Keeping EW ahead of the curve…..maybe!

Professor David W Stupples
d.w.stupples@city.ac.uk

ASSOCIATION OF OLD CROWS

My Message

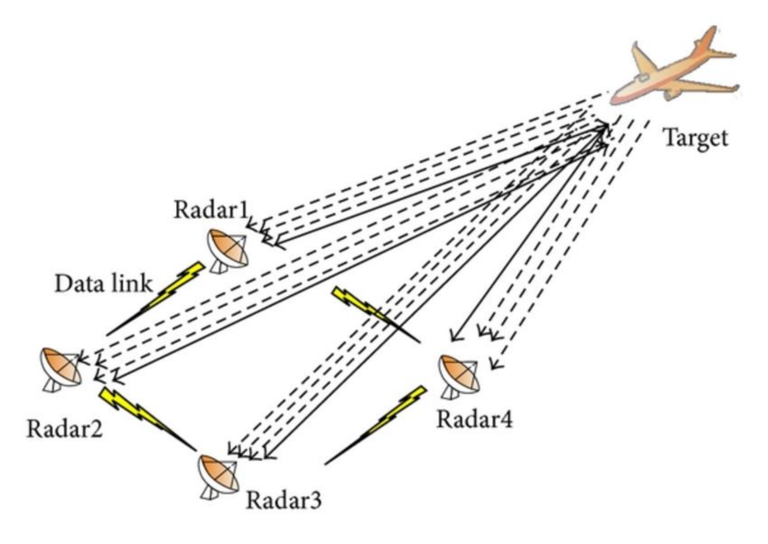
Current EW is beginning to trail technology developments in radar, missiles, communications, command and control, cyber, etc. It is not for the want of trying or lack of investment, it is due to a myopic focus on ‘point source solutions’, meaning EW solutions counter a particular threats! We must think ‘systems’, ‘agility’, ‘rapid development using software defined solutions’. This talk will provide an introduction to the systematic threat and discussion points for the way forward. But……we are looking at a disruptive change in our thinking.

Sorry, we didn’t know it was invisible!

Twenty years ago, Capt. Zoltan Dani achieved a miraculous military feat: wielding outdated missile equipment (S-125 Neva air defence system), his army unit shot down an American F117 "stealth fighter" flying over Serbia as part of NATO's 1999 air strike assault.

ELINT failure, RWR failure, or luck?

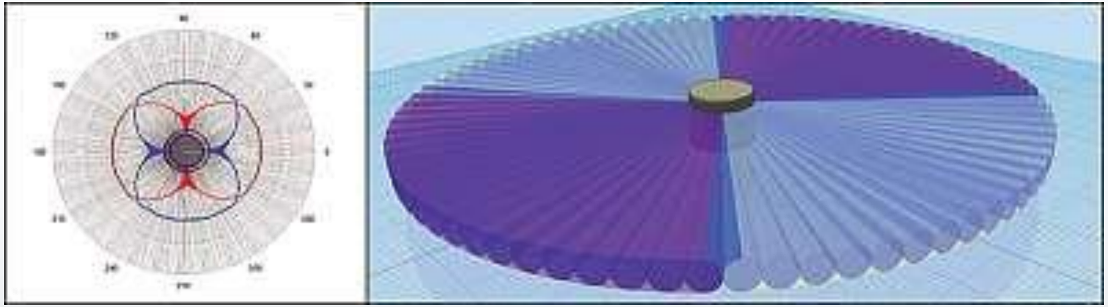
Technology of the future – LPI Radar network

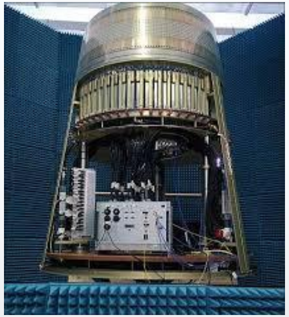


LPI radars acquire and track the target with directional beams. The netted radars; *Radar*1, *Radar*2, *Radar*3, and *Radar*4 transmit orthogonal waveforms (as solid lines) but receive and process all returns. One radar in the network fuses the combined result.

Successful ELINT is difficult – very low power, complex polyphase coding, and mobile. Strategic positioning counteracts stealth.

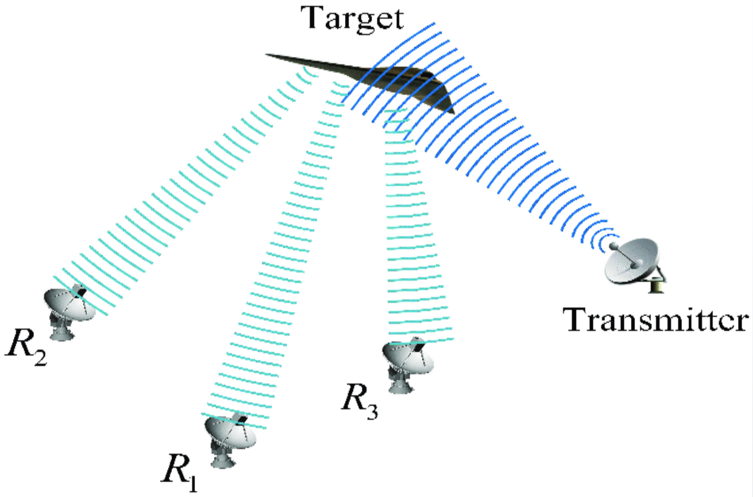
Technology of the future – Ubiquitous Radar





A ubiquitous radar is one that looks everywhere all the time – a staring radar. It does this by using a low-gain omnidirectional or almost omnidirectional transmitting antenna (remote highly mobile antenna) and a receiving antenna that generates a number of contiguous high- gain fixed (non-scanning) beams. Almost immune from current EW systems especially if carried by drone. Ultimate battlefield radar!!!

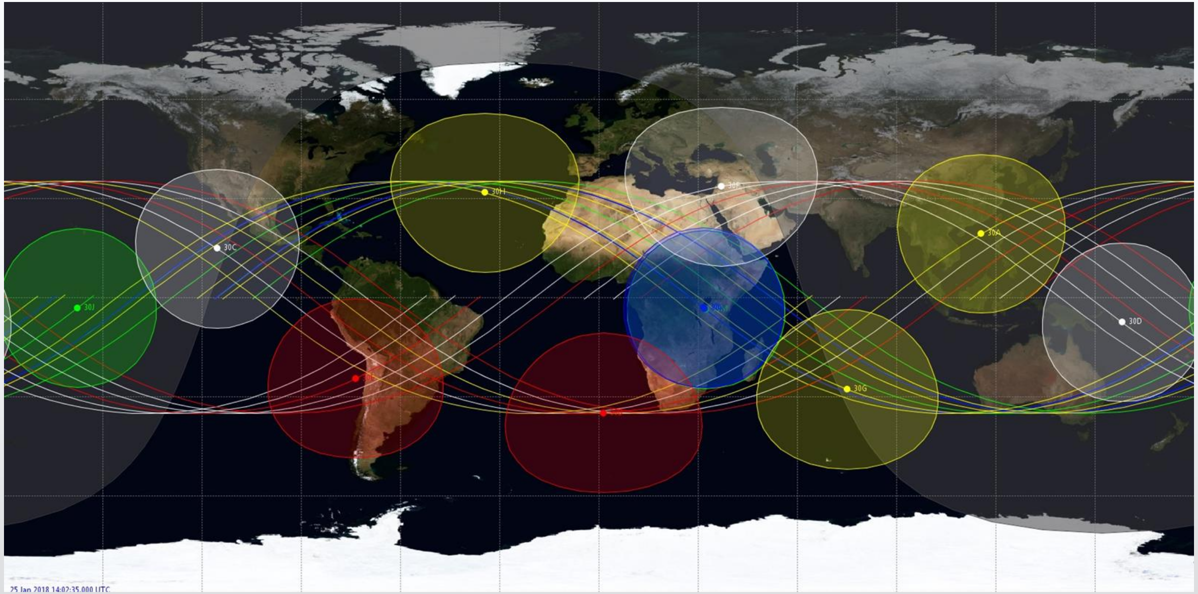
Technology of the future – Multi-static Radar



A multi-static radar system contains multiple spatially diverse mono-static radar or bistatic radar components with shared area of coverage. An important distinction is the requirement for data fusion. The spatial diversity afforded by multi-static systems allows different aspects of a target to be viewed simultaneously.

The potential for information gain can give rise to a number of advantages over conventional systems – good resistance to EW and better detection of stealth aircraft.

Technology of the future – Overhead ELINT



Nine ELINT/COMINT satellites in constellations of 3 can provide almost constant coverage of most conflict areas – mostly immune to current EW

French SIGINT Satellite CERES

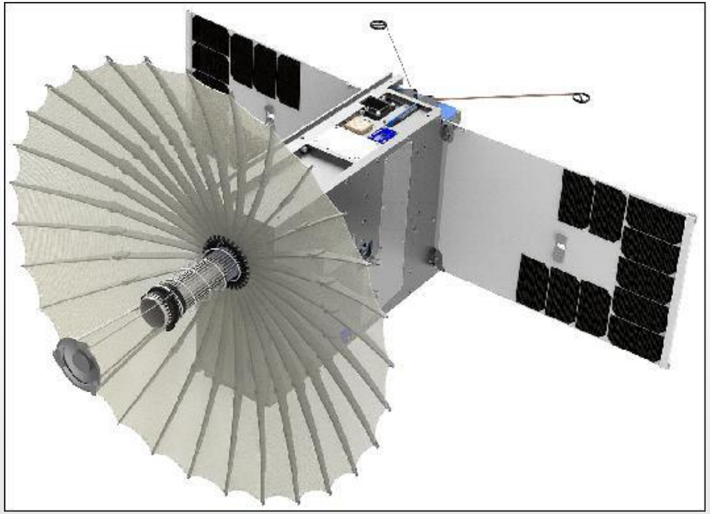
The entire CERES budget is estimated at about 460 million euros including the ground segment and the first two years of operations, which will be handled by the Airbus-Thales team.

Under a contract valued at about 325 million euros ($460 million), France’s arms procurement agency, DGA, expects Airbus and Thales to begin work on the CERES electronics-intercept program in March 2018, with the three satellites to be launched into low Earth orbit in 2020.

As of November 2014, the Ariane 5 commercial launch price for a "midsize satellite in the lower position" is approximately US$60 million.

Technology of the future - CubeSat with Ka-band Radar

RainCube is a technology demonstration mission to enable Ka-band precipitation radar technologies on a low-cost, quick-turnaround platform. The proposed mission is to develop, launch, and operate a 35.75 GHz radar payload on a 6U CubeSat. This mission will validate a new architecture for Ka-band radars and an ultra-compact deployable Ka-band antenna in a space environment. RainCube will also demonstrate the feasibility of a radar payload on a CubeSat platform.



A novel architecture compatible with the 6U class has been developed at JPL (size of 10 x 20 x 30 cm). The key lies in the simplification and miniaturization of the radar subsystems. The RaInCube architecture reduces the number of components, power consumption and mass by over one order of magnitude with respect to the existing spaceborne radars, therefore it opens up a new realm of options for low-cost spacecraft platforms such as CubeSats.

Technology of the future – CubeSat a limiting issue?

RF signals collection by means of interferometry is an area that shows great promise for small satellite applications and is of great interest in military community. Electronic Intelligence (ELINT) is the analysis and geolocation of RF signals. Accuracy demanded from such systems in order to merit their costs is often incongruent with detection techniques that rely on single CubeSats (such as Angle of Arrival methods). Accuracy is strongly related to aperture size; rigid antennas are therefore limited to the available surface area of small satellites.

Typical accuracies that can be expected of AOA techniques range from 0.1° – 1°. Factoring in orbital altitude this results in geolocation accuracies of 10 km or more for RF sources close to the satellite's nadir, increasing rapidly with distance from nadir for missions in LEO.

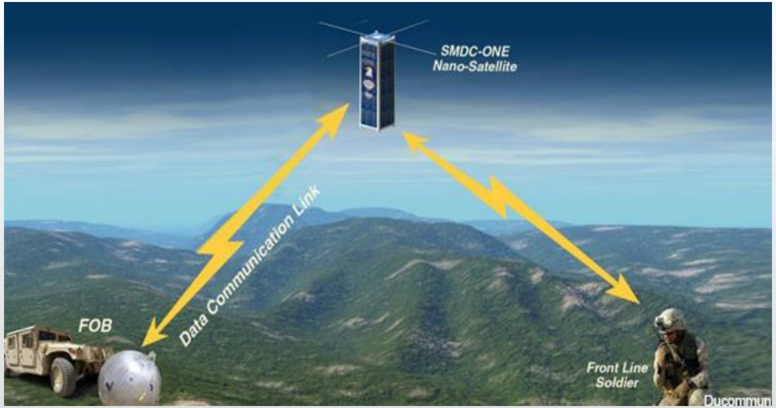
Using a single CubeSat solution with rigid antenna systems limits the type of RF emitters that can be geolocated with high accuracy (<0.1°) to X-band (or shorter wavelengths). A solution to this thorny problem is to employ a constellation of CubeSats and distributing functionality instead of investing in highly sophisticated single satellite payloads.

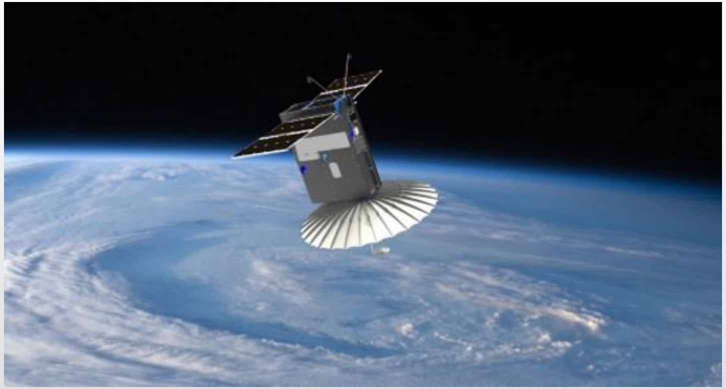
Technology of the future - ELINT CubeSat Constellation

A trio of ELINT CubeSats would have the required frequency coverage and be able to facilitate 'time difference of arrival' (TDOA) and 'angle of arrival" (AOA) with an S/N ratio and sensitivity at about 85% of traditional birds.

Technology of the future - CubeSats can be stealthy

As long as we've been launching spy satellites into space, we've been trying to find ways to hide them. Now, thanks to the small satellite revolution—and a growing amount of space junk— there are new ways to mask its spying in orbit…

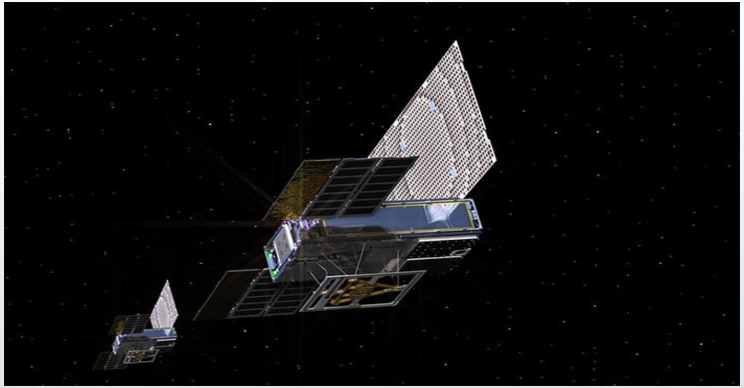


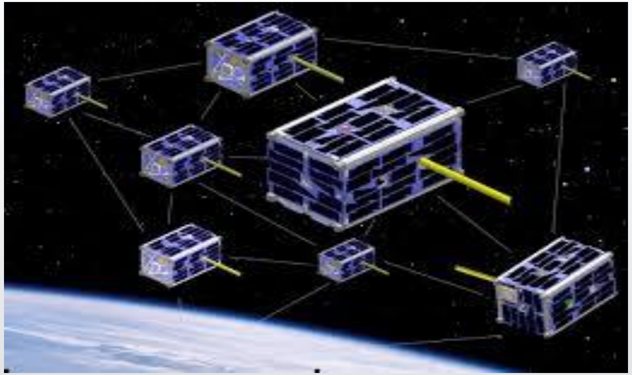


The arrival of this technology requires us to re-think warfare in this domain – developing the technology into the IOT/IOE domain requires disruptive innovation

Technology of the future – CubeSat distributed

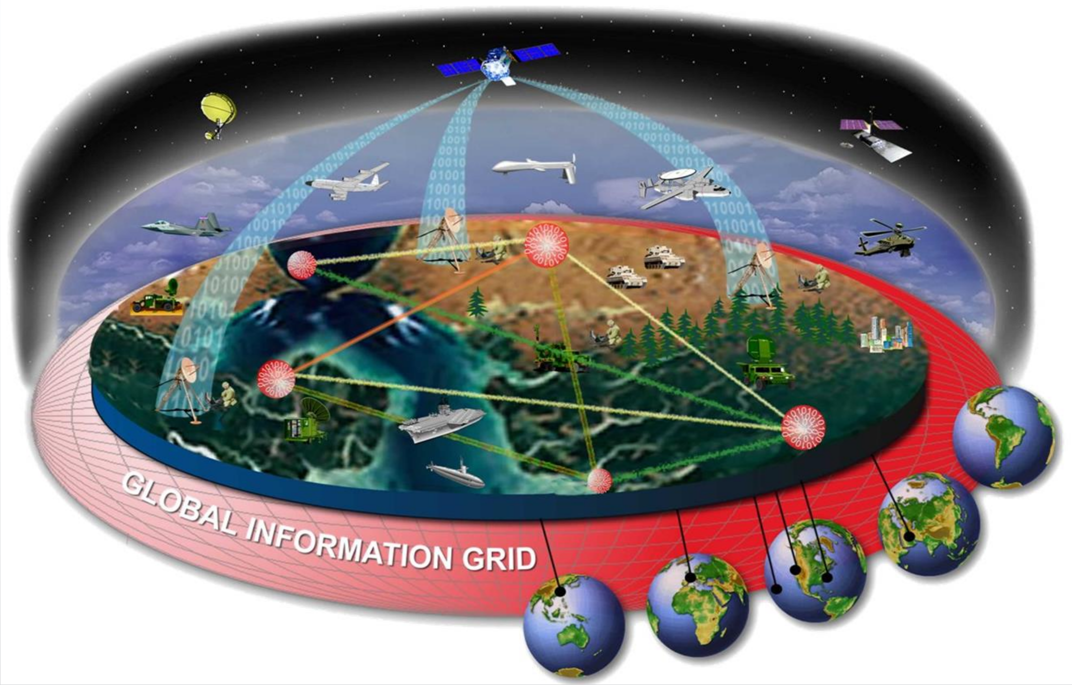
….but a CubeSat does not have the functionality of a 'grown-up' satellite, does it? Cluster in a network and communicate through optical links……..





Cost of Ceres $460MM, cost of CubeSat equivalent $10mm to $20MM. Now within reach of smaller nation states – they can now get a chip in the big game, and stealthily. Assembled in space with unit replacement!

Technology of the future – IoT and IoE

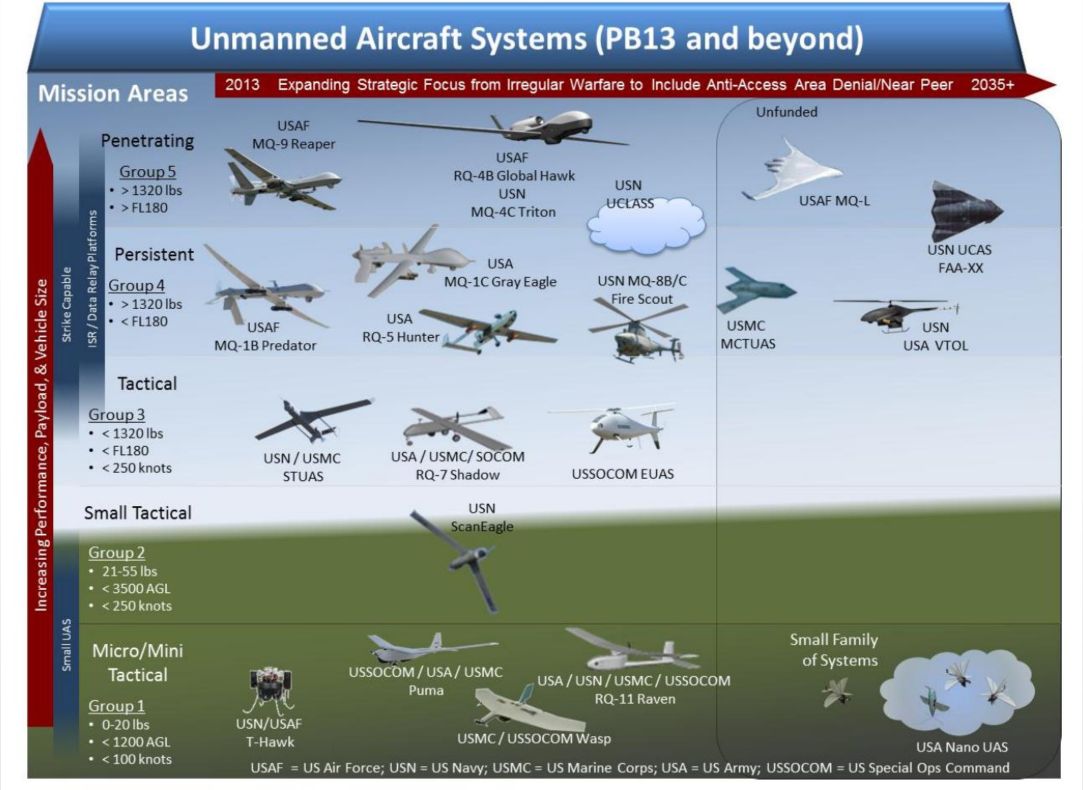


Total communication; everything communicates over fibre, and in the EM spectrum in all bands and it is agile in route and frequency. The global information grid is in space, in the ether and terrestrial. Data is distributed and at different times. How difficult can SIGINT become?

Technology of the future – CubeSat coverage IOE

IOT/IOE coverage will be WW using CubeSat technology through a Internet-like network in space – agile, virtually scale free and virtually EW immune

Technology of the future – take the man out!



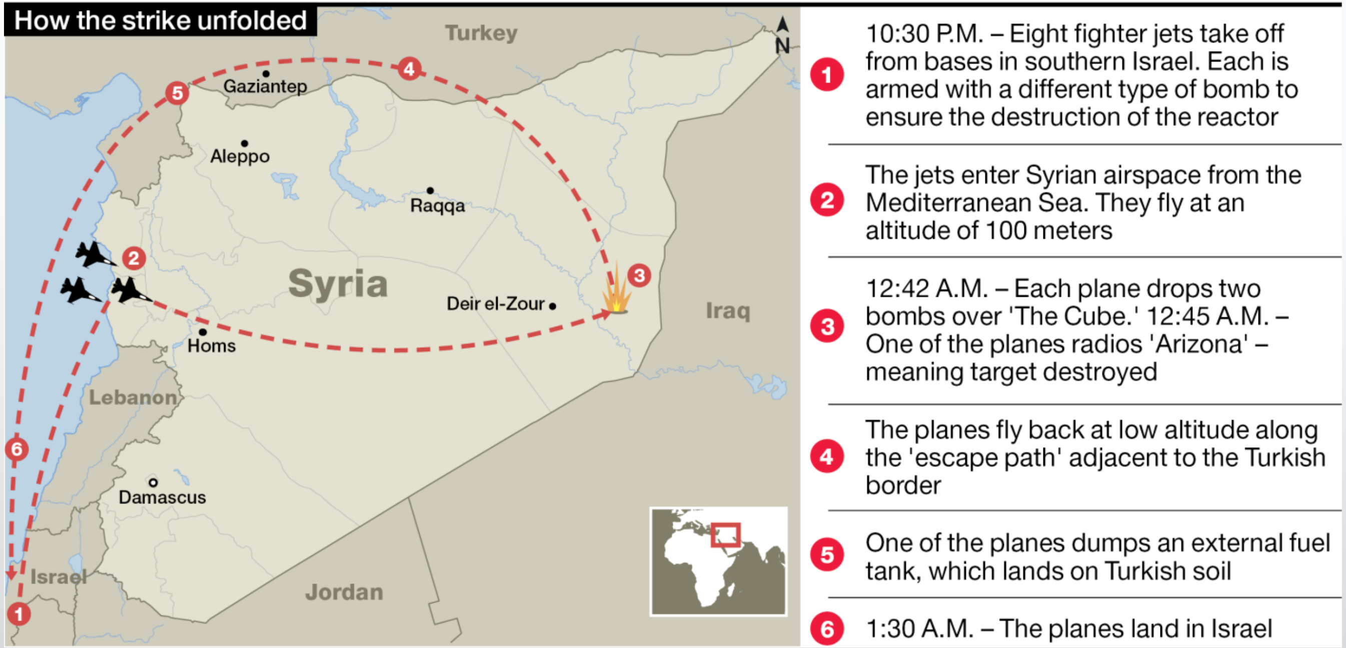
Unmanned systems are being developed a pace and these will/can host EW systems, but what of out our fight in the EM domain against them. Many are virtually EW immune but they are used by Iran, N. Korea, China, Russia AND Al Qaeda & ISIL!

Technology of the future – fighting in cyberspace

Imagining the integration of this technology gives us some vision into the future. All out wars will be fought in two domains – kinetic and cyberspace with the latter becoming ever more significant. We were well versed in the first but not the second especially when it is inextricably linked to the former.

We need to understand how to attack and defend in the integrated domain – we need to understand how to harvest intelligence when most of the domain is cloaked from traditional methods. We are behind the curve!

Fighting in two domains – 5th/6th September 2007



1 10:30 P.M. – Eight fighter jets take off from bases in southern Israel. Each is armed with a different type of bomb to ensure the destruction of the reactor

2 The jets enter Syrian airspace from the Mediterranean Sea. They fly at an altitude of 100 meters

3 12:42 A.M. – Each plane drops two bombs over 'The Cube.' 12:45 A.M. – One of the planes radios 'Arizona' – meaning target destroyed

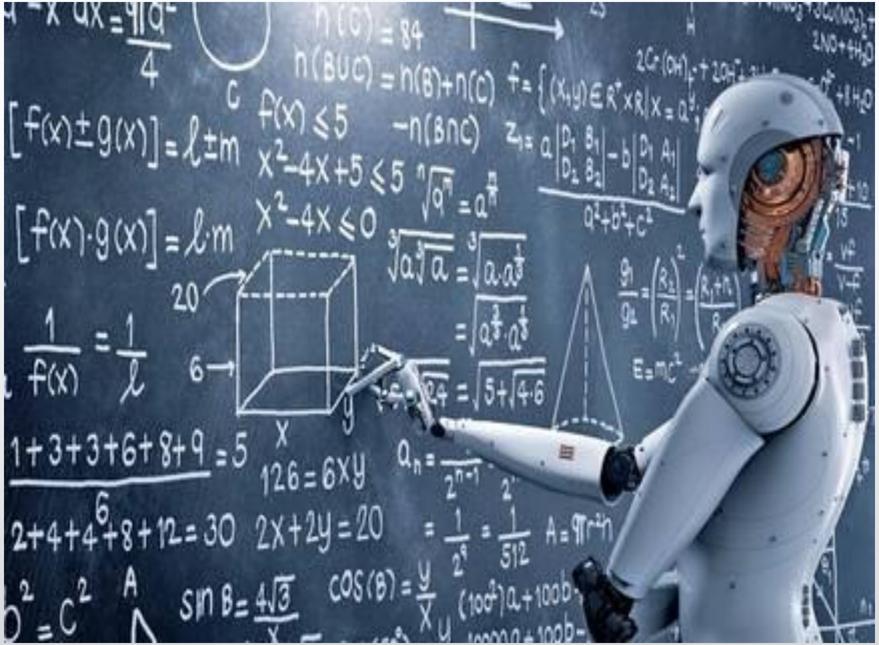
4 The planes fly back at low altitude along the 'escape path' adjacent to the Turkish border

5 One of the planes dumps an external fuel tank, which lands on Turkish soil

6 1:30 A.M. – The planes land in Israel

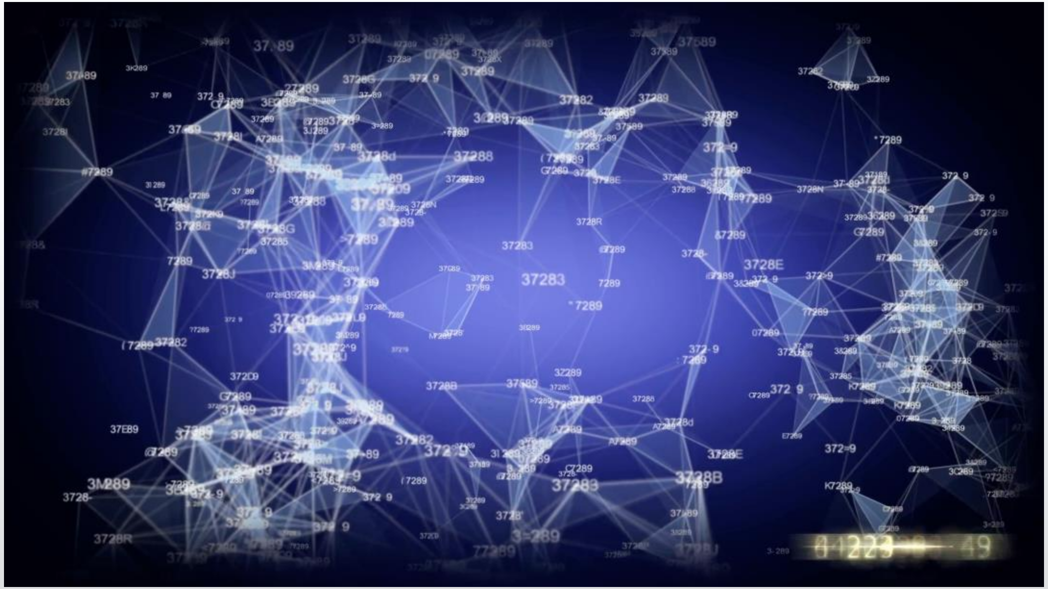
Kinetic action integrated with sophisticated cyber action – jamming by spoofing

Technology of the future – taming big data?



It is claimed that data analytics applied to ‘big data’ together with machine learning will help military planners and war fighters in ‘cold scenarios’ – where they might not have much real intelligence on the ground? The military/intelligence services may dealing with in excess of 10 Zettabytes of data $(10^{21}\ bytes)$ *by 2025.*

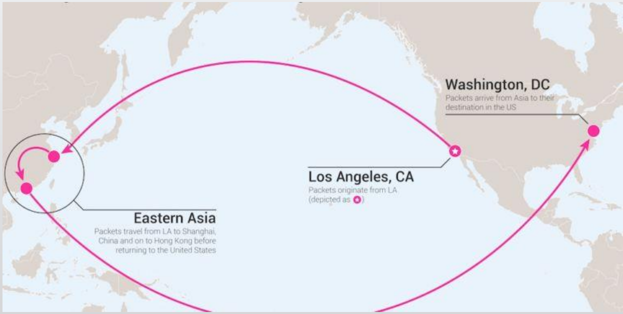
Technology of the future – hosting big data?



Further complexity to military 'big data' originates from military networks that hold the data. The networks are both hierarchical and recursive, they are also homogenous and heterogeneous. They are built with no grand design. The are loosely coupled with no central control and support ubiquitous operations

This problem is not understood let alone solved – it is also subject to cyber attack that is likely to go undetected!

Technology of the Future – buying off-shore


Washington, DC
Packets arrive from Asia to their destination in the US
Los Angeles, CA
Packets originate from LA (depicted as ✪)
Eastern Asia
Packets travel from LA to Shanghai, China and on to Hong Kong before returning to the United States

Technology of the Future – cyber espionage

A growing threat to nation states and the military is reconnaissance malware. This malware aims to prepare for conflict in the cyber domain by mapping operational patterns of systems, the weaknesses of systems structures, access rights and passwords, etc. Information collected is communicated to its owner as intelligence – the practice will increase as technology becomes more sophisticated.

Reconnaissance malware is very difficult to locate and is usually inserted during 'first build' or by rogue systems programmers.

Technology of the Future – Known Knowns….&

Technologies outlined in this presentation are the 'known unknowns' and are is being addressed 'sort of" from an EW perspective. It is mostly evolutionary with a dab of revolution. Our approach to it is a bit more of the same and it may work!!!!!!!

'Unknown unknowns' are submerged and cloaked in the revolutionary 'internet of everything (IoE)'. Everything connected via a massive network of networks hosting system of systems that develop through 'ad-hoc' evolution of operational requirement and connect in an unplanned patchwork. When it works it will greatly benefit the war-fighter and the cost of procuring and owning systems; politicians will love it & embrace it.

BUT ….THE EMERGENT PROPERTY OF THIS IoE IS THE CREATION OF MILLIONS OF UNKNOWN BACKDOOR PORTALS INTO THE OPERATIONAL SYSTEMS, INTELLIGENCE SYSTEMS AND SUPPORT SYSTEMS.

Technology of the future – the CEMA nightmare

………from the opening presentation …….this is my educated guess. More importantly, I have no solution and that is what makes our task challenging.

Thank you……