



Ministry  
of Defence

Ministry of Defence  
Main Building  
Whitehall  
London SW1A 2HB  
United Kingdom

Telephone [MOD]: 020 7218 9000

E-mail: DDC-  
SecretariatParliamentary@mod.gov  
.uk

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

Our Ref: FOI2019/10999

E-mail: [REDACTED]

18 October 2019

Dear [REDACTED]

Thank you for your e-mail of 25 September 2019 requesting the following information:

*Please can I ask for copies of the presentations (text of talks as well as power-point presentations) delivered at the Defence and Security Equipment International (DSEI) event by the following serving officers and MoD officials:*

- [REDACTED] 'The Science of Information Warfare: How Psychology, Big Data & AI will Revolutionise Decision-Making' (10 September 2019)
- [REDACTED] Defence Intelligence, 'Technological Change & the Threat Dynamic' (9th September 2019)
- [REDACTED], 'Joint Forces Command: Information Age Warfare' (10 September 2019)
- [REDACTED] Head of Data, AI, Automation & Digital, 'MoD's Approach to Data: Capability Management, Sharing and Classification' (11 September 2019)

I am treating your correspondence as a request for information under the Freedom of Information Act 2000 (FOIA).

I can confirm that the Ministry of Defence does hold some information within the scope of your request. The PowerPoint presentation used by [REDACTED] is attached separately and titled "DSEI-Psych-Data-AI there were no speaking notes used at the event. The text for [REDACTED] is also attached. Information for [REDACTED] is not held as he did not attend DSEI. Information is also not held for [REDACTED] as he did not use a PowerPoint presentation and used hand written notes for his speech which have not been retained.

If you are not satisfied with this response or you wish to complain about any aspect of the handling of your request, then you should contact me in the first instance. If informal resolution is not possible and you are still dissatisfied then you may apply for an independent internal review by contacting the Information Rights Compliance team, Ground Floor, MOD Main Building, Whitehall, SW1A 2HB (e-mail [CIO-FOI-IR@mod.gov.uk](mailto:CIO-FOI-IR@mod.gov.uk)). Please note that any request for an internal review must be made within 40 working days of the date on which the attempt to reach informal resolution has come to an end.

If you remain dissatisfied following an internal review, you may take your complaint to the Information Commissioner under the provisions of Section 50 of the Freedom of Information Act. Please note that the Information Commissioner will not investigate your case until the MOD internal review process has been completed. Further details of the role and powers of the Information Commissioner can be found on the Commissioner's website [www.ico.org.uk](http://www.ico.org.uk)

Yours sincerely,

DDC Secretariat Parliamentary

# The Science of Information Warfare

DSEI

How Psychology, Big Data & AI will Revolutionise Decision-Making  
10 September 19



**1** Data driven influence campaigns

**2** Cognitive manoeuvre

**3** Out of the loop & off the team

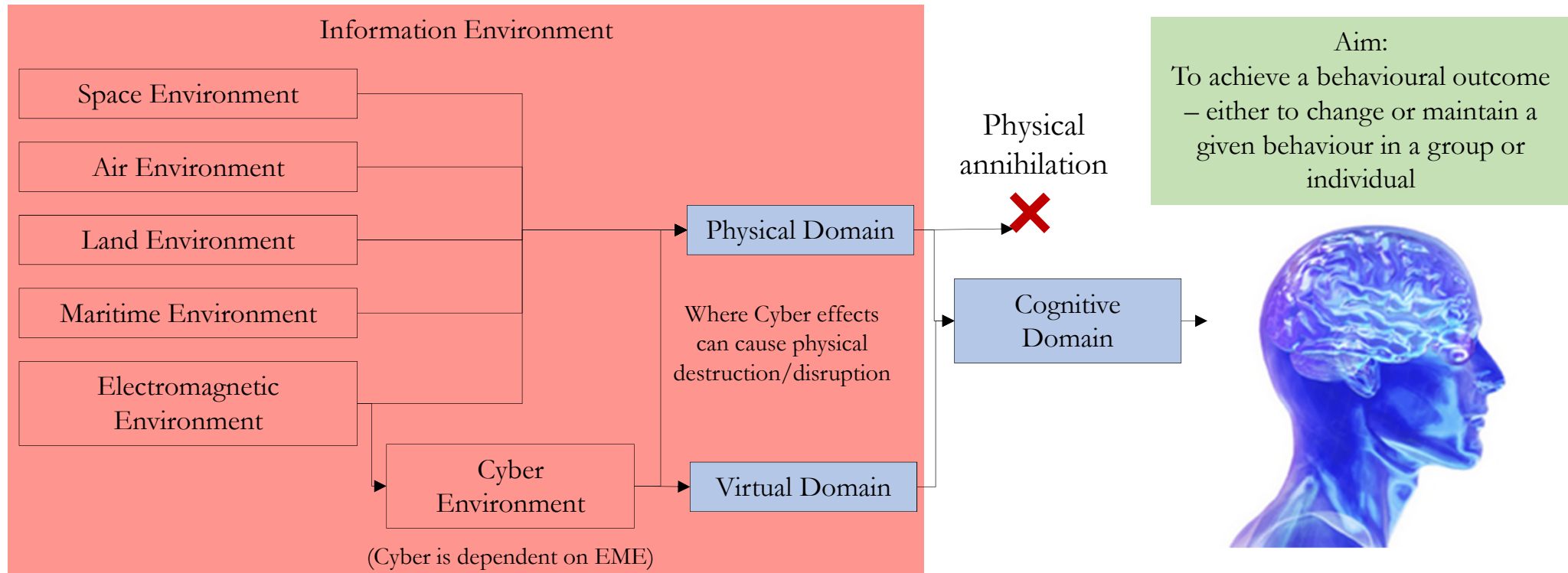
**4** Otherworldly moves

**5** Rigour

# Psychology: the heart of future operational design

*“War is merely the... ..the continuation of policy... ..of political intercourse carried on with other means”*

Clausewitz, *On War*, Ch.1, Sect. 24, Princeton University Press translation (1976)



*“[Violence’s] ...only purpose, unless sport or revenge, must be to influence somebody’s behaviour, to coerce his decision or choice.”*

Thomas Schelling, *Arms and Influence* 1966.



# You are just data



# Living in the Panopticon

## The Data on Data Brokers



**4K** data broker companies worldwide



Axiom, one of the largest data brokering companies, has:

- 23K servers collecting and analyzing consumer data
- Data for 500 million consumers worldwide
- 1.5K data points per person

**1.4K+** "leading brands" sell information from store loyalty cards

**80%** of U.S. email addresses are on file on **towerd@ta**



**38%** of employed Americans' pay stub information is available on **EQUIFAX**



Databases like **Campaign GRID** and **PRO PUBLICA** have political information including party affiliation and campaign contributions for **80%** of registered American voters

Image Credit: Infographic created by WebpageFX: "What Are Data Brokers and What Is Your Data Worth" <https://www.webpagefx.com/blog/>

**5200 GB per person by 2020\* = 18.5 million books.**

\*Source: <https://www.computerworld.com/article/2493701/data-center/by-2020--there-will-be-5-200-gb-of-data-for-every-person-on-earth.html>

## Google knows...

...every google ad you've seen, every app ever searched for, installed, launched or used & when + who you interacted with on them... ...every website ever visited and what time... ...**search history across all devices** even if you've deleted it... ...**the news you've read and the images you search for**... ...what time you sleep... ...your youtube history... ...bookmarks, emails sent & received, contacts, Google drive files... **all of the photos on your phone w/year, date, time, location**... ...the businesses you've bought from and anything you bought through Google... **your calendar, which of the meetings you showed up for and whether you were on time**... ...the music you listen to & books you've purchased... the websites you've created and phones you've owned...how many steps you take in a day.... ...it keeps everything you've save to you google drive including the google docs you've deleted...

...creates an ad profile based on location, gender, age, hobbies, career, interests, relationship status, possible weight, income.

Source: Twitter Dylan Curran @iamdylancurran



# Data Driven Influence Campaigns



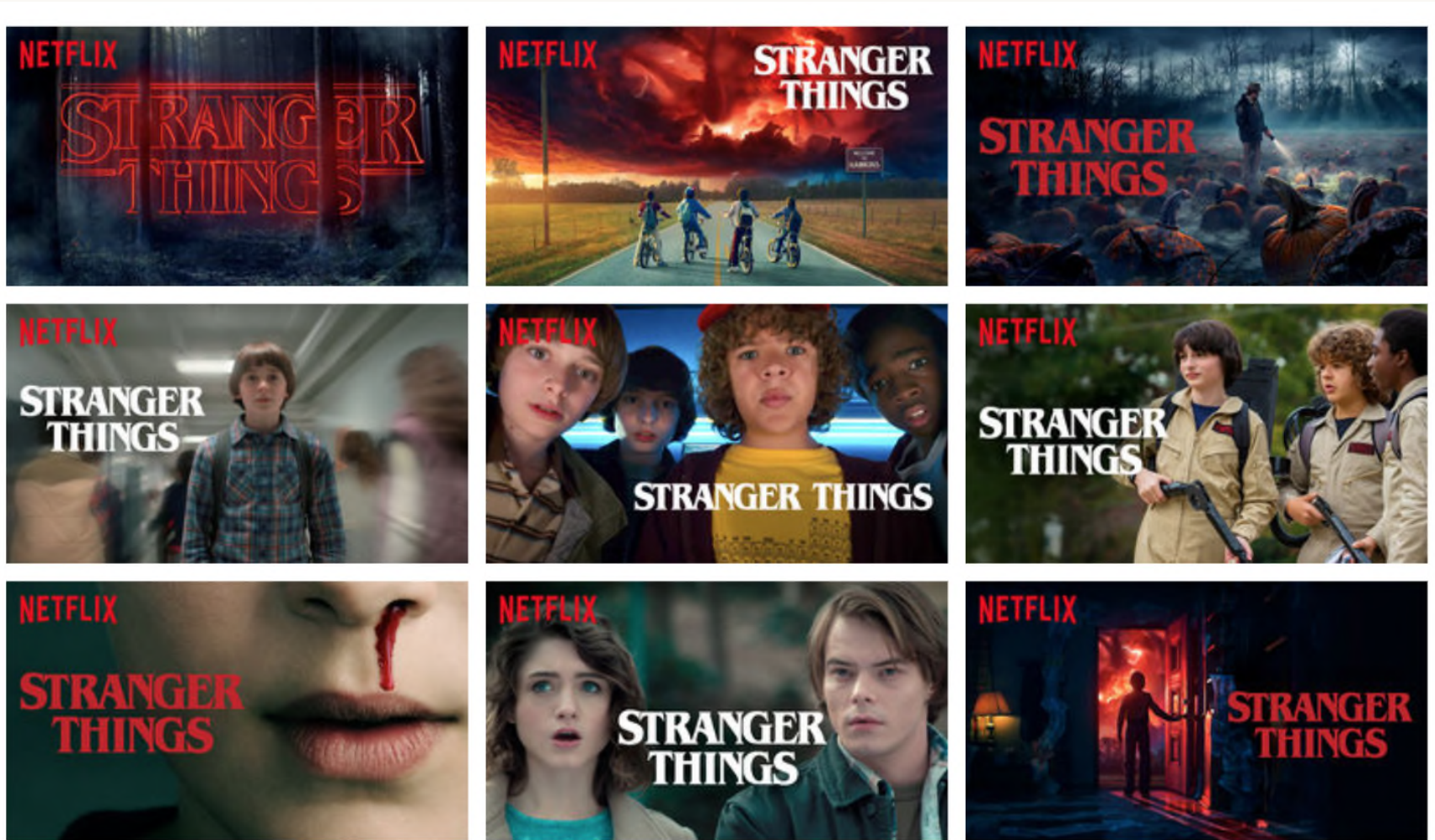
1. Machine learning personality assessments more accurate than:
  - co-worker after 10 likes,
  - friend or co-habitant after 150 likes,
  - spouse after 300 likes
2. Higher external validity in predicting life outcomes – substance abuse, political attitudes, physical health.
3. Sometimes better than self-rated personality surveys.  
**NB. Limitations: 10 item questionnaire.**

OCEAN:

Openness  
Conscientiousness  
Extroversion  
Agreeableness  
Neuroticism



# Personalised Propaganda & Weaponised Experimentation



Threat: Cognitive Security?  
Opportunity...? (Ethics)

# Mathematicians & Physicists?





# Unprecedented Insight. Cognitive Manoeuvre? A Small Sample from the Science of Prediction

- **Predicting (Big Five) personality based on eye movements.** Hoppe, S., Loetscher, T., Morey, S. A., & Bulling, A. (2018). Eye movements during everyday behavior predict personality traits. *Frontiers in human neuroscience*, 12, 105.
- **Computer-based personality judgments are more accurate than those made by humans.** Youyou, W., Kosinski, M., & Stillwell, D. (2015). *Proceedings of the National Academy of Sciences*, 112(4), 1036-1040.
- **Machine learning shows that a single Facebook like can predict who you will vote for.** Kristensen, J. B., Albrechtsen, T., Dahl-Nielsen, E., Jensen, M., Skovrind, M., & Bornakke, T. (2017). Parsimonious data: How a single Facebook like predicts voting behavior in multiparty systems. *PloS one*, 12(9), e0184562.
- **Facebook data used to predict your degree of political engagement or activism.** Brandtzaeg, P. B. (2017). Facebook is no “Great equalizer” A big data approach to gender differences in civic engagement across countries. *Social Science Computer Review*, 35(1), 103-125.
- **Predicting your credit-worthiness based on your call data.** Agarwal RR, Lin CC, Chen KT, Singh VK (2018) Predicting financial trouble using call data—On social capital, phone logs, and financial trouble. *PLOS ONE* 13(2): e0191863.
- **Data scientists given anonymous credit card data could name shoppers with just four random pieces of information from social media sites.** De Montjoye, Y. A., Radaelli, L., & Singh, V. K. (2015). Unique in the shopping mall: On the reidentifiability of credit card metadata. *Science*, 347(6221), 536-539.
- **Determining how many close friendships you can maintain from mobile (cell) phone data.** Saramäki, J., Leicht, E. A., López, E., Roberts, S. G., Reed-Tsochas, F., & Dunbar, R. I. (2014). Persistence of social signatures in human communication. *Proceedings of the National Academy of Sciences*, 111(3), 942-947.
- **Predicting emotional states from social media post content.** Kross, E., Verduyn, P., Boyer, M., Drake, B., Gainsburg, I., Vickers, B., ... & Jonides, J. (2018). Does counting emotion words on online social networks provide a window into people's subjective experience of emotion? A case study on Facebook. *Emotion (Washington, DC)*.
- **Categorising emotion based on eye movements.** Raudonis, V., Dervinis, G., Vilkauskas, A., Paulauskaite-Taraseviciene, A., & Kersulyte-Raudone, G. (2013). Evaluation of human emotion from eye motions. *Evaluation*, 4(8).
- **Predicting Surprise attacks based on leaders languages.** Suedfeld, P., & Bluck, S. (1988). Changes in integrative complexity prior to surprise attacks. *Journal of Conflict Resolution*, 32(4), 626-635.
- **Mood forecasting& predicting PTSD, depression, & schizophrenia from how you swipe and tap your touchscreens, or from phone and wrist-band (fitbit or apple watch style devices) data,** Kaplan, M. (2018), Happy with a 20% chance of sadness., *Nature* 563, 20-22.
- **Atrocity Forecasting,** <http://politicsir.cass.anu.edu.au/research/projects/atrocity-forecasting>
- **Suicide Prevention,** How Facebook AI Helps Suicide Prevention, 10 Sep 18. <https://newsroom.fb.com/news/2018/09/inside-feed-suicide-prevention-and-ai/>
- **Pre-Crime?** <https://www.thejc.com/news/news-features/israel-leads-the-way-in-brave-new-world-of-ai-artificial-intelligence-1.460264>

# Out of the Loop & Off the Team

1. Data Deluge. '*Swimming in sensors, drowning in data, thirsting for insight*'.
2. Humans are limited: overcoming cognitive, attentional and physical limitations.  
e.g. Uruzgan & info overload (*necessity, distinction, proportionality, humanity*)
3. Speed. London-New York's financial industries trades in less than 400 microseconds - a 1 millisecond delay costs >US\$100m a year.
4. Human-Machine teaming is only a short-term answer.



# Other-Worldly Moves

*“There’s some inhuman element in the way AlphaGo plays... ..Because it’s so hard to try to attach a story about what AlphaGo is doing.”*

Michael Redmond.



AlphaGo vs Ke Jie, May 2017

<https://www.theatlantic.com/technology/archive/2017/10/alphago-zero-the-ai-that-taught-itself-go/543450/>

And: <https://www.linkedin.com/pulse/through-glass-darkly-future-character-conflict-john-dowdy/>

Heider, F., & Simmel, M. (1944). An experimental study of apparent behavior. *The American journal of psychology*, 57(2), 243-259.

# AlphaStar, E-sports, Starcraft II

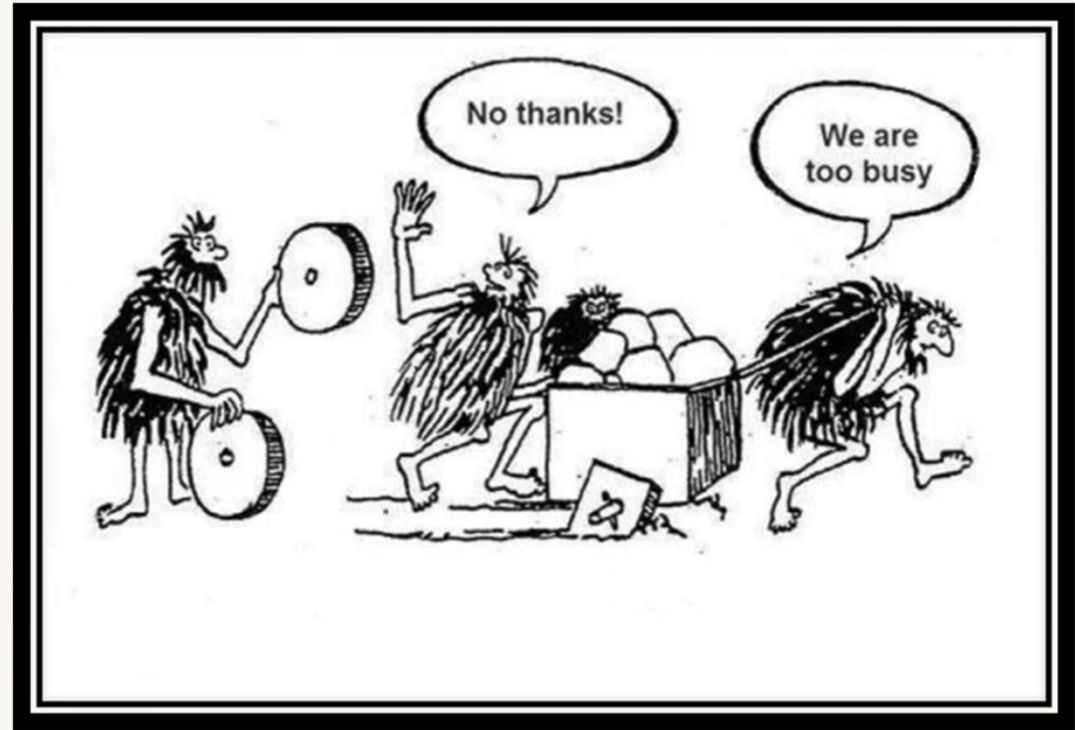
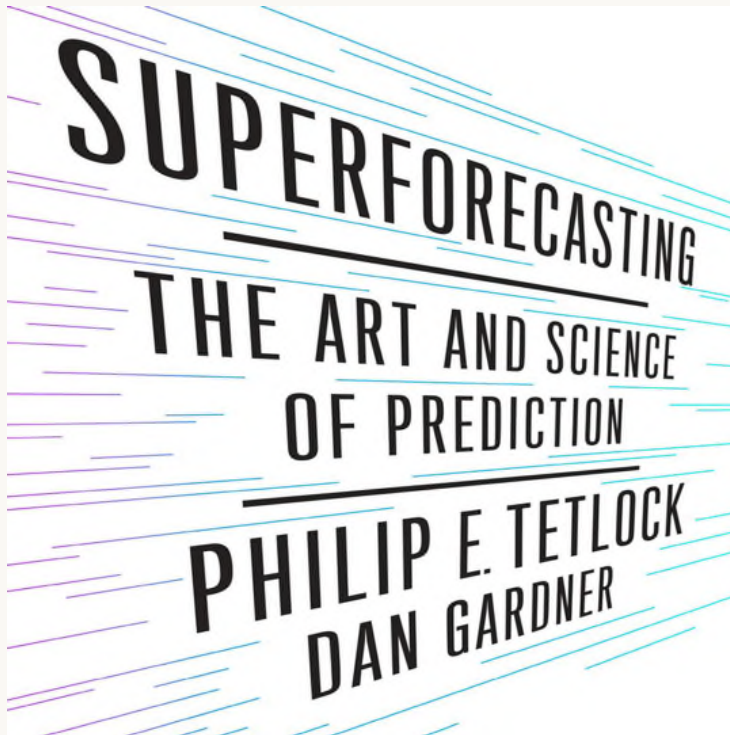
“...early on... ..[AlphaStar]...favoured... ..risky strategies... ..discarded as training progressed, leading to other strategies: for example, gaining economic strength by over-extending a base with more workers, or ...disrupt[ing] an opponent's workers and economy. This process is similar to the way in which players have discovered new strategies, and were able to defeat previously favoured approaches...”



- **Game theory**
- **Imperfect information**
- **Long term planning**
- **Real time**
- **Large action space**



# How good are we?



Baselining:

- Forecasting accuracy;
- Decision confidence.

# Science of Information Warfare

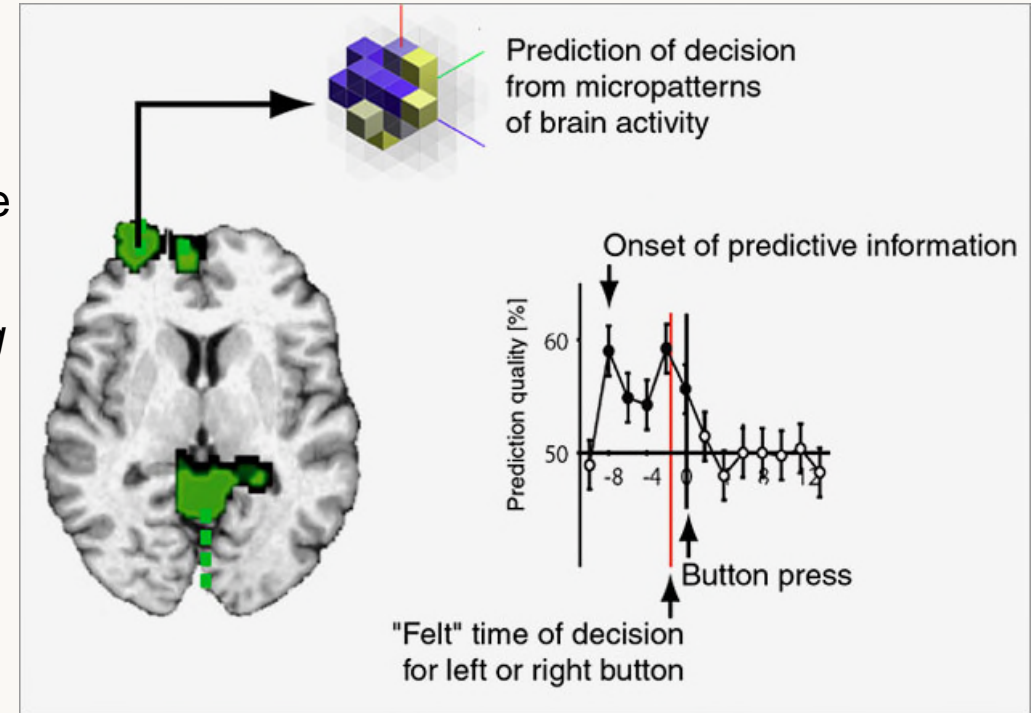
QUESTIONS





# Who's in Charge?

- Libet et al. (1983) & Soon et al. (2008).
- Haidt - moral instincts.
- Gazzaniga – left brain interpreter (confabulator vs the right brain literalist)
- Trivers, R. (2011). *Deceit and self-deception: Fooling yourself the better to fool others*. Penguin UK.



Soon, C. S., Brass, M., Heinze, H. J., & Haynes, J. D. (2008). Unconscious determinants of free decisions in the human brain. *Nature neuroscience*, 11(5), 543.

Libet, B., Gleason, C. A., Wright, E. W., & Pearl, D. K. (1983). Time of conscious intention to act in relation to onset of cerebral activity (readiness-potential) the unconscious initiation of a freely voluntary act. *Brain*, 106(3), 623-642.

Haidt, J. (2001). The emotional dog and its rational tail: a social intuitionist approach to moral judgment. *Psychological review*, 108(4), 814.

Gazzaniga, M. S. (2000). Cerebral specialization and interhemispheric communication: Does the corpus callosum enable the human condition?. *Brain*, 123(7), 1293-1326.

# A Rising Tide



“The human won — but not before the machine had proved itself able to produce compelling and coherent arguments, form rebuttals to Mr Natarajan’s statements, make a closing argument and even throw in a few jokes for good measure.”



Image credit: Ben Edwards Medium Blog (*What do we mean by intelligence, artificial or otherwise?*) illustration of Hans Moravec’s “landscape of human competence” <https://alltext.com/what-do-we-mean-by-intelligence-artificial-or-otherwise-e5f72fbe8698>, original taken from Tegmark, M. (2017). *Life 3.0: Being Human in the Age of Artificial Intelligence*. Knopf. p.53



## DSEI - Technological Change and the Threat Dynamic

### *Technological Change*

Previous roles – command of Army’s Bomb Disposal Group and before that, in Army Headquarters, led capability development for EOD, Search, Electronic Counter Measures and Special Projects.


**Technological change.** Innovation often comes from the unexpected power of the combination of various technologies for new purposes that had never been envisaged – such as the unexpected and highly disruptive combination of phone, GPS, real time tracking and software that led to Uber and similar services that disrupt a traditional service industry.

**In short, technological change is based on both better and more technology.**

There are always some future technology areas that are seized upon enthusiastically in the media: self-serving killer robots, biological weapons of mass destruction, and gene editing technology that could produce even greater horrors, by attacking human DNA and creating genetic changes in future generations.

However, before we leap to some of the more exotic and exiting technologies it might be worth reminding ourselves of some of the technological deficiencies on today’s battlefield. Increasingly we are facing overmatch in the land environment. Much of the military technology we field today has its origin in the 1980’s and 1990’s (**CR2** 1998 and **WR** 1986) – or 1970’s in the case of **CVR(T)**. We have not upgraded our MBT or armoured vehicles since then, despite some of our peers and near-peers having carried out 4 or 5 upgrades in that time. We should not underestimate the enhancements in capability that can be achieved by upgrading old platforms with new technology and software. In modern warfare weapons are increasingly software-driven.

Looking into the immediate future of the land battle there are likely to be some obvious and relatively economical choices to enhance land capability including:

- UAVs and C-UAV technologies
  - Signature Reduction
  - Active Protection Systems
  - Additive manufacturing
- 



- Battery Technology
- Smart munitions
- Lasers/Directed Energy Weapons

However, I think the area of greatest technological impact, and one that has been clearly signposted as the area of technological change affecting all domains including land, lies in the changes that have been brought about by **digitisation**.

Digital change - accelerating at an unprecedented pace. Therefore our efforts might sensibly be focussed on those technology trends that are essential to success in an increasingly digital environment and ones in which our potential adversaries have accelerated their R&D in recent years:

**Information Advantage** as a concept is taking root within Defence. It is defined as the credible advantage gained through the **continuous, adaptive, decisive and resilient employment of information and information systems**. We live in a data-rich information age in which the exponential growth in: **computer capability, data, and digital connectivity** - is fundamentally shaping almost every facet of modern life. Information, and the way we use it to prosecute warfare, pass information and maintain situational awareness, both at home and overseas – is vital. Information advantage is relevant in the land domain – never more prescient than in the pursuit of **Joint Action** – as the land battle will not just be fought on the ground with tanks and artillery, but as part of a much wider and complex multi-domain environment, where information architectures - across domains, systems, Government and Allies – and the effective use of EW and Cyber capabilities - will be key to preserving the land force's operational advantage. As CGS recently stated at the Land Warfare Conference “...*The **measure of military power** is no longer the volume of hardware ie numbers of tanks and armoured vehicles, but the **sophistication of software and associated AI...***”.

**Robotics and autonomous systems** offer huge potential for future land warfare. Advances in machine autonomy relies primarily on research efforts in: **artificial Intelligence, robotics, and control theory**. Our potential adversaries are investing huge amounts of R&D money into this area. Exercise Autonomous Warrior was an excellent start but we must up the ante in this vital area of research.

Technology today, in the civilian sphere, is constantly changing and evolving.

Defence needs to catch up. Our weapon systems have become ever more complex **but** user interfaces are often overly complicated. **An effective human-machine interface** makes decision-making easier, and can accelerate reaction times to incidents.

AI - offers opportunity for the development of human-machine teaming.

Revolutionise land warfare - improve our ability to survey, track and destroy threats.

Turning to technology's impact on the Defence Enterprise (Defence, Industry, and Academia) and the need for **collaboration and innovation**. Keeping up with the **pace of technological change**, and **evermore advanced adversary weapons systems**, is now taxing our traditional organisations and processes. Dstl has long fulfilled the role of providing independent, high quality scientific and technological support to the MoD and UK Armed Forces - in those areas deemed inappropriate for the private sector. Increasingly Dstl finds itself short of key skillsets: software and RF engineers, data scientists, and cyber security experts to name a few. As a result it must bring in those from outside Defence - industry, academia, and international partners – to keep up with technological change and provide the sensitive and specialist S&T support so desperately needed by Defence.

But how?

Private sector - increasingly integrating their core functionalities with third parties and utilising shared cloud-based platforms. The Defence Enterprise could use recent technological developments to **increase collaboration, drive innovation and speed up acquisition cycles**. Some excellent initiatives have been launched such as the Defence Innovation Fund to help drive S&T, and the Defence and Security Accelerator (DASA).- develop and demonstrate a number of novel technologies or applications in the area of Electro-Optics and Infrared (EOIR). However, if we are to utilise **all that technology** has to offer, then the introduction of more reliable and effective **information architectures** – both **resilient and secure** – across the **whole Defence Enterprise** will be needed.

Downside to our **globally-connected world** and **cloud-based systems**, which demands greater efforts in **cyber security**. More effective **security arrangements** and **vetting processes** are needed across the Defence Enterprise to protect against cyber penetration by

██████████

our adversaries, who will continue to target our IT systems and databases to glean defence-related secrets, with a particular emphasis on the Defence supply chain. In addition they **may seek to pre-position software on our networks**, military and industrial, which will enable them to deliver disruptive or destructive information effects in the periods of tension and war. We are at a disadvantage here living in a free, liberal, democratic society. Whilst we are exploring opportunities to respond in kind with offensive cyber tools, the relatively closed nature of the internet in more autocratic societies creates many challenges to overcome. In the meantime we need to focus on hardening our own Defence and industrial information networks, as well as adopting a ‘secure by design’ methodology in our own capabilities.

### ***Threat Dynamic***

Turning now to the Threat Dynamic - **Threat** can be viewed as a complex blend of **Capability, Intent and Opportunity**. Whilst it is relatively easy to gain an understanding of a potential adversaries’ ‘Capability’ – which is largely but not exclusively derived from S&T expertise and the effective exploitation of technology into weapons systems. It is much harder to deduce an adversary’s ‘**Intent**’ and very difficult to bring the necessary military force, or other means, to bear to deter or counter an adversary threat in a timely fashion – hence our constant efforts to spot **key indicators and warnings**.

‘**Opportunity**’ is something we can do something about – by adopting the correct posture and sending out the right messages, we can deny a potential adversary the opportunity to act through effective deterrence, albeit this can be problematic in the hybrid space between war and peace as I shall now explore.

Turning to our **potential adversaries** in detail – it’s no secret that **China, Russia** and maybe to a lesser degree **Iran and North Korea** - pose the UK (and other Western Allies) the most serious challenges for a number of different reasons, but **all are asserting themselves regionally and globally** in ways that challenge our security, stability and prosperity. In the last few years we have seen a recent shift away from the counterterrorism focus of the “Global War on Terror” back towards “great power competition”. China, Russia and Iran have all looked at how the West has fought, in various conflicts since Gulf War One, and

██████████



██████████

then actively worked to exploit the new vulnerabilities to their purposes. To paraphrase the Chief of the General Staff again:

*“...authoritarian regimes have interpreted and dissected Western assumptions on Defence and Security from recent history and are exploiting the hybrid space between peace and war – the roles of warfare are changing as sub-threshold activity is exploited by these regimes thus negating the Western advantage enjoyed for so long...”*

**Russian foreign policy** has been building up - to what it is today - for over two decades. It was first launched by Primakov, who was appointed Russian foreign minister in 1996. Russia determined that it would no longer follow the lead of Western powers, especially the United States, but would instead position itself as an independent centre of power on the world stage. Russia has extended its influence through the annexation of Crimea, the war in Ukraine, and is now fully engaged in offering support to Assad’s regime in Syria. Putin has demonstrated to the world, Russia’s propensity for risk-taking, along with its improved capabilities for warfare and operations short of war in multiple domains. In the words of CDS: *“...Russia is the most complex and capable security challenge we have faced since the Cold War...”*

**China** has certainly laid out its ambitions very clearly – Xi Jinping stated that the **“Strong Military Dream”** is critical to China’s national rejuvenation, and is marked by China’s quest for global military power, built on technological know-how. China also puts the emphasis on **“indigenous innovation”**, with a goal for the country’s reliance on foreign technology to decline. In the economic sphere China’s Belt and Road Initiative (BRI) seeks to connect China seamlessly with Europe to bring greater prosperity to China, but it is clear that China’s aspirations for greater economic prowess and military strength are inextricably linked. To help facilitate this military power, China has adopted an approach it calls **“military-civil fusion”** (MCF), which seeks to break down all barriers between the civilian sector and China’s defence industrial base in order **simultaneously** to achieve economic development and military modernisation.

Chinese industries have long sought the help of foreign suppliers and designers of equipment and components. In the 1970s and 80s, these specialists came primarily from

██████████

██████████

Europe and the US. However, in the early 1990's China turned to Russia, which was keen to bolster its arms sales. It is noticeable that sales agreements to China now include the full range of Russia's non-nuclear weaponry. Of course these systems are being exported elsewhere in the world as shown by the recent purchase of the S-400 system by Turkey.

Chinese companies are increasing their investment in digital hardware and software. China has also started to field its own advanced weapons, as its shift away from Russian exports is in part linked to its own growing manufacturing capabilities. China has not only learned from Russia, but given its financial and defence industrial base, in the future it is likely to have more chances to develop new military technologies as the size of the Chinese economy means that it has more resources to invest in research and development.

The proxy wars playing out in **Yemen and Syria** pose serious security dilemmas for the UK and our Allies in the Middle Eastern region, and perhaps stem from Iran's own regional aspirations. For the past two centuries Iranians have been unhappy about the "great game" of the world's major powers. Iranian governments have continuously strived to convince the world that Iran is a power to be reckoned with. The main goal is to resist the United States' "unilateralism" in world politics, by leading opposition against Western dominance, albeit through ways which would not end up in open conflicts. Following what may prove to be the collapse of the Joint Plan of Action (or Iran nuclear deal), with the US withdrawing and imposing trade sanctions, there have been a number of security incidents in the Gulf of Oman involving oil tankers, that has seen the UK (and other allies) attempt to safeguard international shipping lanes through the Strait of Hormuz with maritime forces. It highlights the fragility of our relationship with Iran, and the potential for escalation.

Most concerning though is the degree to which the West has **conceded its technological advantage** to our potential adversaries. We have seen this new paradigm coming for a few years now. Our advantage has been eroded across a number of **key capability areas**. Many of these systems are now in the hands of proxy states. As such there is a growing imbalance, and we can no longer be assured of technological overmatch.

██████████