‘Weaponising Big Data’

Paul Mobbs
CroughtonWatch, October 2019
email:
croughtonwatch
@fraw.org.uk
web:
http://www.fraw.org.uk/
frn/wbd.html

A summary of how – from mini-nukes, to autonomous drones, to mass surveillance, to industrial-scale hacking – information technology is changing the military and intelligence agencies, making them more injurious to civil and human rights

War was always a driver of technological development. Today, however, it is technology that is driving warfare.

Over the last two decades, the development of global data networks and mobile communications has provided military and intelligence agencies with a new arsenal of tools. These are transforming the nature of conflict and military power.

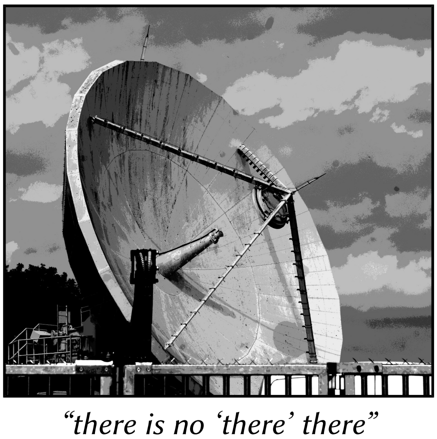
What is emerging from this 'brave new world' of technologically-enabled conflict is not 'conventional' weaponry; it is a troubling mix of: psychological information warfare; clandestine/covert operations on unknown battlefields; and, a worrying blurring of the distinction between who is a civilian and who is a soldier.

“Move fast and break things”

In the 1990s the US military, and thereafter members of NATO, began to embrace a new concept: *‘Network Centric Warfare’* (NCW).

NCW came out of the ill-fated ‘Star Wars’ project of the 1980s, and built upon the new information networking capability of the Internet. It sought to knit together all military forces across the globe within one, seamless system of information and telemetry sharing.

Since the late 1990s, though, the driver for new military technologies has been the development of civilian on-line information technologies.



“there is no ‘there’ there”

Just as the commercial use of networks is challenging traditional industries, so the use of IT by the military is challenging the historic legal and democratic checks on the use of military power:

As ever-more data flows over networks, as ever-more daily human interactions around the globe are digitised, so ever-more of people’s daily lives is available to be tracked, databased, and reviewed by military and intelligence agencies;

As machine learning, artificial intelligence, and ‘intelligence fusion’, is able to assimilate large quantities of data without the need for manual human review, so larger areas of the Earth can be put under constant surveillance – and ‘persons of interest’ constantly monitored to target when the necessity/opportunity arises.

As sensor technology – in the air, in space, or on the ground – provides greater spatial awareness, so smaller military units are required to undertake tactical strikes over longer distances – with few people knowing that these conflicts are taking place; and, combining all of these trends,

As automation takes-over more functions within the military, less people are required to ‘wage war’ – limiting the need for the state to justify the human or financial costs of conflict to the public.

Most of these systems were developed by the large IT consultancies. Inevitably some of these ‘military grade’ surveillance and automation technologies are now ‘leaking’ into civilian use – often under the guise of ‘anti-terror’ or homeland security.

As a result the lines between what is ‘civilian’ data, and what is ‘military’ or ‘intelligence’ data, has become blurred. Every human activity has now become ‘suspect’.

Surveillance is mandatory

The leading edge of these new military technologies is *information fusion*; the creation of complex databases of every piece of information it is practical for intelligence agencies to hoover-up on a daily basis.

In order to address unpredictable situations intelligence fusion systems must collect, categorise and store vast amounts of data continuously. This is fed into machine learning or artificial intelligence systems, to find patterns or evidence, presented on demand as a ‘situation report’ to the military and intelligence agencies.

The commercial world is now undertaking mass surveillance of the public at a level which would never have been permitted had it been a state undertaking these operations. This is largely the result of new social media, mobile computing, ‘smart devices’, and the developing ‘Internet of Things’ – all of which provides large amounts of additional data for potential military surveillance.

It would be impossible for ‘people’ to do this. It represents the leading edge of information automation, developed for civilian marketing or service corporations, and adapted for the lucrative military and intelligence market too. And as the line between military and civilian applications becomes blurred, more of this data finds its way into military systems.

E.g., Google’s *Maven* and IBM’s *Watson* AI systems are already undertaking military and intelligence work, sifting and classifying data.

As the Edward Snowden leaks outlined, many telecommunications and large data processing companies are also co-operating with military and security agencies to provide data – often, it has been judged, in breach of privacy and data protection laws.

At the same time though, as these systems become commonplace, a shift is taking place in the other direction too. Those with sufficient wealth can purchase both the hardware, and the data, to create their own 'intelligence' capacity.

This is not every-day 'marketing' or 'public relations'. It is branded, 'strategic communications'.

As the recent case involving Monsanto shows, large corporations are employing these techniques to counteract civil society groups.

Speed generates instability

The growth in global information systems, operating in real-time, has dramatically shortened the time between an event when countries far away are able to respond. The problem for the military is the mechanisms for response are still very slow.

As a result efforts now focus on speeding the response time of both 'hard' and 'cyber' weapons:

Firstly, the race is on to develop autonomous armed drones. These are designed to take to the air, sea, or ground, not simply to replace a person, but to do so for months or weeks at a time without requiring attention. There they can wait, either carrying out surveillance, or until they are tasked with an operation – cutting the time taken to move weapons into that area of the globe.

Secondly, quite separately from drones, the race is on to create *hypersonic aircraft*. These are missiles, but may in future be vehicles carrying other drones, flying at 4,000 miles per hour or more, and able to cross the globe in a few hours. This allows them not just to arrive quickly, but to evade air defences.

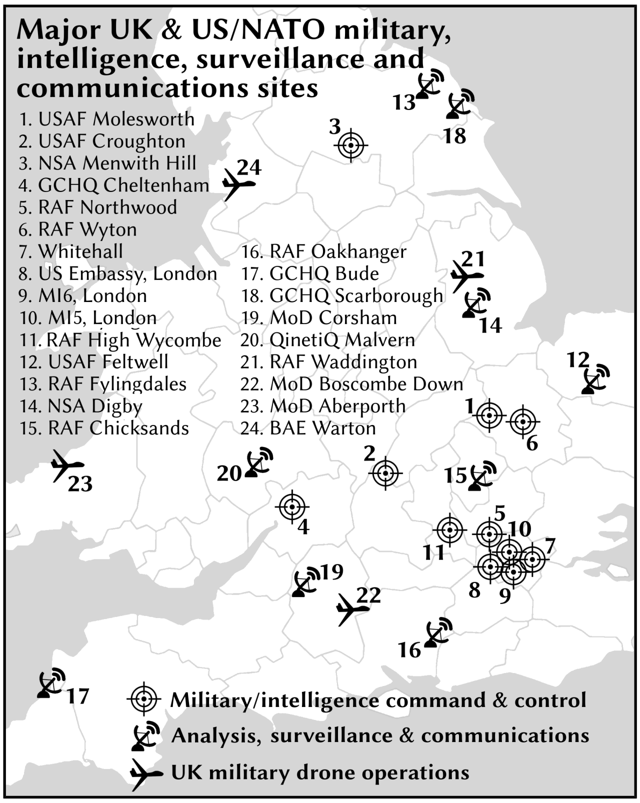
The recent 'radiation accident' in Russia is an example of when the technologies currently being developed to fuel long endurance or hypersonic craft go wrong.

We have also seen the re-emergence of "mini-nukes" – small tactical nuclear weapons designed for demolishing underground bunkers or small sites. Likewise, the use nuclear weapons to create an electromagnetic pulse would, in the modern computer age, could cause a scale of economic damage without the attendant need for physical destruction required during the Cold War.

The shift in the 1960s from long-range bombers to ballistic missiles changed the Cold War into a hair-trigger nuclear stand-off – portending global annihilation at any time as the speed of delivery did not allow time for deliberation or negotiation.

Military and intelligence networks are not based at a single location. They are made up by the contributions of many sites, working together to provide the functions for the network as a whole.

This map shows the core network of sites which contribute to the UK, US, and NATO combined military and intelligence network. Each performs one or more specialist roles to create the 'network-centric warfare' system which spans not simply Britain or Europe, but, indivisibly, the entire globe.



Major UK & US/NATO military, intelligence, surveillance and communications sites

1. USAF Molesworth
2. USAF Croughton
3. NSA Menwith Hill
4. GCHQ Cheltenham
5. RAF Northwood
6. RAF Wyton
7. Whitehall
8. US Embassy, London
9. MI6, London
10. MI5, London
11. RAF High Wycombe
12. USAF Feltwell
13. RAF Fylingdales
14. NSA Digby
15. RAF Chicksands
16. RAF Oakhanger
17. GCHQ Bude
18. GCHQ Scarborough
19. MoD Corsham
20. QinetiQ Malvern
21. RAF Waddington
22. MoD Boscombe Down
23. MoD Aberporth
24. BAE Warton

Military/intelligence command & control

Analysis, surveillance & communications

UK military drone operations

In the same way, hypersonic craft, long endurance autonomous drones, and AI-powered hacking 'bots', speed response times, allowing less time for analysis and deliberation. They therefore make conflict more rather than less likely as mistakes may quickly escalate into full conflict.

Crashing the system

Recent high-profile malware cases, such as *Stuxnet* or *WannaCry*, show how carefully crafted malware can affect or destroy the operation of national infrastructure.

While losing data is problematic for most people, the increasing automation of essential national services means a cyber-attack could disrupt a single corporation, or an entire country or region. This means network-based attacks are increasingly being exploited by states as a military technology – *including Britain.*

Asymmetry & "drone vs. drone"

As the recent drone attacks on Saudi Arabia show, and the alleged cyber-attacks both from states and organised crime, it is no longer only large, highly-developed states who are able to wield these new technological weapons. Anyone who developed the required skills, and can create the basic infrastructure required, can undertake these relatively cheap and difficult to attribute actions.

This is another facet of how networked technology creates greater global instability.

The mainstream solution to this problem is to "take the people out of the loop" – to put the computers and automated systems in charge and let them battle each other. That could also, arguably, infringe international humanitarian law.

Banning weaponised IT

There is, of course, another solution: ***turn the technology off.***

There are barely any legal controls governing the use of cyber-weapons, information fusion, armed/surveillance drones or hypersonic craft.

In 2017, against lobbying by nuclear states, the UN passed the *Nuclear Weapons Ban Treaty*.

We need a similar kind of agreement: banning armed and surveillance drones; protections in 'cyberspace' against the use of weaponised information technologies; and, from the intrusive surveillance of state or private agencies.

Without such rules, these systems will inevitable drag society into an inhuman, automated technological conflict – fuelled by the arms race in 'artificial intelligence' that has already begun.