ML Risk Management Analytics beyond Prediction to 'Anticipation of Surprise'™
Latest Research: AI & Machine Learning for Risk & Uncertainty Management
AI-Algorithms-Machine Learning: 63 SSRN Top-10 Rankings, Top-2% Authors
Princeton University Presentations Pioneering Model Risk Arbitrage™

CIO FORTUNE Inc.

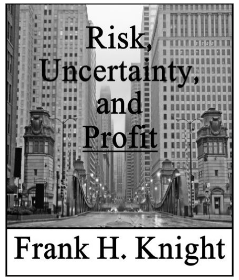
http://ModelRiskArbitrage.com/

PRINCETON UNIVERSITY MIT MANAGEMENT SLOAN SCHOOL MIT CSAIL

Frank Knight in Risk, Uncertainty & Profit

"It is this true uncertainty, and not risk, as has been argued, which forms the basis of a valid theory of profit and accounts for the divergence between actual and theoretical competition... It is a world of change in which we live, and a world of uncertainty...If we are to understand the workings of the economic system we must examine the meaning and significance of uncertainty; and to this end some inquiry into the nature and function of knowledge itself is necessary."

'Knight Reconsidered': Risk, Uncertainty, & Profit for the Cyber Era



www.YogeshMalhotra.com

"The new business model of the Information Age, however, is marked by fundamental, not incremental, change. Businesses can't plan long-term; instead, they

Goldman Sachs: How to Anticipate Risk?
25 Years: Model Risk Management Program

25-Years Leading Global R&D & Industrial Practices Pioneering **Human-Centered AI** and **AI-Machine Learning Augmentation**

Goldman Sachs: Beyond 'Prediction' to 'Anticipation of Surprise'™
Computational Quant Analytics: Beyond Predictive to Anticipatory Risk Analytics
Finance-IT-Risk Analytics: Leading Industry Leaders & Learning from Them
Latest Research: AI & Machine Learning for Risk & Uncertainty Management
AI-Algorithms-Machine Learning: 63 SSRN Top-10 Rankings, Top-2% Authors
JP Morgan Portfolio Liquidity Risk Modeling Framework for $500-600Bn AUM
JP Morgan Portfolio Optimization, VaR & Stress Testing: 17-Asset Class Portfolio
JP Morgan Private Bank: Hedge Funds: Bayesian vs. VaR: Model Risk Management
PRMIA Presentation: Beyond Value-At-Risk: Measuring Risks with Better Measures

Goldman Sachs

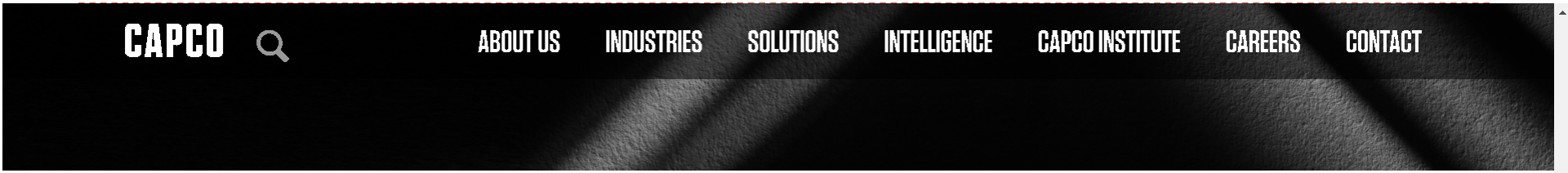
The 'Anticipation of Surprise' Framework: Anticipatory Risk Analyt
- 25 Years of Computational Quant Risk Analytics Leading Industry Leaders.
- Download Research: Model Risk Management (MRM) Research Program.
- Federal Reserve/OCC Model Risk Management Guidance SR11-7/OCC 2011-1
- Global Footprint of Our Research in Worldwide Firms, Governments, Instituti
- World's Largest Firms, Governments, & Organizations Applying our Research.

Over 25 Years of Computational Quantitative Anticipatory Risk Ana
- Risk Models: Statistics, Finance, Econometrics, IT, OR, Computer Sc., Telecor
- Risk Management & Controls: ERM, MRM, Assets, Markets, Exchanges, Netw

Goldman Sachs CEO Lloyd Blankfein told the Australian Institute of Company Directors at a brea 26 2013, **how investors should prepare for the most extreme risk scenario**. His comments ab the essence of the 'anticipation of surprise' model mentioned above and explained in Dr. Yogesh M research monographs published over the last decade or so.

http://FutureOfFinance.org/ http://FutureOfFinance.org/CFA/

25-Years Leading Global R&D & Industrial Practices Pioneering **Human-Centered AI** and **AI-Machine Learning Augmentation**



https://bit.ly/2VGOm1M

https://www.capco.com/Capco-Institute/Journal-49-Alternative-Capital-Markets/AI-AUGMENTATION-FOR-LARGE-SCALE-GLOBAL-SYSTEMIC-CYBER-RISK-MANAGEMENT-PROJECTS

AI AUGMENTATION FOR LARGE-SCALE GLOBAL SYSTEMIC AND CYBER RISK MANAGEMENT PROJECTS : MODEL RISK MANAGEMENT FOR MINIMIZING THE DOWNSIDE RISKS OF AI AND MACHINE LEARNING

Published: 29 April 2019

YOGESH MALHOTRA | Chief Scientist and Executive Director, Global Risk Management Network, LLC

This article discusses how model risk management in operationalizing machine learning or algorithm deployment can be applied in national systemic and cyber risk management projects such as Project Maven.

After an introduction about why model risk management is crucial to robust AI, ML, deep learning, and neural networks deployment, the article presents a knowledge management framework for model risk management to advance beyond 'AI automation' to 'AI augmentation.'

DOWNLOAD PAPER

https://bit.ly/2V3O2uC

Foreground

Background Time Line "Post-WWW" Era

- **R&D Program: Years & Engagements**

RISKS

Strategy, Operations, Tactics: People, Processes, Technologies

Big-3 IT, Big-3 Banking & Finance: Global Financial Systems: USA, Hong Kong, India

DIGITAL

1993-1998: Top Digital Site, Top-3 Search Engine, Top-10 Social Network
Computerworld, CIO Magazine, Wall Street Journal, Information Week

1993-2001: AI-ML: John Holland: NSA-CIA, US, Netherlands, Mexico, South Korea
Business Week, Fortune, Inc. Wall Street Journal, New York Times…

CYBER

2001-2008: National Science Foundation, United Nations, **CISSP**, **CISA**
AACSB Impact of Research, CNet Networks Computing Award
Canada-Fulbright Chair Invitation: Queen's University

QUANT

1998-2008: BT, Goldman Sachs, Google, Intel, IBM, Microsoft, Harvard, MIT,…
Largest Digital Transformation CoP: CIO Magazine, CIO Insight

CRYPTO

2008-2019: **MIT** AI-Machine Learning, **Princeton** Cyber Finance, **CEH**, NYS-CRI
2015-2018: SSRN: 63 Top-10 Research Rankings, Top-2% Authors.
GIBC Digital **AI-ML MD**, New York State **CISO**, JP Morgan **Quant**.
ACM, **AFCEA**, **AFRL**, CFA, NAIC, NYS, Switzerland, Wall Street…

QUANTUM

Books, Papers, Presentations, Keynotes

www.YogeshMalhotra.com [Download Our Research](#)

SSRN tomorrow's research today

https://papers.ssrn.com/author_id=2338267

19th New York State Cyber Security Conference Presentation, Albany, NY
June 8 - 9, 2016, Empire State Plaza - Albany, NY

CyberFinance: Why Cybersecurity Risk Analytics must Evolve to Survive 90% of Emerging Cyber Financial Threats, and, What You Can Do About It?

Advancing Beyond '<u>Predictive</u>' to '<u>Anticipatory</u>' Risk Analytics

Yogi

Dr. Yogesh Malhotra
PhD, MSQF, MS-CS, MS-NCS, MS-Acc, MBA-Eco, C.Eng., CISSP, CISA, CEH, CCP/CDP
Who's Who in America®, Who's Who in the World®,
Who's Who in Finance & Industry®,
Who's Who in Science & Engineering®
www.yogeshmalhotra.com
dr.yogesh.malhotra@gmail.com

www.its.ny.gov

FinRM™

Global Risk Management Network, LLC,
757 Warren Rd, Cornell Business & Technology Park, Ithaca, NY 14852-4892
Phone: 646-770-7993

"The **new business model** of the Information Age, however, is marked by **fundamental, not incremental, change**. Businesses **can't plan long-term**; instead, they **must shift** to a more flexible **"anticipation-of-surprise" model**."
-- Dr. Yogesh Malhotra in ***CIO Magazine*** interview, Sep. 15, 1999.

CIO

C4I and Cyber Security in Defense and Finance

- Princeton University Presentations & MIT AI-Machine Learning Program

The current presentation builds upon the following C4I and Cyber themes that were subject of invited presentations over 2015-2018 at the Princeton University:

(i) Risk Modeling for Managing Uncertainty in an Increasingly Non-Deterministic Cyber World;

(ii) How to Navigate 'Uncertainty'... When 'Models' Are 'Wrong'... and 'Knowledge'... 'Imperfect'!;

(iii) Model Risk Management in AI, Machine Learning & Deep Learning.

It also builds upon recent development of MIT AI-Machine Learning (ML) Executive Guide that advances sophisticated understanding about 'AI Augmentation' for guiding MIT Management and Leadership industry executives in the **MIT Sloan School of Management** and the **MIT Computer Science and Artificial Intelligence Laboratory (CSAIL)**.

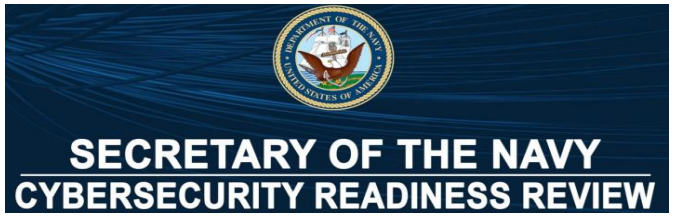
MIT AI-Machine Learning Executive Guide http://FutureOfFinance.org/MIT/
https://www.linkedin.com/pulse/dear-ceo-ai-machine-learning-advice-top-industry-leading-malhotra

Princeton Quant Trading-Cyber Finance Presentations
http://ModelRiskArbitrage.com/

Exponentially Increasing "Invisible Risks"

"The **greatest enemy** we face these days is one **we can't even see**..."

If We Sacrifice Cyber, We Sacrifice Everything Because **Cyber is Everything!**



MARCH 2019

https://www.navy.mil/strategic/CyberSecurityReview.pdf

Recent report to the Secretary of the Navy warned that the service is preparing for the **wrong war**, one fought not with bombs and artillery but with **terabytes and artificial intelligence**. "We find the Navy preparing to win some future kinetic battle, while it is losing the **current global, counter-force, counter-value, cyber war**." "This time **technology**, not the naval service, or its opponents, have imposed a definition of what navies will be for the rest of the 21st Century." "Navies must become information enterprises who happen to operate on, over, under, and from the sea; a vast difference from a 355 ship mindset."

http://time.com/5582063/trump-navy-truman-cybersecurity/

Cyber is Everything (AFRL, NYS-CRI)
https://ssrn.com/abstract=2553547

"America once won wars with overwhelming manpower, then later won with superior industrial might, and with the Cold War, won with better technology... **The cyber war has been ongoing for some time. The threat is long past the emergent or developing stage. While its 'guns' go unheard, it is real, and with as or more devastating consequences**." "The systems the U.S. relies upon to mobilize, deploy, and sustain forces have been extensively targeted by potential adversaries, and compromised to such as extent that their reliability is questionable."

Exponentially Increasing "Invisible Risks"

THE WALL STREET JOURNAL.

U.S. Edition ▾ | March 19, 2019 | Print Edition | Video

Home World U.S. Politics Economy Business Tech Markets Opinion Life & Arts Real Estate WSJ. Magazine

POLITICS

Navy, Industry Partners Are 'Under Cyber Siege' by Chinese Hackers, Review Asserts

Hacking threatens U.S.'s standing as world's leading military power, study says

By Gordon Lubold and Dustin Volz

March 12, 2019 2:32 p.m. ET

WASHINGTON—The Navy and its industry partners are "under cyber siege" by Chinese hackers and others who have stolen national security secrets in recent years, exploiting critical weaknesses that threaten the U.S.'s standing as the world's top military power, an internal Navy review concluded.

The assessment, delivered to Navy Secretary Richard Spencer last week and reviewed by The Wall Street Journal, depicts a branch of the armed forces under relentless cyber attack by foreign adversaries and struggling in its response to the scale and sophistication of the problem.

Source: https://www.wsj.com/articles/navy-industry-partners-are-under-cyber-siege-review-asserts-11552415553

Exponentially Increasing "Invisible Risks"

Townhall COLUMNISTS TIPSHEET CARTOONS PODCASTS ELECTION TOWNHALL TV SECTIONS SITES

OPINION

FBI Director on Cyber Threat: 'It's bigger than the government itself,'

Julio Rivera | Posted: Mar 17, 2019 12:01 AM

Share (242) Tweet

The opinions expressed by columnists are their own and do not represent the views of Townhall.com.

"The scope, breadth, depth, sophistication and diversity of the threat we face now is unlike anything we've had in our lifetimes."

Trending

Kurt Schlichter
An Armed Citizenry Is A Free Citizenry, Which Is Why Liberals Want You Disarmed

Dennis Prager
Your Kid Goes to Yale? So What?

The United States entered 2019 under a partial government shutdown and coming off a year where America was victimized by some of the most dangerous and high leverage cyber-attacks ever seen in our history. Many of these strikes victimizing targets ranging from US Navy contractors, to critical infrastructure and even financial institutions. America seems to be leading from behind on an issue where major breaches are still a far too common occurrence during the current administration.

Source: https://townhall.com/columnists/juliorivera/2019/03/17/fbi-director-on-cyber-threat-its-bigger-than-the-government-itself-n2543228

Exponentially Increasing "Invisible Risks"

FINANCIAL TIMES

HOME WORLD US COMPANIES TECH MARKETS GRAPHICS OPINION WORK & CAREERS LIFE & ARTS HOW TO SPEND IT

Get a fresh start. Choose your FT trial

Latest on Cyber Security

The Great Firewall of China — web of control

The web has fallen in with a bad crowd

Citrix investigates FBI report about cyber breach

Cyber Security + Add to myFT

Cyber attacks on financial services sector rise fivefold in 2018

Investment banks report highest number of data breaches to financial regulator

Madhumita Murgia and Nicholas Megaw in London FEBRUARY 25, 2019

1

Save

Financial services companies in the UK saw a fivefold rise in data breaches in 2018 compared with the year before, according to the Financial Conduct Authority, in the latest sign of how the sector is under relentless attack from hackers.

Companies reported 145 breaches to the FCA last year, up from 25 in 2017, with investment banks reporting the highest number of incidents at 34, up from just three the previous year.

Retail banks saw the sharpest rise in percentage terms, from 1 to 25. The data

nsent/consent-record-cookie?redirect=https://www.ft.com

igh a freedom of information request by the law firm RPC.

Source: https://www.ft.com/content/6a2d9d76-3692-11e9-bd3a-8b2a211d90d5

Exponentially Increasing "Invisible Risks" Where AI and Cyber Security Converge

Defense One

The Newest AI-Enabled Weapon: 'Deep-Faking' Photos of the Earth

High resolution satellite image of Cairo TOMMOT/SHUTTERSTOCK.COM

By PATRICK TUCKER // Defense One // APRIL 1. 2019

Worries about **deep fakes** — machine-manipulated videos of celebrities and world leaders purportedly saying or doing things that they really didn't — are quaint compared to a **new threat: doctored images of the Earth itself**.

China is the acknowledged leader in using an emerging technique called **generative adversarial networks** to trick computers into seeing objects in landscapes or in satellite images that aren't there, says Todd Myers, automation lead for the CIO-Technology Directorate at the National Geospatial-Intelligence Agency.

Source: https://www.defenseone.com/technology/2019/03/next-phase-ai-deep-faking-whole-world-and-china-ahead/155944/

Exponentially Increasing "Invisible Risks" Where AI and Cyber Security Converge

SMALL WARS JOURNAL

THE ART OF DIGITAL DECEPTION: GETTING LEFT OF BANG ON DEEPFAKES

Source: https://smallwarsjournal.com/jrnl/art/art-digital-deception-getting-left-bang-deepfakes

This article explores how state actors are using advanced software development tools and artificial intelligence (AI) to invent and perfect new deception capabilities to fool both people and machines on the **virtual battlefield**. It examines intelligent computer vision systems and their capabilities to support **state-sponsored hybrid warfare**.

We explore these capabilities in the context of two Russian disinformation campaigns, specifically **Ukraine in 2014**, and **Venezuela in 2019**. We then offer innovative concepts to mitigate these emerging enemy capabilities and threats.

Our **first adversarial example** explores how our enemies are using AI to accelerate the creation of synthetic generated media known as "Deep Fakes." The adversary was perfecting their **disinformation** capabilities to drive a wedge between US citizens and our government by creating **mistrust** through these echo chambers as a type of herd mentality.

Our **second adversarial example** uses AI to manipulate digital content to deceive other machines. This example uses AI to manipulate images before they are received and processed by visual classifier services, **enabling our enemies to hide** in **plain digital sight**.

DATA INTEGRITY & AUTHENTICITY

Exponentially Increasing "Invisible Risks" Where AI and Cyber Security Converge

Cracking the Code on Adversarial Machine Learning

THECYBEREDGE

March 1, 2019

Army Research Laboratory scientists advance the element of AI by understanding deep neural networks.

The **vulnerabilities** of **machine learning models** open the door for **deceit**, giving **malicious operators** the opportunity to interfere with the **calculations or decision making** of machine learning systems.

Often, in a **data set**, **corrupted inputs** or an **adversarial attack** enters a **machine learning model undetected**. **Adversaries also impact a model** whether or not they know the machine learning algorithm in use, training a substitute machine learning model for use on a "victim" model.

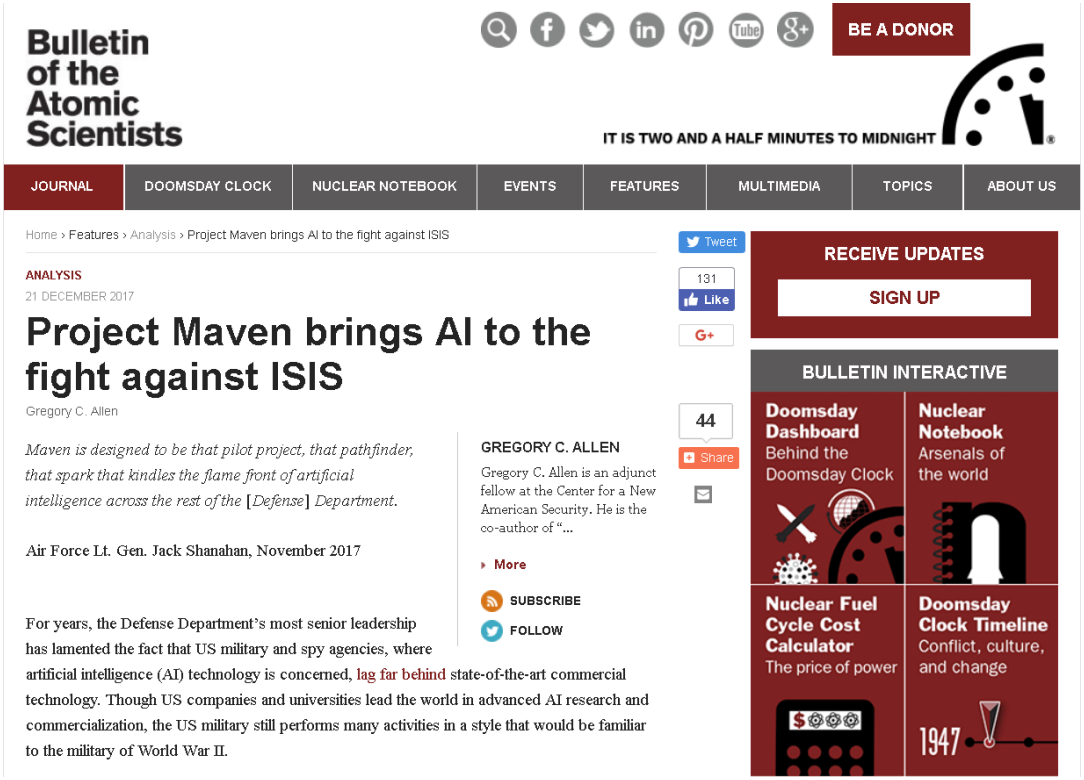
Given the rise in the use of **machine learning** as an important tool for **autonomous systems** to learn and act independently of human interaction—as in self-driving cars, data analytics, financial trading—the **risks of failure due to adversarial machine learning could be disastrous**.

Source: https://www.defenseone.com/technology/2019/03/next-phase-ai-deep-faking-whole-world-and-china-ahead/155944/

Introduction: Project Maven

Algorithmic Warfare Cross-Functional Team

- Project Maven: First operational use of deep learning AI technologies in the defense intelligence enterprise.
- Analysis of full-motion video data from tactical aerial drone platforms such as the ScanEagle and medium-altitude platforms such as the MQ-1C Gray Eagle and the MQ-9 Reaper.



Bulletin of the Atomic Scientists

BE A DONOR

IT IS TWO AND A HALF MINUTES TO MIDNIGHT

JOURNAL | DOOMSDAY CLOCK | NUCLEAR NOTEBOOK | EVENTS | FEATURES | MULTIMEDIA | TOPICS | ABOUT US

Home › Features › Analysis › Project Maven brings AI to the fight against ISIS

ANALYSIS

21 DECEMBER 2017

Project Maven brings AI to the fight against ISIS

Gregory C. Allen

Maven is designed to be that pilot project, that pathfinder, that spark that kindles the flame front of artificial intelligence across the rest of the [Defense] Department.

Air Force Lt. Gen. Jack Shanahan, November 2017

For years, the Defense Department's most senior leadership has lamented the fact that US military and spy agencies, where artificial intelligence (AI) technology is concerned, lag far behind state-of-the-art commercial technology. Though US companies and universities lead the world in advanced AI research and commercialization, the US military still performs many activities in a style that would be familiar to the military of World War II.

GREGORY C. ALLEN

Gregory C. Allen is an adjunct fellow at the Center for a New American Security. He is the co-author of "...

More

SUBSCRIBE

FOLLOW

Tweet 131 Like G+ 44 Share

RECEIVE UPDATES

SIGN UP

BULLETIN INTERACTIVE

Doomsday Dashboard Behind the Doomsday Clock

Nuclear Notebook Arsenals of the world

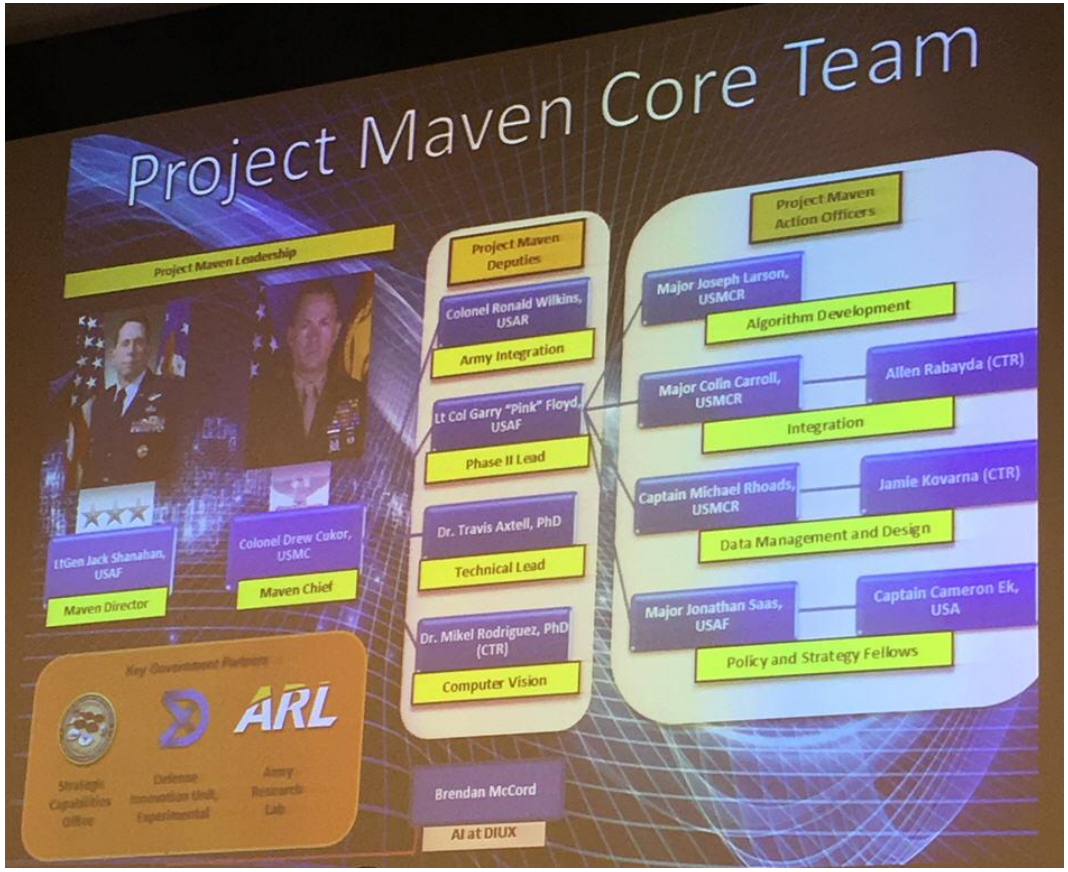
Nuclear Fuel Cycle Cost Calculator The price of power

Doomsday Clock Timeline Conflict, culture, and change 1947

Source: https://thebulletin.org/project-maven-brings-ai-fight-against-isis11374

Project Maven Core Team

"Maven is designed to be that pilot project, that pathfinder, that spark that kindles the flame front of artificial intelligence across the rest of the Department."

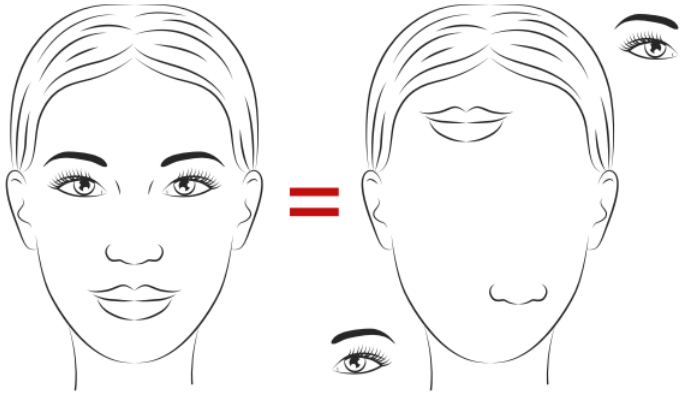


Source: https://ssrn.com/abstract=3167035

With Great Power Comes Great Responsibility

- Maven's success is clear proof that AI-ML-DL is ready to revolutionize many national security missions even if DoD is not yet ready for the organizational, ethical, and strategic implications of that revolution.
- Having met sky-high expectations of the DoD, it's likely to spawn 100 copycat 'Mavens' in ISR.
- "I don't think honestly there is any aspect of Department that is not ripe for introducing some type of AI and machine learning into it."
- "Convolutional Neural Networks are doomed" – Geofferey Hinton

THE CAPCO INSTITUTE
JOURNAL
OF FINANCIAL TRANSFORMATION



Conditional Optimism & Artificial Intelligence

- "By this I mean that, if humanity successfully navigates the technical, ethical and political challenges of developing and diffusing powerful AI technologies, AI may have enormous and potentially very positive impact on humanity's wellbeing."

- "To justify this conclusion, I first review the characteristic, powerful AI's can in principle be given nearly **any goal** (Bostrom, 2014), which is a source of both **risk** and **opportunity**. Finally, both in narrows domains today and in intelligent decision-making more broadly over the long term, AI can exceed human performance, opening up the opportunity of directing large numbers of fast, competent systems to the achievement of nearly **arbitrary goals**."

Should we fear artificial intelligence?

Source: http://www.europarl.europa.eu/RegData/etudes/IDAN/2018/614547/EPRS_IDA(2018)614547_EN.pdf

Conditions For Success

- "There are myriad possible **malicious uses** of AI (Brundage and Avin et al., 2018) and many ways in which it might be used in a harmful manner unintentionally, such as with algorithmic bias (Kirkpatrick, 2016)."

- "The **control problem** will have to be addressed-that is, we will need to learn how to ensure that AI systems achieve the goals we want them to (Bostrom, 2014: Bostrom, Dafoe and Flynn, 2017) without causing harm during their learning process, misinterpreting what is desired of them, or resisting human **control**."

- "**Solving the control problem is a critical prerequisite** over the long term in order for more powerful AI systems to have positive impacts on society."

- "The political challenges of AI will have to be successfully navigated, including risk associated with the undue concentration of power and wealth (Bostrom, et al. 2017) and risky development races that encourage inattention to safety in order to gain an advantage (Armstrong et al., 2016; Bostrom, 2017)."

Source: http://www.europarl.europa.eu/RegData/etudes/IDAN/2018/614547/EPRS_IDA(2018)614547_EN.pdf

What Will A Super intelligent AI Decide To Do?

- "So let us further imagine that the super intelligent AI is no longer boxed in, but able to freely roam the Internet (including the internet of things), to create numerous back up copies of itself, to use it's superior intelligence to walk through (or past) whatever firewalls come in its way, and so on."

- "We are then no longer in control, and the future **survival and well-being of humanity** will depend on **what the machine chooses to do so**. So what will it decide to do? This depends on what the **goals** are. **Predicting that is not an easy task**, and any discussion about this has to be speculative at least to some degree."

Should we fear artificial intelligence?

Source: http://www.europarl.europa.eu/RegData/etudes/IDAN/2018/614547/EPRS_IDA(2018)614547_EN.pdf

Why Can't We Use Math To Make AIs

- "We do use a lot of clever maths and because of this some Machine Learning methods produce predictable results, enabling us to understand exactly what these AIs can and cannot do. However, most practical solutions are unpredictable, because they are so complex and they may use randomness within their algorithms meaning that our mathematics cannot cope, and because they often receive unpredictable inputs. While we do not have mathematics to predict the capabilities of a new AI, we do have mathematics that tells us about the limits of computation."

- "The second law of AI tell us that resources are not enough. *We still have to design new algorithms and structures within (and in support of) the AI's, for every new challenge that the AI faces.* "

- "It is for these reasons *that we cannot create general purpose intelligences using a single approach.* There is no single AI on the planet (not even the fashionable "Deep Learning") that can use the same method to process speech, drive a car, learn how to play a complex video game, control a robot to run along a busy city street, wash dishes in a sink, and plan a strategy to achieve investment for a company."

Source: http://www.europarl.europa.eu/RegData/etudes/IDAN/2018/614547/EPRS_IDA(2018)614547_EN.pdf

AI, Machine Learning, Deep Learning, and, Neural Networks

AI for Automation & Optimization

"a computer can make an error in a minute that can take years for humans to correct"

Relationship Security-Convenience
(Figure 1-2)

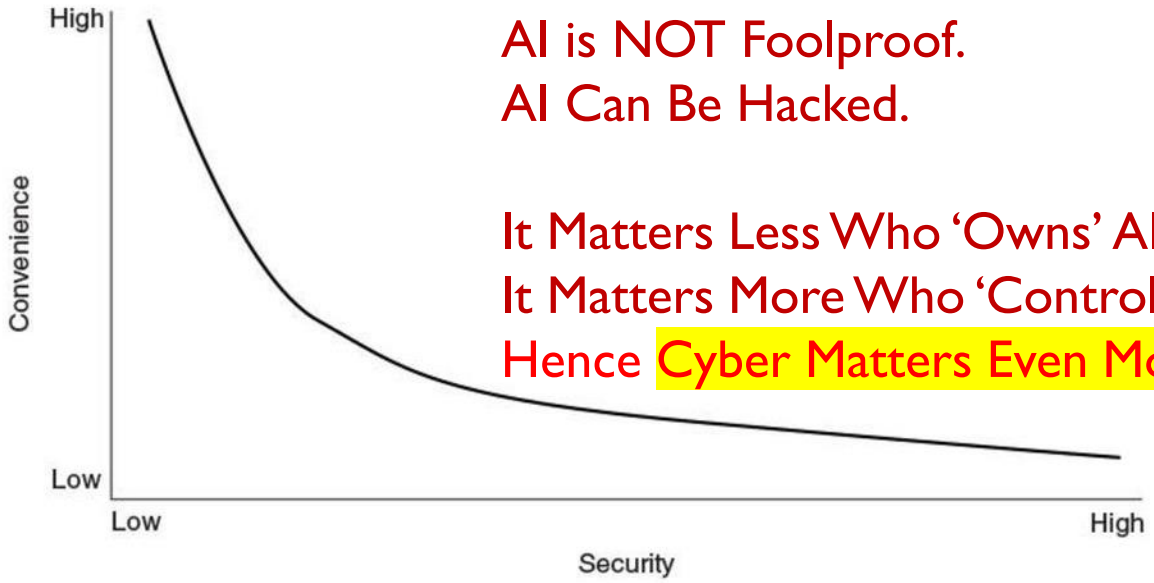


Figure 1-2 Relationship of security to convenience

Security+ Guide to Network Security Fundamentals, Fifth Edition 14

AI is NOT Foolproof.
AI Can Be Hacked.

It Matters Less Who 'Owns' AI
It Matters More Who 'Controls' AI
Hence Cyber Matters Even More!

Security Costs Convenience

The Dark Secret of AI: It Can Fail!

Intelligent Machines

AI is sending people to jail—and getting it wrong

Source: https://www.technologyreview.com/s/612775/algorithms-criminal-justice-ai/

Using historical data to train risk assessment tools could mean that machines are copying the mistakes of the past.

Past is NOT Future.
Correlation is NOT Causation.

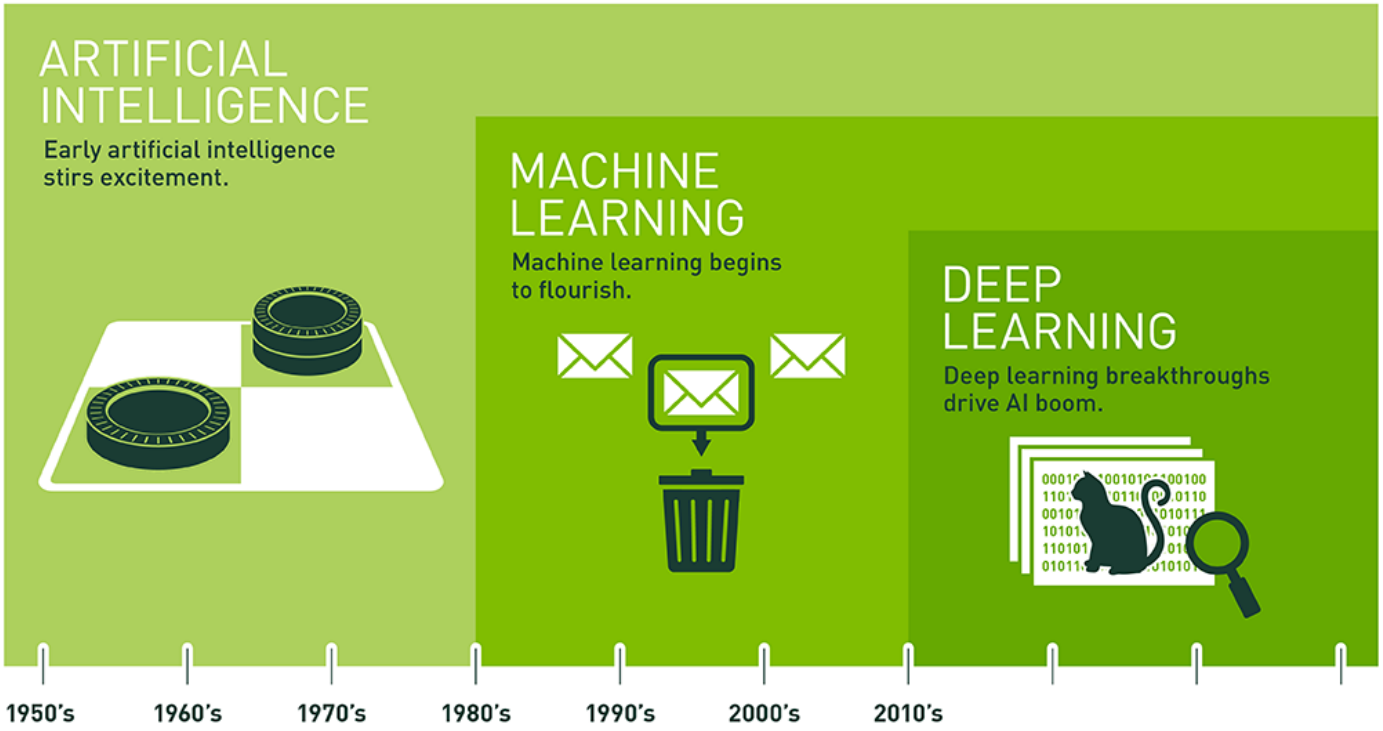
An algorithm can determine the trajectory of your life. Police departments use **predictive algorithms** to strategize about **where to send their ranks**. Law enforcement agencies use **face recognition systems** to help **identify suspects**. These practices have garnered well-deserved scrutiny for **whether they in fact improve safety or simply perpetuate existing inequities**. Researchers and civil rights advocates, for example, have repeatedly demonstrated that **face recognition systems can fail spectacularly**, particularly for dark-skinned individuals—even mistaking members of Congress for convicted criminals.

But the **most controversial tool** by far comes after police have made an arrest. Say hello to **criminal risk assessment algorithms**.

Modern-day **risk assessment tools** are often driven by **algorithms** trained on **historical crime data**.

Deep Learning in a Nutshell

- AI: Labeling, Machine Learning: Learning from Data Examples

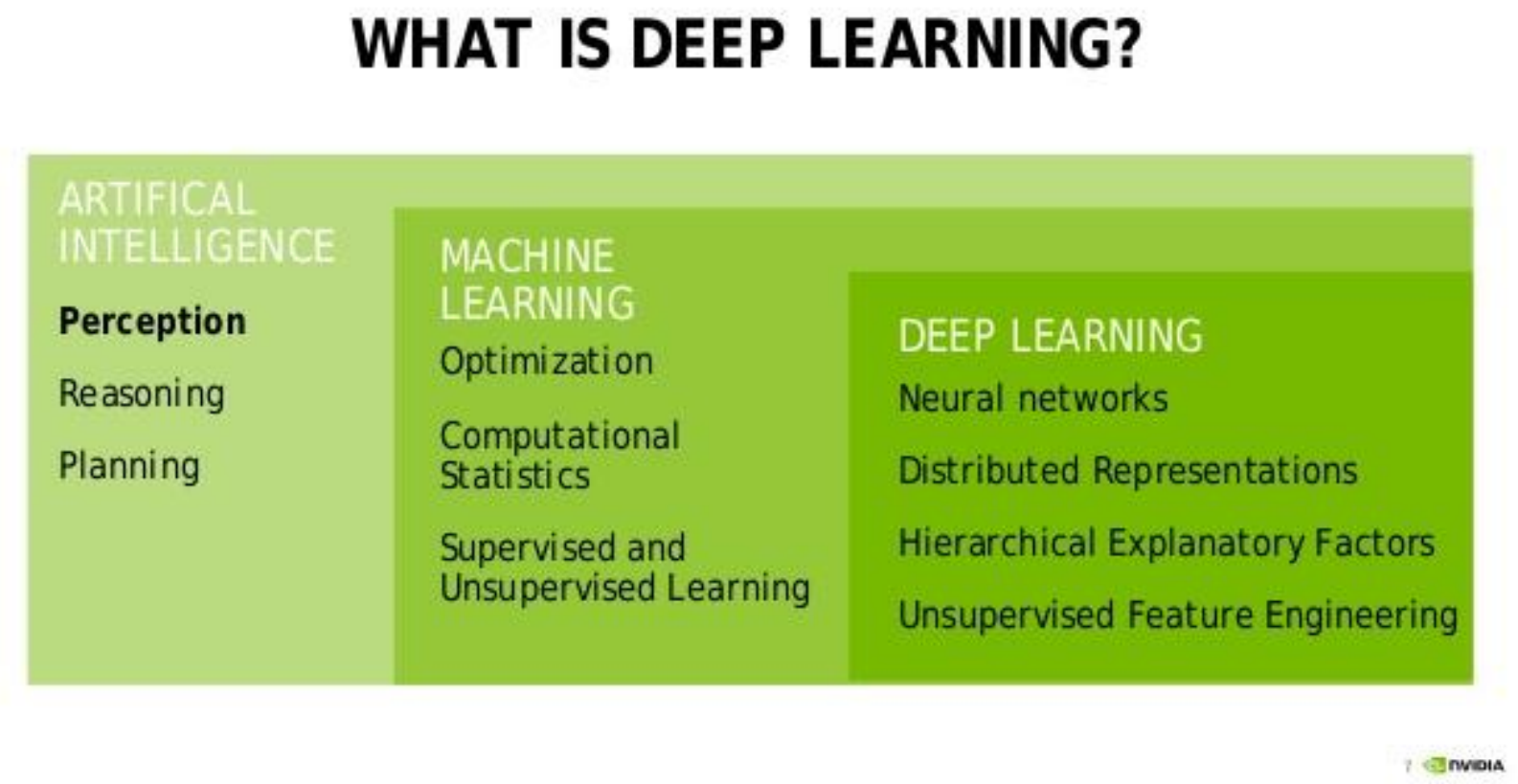


Since an early flush of optimism in the 1950s, smaller subsets of artificial intelligence – first machine learning, then deep learning, a subset of machine learning – have created ever larger disruptions.

Source: https://blogs.nvidia.com/blog/2016/07/29/whats-difference-artificial-intelligence-machine-learning-deep-learning-ai/

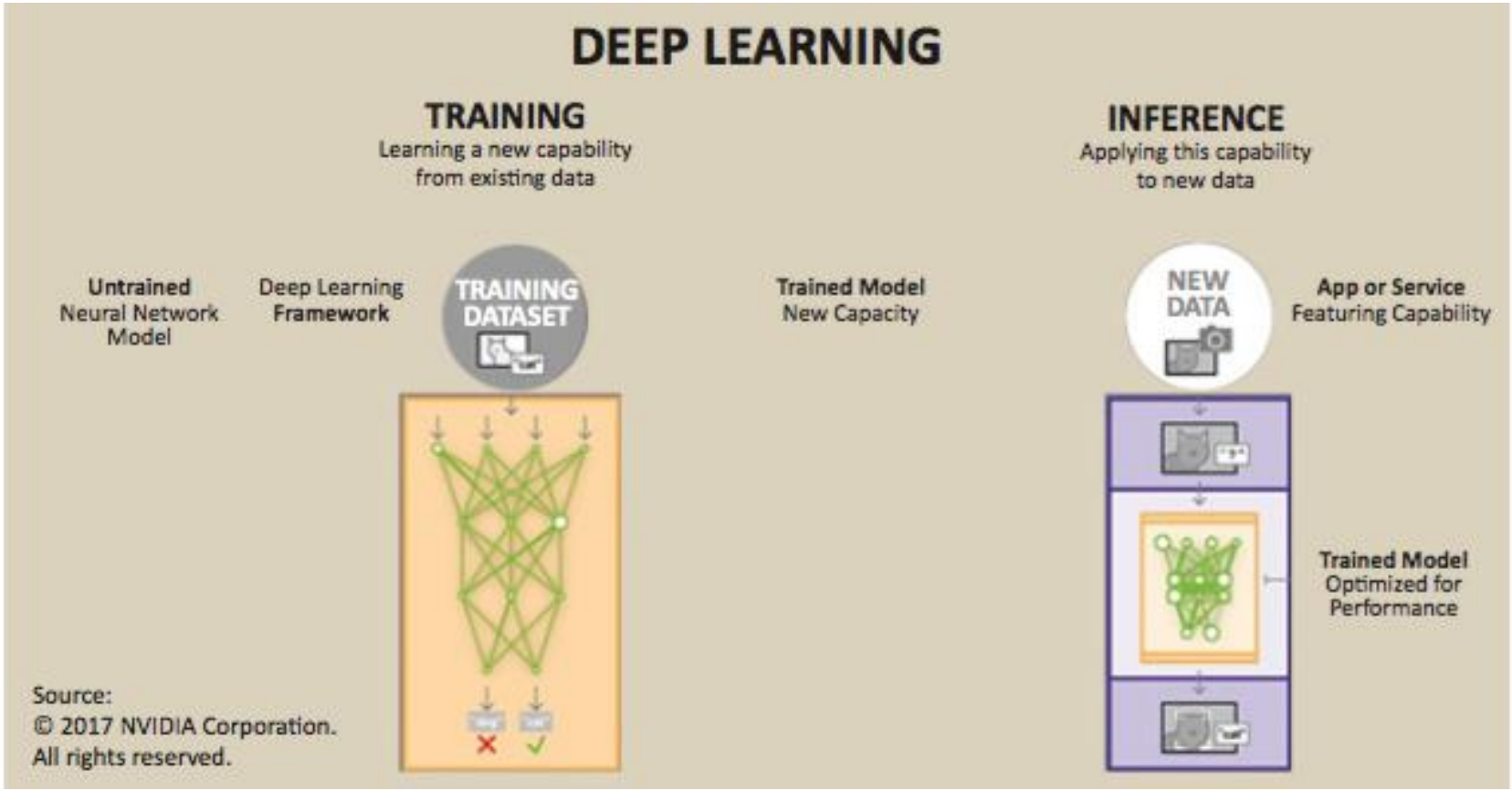
Deep Learning in a Nutshell

- AI: Labeling, Machine Learning: Learning from Data Examples



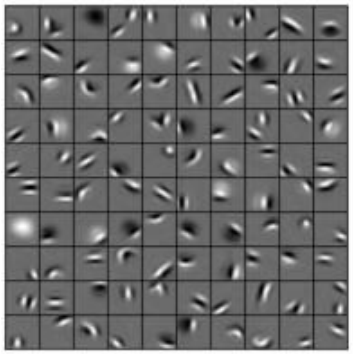
Deep Learning in a Nutshell

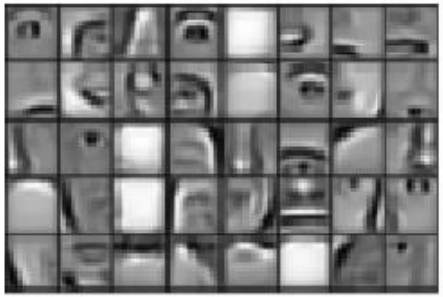
- AI: Labeling, Machine Learning: Learning from Data Examples



Deep Learning in a Nutshell

- AI: Labeling, Machine Learning: Learning from Data Examples
- Deep Learning: Number of Layers of Neural Networks

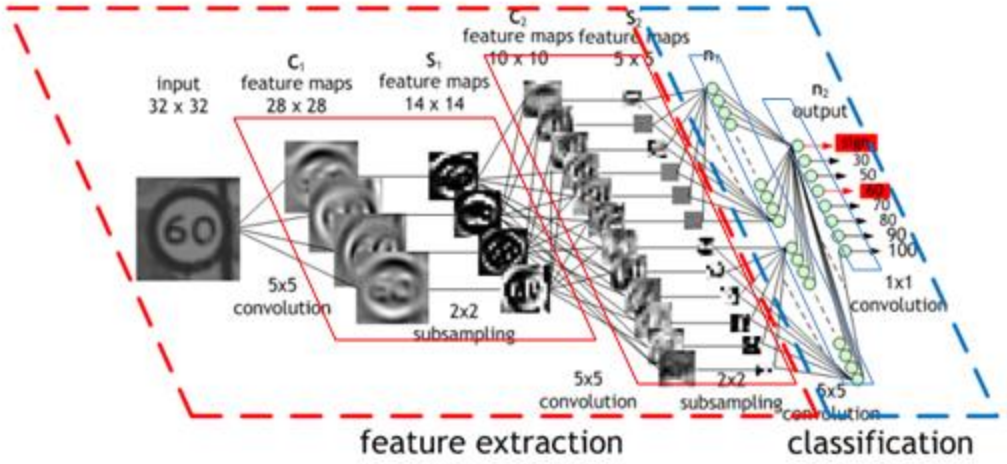




consolidation

Low to Hi

CORNERS
EDGES
BLOBS
OBJECTS



Source: https://devblogs.nvidia.com/deep-learning-nutshell-core-concepts/

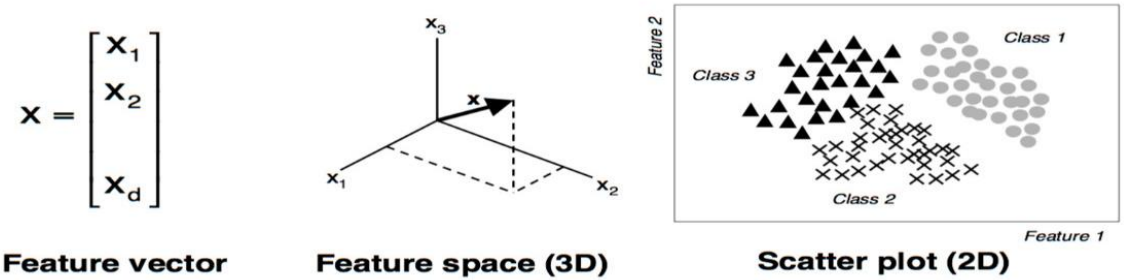
How Convolutional Neural Networks Work

- DATA POINT: FEATURE: e.g. Black or White (0 or 1)

Source: https://distill.pub/2018/building-blocks/

How Convolutional Neural Networks Work

- ARRAY: FEATURE VECTOR



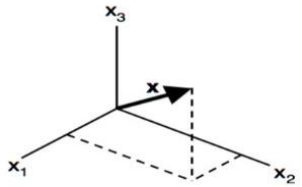
Source: https://distill.pub/2018/building-blocks/

How Convolutional Neural Networks Work

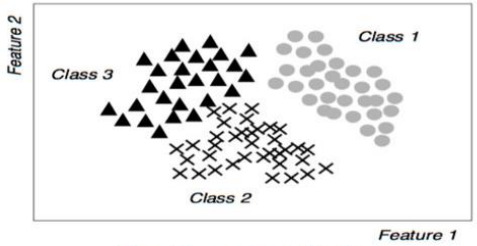
- PLANE: FEATURE MAP

$$x = \begin{bmatrix} x_1 \\ x_2 \\ \\ x_d \end{bmatrix}$$

Feature vector



Feature space (3D)



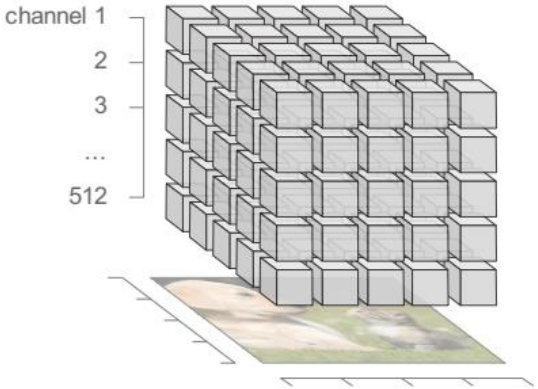
Scatter plot (2D)

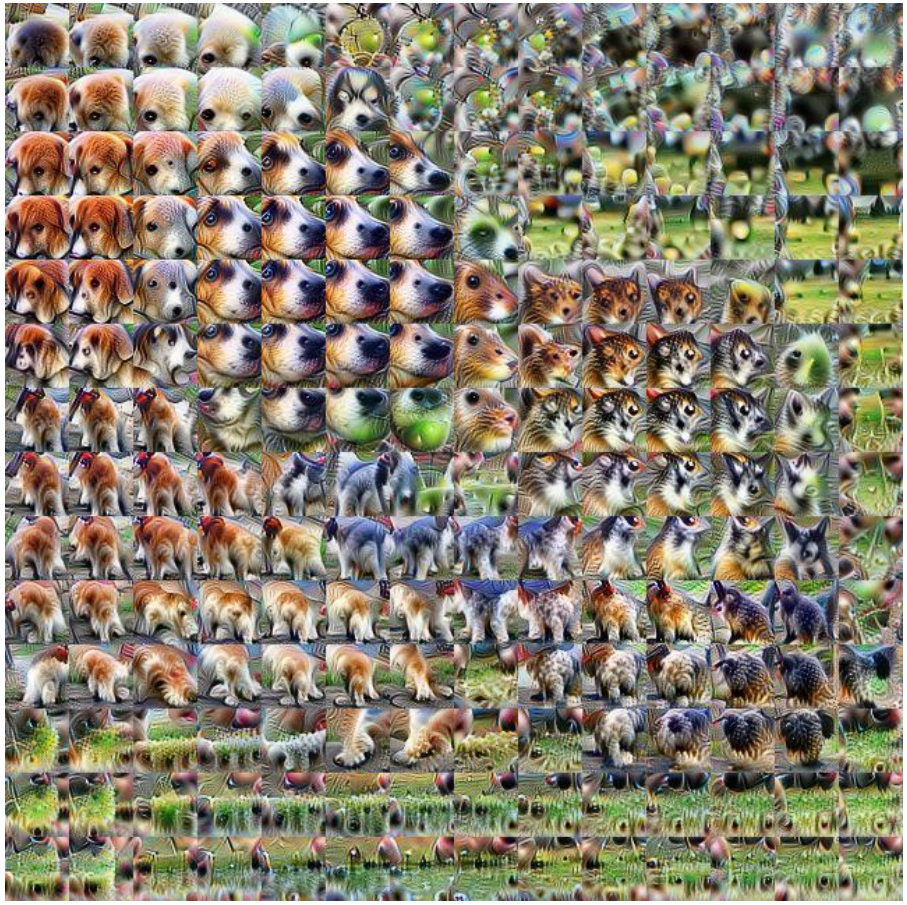
Source: https://distill.pub/2018/building-blocks/

How Convolutional Neural Networks Work

CUBE: STACKED FEATURE MAP

- The Building Blocks of Interpretability
- Interpretability techniques are normally studied in isolation. We explore the powerful interfaces that arise when you combine them and the rich structure of this combinatorial space.





Source: https://distill.pub/2018/building-blocks/

How Convolutional Neural Networks Work

- OBJECTS in the Images

Labrador retriever and tiger cat

- Several floppy ear detectors seem to be important when distinguishing dogs, whereas pointy ears are used to classify "tiger cat".
- The Building Blocks of Interpretability
- Interpretability techniques are normally studied in isolation.
- We explore the powerful interfaces that arise when you combine them and the rich structure of this combinatorial space

Source: https://distill.pub/2018/building-blocks/

Why Model Risk Management is Crucial to Robust AI-ML-DL Use

What Caused the Failure of the Systems?

What are the Key Systems That Failed?

Perfect Weather Conditions and Perfect Road Conditions in AZ

Source: https://ssrn.com/abstract=3167035

- What Would Happen in the "Typical" "Zero-Visibility" Winter Weather in Central NY?
- When 65 MPH I-90 "Thruway" Traffic Drives 'Normally' in Day at 10 MPH for Safety
- Or When All Traffic is Off the 65 MPH I-90 "Thruway" as it's Frozen

Model Risks, Black Swans, Extreme Events

“Not everything that counts can be counted, and not everything that can be counted counts."

"If you give a pilot an altimeter that is sometimes defective he will crash the plane. Give him nothing and he will look out the window. Technology is only safe if it is flawless.”
NNT

Source: https://ssrn.com/abstract=3167035

"As far as the laws of mathematics refer to reality, they are not certain, and as far as they are certain, they do not refer to reality."

The Dark Secret of AI: It Can Fail!

No one really knows HOW [or WHY] the most advanced algorithms do what they do.

The Dark Secret at the Heart of AI

Intelligent Machines

The Dark Secret at the Heart of AI

No one really knows how the most advanced algorithms do what they do. That could be a problem.

by **Will Knight** Apr 11, 2017

The mysterious mind of this vehicle points to a looming issue with artificial intelligence. The car's underlying AI technology, known as deep learning, has proved very powerful at solving problems in recent years, and it has been widely deployed for tasks like image captioning, voice recognition, and language translation. There is now hope that the same techniques will be able to diagnose deadly diseases, make million-dollar trading decisions, and do countless other things to transform whole industries.

But this won't happen—or shouldn't happen—unless we find ways of making techniques like deep learning more **understandable** to their creators and **accountable** to their users. **Otherwise it will be hard to predict when failures might occur—and it's inevitable they will.**

EXPLAINABILITY INTERPRETABILITY: **HOW?**
CAUSALITY (MOST CHALLENGING): **WHY?**

Source: https://www.technologyreview.com/s/604087/the-dark-secret-at-the-heart-of-ai/

‘Way We’re Doing Computer Vision is Wrong’

"a young boy is holding a baseball bat."

bad-data-**achilles-heel**-of-artificial-intelligence

Do you see a baseball bat?

Source: https://breakingdefense.com/2018/11/big-bad-data-achilles-heel-of-artificial-intelligence/
https://cacm.acm.org/magazines/2016/1/195740-seeing-more-clearly/abstract

‘Way We’re Doing Computer Vision is Wrong’

- If you want to blame someone for the hoopla around artificial intelligence, 69-year-old Google researcher Geoff Hinton is a good candidate. The droll University of Toronto professor jolted the field onto a new trajectory in October 2012.
- Hinton showed that an unfashionable technology he’d championed for decades called artificial neural networks permitted a huge leap in machines’ ability to understand images. Today neural networks transcribe our speech, recognize our pets, and fight our trolls.
- “I think the way we’re doing computer vision is just wrong,” he says. “It works better than anything else at present but that doesn’t mean it’s right.”

Google’s AI Wizard Unveils a New Twist on Neural Networks

TOM SIMONITE BUSINESS 11.01.17 07:00 AM

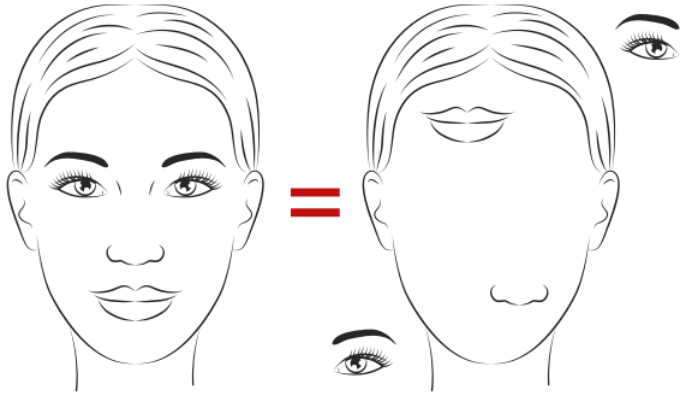
GOOGLE’S AI WIZARD UNVEILS A NEW TWIST ON NEURAL NETWORKS

AARON VINCENT ELKAIM/REDUX

Source: https://www.wired.com/story/googles-ai-wizard-unveils-a-new-twist-on-neural-networks/

Convolutional Neural Networks Are 'Doomed'

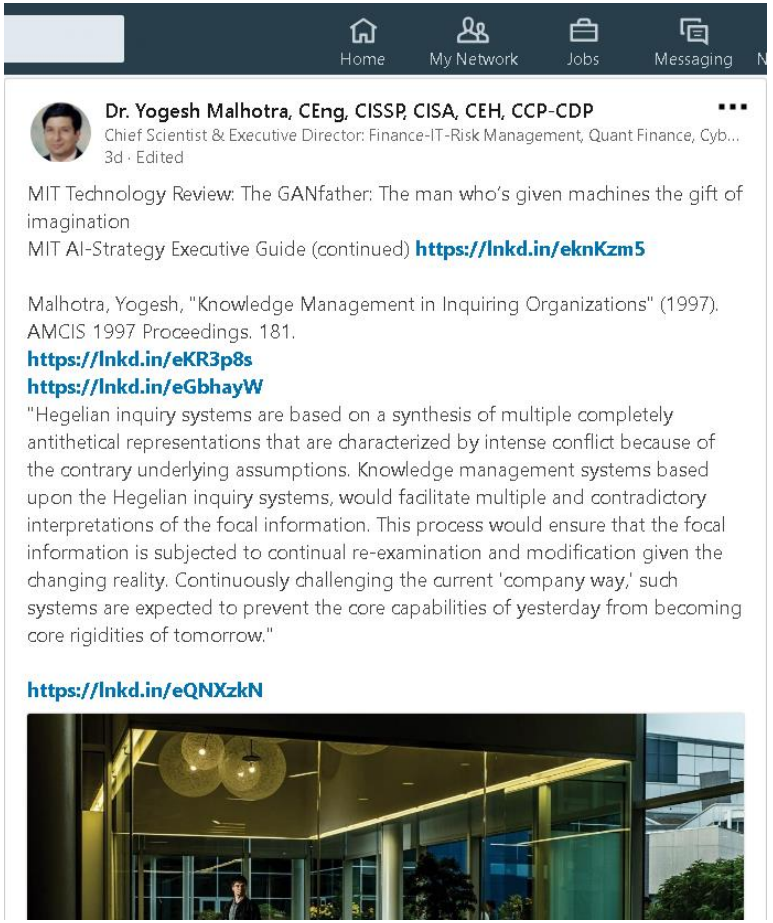
- "Imagine a face. What are the components? We have the face oval, two eyes, a nose and a mouth. For a CNN, a mere presence of these objects can be a very strong indicator to consider that there is a face in the image."
- "Orientation-al and relative spatial relationships between these components are not very important to a CNN."
- Internal data representation of a convolutiona neural network does not take into account important spatial hierarchies between simple and complex objects.
- "As far as the laws of mathematics refer to reality, they are not certain, and as far as they are certain, they do not refer to reality."
- "Certainly the statement 2 x (1/2) = 1 is arithmetically correct. But do two half-sheets of paper make one whole sheet and do two half-shoes make one whole shoe?" – Morris Kline



Source: https://medium.com/ai%C2%B3-theory-practice-business/understanding-hintons-capsule-networks-part-i-intuition-b4b559d1159b

Faking Voices and Videos with GANs

- DARPA's technologists are especially concerned about a relatively new AI technique that could make AI fakery almost impossible to spot automatically.
- Using what are known as generative adversarial networks, or GANs, it is possible to generate stunningly realistic artificial imagery.
- A GAN consists of two components. The first, known as the "actor" or "generator," tries to learn the statistical patterns in a data set, such as a set of images or videos, and then generate convincing synthetic pieces of data.
- The second, called the "critic" or "discriminator," tries to distinguish between real and fake examples.
- Feedback from the critic enables the actor to produce evermore-realistic examples.
- And because GANs are designed to outwit an AI system already, it is unclear if any automated system could catch them.



Source: https://www.technologyreview.com/s/611146/the-us-military-is-funding-an-effort-to-catch-deepfakes-and-other-ai-trickery/

Five emerging cyber-threats to worry about

MIT Technology Review

EXPLOITING AI-GENERATED FAKE VIDEO AND AUDIO

It's now possible to create fake video and audio messages that are incredibly difficult to distinguish from the real thing. These "**deepfakes**" could be a boon to hackers in a couple of ways. AI-generated "phishing" e-mails that aim to trick people into handing over passwords and other sensitive data have already been shown to be more effective than ones generated by humans. Now hackers will be able to throw highly realistic fake video and audio into the mix, either to reinforce instructions in a phishing e-mail or as a standalone tactic.

POISONING AI DEFENSES

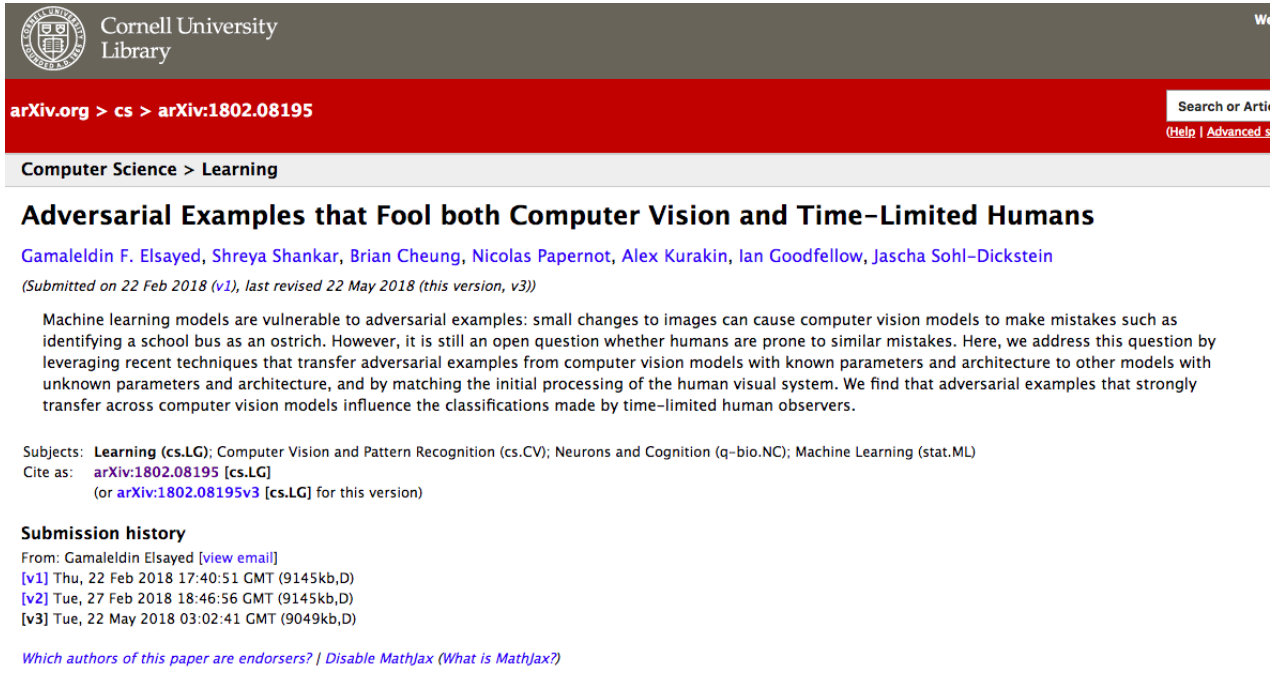
Security companies have rushed to embrace AI models as a way to help anticipate and detect cyberattacks. However, sophisticated hackers could try to corrupt these defenses. In the hands of the wrong people, it's also AI that's going to generate the most sophisticated attacks.

GANs can be used to try to guess what algorithms defenders are using in their AI models. Another risk is that hackers will target data sets used to train models and poison them—for instance, by switching labels on samples of malicious code to indicate that they are safe rather than suspect.

Source: https://www.technologyreview.com/s/612713/five-emerging-cyber-threats-2019/

AI-ML Models are Vulnerable to Adversarial Examples

- "Machine learning models are vulnerable to adversarial examples: small changes to images can cause computer vision models to make mistakes such as identifying a school bus as an ostrich. However, it is still an open question whether humans are prone to similar mistakes."



Cornell University Library

arXiv.org > cs > arXiv:1802.08195

Search or Arti

(Help | Advanced s

Computer Science > Learning

Adversarial Examples that Fool both Computer Vision and Time-Limited Humans

Gamaleldin F. Elsayed, Shreya Shankar, Brian Cheung, Nicolas Papernot, Alex Kurakin, Ian Goodfellow, Jascha Sohl-Dickstein

(Submitted on 22 Feb 2018 (v1), last revised 22 May 2018 (this version, v3))

Machine learning models are vulnerable to adversarial examples: small changes to images can cause computer vision models to make mistakes such as identifying a school bus as an ostrich. However, it is still an open question whether humans are prone to similar mistakes. Here, we address this question by leveraging recent techniques that transfer adversarial examples from computer vision models with known parameters and architecture to other models with unknown parameters and architecture, and by matching the initial processing of the human visual system. We find that adversarial examples that strongly transfer across computer vision models influence the classifications made by time-limited human observers.

Subjects: **Learning (cs.LG)**; Computer Vision and Pattern Recognition (cs.CV); Neurons and Cognition (q-bio.NC); Machine Learning (stat.ML)
Cite as: arXiv:1802.08195 [cs.LG]
(or arXiv:1802.08195v3 [cs.LG] for this version)

Submission history

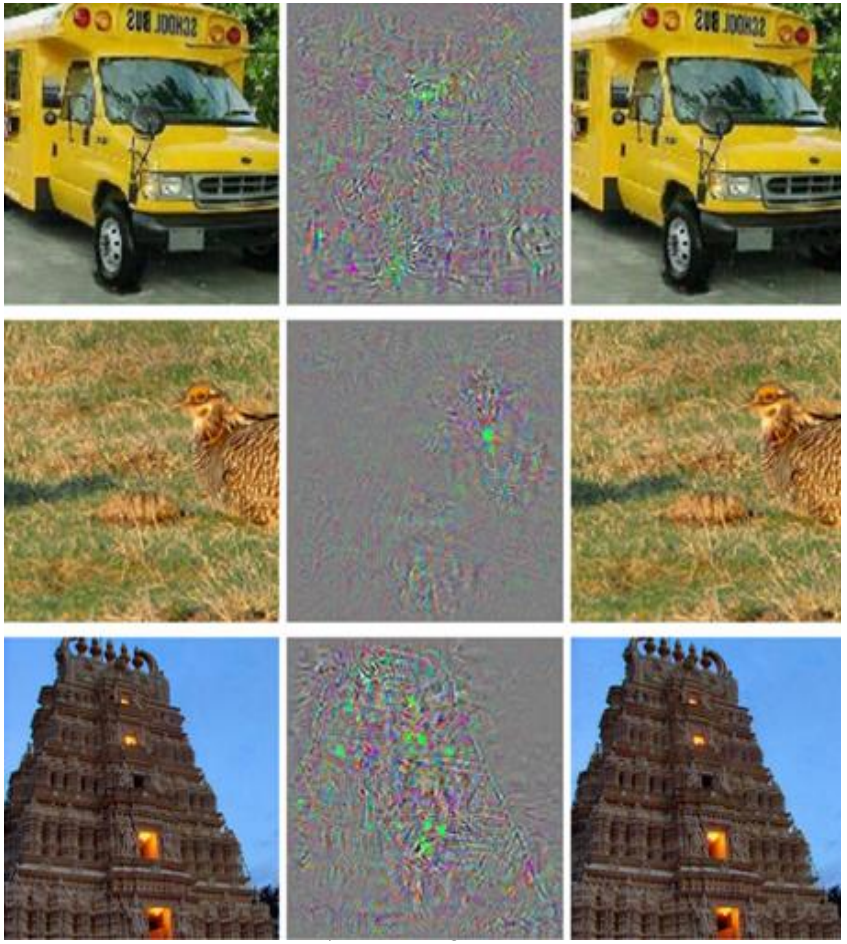
From: Gamaleldin Elsayed [view email]
[v1] Thu, 22 Feb 2018 17:40:51 GMT (9145kb,D)
[v2] Tue, 27 Feb 2018 18:46:56 GMT (9145kb,D)
[v3] Tue, 22 May 2018 03:02:41 GMT (9049kb,D)

Which authors of this paper are endorsers? | Disable MathJax (What is MathJax?)

Source: https://arxiv.org/abs/1802.08195

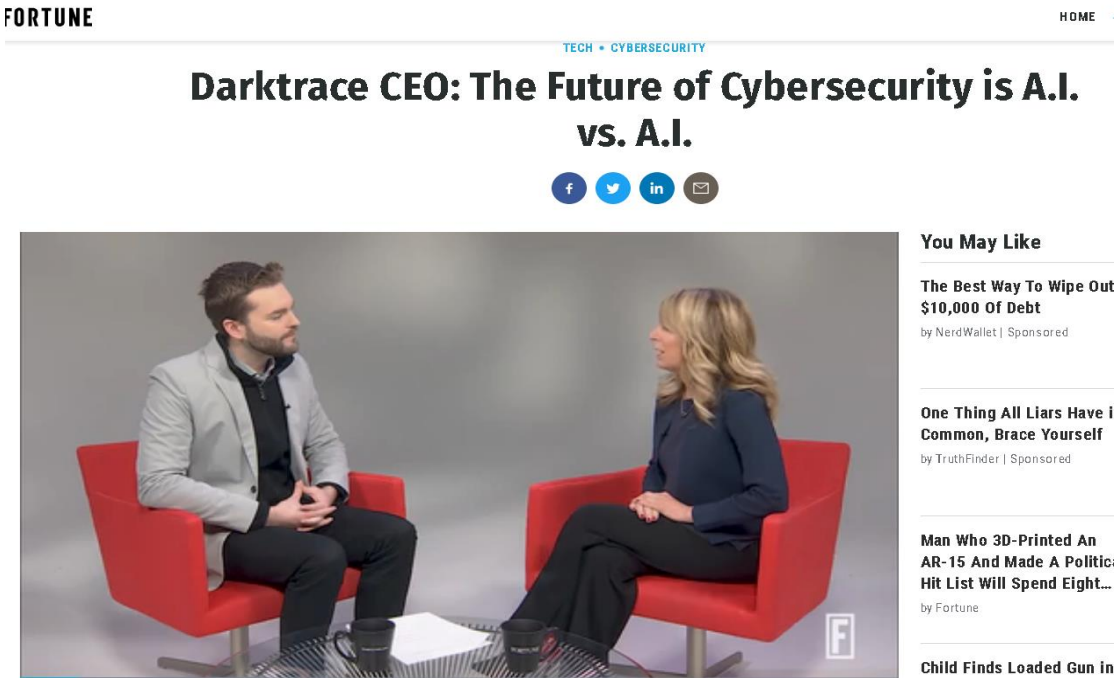
AI-ML Models are Vulnerable to Adversarial Examples

- "Images on the Right are slightly distorted versions of the images on the Left."
- "The difference between Left and Right set of images is imperceptible to the human eye."
- "However, where human eye sees the same object on the Right, the Convolutional Neural Network sees an ostrich for all the three images."



Source: https://arxiv.org/abs/1802.08195

AI-ML Models are Vulnerable to Adversarial Examples



FORTUNE

HOME

TECH • CYBERSECURITY

Darktrace CEO: The Future of Cybersecurity is A.I. vs. A.I.

You May Like

The Best Way To Wipe Out $10,000 Of Debt
by NerdWallet | Sponsored

One Thing All Liars Have i Common, Brace Yourself
by TruthFinder | Sponsored

Man Who 3D-Printed An AR-15 And Made A Politic Hit List Will Spend Eight...
by Fortune

Child Finds Loaded Gun in

Darktrace last year warned an A.I. committee organized by Britain's House of Lords that A.I.-aided attackers could learn to imitate people's writing styles in order to craft more effective phishing attacks, phony messages that aim to dupe their recipients. Dave Palmer, director of technology Darktrace and author of the parliamentary submission, noted at the time that even hackers with no understanding of A.I. techniques could get up to speed and cause havoc in a matter of months.

Source: http://fortune.com/2019/03/15/cybersecurity-ai-darktrace-ceo/

AI-ML Models are Vulnerable to Adversarial Examples

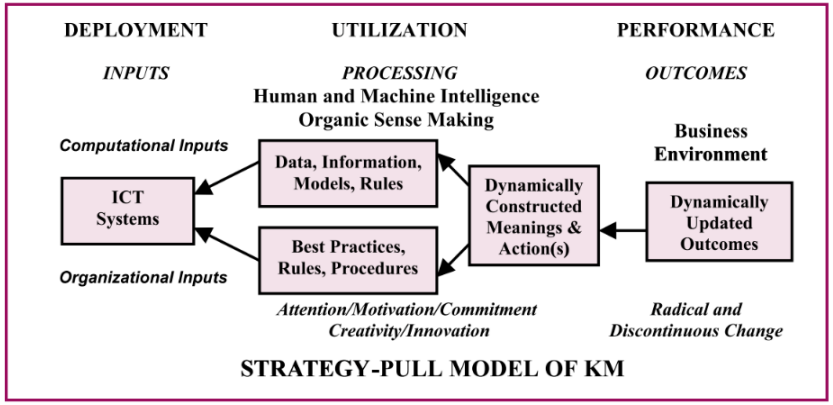
Source: https://www.welivesecurity.com/2019/02/22/ml-era-cybersecurity-step-toward-safer-world-brink-chaos/

AI-ML has No 'Common Sense'…
No 'Sense Making'…No Sense of 'Meaning'…

- Patrick Winston, a professor of AI and computer science at MIT, says it would be more helpful to describe the developments of the past few years as having occurred in "computational statistics" rather than in AI.

- A leading researcher in the field, Yann LeCun, Facebook's director of AI, said at a Future of Work conference at MIT in November that machines are far from having "the essence of intelligence." That includes the ability to understand the physical world well enough to make predictions about basic aspects of it—to observe one thing and then use background knowledge to figure out what other things must also be true.

- Another way of saying this is that machines don't have common sense. "The computer that wins at Go is analyzing data for patterns. It has no idea it's playing Go as opposed to golf, or what would happen if more than half of a Go board was pushed beyond the edge of a table… "



Malhotra, Y., Integrating Knowledge Management Technologies in Organizational Business Processes: Getting Real Time Enterprises to Deliver Real Business Performance, Journal of Knowledge Management, Vol. 9, Issue 1, April 2005, 7-28.

MIT AI-Machine Learning Executive Guide: including Deep Learning, Natural Language Processing, Autonomous Cars, Robotic Process Automation

Published on February 13, 2018 Edit article | View stats

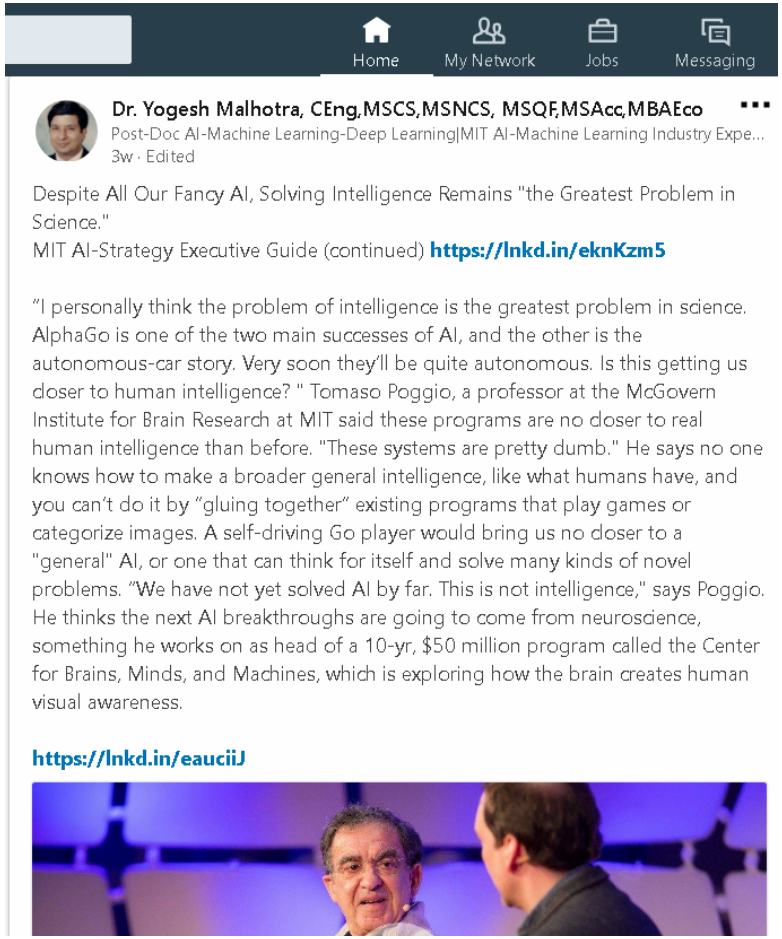
Source: https://www.linkedin.com/pulse/dear-ceo-ai-machine-learning-advice-top-industry-leading-malhotra/

This is Not Intelligence

- "I personally think the problem of intelligence is the greatest problem in science. AlphaGo is one of the two main successes of AI, and the other is the autonomous-car story. Very soon they'll be quite autonomous. Is this getting us closer to human intelligence? " Tomaso Poggio, a professor at the McGovern Institute for Brain Research at MIT said these programs are no closer to real human intelligence than before. "These systems are pretty dumb."

- He says no one knows how to make a broader general intelligence, like what humans have, and you can't do it by "gluing together" existing programs that play games or categorize images. A self-driving Go player would bring us no closer to a "general" AI, or one that can think for itself and solve many kinds of novel problems.

- "We have not yet solved AI by far. This is not intelligence," says Poggio. He thinks the next AI breakthroughs are going to come from neuroscience, something he works on as head of a 10-yr, $50 million program called the Center for Brains, Minds, and Machines, which is exploring how the brain creates human visual awareness.



Source: https://www.technologyreview.com/s/609330/despite-all-of-our-fancy-ai-solving-intelligence-remains-the-greatest-problem-in-science/

Need for "Human-Centered AI", 2019 Mar 13

Artificial Intelligence / Voice assistants

The man who helped invent virtual assistants thinks they're doomed without a new AI approach

Boris Katz has spent his career trying to help machines master language. He believes that current AI techniques aren't enough to make Siri or Alexa truly smart.

by **Will Knight** Mar 13

What do you make of Siri, Alexa, and other personal assistants?

...These programs are so incredibly stupid. So there's a feeling of being proud and being almost embarrassed. You launch something that people feel is intelligent, but it's not even close.

What is a better approach?

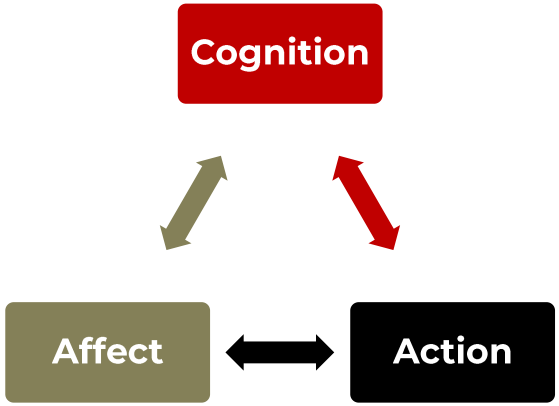
One way forward is to **gain a greater understanding of human intelligence** and then use that understanding in order to create intelligent machines. AI research needs to build on ideas from **developmental psychology, cognitive science, and neuroscience**, and **AI models ought to reflect what is already known about how humans learn and understand the world**.

Source: https://www.technologyreview.com/s/612826/virtual-assistants-thinks-theyre-doomed-without-a-new-ai-approach/

We Pioneered the "Better Approach…" 25-Years Ago… The '**Human Centered AI**'

- Inspired by the Artificial Intelligence Pioneer, Dr. John Holland, University of Michigan Computer Scientist & Psychologist, then at the Santa Fe Institute (1995)
- Missing "**MEANING**" in Claude Shannon's Information Theory
- Our Path-Breaking Discovery was in Solving the Problem of Missing "MEANING" in Information Theory posed by John Holland
- First IT-MIS Papers on "MEANING" in AI-ML-KM Systems
- Inspired by another AI Pioneer who was a Psychiatry Pioneer too.
- Caught Attention of Both NSA and CIA on Publication.

Malhotra, Y., Expert Systems for Knowledge Management: Crossing the Chasm between Information Processing and Sense Making, Expert Systems with Applications: An International Journal, 20(1), 7-16, 2001.
http://www.brint.org/expertsystems.pdf
Original R&D:
http://www.yogeshmalhotra.com/publications.html
Latest R&D: https://papers.ssrn.com/author_id=2338267



A Knowledge Management Framework for MRM

One way forward is to **gain a greater understanding of human intelligence** and then use that understanding in order to create intelligent machines. AI research needs to build on ideas from **developmental psychology, cognitive science, and neuroscience**, and **AI models ought to reflect what is already known about how humans learn and understand the world**.

Above R&D Reference: Download Papers from here:
http://www.YogeshMalhotra.com/publications.html

"Human-Centered AI" & 'AI Augmentation'

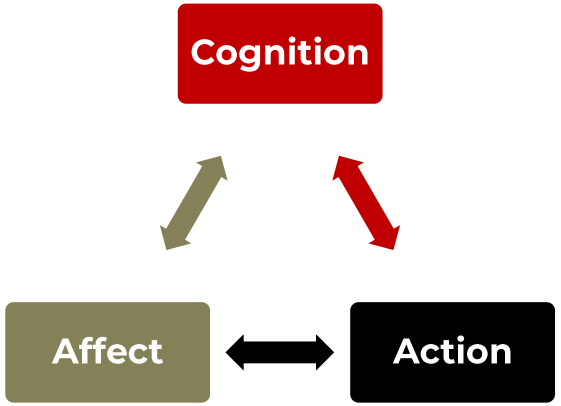
- Inspired by AI Pioneer, Dr. John Holland, University of Michigan Computer Scientist & Psychologist, then at Santa Fe Institute (1995)
- Missing "**MEANING**" in Claude Shannon's Information Theory
- Our Path-Breaking Discovery was in Solving the Problem of Missing "MEANING" in Information Theory posed by John Holland
- First IT-MIS Papers on "MEANING" in AI-ML-KM Systems
- Inspired by another AI Pioneer who was a Psychiatry Pioneer too.
  - George Kelly, Founder of Personal Construct Theory & Repertory Grids
- Caught Attention of Both NSA and CIA on Publication.

IQ
EQ
Do-Q

Malhotra, Y., Expert Systems for Knowledge Management: Crossing the Chasm between Information Processing and Sense Making, Expert Systems with Applications: An International Journal, 20(1), 7-16, 2001.
http://www.brint.org/expertsystems.pdf

Original R&D:
http://www.yogeshmalhotra.com/publications.html

Latest R&D: https://papers.ssrn.com/author_id=2338267



http://www.brint.com/PCT.htm

Model Risk Management

Advancing Cyber Risk Insurance Underwriting Model Risk Management Beyond VaR To Pre-empt and Prevent The Forthcoming Global Cyber Insurance Crisis

- Model use entails model risk (Derman, 1996; Morini, 2011) because a statistical model is used for risk estimation.
- The problem of model risk for any risk model such as VaR results from the fact that risk cannot be measured, but must be estimated using a statistical model (Boucher et al., 2014; Danielsson et al., 2014) .
- Using a range of different plausible models which can be robustly discriminated between, the variance between corresponding range of estimates is a succinct measure of model risk (Danielsson et al., 2014).
- We apply this notion of multi-model comparison of estimates and extend it to multi-methods comparison to manage model risk advancing estimation of cyber risk related loss beyond the limitations of VaR discussed earlier.

Source: https://ssrn.com/abstract=3081492

Model Risk Management in Global Finance

Beyond 'Bayesian vs. VaR' Dilemma to Empirical Model Risk Management: How to Manage Risk (After Risk Management Has Failed) for Hedge Funds

50 Pages • Posted: 16 Dec 2014 • Last revised: 17 Apr 2015

Yogesh Malhotra
Global Risk Management Network, LLC

https://ssrn.com/abstract=2538401

Date Written: December 4, 2014

Abstract

In aftermath of the Financial Crisis, some risk management practitioners advocate wider adoption of Bayesian inference to replace Value-at-Risk (VaR) models for minimizing risk failures (Borison & Hamm, 2010). They claim reliance of Bayesian inference on subjective judgment, the key limitation of Bayesian methodology as underscored by statisticians (Kass & Raftery, 1995; Kruschke, 2011; Lynch, 2007), as the most significant advantage compared with VaR (Christoffersen, 2012). Despite its well-known limitations, just like all other quantitative models (Derman, 1996; Morini, 2011), VaR – [mostly] non-Bayesian and [increasingly] Bayesian – continues to be a key methodological foundation of risk management and regulation related risk modeling practices in global Finance (Danielsson et al., 2014; Zangari, 1996). Bayesian inference modeling and VaR modeling frameworks are outlined to facilitate model risk management (Derman, 1996; Morini, 2011; US Fed & OCC, 2011) for minimizing risk of any model – Bayesian, VaR, or Bayesian VaR. VaR frameworks are empirically applied for hedge fund risk modeling (Darbyshire & Hampton, 2012, 2014) of a multi-asset fund of funds portfolio of a large Wall Street investment bank. Multiple risk models and measures with transparent assumptions to cross-validate convergent findings across multiple levels of risk analysis are examined for empirical model risk management.

Keywords: Model Risk Management, Risk Modeling, Bayesian Inference, VaR, Portfolio Construction, Portfolio Optimization, Fund of Funds, Hedge Funds.

Source: https://ssrn.com/abstract=2538401

Model Risk Management in Cyber Insurance

Stress Testing for Cyber Risks: Cyber Risk Insurance Modeling beyond Value-at-Risk (VaR): Risk, Uncertainty, and, Profit for the Cyber Era

National Association of Insurance Commissioners (NAIC) Expert Paper: Advancing Cyber Risk Insurance Underwriting Model Risk Management beyond VaR to Pre-Empt and Prevent the Forthcoming Global Cyber Insurance Crisis (June 24, 2017)

189 Pages • Posted: 23 Jan 2015 • Last revised: 12 Dec 2017

Yogesh Malhotra
Global Risk Management Network, LLC

Date Written: January 19, 2015

https://ssrn.com/abstract=2553547

Abstract

To avert the impending global Cyber-Finance Insurance Crisis based upon large-scale commercial reliance upon quantitative models with inherent model risks, tail risks, and systemic risks in current form, this post-doctoral thesis makes the following key contributions: Develops the first known Cyber-Finance-Trust™ framework for Cyber insurance modeling; Develops the first known model risk management framework for Cyber insurance modeling; Develops first known analysis of significant and extreme model risks, tail risks, and, systemic risk; Develops multi-method empirical study of VaR and Bayesian inference for containing model risks; Analyzes Markov Chain Monte Carlo for enabling Bayesian inference to minimize model risk; Develops Cyber insurance portfolio framework to minimize model risks, tail risks, systemic risks; Develops framework for Knightian uncertainty management beyond model risk management.

National Association of Insurance Commissioners Expert Paper

Advancing Cyber Risk Insurance Underwriting Model Risk Management beyond VaR to Pre-Empt and Prevent the Forthcoming Global Cyber Insurance Crisis

22 Pages • Posted: 7 Dec 2017 • Last revised: 14 Dec 2017

Yogesh Malhotra
Global Risk Management Network, LLC

Date Written: December 7, 2017

https://ssrn.com/abstract=3081492

Abstract

Mainstream insurance industry practices have adopted Value-at-Risk (VaR) from global financial industry as the pre-dominant cyber insurance model being oblivious to both distinguishing characteristics of cyber-risks as well as statistical properties of VaR. Such widespread misapplication of VaR for cyber risk insurance underwriting unless abated and corrected is expected to lead to a global cyber-insurance crisis that may dwarf the worldwide economic shock from the global financial crisis. Given worldwide high impact of increasingly global cyber-attacks, the current paper advances cyber risk insurance underwriting model risk management beyond VaR to pre-empt and prevent the forthcoming global cyber-insurance crisis.

Note: National Association of Insurance Commissioners Expert Paper: Expert Paper prepared and submitted on the request of the National Association of Insurance Commissioners on June 24, 2017 with latest revision of December 07, 2017. The National Association of Insurance Commissioners (NAIC) is the U.S. standard-setting and regulatory support organization created and governed by the chief insurance regulators from the 50 states, the District of Columbia and five U.S. territories.

Keywords: Network Security, Measurement, Methods, Models, Risk, Uncertainty, Profit, Knight, VaR, Value-at-Risk, Quantitative Finance, Cyber Insurance, Cyber Risk, Cybersecurity

Source: https://ssrn.com/abstract=2538401

Cognitive Computing for Anticipatory Risk Analytics in Intelligence, Surveillance, & Reconnaissance (ISR)

Cognitive Computing for Anticipatory Risk Analytics in Intelligence, Surveillance, & Reconnaissance (ISR): Model Risk Management in Artificial Intelligence & Machine Learning (Presentation Slides)

44 Pages • Posted: 8 Feb 2018

Yogesh Malhotra
Global Risk Management Network, LLC

https://ssrn.com/abstract=3111837

Date Written: January 28, 2018

Abstract

Drawing upon insights shared in the MIT: AI & Machine Learning: Management and Leadership learning community of practice, the current Intelligence, Surveillance, Reconnaissance (ISR) presentation advances the focus on "collective intelligence of people and computers" in the context of Cognitive Computing for Anticipatory Risk Analytics in Intelligence, Surveillance, & Reconnaissance (ISR). It defines as well as distinguishes multi-level Cognitive Computing process engineering frameworks of Artificial Intelligence (AI) & Machine Learning as applied in KM practices of US and worldwide firms, governments, and ISR agencies from Cognitive-Neuromorphic Chips. A recent IEEE Spectrum report also published as "The Neuromorphic Chip's Make-or-Break Moment" observes that "Neuromorphic Chips Are Destined for Deep Learning—or Obscurity" given that the Neuromorphic Chip researchers "have hitched their wagon to deep learning's star." Drawing upon insights on Model Risk Management and Anticipatory Risk Analytics focus of top Wall Street investment banks and hedge funds beyond the Global Financial Crisis currently guiding national and global Cyber Risk Insurance industry practices, we demonstrate how Model Risk Management (MRM) and Anticipatory Risk Analytics are even more critical in the global and national domains of Intelligence, Surveillance, Reconnaissance (ISR). The first operational use of AI and Deep Learning AI technologies in the Defense Intelligence Enterprise led by Project Maven and Algorithmic Warfare Cross-Functional Team is used as a case study for illustrating how Anticipatory Risk Analytics & MRM assume even greater significance at the intersections of Space and Cyberspace wherein Offensive and Defensive Cybersecurity strategies, such as discussed in the recent 2015 and 2016 presentations at the Princeton Quant Trading Conference, are deployed.

Source: https://ssrn.com/abstract=2538401

Model Risk Management in Defense & Space, 'ISR' C4I Drones Enabled Warfare

AI, Machine Learning & Deep Learning Risk Management & Controls: Beyond Deep Learning and Generative Adversarial Networks: Model Risk Management in AI, Machine Learning & Deep Learning

Paper Accepted for Presentation at the 2018 Armed Forces Communications and Electronics Association (AFCEA) C4I and Cyber Conference, Erie Canal Chapter, New York, June 19 & 20, 2018.

7 Pages • Posted: 16 Jul 2018

Yogesh Malhotra
Global Risk Management Network, LLC

https://ssrn.com/abstract=3193693

Date Written: May 16, 2018

Abstract

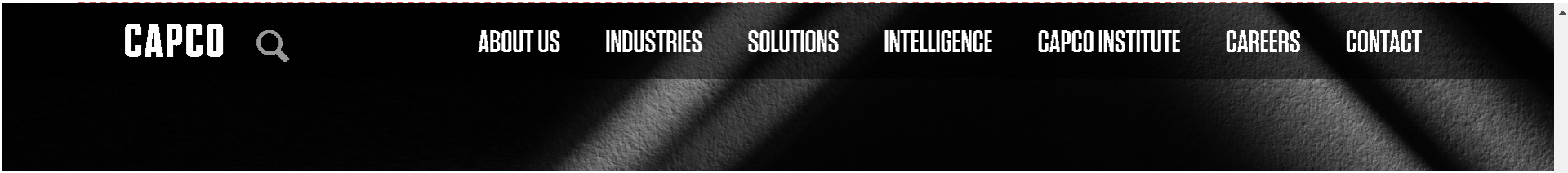
The current paper proposes how model risk management in operationalizing machine learning for algorithm deployment can be applied in national C4I and Cyber projects such as Project Maven. It builds upon recent leadership of global Management and Leadership industry executives for AI and Machine Learning Executive Education for MIT Sloan School of Management and the MIT Computer Science and Artificial Intelligence Laboratory (CSAIL) and invited presentations at Princeton University. After building understanding about why model risk management is most crucial to robust AI, Machine Learning, Deep Learning, and, Neural Networks deployment, it introduces a Knowledge Management Framework for Model Risk Management to advance beyond 'AI Automation' to 'AI Augmentation.'

Keywords: Project Maven, AI, Artificial Intelligence, Machine Learning, Deep Learning, Neural Networks, Model Risk Management, Knowledge Management, AI Augmentation, AI Automation

Suggested Citation:

Malhotra, Yogesh, AI, Machine Learning & Deep Learning Risk Management & Controls: Beyond Deep Learning and Generative Adversarial Networks: Model Risk Management in AI, Machine Learning & Deep Learning (May 16, 2018). Paper Accepted for Presentation at the 2018 Armed Forces Communications and Electronics Association (AFCEA) C4I and Cyber Conference, Erie Canal Chapter, New York, June 19 & 20, 2018. . Available at SSRN: https://ssrn.com/abstract=3193693 or http://dx.doi.org/10.2139/ssrn.3193693

25-Years Leading Global R&D & Industrial Practices Pioneering **Human-Centered AI** and **AI-Machine Learning Augmentation**



https://bit.ly/2VGOm1M

https://www.capco.com/Capco-Institute/Journal-49-Alternative-Capital-Markets/AI-AUGMENTATION-FOR-LARGE-SCALE-GLOBAL-SYSTEMIC-CYBER-RISK-MANAGEMENT-PROJECTS

AI AUGMENTATION FOR LARGE-SCALE GLOBAL SYSTEMIC AND CYBER RISK MANAGEMENT PROJECTS : MODEL RISK MANAGEMENT FOR MINIMIZING THE DOWNSIDE RISKS OF AI AND MACHINE LEARNING

Published: 29 April 2019

YOGESH MALHOTRA | Chief Scientist and Executive Director, Global Risk Management Network, LLC

This article discusses how model risk management in operationalizing machine learning or algorithm deployment can be applied in national systemic and cyber risk management projects such as Project Maven.

After an introduction about why model risk management is crucial to robust AI, ML, deep learning, and neural networks deployment, the article presents a knowledge management framework for model risk management to advance beyond 'AI automation' to 'AI augmentation.'

DOWNLOAD PAPER

https://bit.ly/2V3O2uC

First Network & Computer Security Thesis on Quantitative Risk & Uncertainty Assessment and Management Models Generalized to Multiple Applied-Industrial Domains

Stress Testing for Cyber Risks: Cyber Risk Insurance Modeling beyond Value-at-Risk (VaR): Risk, Uncertainty, and, Profit for the Cyber Era

National Association of Insurance Commissioners (NAIC) Expert Paper: Advancing Cyber Risk Insurance Underwriting Model Risk Management beyond VaR to Pre-Empt and Prevent the Forthcoming Global Cyber Insurance Crisis (June 24, 2017)

189 Pages • Posted: 23 Jan 2015 • Last revised: 12 Dec 2017

Yogesh Malhotra
Global Risk Management Network, LLC

https://ssrn.com/abstract=2553547

Date Written: January 19, 2015

Abstract

To avert the impending global Cyber-Finance Insurance Crisis based upon large-scale commercial reliance upon quantitative models with inherent model risks, tail risks, and systemic risks in current form, this post-doctoral thesis makes the following key contributions: Develops the first known Cyber-Finance-Trust™ framework for Cyber insurance modeling; Develops the first known model risk management framework for Cyber insurance modeling; Develops first known analysis of significant and extreme model risks, tail risks, and, systemic risk; Develops multi-method empirical study of VaR and Bayesian inference for containing model risks; Analyzes Markov Chain Monte Carlo for enabling Bayesian inference to minimize model risk; Develops Cyber insurance portfolio framework to minimize model risks, tail risks, systemic risks; Develops framework for Knightian uncertainty management beyond model risk management.

Updated, revised, summary version of the thesis invited for submission by NAIC as:

We Must Think Beyond Models & Measures

- *"What gets measured gets managed"* – Peter Drucker

  Model Risk Management corollaries
- " What doesn't get measured doesn't get managed. "
- "What gets mis-measured gets mismanaged. "
  Mainstream insurance industry practices have adopted Value-at-Risk (VaR) from global financial industry as the pre dominant cyber insurance model being oblivious to both distinguishing characteristics of cyber-risks as well as the statistical properties of VaR. Such widespread misapplication of VaR for cyber risk insurance underwriting unless abated and corrected is expected to lead to a global cyber-insurance crisis that may dwarf the worldwide economic shock from the global financial crisis. Given worldwide high impact of increasingly global cyber-attacks, the current paper advances cyber risk insurance underwriting model risk management beyond VaR to pre-empt and prevent the forthcoming global cyber-insurance crisis
- "All Models are Wrong."- Derman
- "Some Models are Useful."- Derman

Forthcoming Global Cyber Risk Insurance Crisis

Home | My Network | Jobs | Messaging

Dr. Yogesh Malhotra, CISSP, CISA, CEH, CCP-CDP, CEng
Chief Data Scientist-Machine Learning Engineer: AI-ML: Cybersecurity, Quantitative...
3mo · Edited

Swiss Re chief urges governments to back cyber insurers: To understand why the Swiss Re chief is highlighting that insurers are worried about "accumulation risk" and why unlike natural catastrophes the cyber "cat" risk accumulations pose a plausible impending threat, read the National Association of Insurance Commissioners (NAIC) Expert Paper:
"Advancing Cyber Risk Insurance Underwriting Model Risk Management beyond VaR to Pre-Empt and Prevent the Forthcoming Global Cyber Insurance Crisis": **https://lnkd.in/ea27wsh** .

Related Princeton University Presentations on Unprecedented Cyber-Finance Risks, Vulnerabilities, and Exposures for Global Financial Markets & Exchanges and National Economies:

2015 Princeton Quant Trading Conference: Sponsors: Princeton University, Citadel: Knight Reconsidered: Risk, Uncertainty & Profit for the Cyber Era: Future of Finance beyond 'Flash Boys': Cyber Finance™: FinTech Model Risk Management & Defensive Cybersecurity: **https://lnkd.in/eyP9Npd**.

2016 Princeton Quant Trading Conference: Sponsors: Princeton University, Goldman Sachs: Knight Reconsidered Again: Risk, Uncertainty & Profit beyond ZIRP & NIRP: FinTech Model Risk Arbitrage™ & Offensive Cybersecurity. **https://lnkd.in/dJ-Gnxx**.

More: FutureOfFinance.org: **https://lnkd.in/eW4bqch**.

Swiss Re
177,960 followers

In an interview with **Financial Times**, Swiss Re's Christian Mumenthaler has said that governments need to provide a backstop in case of huge cyber attacks, much as they do for terror incidents. **https://lnkd.in/dV-vmUp**

Swiss Re AG + Add to myFT

Swiss Re chief urges governments to back cyber insurers

Mumenthaler decries lack of enthusiasm to engage with insurance industry

Christian Mumenthaler is sceptical of the growing trend for insurers to buy up stakes in start-ups © Bloomberg

Oliver Ralph in London and **Ralph Atkins** in Zurich DECEMBER 28, 2017 2

Governments need to step up and help the insurance industry cover growing threats from cyber attacks, the head of reinsurer Swiss Re has said.

Christian Mumenthaler said governments around the world need to provide a backstop in case of huge attacks, much as they do for terror incidents. "You need the same here, otherwise the public market cannot really develop fully,"

Source: https://www.ft.com/content/0212ad0e-e72d-11e7-8b99-0191e45377ec

How ‘Best Practices’ Become ‘Worst Practices’

Reference: Malhotra, Y., When Best Becomes Worst, Momentum: The Quality Magazine of Australasia [Quality Society of Australasia], NSW, Australia, September 2002, 29-30.

management

When best becomes worst

How can organisations prevent best practices from impeding their progress during ‘interesting times’? Dr Yogesh Malhotra shares his views.

The current thrust of organisational business and performance management initiatives focus on archiving ‘best practices’ so other employees can access them later.

Archival and the subsequent referral of information are believed to facilitate efficient problem solving and prevent unnecessary allocation of resources to inefficient search processes. Incidentally, in due course, the archived ‘best practices’ tend to define the ‘company way’.

Business solutions characterised by memorisation of best practices might define the assumptions that are embedded not only in information databases, but also in the organisation’s strategy, reward systems and resource allocation systems.

Within a changing business situations during stable or incrementally changing environments. However, when change is radical and discontinuous, there is a persistent need for continual renewal of the basic premises underlying best practices. Organisations in such environments need imaginative suggestions more than they do best practices.

in best practices, could become tomorrow’s core rigidities. Institutionalisation of best practices by embedding them in information repositories might facilitate efficient handling of routine, linear or predictable

- reinforcement and exploration
- learning and unlearning
- efficiency and effectiveness
- construction and deconstruction.

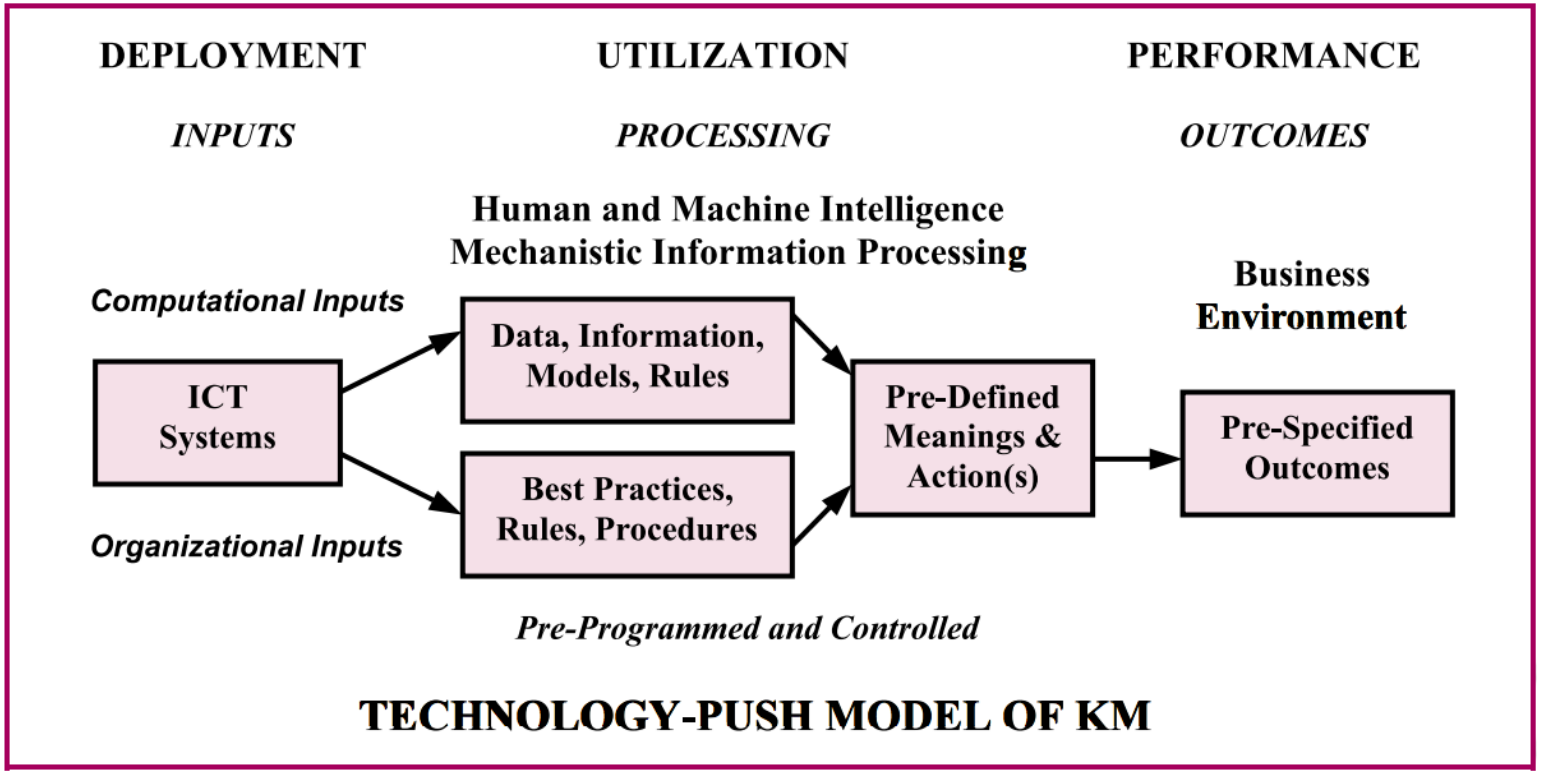
The basic intent is to set up a ‘real-time’ feedback-and-feed forward loop of actively scanning the unstructured reality (or what Ackoff called ‘messes’) for emerging patterns that suggest the emergence of something new. Meanwhile, you must ensure there is a mechanism for testing perceived patterns and implementing the resultant lessons learned into the extant logic of the processes.

Yesterday’s core capabilities embedded in best practices, could become tomorrow’s core rigidities

Source: http://www.brint.org/bestpractices.pdf

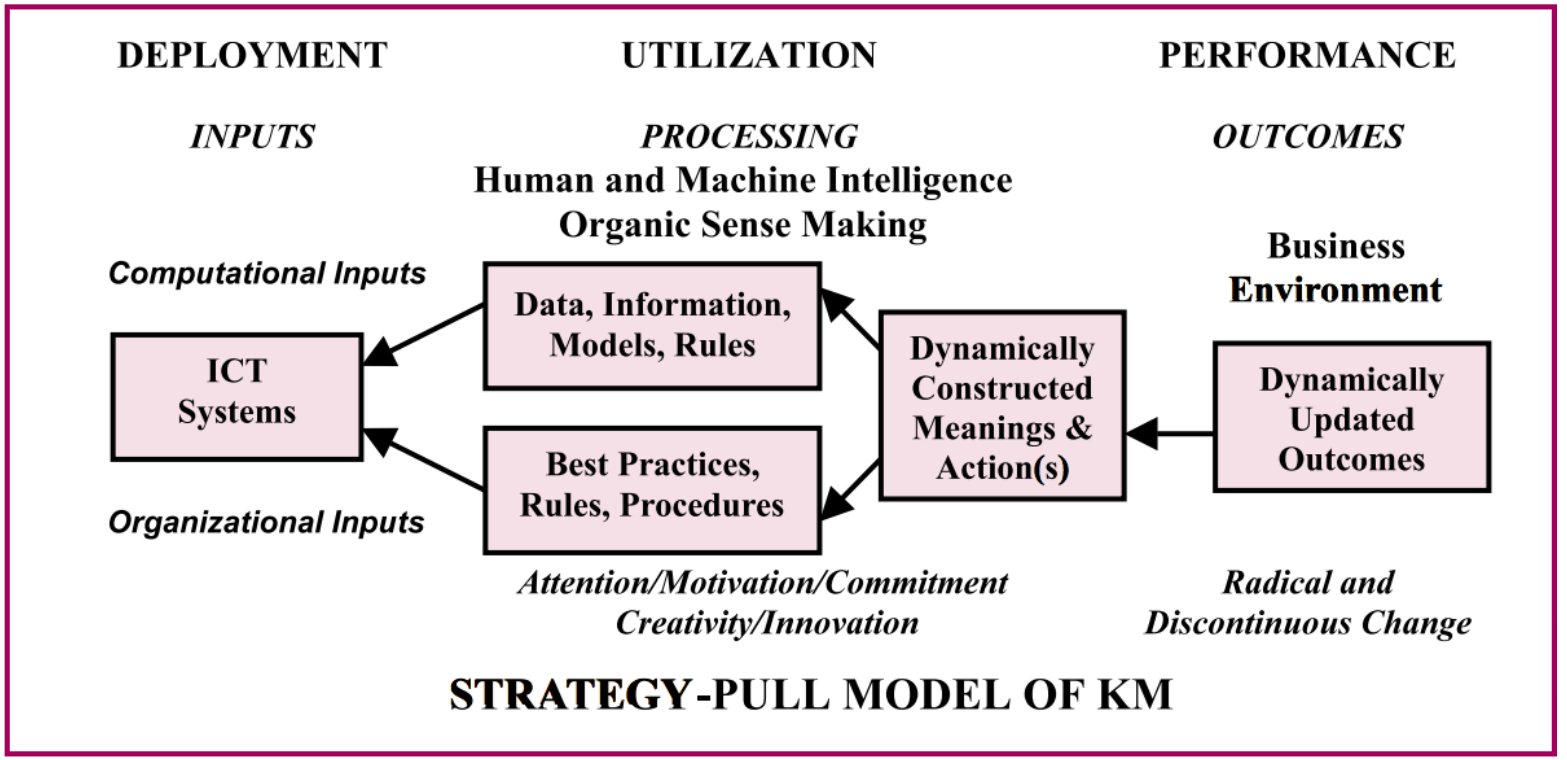
ADVISING BIG-4 CONSULTING PARTNERS & SENIOR LEADERS IN MID-1990S

Technology-Push Model of KM



Source: http://www.kmnetwork.com/RealTime.pdf

Strategy-Pull Model of KM



Source: http://www.kmnetwork.com/RealTime.pdf

Pioneering 'Sense-Making' AI-ML-KM Digital Transformation for over 25 Years

"There are many definitions of knowledge management. It has been described as "a systematic process for capturing and communicating knowledge people can use." Others have said it is "understanding what your knowledge assets are and how to profit from them." Or the flip side of that: "to obsolete what you know before others obsolete it." (Malhotra) "
- U.S. Department of Defense, Office of the Under Secretary of Defense (Comptroller)

OFFICE OF THE UNDER SECRETARY OF DEFENSE (COMPTROLLER)

"KM is obsoleting what you know before others obsolete it and profit by creating the challenges and opportunities others haven't even thought about -- Dr. Yogesh Malhotra, Inc. Technology"
- U.S. Defense Information Systems Agency Interoperability Directorate

DISA
Defense Information Systems Agency
Department of Defense
EncoreII

http://FinRM.com/globalimpact.html

Pioneering 'Sense-Making' AI-ML-KM Digital Transformation for over 25 Years

"If you spend some time at [the digital research lab] founded by Dr. Malhotra you will be blessed by some of the world's most astute thinking on the nature of knowledge and its value."
- **U.S. Army** Knowledge Symposium, Theme: "Knowledge Dominance: Transforming the Army...from Tooth to Tail", Department of Defense, United States Army.

"We are observing diminishing credibility of information technologists. A key reason for this is an urgent need to understand how technologies, people and processes *together* combine to influence enterprise performance. Today's effective CIO doesn't deliver IT. He delivers business transformation services."
- Yogesh Malhotra, *Journal of Knowledge Management*, 2005
- **United States Air Force Research Lab CIO** Col. Tom Hamilton
in presentation to the Armed Forces Communications Electronics Association titled 'Enterprise IT Solutions Are Tough But They're Tougher If You're Stupid', July 21, 2005.

http://FinRM.com/globalimpact.html

Pioneering 'Sense-Making' AI-ML-KM Digital Transformation for over 25 Years

"Knowledge Management refers to the critical issues of organizational adaptation, survival and competence against discontinuous environmental change. Essentially it embodies organizational processes that seek synergistic combination of data and information processing capacity of information technologies, and the creative and innovative capacity of human beings." -- Yogesh Malhotra
- **United States Department of Navy**

"Dr. Yogesh Malhotra, PhD, drawing upon numerous sources, proposes several theories as to how IT can be used to drive the change of organizations. As environments become more turbulent, organizations must adapt at the same rate to maintain its advantage. Among his theories are that the turbulent environments (in this case, business, but can translate to the turbulent military conflict environment) drive organizations to use IT for empowering workers at all levels, increasing span of control, and increasing lateral communications."
- **United States Marine Corps**, Reorganization Of The Marine Air Command And Control System To Meet 21St Century Doctrine And Technology, Thesis, September 2001.

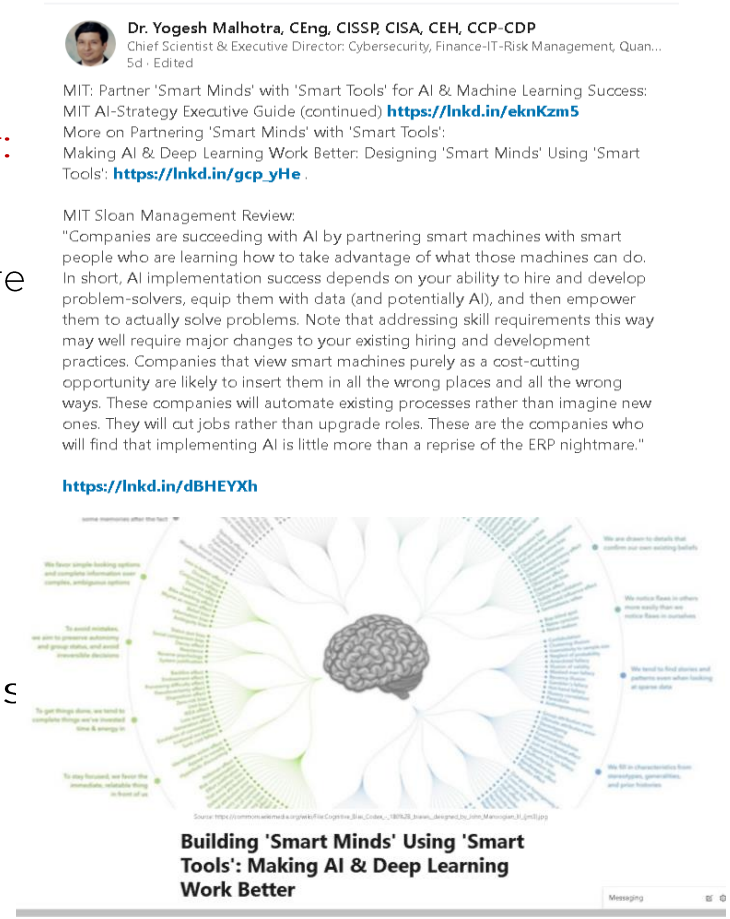
Conclusion:
Beyond ‘AI Automation’ to ‘AI Augmentation’

Building ‘Smart Minds’ Using ‘Smart Tools’

AI-AUTOMATION vs. AI-AUGMENTATION

- More on Partnering 'Smart Minds' with 'Smart Tools': Making AI & Deep Learning Work Better: Designing 'Smart Minds' Using 'Smart Tools': https://lnkd.in/gcp_yHe .
- MIT Sloan Management Review: "Companies are succeeding with AI by partnering smart machines with smart people who are learning how to take advantage of what those machines can do. In short, AI implementation success depends on your ability to hire and develop problem-solvers, equip them with data (and potentially AI), and then empower them to actually solve problems.”

- “Companies that view smart machines purely as a cost-cutting opportunity are likely to insert them in all the wrong places and all the wrong ways. These companies will automate existing processes rather than imagine new ones. They will cut jobs rather than upgrade roles. These are the companies who will find that implementing AI is little more than a reprise of the ERP nightmare." https://lnkd.in/dBHEYXh



Source: https://www.linkedin.com/pulse/designing-smart-minds-using-tools-utopian-view-ai-yogesh-/

Math, Intuition, Meaning, & Reality

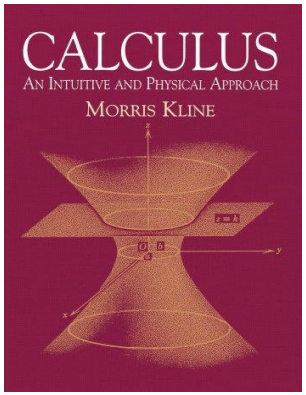
"We do need models and mathematics – you cannot think about finance and economics without them – but one must never forget that models are not the world. Whenever we make a model of something involving human beings, we are trying to force the ugly stepsister's foot into Cinderella's pretty glass slipper. It doesn't fit without cutting off some essential parts. And in the cutting off parts for the sake of beauty and precision, models inevitably mask the true risk rather than exposing it. The most important question about any financial model is how wrong it is likely to be, and how useful it is despite its assumptions. You must start with models and then overlay them with common sense and experience."

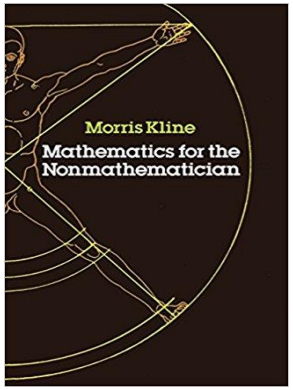
"Building financial models is challenging and worthwhile: you need to combine the qualitative and the quantitative, imagination and observation, art and science, all in the service of finding approximate patterns in the behavior of markets and securities. The greatest danger is the age-old sin of idolatry. Financial markets are alive but a model, however beautiful, is an artifice. No matter how hard you try, you will not be able to breath life into it. To confuse the model with the world is to embrace a future disaster driven by the belief that humans obey mathematical rules."

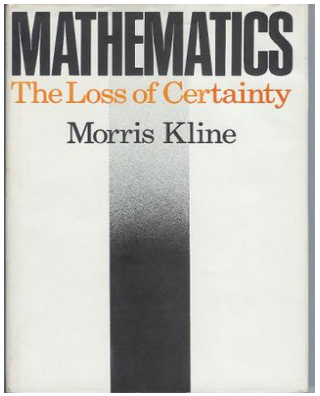
- Emanuel Derman and Paul Wilmott: The Financial Modelers' Manifesto

Math, Intuition, Meaning, & Reality

- Source: Following Quotes attributed to Morris Kline from his various publications shown below. Respective images of his authored books shown below are attributed to respective publishers and copyright holders.
- "One of the first difficulties in applying statistics is to decide the **meaning** of the concepts involved."
- "When creating a mathematical proof, the **mind** does not see the cold, ordered arguments which one reads in texts, but rather it perceives an idea or a scheme which when properly formulated constitutes deductive proof. The formal proof, so to speak, merely sanctions the conquest already made by the **intuition**."
- "In the search for a method of proof, as in finding what to prove, the **mathematician must use audacious imagination, insight, and creative ability**. His **mind** must see possible lines of attack where others would not."

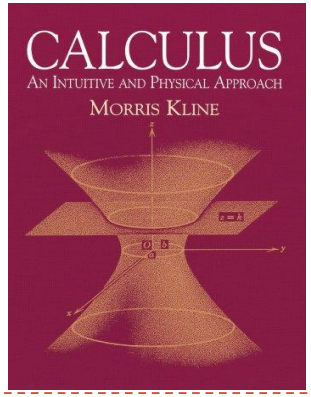


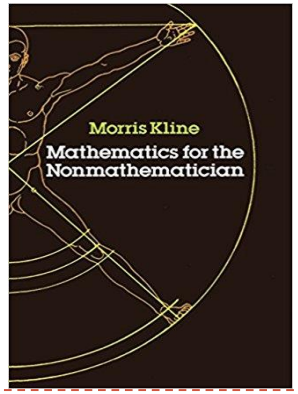


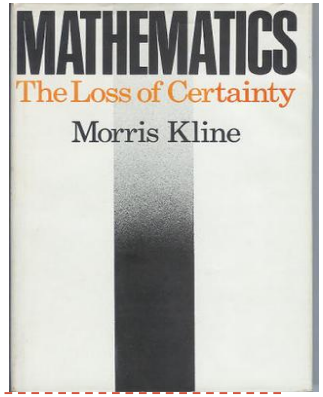


Math, Intuition, Meaning, & Reality

- "One should question the extent to which mathematics really represents the physical world. It treats those physical concepts which can be represented by numbers or geometrical figures. But physical objects possess other properties as well. We do not usually think of human beings as chunks of matter moving in space and time."
- "All scientific work depends upon measurement. However, all measurements are approximate."
- "Is then mathematics a collection of diamonds hidden in the depths of the universe and gradually unearthed one by one or is it a collection of synthetic stones manufactured by man but nevertheless so brilliant that it bedazzles those mathematicians who are already partially blinded by pride in their own creations? Several considerations incline us to the latter point of view."







Math, Intuition, Meaning, & Reality

- "One finds among the supreme mathematicians men, such as Newton, Lagrange, and Laplace, who even cared little or nothing for mathematics proper, but felt compelled to take up mathematical problems in order to solve physical problems."
- "If herds of cattle behaved like volumes of gases or like raindrops, then the arithmetic would not apply, and it is only through experience that we learn how they do behave. Hence, we have no guarantee that arithmetic per se represents truths about the physical world."
- "Human nature is a more complicated structure than a mass sliding down an inclined plane or a bob vibrating on a spring."
- "The mathematician really creates models of reality. Each model has a limited applicability. Moreover, one must distinguish between the mathematical model and the physical world or between mathematical theories and physical reality."

"Suppose, next, that one raindrop is added to another raindrop. Do we now have two raindrops? If one cloud is joined to another cloud do we now have two clouds? One may protest that in these examples the merged objects have lost their identity, and that the addition process of arithmetic does not contemplate such loss. And precisely for this reason, **arithmetic in the normal sense no longer applies**."

Math, Intuition, Meaning, & Reality

'Gut instinct' told Lt Col Stanislav Petrov that apparent launch of US missiles was actually early warning system malfunction

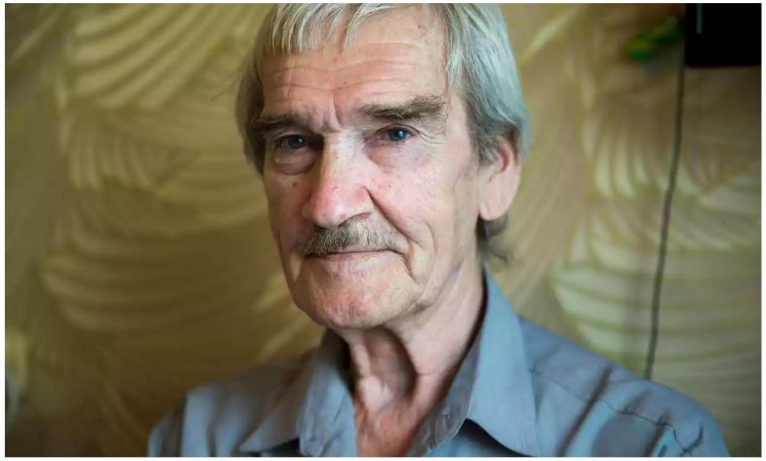
Soviet officer who averted cold war nuclear disaster dies aged 77

The Washington Post

The Post's View • Opinion

The night one Russian military officer may have saved the world

'Gut instinct' told Lt Col Stanislav Petrov that apparent launch of US missiles was actually early warning system malfunction



▲ Stanislav Petrov: 'The siren howled, but I just sat there for a few seconds, staring at the big, back-lit, red screen with the word 'launch' on it.' Photograph: Pavel Golovkin/AP

"a computer can make an error in a minute that can take years for humans to correct"

Stanislav Petrov was on duty in a secret command centre outside Moscow on 26 September 1983 when **a radar screen showed that five Minuteman intercontinental ballistic missiles had been launched by the US towards the Soviet Union**.

Red Army protocol would have been to order a retaliatory strike, but Petrov – then a 44-year-old lieutenant colonel – ignored the warning, relying on a "**gut instinct**" that told him it was a false alert.

It later emerged that the false alarm was the result of a satellite mistaking the reflection of the sun's rays off the tops of clouds for a missile launch.

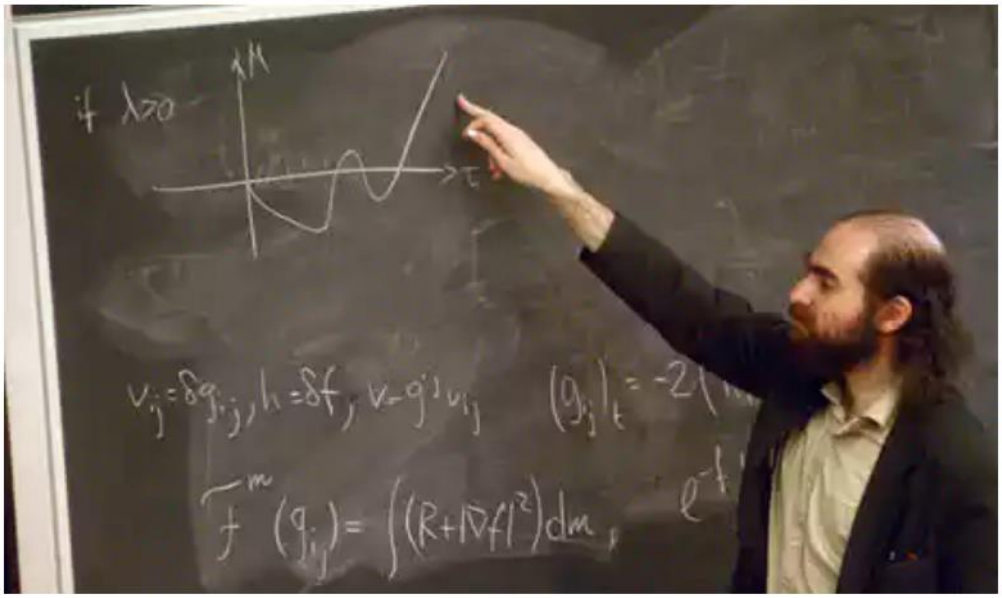
The Guardian

"We are wiser than the computers," Petrov said in a 2010 interview with the German magazine Der Spiegel. "We created them."

Math, Intuition, Meaning, & Reality

Perfect Rigour: A Genius and the Mathematical Breakthrough of the Century by Masha Gessen – review

Robin McKie enjoys a dogged attempt to shed some light on the life and work of the eccentric maths genius Grigori Perelman



▲ Grigori Perelman, solver of Poincaré conjecture, gives a lecture on his solution at New York's Weaver Hall in 2003. Photograph: Frances M Roberts

Arguably the world's greatest mathematician, he worked out a solution to one of the seven great unsolved mathematical problems, the Poincaré conjecture, in 2002. It was a magnificent achievement. Honours, cash, offers of world lecture tours and lucrative teaching posts were hurled at the Russian theorist.

But Perelman turned down the lot, including the Fields medal, the mathematical world's equivalent of a Nobel prize, and a million dollars in prize money that the Clay Institute wanted to give him for his work. Since then, he has announced he has given up the study of mathematics altogether and has cut off communications with all journalists and nearly all his friends.

Source: https://www.theguardian.com/books/2011/mar/27/perfect-rigour-grigori-perelman-review/

Need for "Human-Centered AI", 2019 Mar 13

Artificial Intelligence / Voice assistants

The man who helped invent virtual assistants thinks they're doomed without a new AI approach

Boris Katz has spent his career trying to help machines master language. He believes that current AI techniques aren't enough to make Siri or Alexa truly smart.

by **Will Knight** Mar 13

What do you make of Siri, Alexa, and other personal assistants?

...These programs are so incredibly stupid. So there's a feeling of being proud and being almost embarrassed. You launch something that people feel is intelligent, but it's not even close.

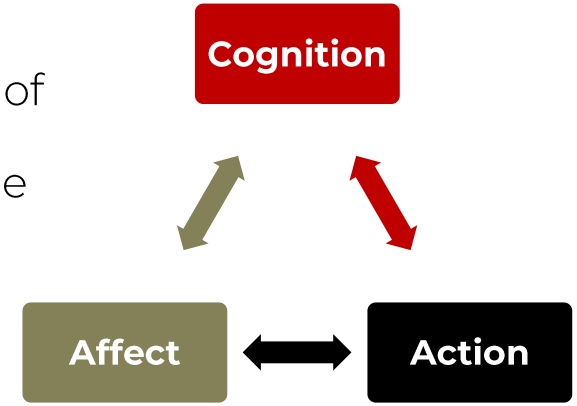
What is a better approach?

One way forward is to **gain a greater understanding of human intelligence** and then use that understanding in order to create intelligent machines. AI research needs to build on ideas from **developmental psychology, cognitive science, and neuroscience**, and **AI models ought to reflect what is already known about how humans learn and understand the world**.

Source: https://www.technologyreview.com/s/612826/virtual-assistants-thinks-theyre-doomed-without-a-new-ai-approach/

Socio-Psychology and Neuroscience of 'Making Sense' and Sensing 'Meaning'

"Damasio's essential insight is that feelings are "mental experiences of body states," which arise as the brain interprets emotions, themselves physical states arising from the body's responses to external stimuli. (The order of such events is: I am threatened, experience fear, and feel horror.) He has suggested that consciousness, whether the primitive "core consciousness" of animals or the "extended" self-conception of humans, requiring autobiographical memory, emerges from emotions and feelings."

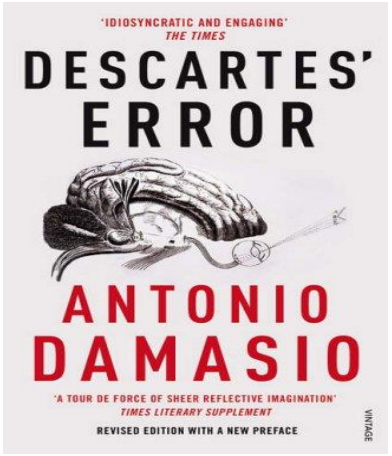


Source: https://www.technologyreview.com/s/528151/the-importance-of-feelings/

"Thinking, feeling, and deciding are the most intimately human of all things... we understand them hardly at all."

Damásio proposed a mechanism by which emotions guide (or bias) behavior and decision-making, and positing that rationality requires emotional input. He argues that René Descartes' "error" was the dualist separation of mind and body, rationality and emotion.

Source: https://www.technologyreview.com/s/528221/peering-inside-the-workings-of-the-brain/



Source: https://en.wikipedia.org/wiki/Descartes%27_Error

"Human-Centered AI" & 'AI Augmentation'

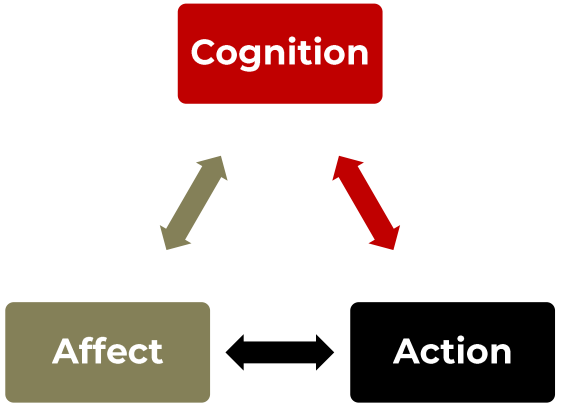
- Inspired by AI Pioneer, Dr. John Holland, University of Michigan Computer Scientist & Psychologist, then at Santa Fe Institute (1995)
- Missing "**MEANING**" in Claude Shannon's Information Theory
- Our Path-Breaking Discovery was in Solving the Problem of Missing "MEANING" in Information Theory posed by John Holland
- First IT-MIS Papers on "MEANING" in AI-ML-KM Systems
- Inspired by another AI Pioneer who was a Psychiatry Pioneer too.
  - George Kelly, Founder of Personal Construct Theory & Repertory Grids
- Caught Attention of Both NSA and CIA on Publication.

IQ
EQ
Do-Q

Malhotra, Y., Expert Systems for Knowledge Management: Crossing the Chasm between Information Processing and Sense Making, Expert Systems with Applications: An International Journal, 20(1), 7-16, 2001.
http://www.brint.org/expertsystems.pdf

Original R&D:
http://www.yogeshmalhotra.com/publications.html

Latest R&D: https://papers.ssrn.com/author_id=2338267



http://www.brint.com/PCT.htm

Outline of Presentation

- References
- Foreground
- Introduction: Project Maven
- AI, Machine Learning, Deep Learning, and, Neural Networks
- Why Model Risk Management is Crucial to Robust AI-ML-DL Use
- A Knowledge Management Framework for MRM
- Conclusion: Beyond 'AI Automation' to 'AI Augmentation'

Background Time Line "Post-WWW" Era

- **R&D Program: Years & Engagements**

RISKS

Strategy, Operations, Tactics: People, Processes, Technologies

Big-3 IT, Big-3 Banking & Finance: Global Financial Systems: USA, Hong Kong, India

DIGITAL

1993-1998: Top Digital Site, Top-3 Search Engine, Top-10 Social Network
Computerworld, CIO Magazine, Wall Street Journal, Information Week

1993-2001: AI-ML: John Holland: NSA-CIA, US, Netherlands, Mexico, South Korea
Business Week, Fortune, Inc. Wall Street Journal, New York Times…

CYBER

2001-2008: National Science Foundation, United Nations, **CISSP**, **CISA**
AACSB Impact of Research, CNet Networks Computing Award
Canada-Fulbright Chair Invitation: Queen's University

QUANT

1998-2008: BT, Goldman Sachs, Google, Intel, IBM, Microsoft, Harvard, MIT,…
Largest Digital Transformation CoP: CIO Magazine, CIO Insight

CRYPTO

2008-2019: **MIT** AI-Machine Learning, **Princeton** Cyber Finance, **CEH**, NYS-CRI
2015-2018: SSRN: 63 Top-10 Research Rankings, Top-2% Authors.
GIBC Digital **AI-ML MD**, New York State **CISO**, JP Morgan **Quant**.
ACM, **AFCEA**, **AFRL**, CFA, NAIC, NYS, Switzerland, Wall Street…

QUANTUM

Books, Papers, Presentations, Keynotes

www.YogeshMalhotra.com [Download Our Research](#)

SSRN tomorrow's research today

https://papers.ssrn.com/author_id=2338267

25-Years Leading Global R&D & Industrial Practices Pioneering **Human-Centered AI** and **AI-Machine Learning Augmentation**

www.YogeshMalhotra.com

2019 New York State Cyber Security Conference, Albany, NY
June 4 - 5, 2016, Empire State Plaza - Albany, NY

AI-Machine Learning Augmentation and Cybersecurity: Why Smart Minds Using Smart Tools are critical for Minimizing Risks, and, What You Can Do About It?

Advancing Beyond 'Automation' to 'AI Augmentation'

Yogi http://www.linkedin.com/in/yogeshmalhotra

Dr. Yogesh Malhotra
Post-Doctoral R&D: AI-Machine Learning-CyberSecurity
PhD, MS-NCS, MS-CS, MS-QF, MS-Acc, MBA-Eco,
C.Eng., CISSP, CISA, CEH, CCP, CPA Education
Who's Who in America®, Who's Who in the World®,
Who's Who in Finance & Industry®,
Who's Who in Science & Engineering®
www.yogeshmalhotra.com dr.yogesh.malhotra@gmail.com

www.its.ny.gov

FinRM™

Global Risk Management Network, LLC,
Griffiss Air Force Base, Griffiss Business & Technology Park, Rome, NY 13441
Phone: 646-770-7993

"The **new business model** of the Information Age, however, is marked by **fundamental, not incremental, change**. Businesses **can't plan long-term**; instead, they **must shift** to a more flexible **"anticipation-of-surprise" model**."
-- Dr. Yogesh Malhotra in ***CIO Magazine*** interview, Sep. 15, 1999.

CIO