Data Exploitation:
Artificial Intelligence for Defence Applications

Adam Zagorecki, Ph.D.

Senior Research Fellow
Cranfield Defence and Security
Cranfield University / Defence Academy of the UK

DSEI 2019

London, 9th September 2019

www.cranfield.ac.uk

Some Facts…

- Every two days now we create as much information as we did from the dawn of civilisation up until 2003*

- Internet users are responsible for large part of it:
  - Twitter: 500 million tweets per day.
  - 300 hours of video is uploaded to YouTube every minute.

- Wide Area Persistent Surveillance such as Gorgon Stare produce GBs of data per minute.

- Data processing and analysis − volumes of data delivered exceed human abilities to analyze it.

*Erick Schmidt, Google

Advances in Data Processing over last 20 years

Data Collection
- Remote Sensing, digital sensors
- Networked affordable sensors

Communication
- Computer networks, wireless communication
- Smartphones, Internet of Things, 5G

Data Storage
- Inexpensive data storage
- New storage technologies – Big Data

Data Analysis
- Cloud computing
- Machine Learning, advances in Artificial Intelligence

Sensing Technologies – Enabling Big Data

- Dramatic development of sensing technologies in last decade:
  - Accelerometers – cheap, installed *just in case*
  - Digital cameras – low costs
  - Temperature, pressure, light, etc.
- ... and all these connected: Wi-Fi, Bluetooth, IR, etc.

- Looking into the Future:
  - Enables rapid development of Autonomous Systems
  - Opportunities of exploiting these technologies are not yet fully understood (start-ups)
  - Security implications: Fitness app Strava

Big Data

- The term **Big Data** describes data collection:

    - **Volume** – too big to be stored and analysed on a single computer, not suitable to be processed using traditional database systems – **cloud computing**

    - **Variety** – heterogeneous: databases, text, audio and video, etc.

    - **Velocity** – how fast it should be analysed, for example a query to Google search

- Sometimes **veracity** is added – how reliable is the data (example: twitter posts)
- Multidimensional aspect and complex dependencies are distinguishing factors

    ... it's not all about size, it's about **complexity**

Big Data or Too Big Data?

Paradox: too much data can be a problem

- **Information overload** occurs when the amount of input to a system exceeds its processing capacity.

- Studies suggest that only 0.5% world's data is used for analysis

- It is not only technical problem, can affect individuals and organisations
  - Decision makers operate under stress and high-stakes situations (e.g. disaster response)
  - Humans have limited information processing capabilities

- Example: intelligence data collected by UAVs exceeds analysts' capability to analyse it

- The idea is to machines that will analyse data for us – the answer is **artificial intelligence**

Big Data and Artificial Intelligence (AI)

Big Data is enabling technology for Artificial Intelligence

- Artificial Intelligence concerns with creating intelligent machines to help or replace humans at tasks involving thinking and creativity

- Fundamentally there are two sources of knowledge
  - Human **expertise** (mimic human thinking)
  - Create mathematical models (brain) from **data** – data driven methods
  - … hybrid approaches are possible as well

- Modern Artificial Intelligence is primarily driven by Machine Learning

*Machine learning, a branch of artificial intelligence, concerns the construction and study of **systems that can learn** from **data**.*

Big Data and AI in Defence

Big Data is relatively well established in Defence Applications

- Unmanned Vehicles are basically sensor suites that generate incredible amounts of data

- Autonomous Systems – as AI develops we should expect gradually more autonomy from weapon systems

- Areal Reconnaissance – processing of large volumes of image data, identifying targets, changes in environment, etc.

- Naval Traffic Monitoring – including prediction of intend, popular because of open source data

- Communications and Spectrum Monitoring – ability to store and later analyse spectrum monitoring on unprecedented scale

- Cybersecurity – the nature, speed and volumes of data in the cyber domain require new tools to achieve situational awareness and superiority.

- Predictive Maintenance – modern ships, weapon systems, etc. have advanced monitoring systems that generate usage data that can be used to improve availability, reduce operational costs, etc.

- Intelligence and rise of open source intelligence – intelligence, surveillance and reconnaissance require new analytical tools that can allow efficiently analyse available (multi-source) data.

- Using training performance to shape career paths for personnel…

AI – Global Perspective

**"Artificial Intelligence is the future, not only for Russia but for all humankind...
Whoever becomes the leader in this sphere will become the ruler of the world"**

Russian President Vladimir Putin

- All leading global players agree that superiority in AI adoption will lead to military superiority

- … some argue that AI arms race has already started

- The challenge is that AI is a truly general purpose technology
  - Algorithms, software solutions are mostly application agnostic
  - This race is driven by civilian capabilities
  - … however applications are heavily specialised, require competent defence sector

- Countries have different strategies to tackle the problem

AI Strategy – China

China spends more on AI research than the U.S. does

China has outdone the US in AI-related patent applications
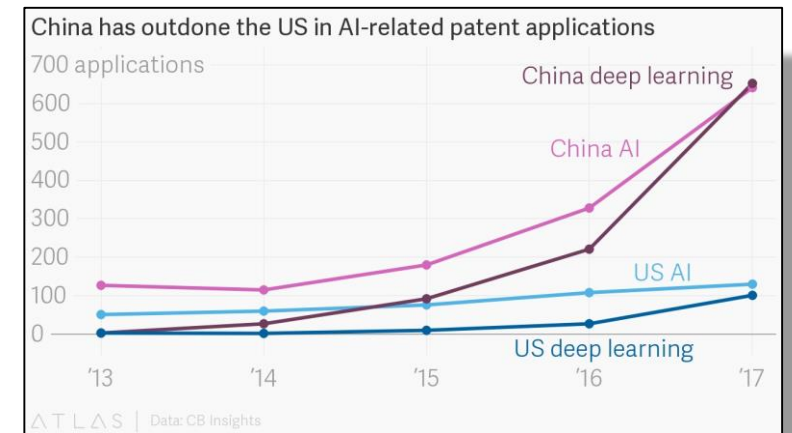
- Chinese leadership believes that AI technology is the future of military and economic global competition – convoluted relation between government, industry and military

- China is aggressively pursuing military use of AI
  - Specialises in applications of AI
  - Most of academic papers on AI
  - Most patents related to AI
  - Lack of development of software tools and platforms

- Ministry of National Defense established two new major research centres:
  - Artificial Intelligence and Autonomous Systems

- Challenge: ease of access to advanced know-how through online learning

What Can We Learn from Best Practices?

Surprisingly, Data Science is NOT about Best Algorithms

"Amateurs talk strategy. Professionals study logistics."

- What are the best algorithms?
  - The answer is simple: there are no best algorithms
  - It depends on the nature of the problem
  - It depends on the nature of the data set
- What are the best tools?
  - Again, it is not really about software
  - Availability of free software packages that are up to the task
- What is **important**:
  - Creative way to encode, reshape the data
  - … basically expertise in AI algorithms, statistics, programming and business sense
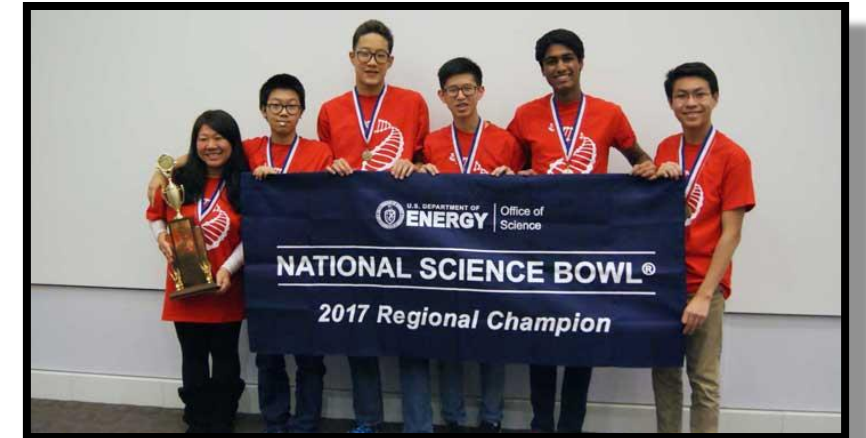
Acquiring Talent – Challenges

Defence sector competes for talent with other sectors

- Development of analytical solutions is far from being automated process
  - Shortage of skilled professionals is a real problem

- Defence has unique appeal and there are various approaches possible
  - Stability, career progression schemes
  - Combination of service and civilian work
  - Learn from cybersecurity:
    - Very impressive programmes sponsored by UK MOD

- Acquiring talent by other countries?
  - Ideological motivations
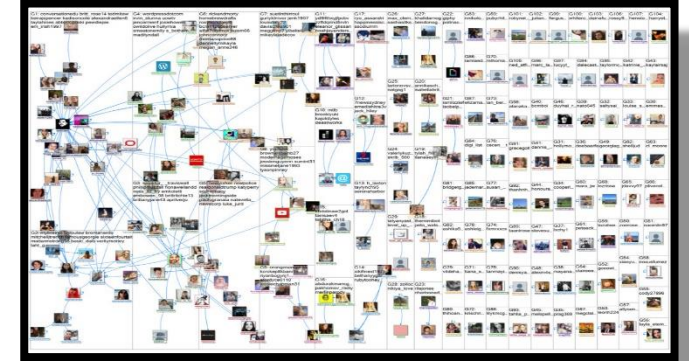
Challenges

- Defence is always facing dynamically changing environment, many wicked problems
  - For example healthcare, retail are relatively static
  - Providing data driven AI solutions is much harder for dynamically changing domains
- Nature of AI projects – it is good at solving well defined, specific problems
  - Implies *focus on projects and* **teams**
  - Success stories are best selling points
  - Please keep an eye on Project Nelson – this is a prime example how it should be done
- Organisational resistance to change vs. need for change
  - Emergence of AI and Cyber affecting defence in many aspects
  - New mindset and skillsets are required!