Global Forum
Shaping the future 2017

The University of WINNIPEG

Artificial Intelligence (AI) & Cybersecurity (CS)

Don Davidson

Office of the US DoD-CIO

ITEMS INTERNATIONAL

© ITEMS International 2017

What is AI ?

AI is a sub-division of computer science dealing with the development of systems and software capable of acting intelligently, and doing things that would normally be done by people – equally as well, or sometimes better. AI refers to the science and methodology itself, and to the behavior exhibited by the machines and programs which result from it.

---John McCarthy started all this in 1956---

Wikipedia says:

Artificial intelligence (**AI**, also **machine intelligence**, **MI**) is apparently intelligent behavior by machines, rather than the *natural intelligence* (*NI*) of humans and other animals.

In computer science AI research is defined as the study of "intelligent agents": any device that perceives its environment and takes actions that maximize its chance of success at some goal. Colloquially, the term "artificial intelligence" is applied when a machine mimics "cognitive" functions that humans associate with other human minds, such as "learning" and "problem solving".[

The scope of AI is disputed: as machines become increasingly capable, tasks considered as requiring "intelligence" are often removed from the definition, a phenomenon known as the AI effect, leading to the quip "AI is whatever hasn't been done yet." For instance, optical character recognition is frequently excluded from "artificial intelligence", having become a routine technology. Capabilities generally classified as AI as of 2017 include successfully understanding human speech, competing at a high level in strategic game systems (such as chess and Go, autonomous cars, intelligent routing in content delivery networks, military simulations, and interpreting complex data.

Narrow AI, General AI & Super AI

not yet

© ITEMS International 2017

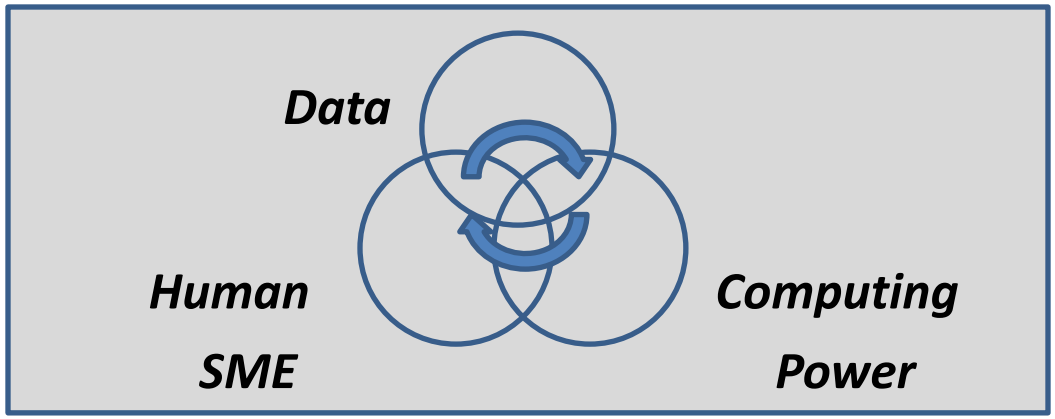
Do you want to play a game ? from *WarGames*

HAL from *2001: A Space Odyssey*

SkyNet from *Terminator*

Enterprise Capability *comes from* ***People, Process & Technology***

AI Capability *comes from* ***Data, Computing Power & Human SME***

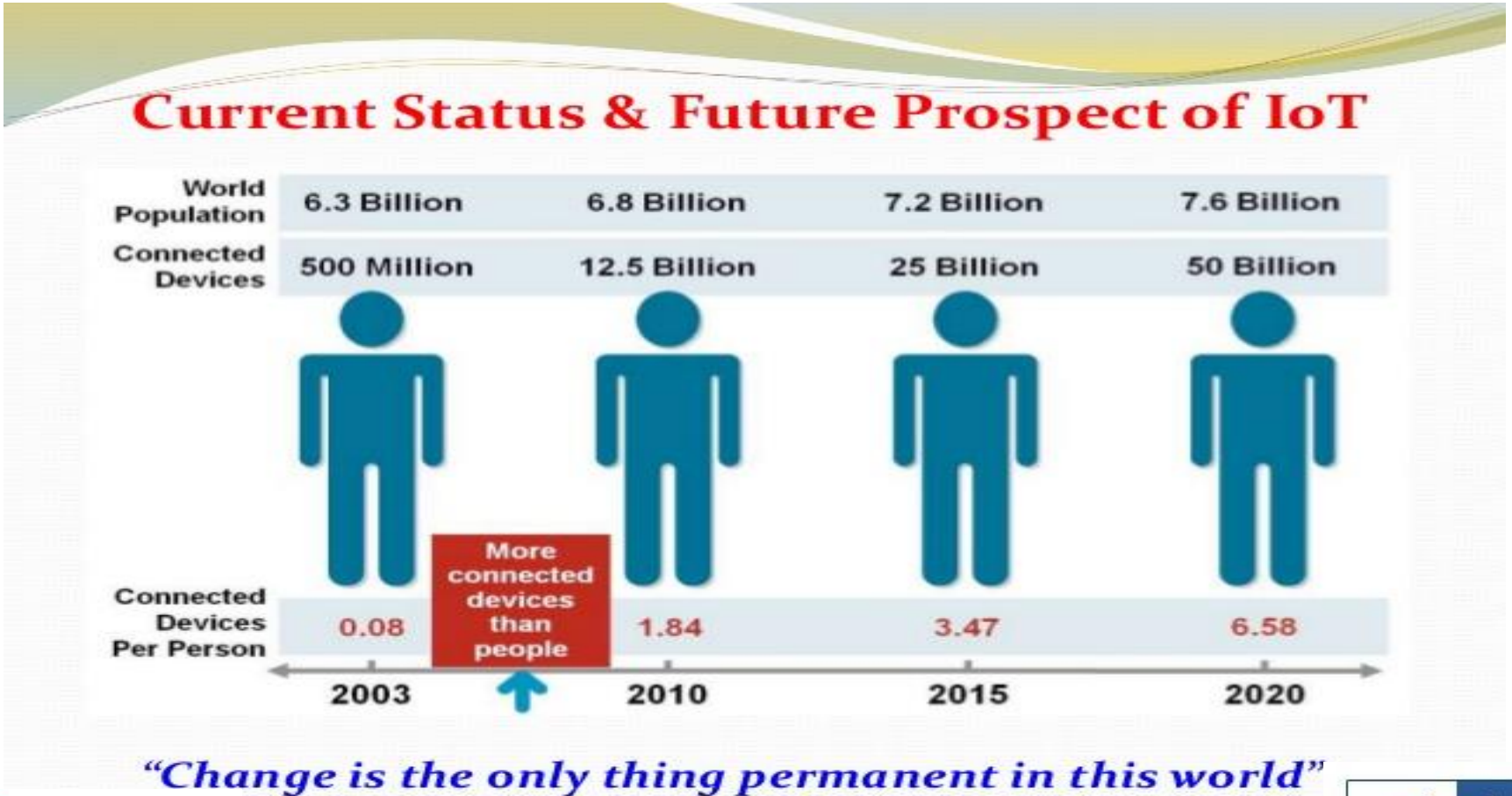


It's really about balancing Man & Machine.

…some of the greatest minds of today, including **Bill Gates, Stephen Hawking and Elon Musk**, have ALL voiced their concerns on the repercussions AI could bring and how it has the ability of directing itself and getting out of human control.

© ITEMS International 2017

Where are we today ? on IoT



Global Forum
Shaping the future

© ITEMS International 2017

ITEMS INTERNATIONAL

Where are we today ? on Cybersecurity (CS)

- Advanced cyber attacks often go 99 Days undetected (down from 145 in 2015)
- Each major breach costs over $ 3.5M
- Total cost to global economy could reach $ 500B
- Lost productivity and lost growth could reach $ 3T

Source: *Lockheed Martin Advanced Threat Monitoring Page, Microsoft Advanced Threat Analytics Page & the Ponemon Institute*

- 35 B Messages Scanned Monthly
- 600 K Known spam email addresses tracked
- 600 M Computers reporting monthly
- 8.5 B+ Web-pages scans per month

CYBER BASICS
Attk Surface ---Access/Auth
Keep Config (HW/SW)---CDM

Source: Microsoft Security Intelligence Report (SIR)

--- There are roughly 1M vacant CS-jobs today in the US… projected to be 3.5m globally by 2021
--- We are spending a lot of our Human Capital SME responding to poor design & bad practices.

WE NEED TO FOCUS ON BETTER DESIGNED SYSTEMS
(can AI help)

© ITEMS International 2017

Artificial Intelligence & Cybersecurity

- One of the industries that could benefit most of all from the introduction of Artificial Intelligence is CYBERSECURITY.

Intelligent machines could implement algorithms designed to identify cyber threats in real time and provide an instantaneous response.

Despite that the majority of security firms are already working on a new generation of automated systems, we're still far from creating a truly self-conscious entity.

The security community is aware that many problems could not be solved with conventional methods and requests the application of **machine-learning algorithms**.

Global Forum
Shaping the future

© ITEMS International 2017

ITEMS
INTERNATIONAL

Machine Learning (+AI) Algorithms for CS

- How much/How many?
- Which category?
- Which groups?
- Is it weird?
- Which option?

Regression

Classification

Clustering

Anomaly Detection

Recommendation

After AI helps us Respond better, then AI focuses on Better Designs.

Global Forum
Shaping the future

ITEMS INTERNATIONAL

Real Considerations pre-AI

A look to the future to prevent malicious AI

The development and the adoption of AI systems seems to be impossible to control due to the enormous advantage that the paradigm could bring to every industry.

Scientist Steve Omohundro, wrote a paper that identifies three ways to keep AI safe:

- **To prevent harmful AI systems from being created in the first place.** It is desirable that scientist could be able to carefully program intelligence machines with a **Hippocratic emphasis ("First, do no harm").**
- **To detect malicious AI early in its life before it acquires too many resources.** Monitor the evolution of such systems over the time by **measuring the processes implemented** by the AI systems and the resources that is continuously consuming.
- **To identify malicious AI after it's already acquired lots of resources.** It is essential to **maintain the human control over the machine** even after the AI systems has already acquired a significant amount of resources.

The lesson learned is:

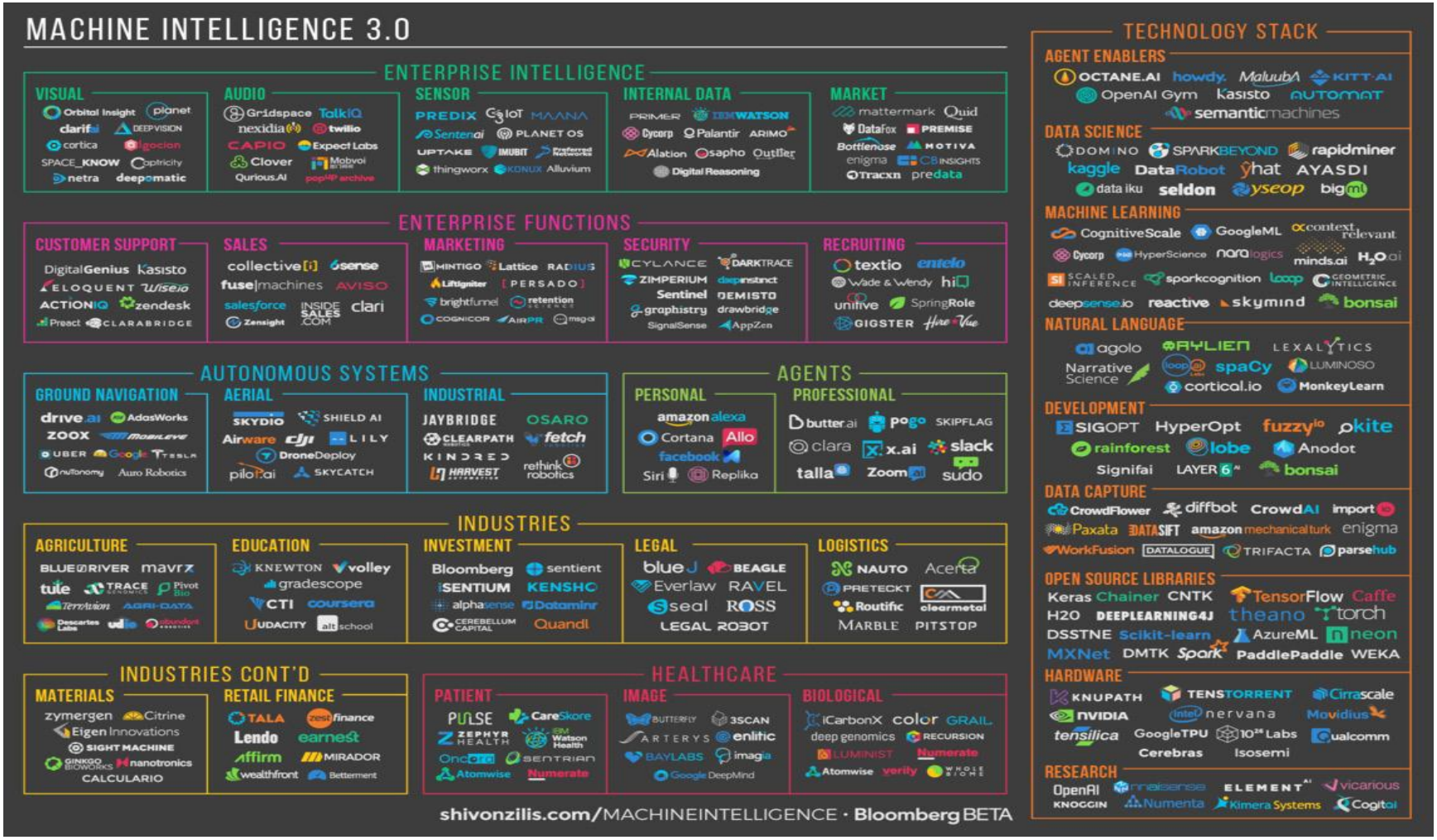
"do not create conditions of competition for any resources between humans and machines …"

Global Forum
Shaping the future

© ITEMS International 2017

ITEMS INTERNATIONAL

AN OVERVIEW OF THE COMPETITIVE MARKET LANDSCAPE FOR MACHINE INTELLIGENCE.



2017 The Hague Centre for Strategic Studies.