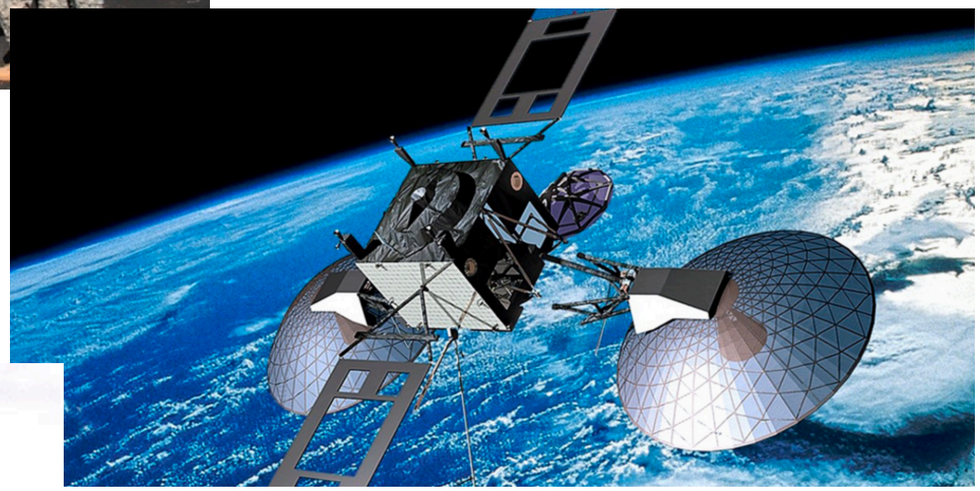
GRESHAM COLLEGE

Computers and Warfare

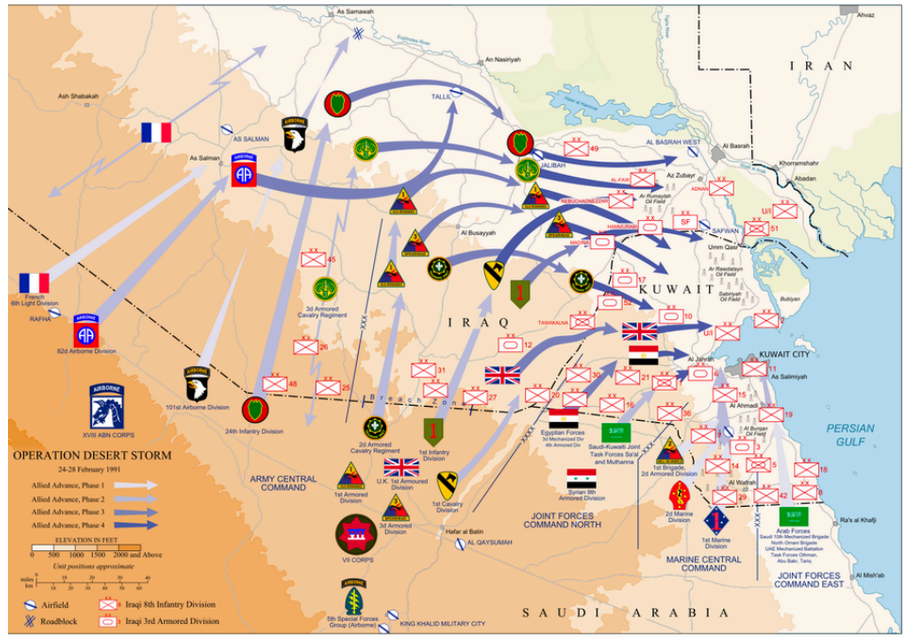
Martyn Thomas CBE FREng
Livery Company Professor of Information Technology

Computers and Warfare

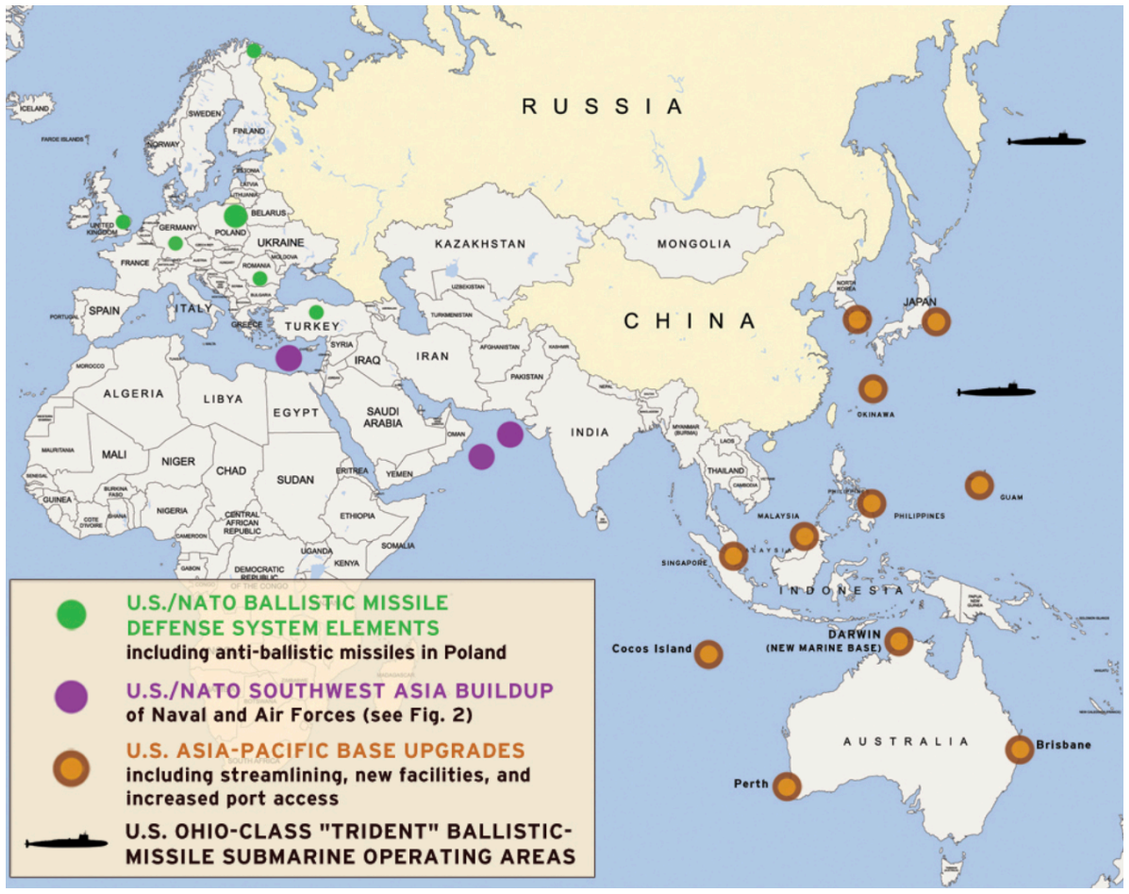


Warfare is traditionally geographic

- Defending your own territory
- controlling enemy territory
- Freedom of movement



- Controlling strategic locations
- supply lines …
- but cyberspace is a different dimension that has no borders



Cyberspace

- Computers, networks, online and offline data, sensors actuators, software and hardware, applications …

- It carries information and commands that may be trivial or may be critical

- Cyberspace reaches across borders and through walls and its topology changes every microsecond, as connections are made and unmade

- It is addressable, but the addresses are not fixed to locations or to physical devices

- It is almost instantaneous and is the world’s most trusted source of news

Warfare in Cyberspace must change Military Strategy

- Land, Sea, Air, Space **and now cyberspace**

- cyberspace has no borders and almost no latency - weapons can be deployed instantly from anywhere to anywhere

- Offensive Cyber weapons are cheap - especially if you steal them

- Cyber warfare erodes the advantage traditionally held by rich nation states.

“War is the continuation of policy with other means”

Carl von Clausewitz

Cybersecurity and National Defence

- How will nations defend their critical national infrastructure … or the many other vulnerable major hazard sites?
- Security of supply chains depends as much on industrial strategy as on military strategy
- Will major military platforms still be able to be used to exert diplomatic pressure?
- Can ships and aircraft protect themselves and their supply chains from cyberattack?
- How can a cyber attacker be identified with enough certainty for a counterattack?
- Western societies depend heavily on cyber space, which makes them particularly vulnerable to a cyber or EMP attack

Nation State cyberattacks

Stuxnet 2005 - 2010

An attack on the >7,000 gas centrifuges that were used to enrich Uranium for the Iranian nuclear programme

“Yellowcake” uranium oxide is 99.3% U238, 0.7% U235
(reactor: 3-4% U235, bomb >90%)

This recent undated satellite image provided by Space Imaging/Inta SpaceTurk shows the once-secret Natanz nuclear complex in Natanz, Iran, about 150 miles south of Tehran.

AP PHOTO/SPACE IMAGING/INTA SPACETURK, HO

Nation State cyberattacks

DDoS attack on Estonia 2007

A major attack on government departments, banks and media websites

Attributed to Russia by the Estonian Foreign Minister

Iran: Stuxnet 2005 - 2010

Attributed to the USA and Israel

Saudi Arabia 2012

Caused crashes and data loss. Every office worldwide had to be disconnected. 30,000 computers damaged. Oil had to be given away free. 50,000 hard drives purchased …

Claimed by “Cutting Sword of Justice”

Attributed to Iran

Saudi Arabia December 2017

EXCLUSIVE

Cyberattack Targets Safety System at Saudi Aramco

One report points to Iran, but the evidence is far from conclusive.

BY ELIAS GROLL | DECEMBER 21, 2017, 6:08 PM

A flame from a Saudi Aramco oil installation burns brightly during sunset in the Saudi desert on June 23, 2008. (AFP/Marwan Naamani)

Attributed to Iran and Russia

Nation State cyberattacks

DDoS attack on Six US Banks in September 2012

This DDoS attack cost the banks tens of millions of $.
Claimed by an Islamist group but attributed to Iran

Cyberattacks against South Korea in 2013

Three TV stations and three banks infected with *Dark Seoul* malware
Attributed to North Korea

The attack on Sony Pictures in the USA in 2014

Infection and destruction of several computers and theft of data
Claimed by "Guardians of Peace" but Attributed to North Korea

Nation State cyberattacks

The attacks on the Ukranian Power Grid in 2015 and 2017

"The UK Government judges that the Russian government, specifically the Russian military, was responsible for the destructive NotPetya cyber attack."

Lord Ahmad of Wimbledon, UK Foreign Office minister.

Wannacry attack that seriously affected the NHS in May 2017

Serious disruption to the NHS and to 300,000 computers in 150 countries worldwide.

Nation state offensive cyber developed by the US NSA TAO, stolen by Russian *Shadow Brokers,* released on the internet and exploited by cyber criminals.

Cyberattacks attributed to China

Hacking of the Dalai Llama in 2008. 10 attacks reported up to 2010, an attack on 48 chemical and defence companies in 2011 and many more

Nation State Cyberattacks

Motives

- The motives for cyberattacks have mainly been
    - theft of intellectual property (such as weapons designs, university research and industrial IP)
    - Disruption of economic, political and social activities
    - Financial gain
    - demonstrations of power for policy reasons
    - reconnaissance and pre-deployment of cyber weapons

Nation State Cyberattacks

Reconnaissance

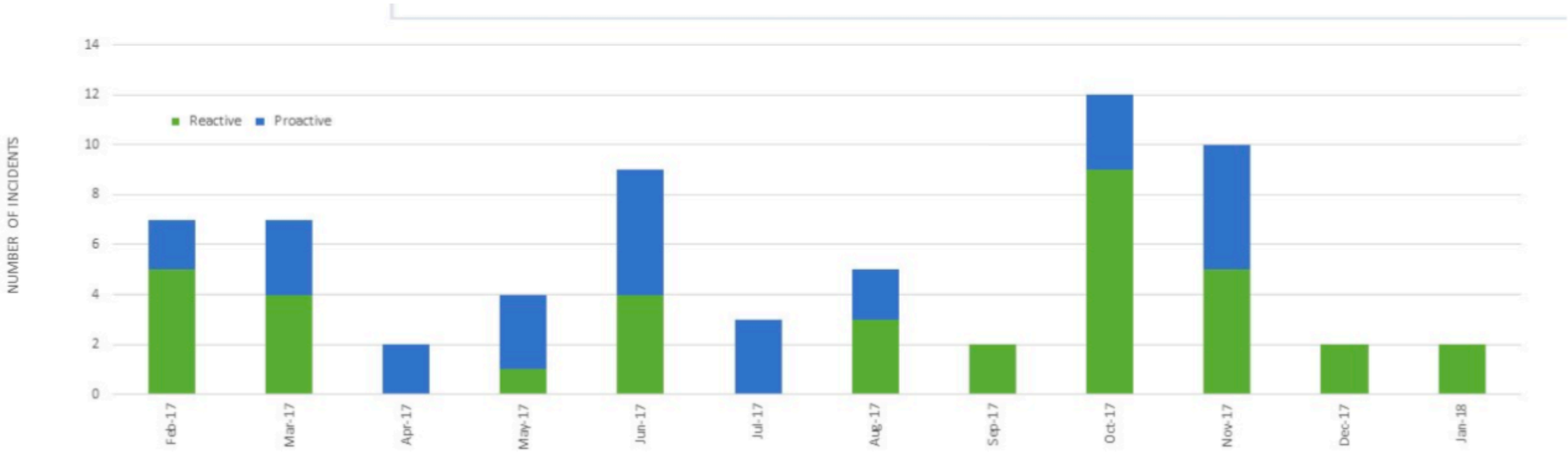
- Most major companies experience hundreds of “cyberattacks” every day:
    - trivial probes to determine what software is running
    - malicious emails (specifically targeted or not)
    - Serious attempts to penetrate networks or equipment
- Some of these will be nation state associated, either to steal data or to compromise systems.

BT Group data

evidence published by the Joint National Security Strategy Committee in 2018

BT Group data

evidence published by the Joint National Security Strategy Committee in 2018



BT Group data

evidence published by the Joint National Security Strategy Committee in 2018

2.2 As figure 3 shows, we are at risk from a range of attackers: hackers, criminals, nation states and terrorists. However, the majority of the threats we see come from organised criminal groups.

Figure 3: Origin of cyber risk to BT

State-sponsored attacks on Industrial Control Systems

"The NCSC is aware of connections from multiple UK IP addresses to infrastructure associated with advanced state-sponsored hostile threat actors, who are known to target the energy and manufacturing sectors … NCSC believes that due to the use of wide-spread targeting by the attacker, a number of Industrial Control System engineering and services organisations are likely to have been compromised."

Leaked NCSC Report, July 2017

The UK seems against the idea of an *Offensive Cyber non-proliferation treaty*

"We affirm states' legitimate right to develop both offensive and defensive cyber capabilities, and emphasise their obligation to ensure their use is governed in accordance with international law."

UK-Poland cyber co-operation commitment published 21 December 2017

Propaganda, Persuasion and PsyOps

- Propaganda and other psychological operations are one of the oldest weapons of war

- Modern social media and the commercial collection of personal data on whole populations make PsyOps easier

- Examples are the Russian interference in the election of Donald Trump and in the BREXIT referendum

- Soldiers can be identified and their families targeted

- Facebook is the world’s most trusted source of news

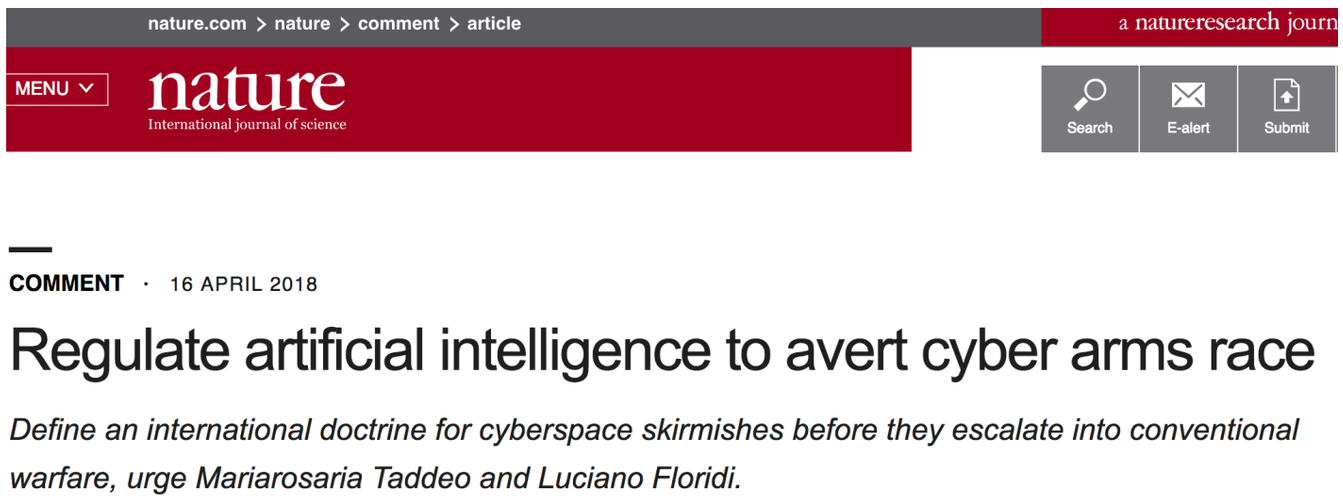
Autonomous Weapons

- Landmines: banned by the Ottawa Treaty of 1999
  - As of January 2018, 164 states are party to the treaty
  - There are 34 non-signatories, including major powers such as the United States, Russia, and China
  - Few countries in the Middle East and South Asia have opted to participate
- Autonomous Air Defence systems?
  - Most Western countries require a “Man in the loop” …
  - … but consider the USS Vincennes, which shot down Iran Air flight 655 on a scheduled flight at 12,000 ft on July 3 1988, killing 290 passengers

StratoEnergetics LIVE STREAM
http://www.stratoenergetics.com
Buenos Aires Event
TV Truck 02

Ethics, regulations and practicalities

- More and more AI will be used in weapons systems
- *Should* the decision to kill be delegated to systems that cannot explain the decisions that they took?
- The cybersecurity of machine learning systems is an unsolved research problem
- What national or international controls should there be on the use of AI in lethal weapons – and on cyber weapons?
- Is it practical to regulate such technologies? Would regulation weaken law-abiding countries relative to terrorists and rogue states?



Conclusions

- All of society depends on digital systems and these systems are vulnerable to cyberattack, because people are careless and software is not well engineered

- Offensive Cyber must change most military strategy radically

- The military advantages that major powers have possessed will increasingly become weaker

- Preparation for cyber warfare has already started. Some malware is already in place in critical systems

- Future national security will depend on changes to industrial strategy and on much stronger software engineering

Questions?