UK CHAPTER NEWSLETTER

November 2023

Introduction

I must apologise for this Newsletter being a little later than I had planned. The past 8 weeks disappeared in a bit of a blur with some family matters needing my attention, resulting in delays in writing material for the Newsletter. Since it should have been issued in October, I think I need to reset the schedule and recognise that this is the November Issue which will be followed by one after Christmas in January.

Good news is that we have been present at various events in the past two months. John Stubbington has presented papers for the RAF Historical Society and at the DEHS event; full information on these should be in the relevant journals - I have provided short synopses as Annexes to this Newsletter. Most importantly, Sue Robertson arranged a visit to Y Squadron Royal Marines, which is reported later in this Newsletter.

Advocacy and Advice - What could AI/ML do for EW?

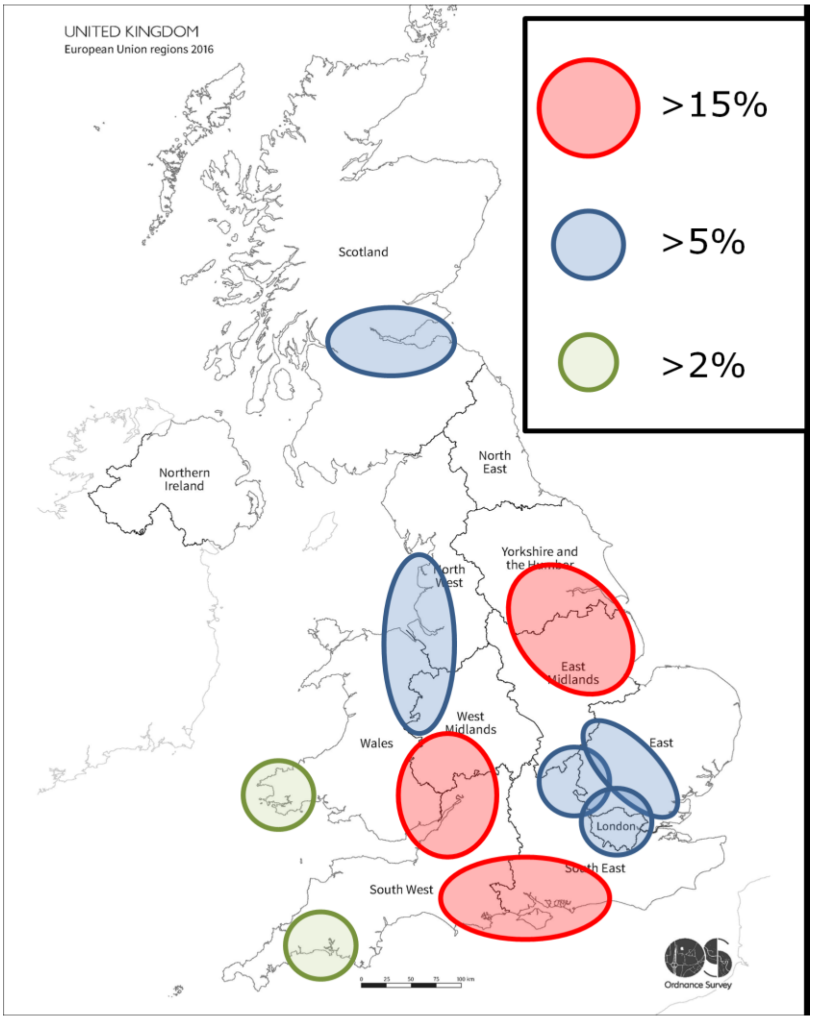
I have been invited to attend a couple of events in the last months where I met some well-regarded experts (and AOC members) in the EW field. Discussions at these events covered a range of topics, but a recurrent theme has been the application of AI/ML to the EW domain. I wondered if this was one of the topics covered in the recent discussions between the UK Prime Minister and Elon Musk, but suspect it wasn't.

However, I have noted that Google's CEO has stated that developments in AI will have a more profound effect on humanity than fire or electricity. My response to this has been: "Yes, but both fire and electricity have created great destruction in the environment when uncontrolled". This kind of thought is what lay behind the 'killer drone' editorial in the last newsletter and AI 'going rogue' was definitely part of the Rishi/Elon discussion. The King's Speech at the Opening of Parliament included the announcement of the Automated Vehicles Bill. A key element of this, according to the GOV.UK website, is that the bill "has safety and protection of the user at its core...ensuring clear legal liability at all times: making companies responsible for how their self-driving vehicles behave on the road and protecting users from being unfairly held accountable...". It will be interesting to see if this extends beyond vehicles.

At a much lower level, the EW community have noted how AI/ML can help with data analysis (e.g. processing of intelligence information) and have postulated that it could have a role in some types of sensor. I think there is currently a degree of uncertainty about its use in tactics and countermeasure deployment, but perhaps this is due to a lack of data to support the training of the AI/ML. Maybe the use of AI generated virtual environments for development of tactics and countermeasures may be the turning point on this. *Send in your thoughts and ideas on the AI/ML topic and we may be able to collect some people together for an on-line webinar.*

Membership: Where are we now?

We have been able to access some of the data about the current members of the Chapter. I used this to work out the Counties in which you have registered your home address, which I then used to evaluate the areas where we had some obvious clusters of members. In geographic terms, these map pretty well onto the various Regions that were used to subdivide the UK in recent EU categorisation and in ancient history - some could best be described in terms of Wessex, Mercia, Northumbria (including Edinburgh!) and the Danelaw. The map shows where the clusters exist: the 3 biggest are really centred on Lincoln, Southampton and Bristol (each has between 15%-25% of our members); 3 smaller clusters around London are - in total - more than 30% of our membership, but are definitely mapped into the NW of London, East of the Lea valley and Close to the Thames.



Without knowing more about individual members, the main groupings seem to reflect the locations of specific industries and military establishments - this is not a surprise. We have also extracted some data on the industries which are members of the AOC and those with significant number of AOC members (not always the same). I will be working with the other Board members to consider the implications of these distributions on things like organising events.

Latest EW News Roundup

(Kindly supplied by Dr Thomas Withington – Writer and analyst, editor of the Armada International EW webpage and newsletter)

Lockheed Conducts AI-Commanded Electronic Warfare Mission

In September Lockheed Martin announced that it had performed a test during which Artificial Intelligence (AI) technology was used to direct piloted aircraft to provide jamming support during an air-to-ground mission. The fascinating account of this experiment is chronicled in this article:
https://www.thedefensepost.com/2023/09/19/lockheed-ai-electronic-warfare/?expand_article=1

A New Micro Kind of Electronic Warfare May Be Unfolding in Gaza

Reports of the death of counter-insurgency warfare, and electronic warfare's role within it, seem to have been greatly exaggerated! With Israel and Hamas looking horns following the attacks on the latter by the former in early October, EW will be used extensively by both sides as hostilities intensify, as explained in this recent piece:
https://www.forbes.com/sites/erictegler/2023/11/03/a-new-micro-kind-of-electronic-warfare-may-be-unfolding-in-gaza/

Soviet Television Reconnaissance Satellites

Back in the Cold War, the Soviet Union worked hard to develop ways to relay images from its reconnaissance satellites back to Earth. To this end, Soviet engineers devised methods to transmit video imagery to users on the ground, as this fascinating article describes.
https://www.thespacereview.com/article/4646/1

Nigerian Army acquired Electronic Warfare Capabilities

Little is known about the EW capabilities of militaries in Africa. Nonetheless, interest and investment are flowing into electronic warfare across the continent. Ghana and Ethiopia have recently reinvigorated their armies' EW attributes. Nigeria is taking a similar path, as articulated in this article:
https://www.military.africa/2023/10/nigerian-army-acquires-electronic-warfare-capabilities/

The Russians Installed a GPS Jammer in Ukraine. The Ukrainians Blew It Up – With a GPS-Guided Bomb

Using a powerful jammer on the battlefield can be fraught with risk, particularly if that jammer announces your presence to the world. Russian forces using GPS jammers in the Ukraine theatre of operations learned this lesson the hard way when their attempts to jam PNT signals wrought their own destruction:
https://www.forbes.com/sites/davidaxe/2023/10/31/the-russians-installed-a-gps-jammer-in-ukraine-the-ukrainians-blew-it-up-with-a-gps-guided-bomb/

New Ukrainian Electronic Warfare Systems Aim to Counter Russian UAVs

It is a truism that conflict accelerates innovation and the ongoing war in Ukraine is no exception. Both sides are fighting for spectrum superiority and supremacy, concentrating the minds of Ukrainian electronic warfare engineers. The net result is several new Ukrainian EW systems which can jam Russian drones: ***https://www.ukrinform.net/rubric-ato/3782010-ukraine-creates-piranha-ew-system-to-protect-armored-vehicles-against-drones.html***

Georgia On My Mind

Despite being a somewhat 'frozen' conflict, Russia has deployed electronic warfare assets to parts of Georgia under Moscow's control. Interestingly, assets deployed include not only Russian Army EW systems, but additional platforms owned by Russia's GRU military intelligence service. This article provides more details on this quiet deployment. ***https://www.armadainternational.com/2023/11/russian-electronic-warfare-in-georgia/***

EDITORIAL - Countering mini- and micro-UAV

Following on from the 'thought-piece' on 'Killer Drones', here's a shorter piece about a specific type of drone - the mini- and micro-UAV. This will be a starting point for further discussion about Counter-UAS systems (CUAS) in subsequent Newsletters.

Recent development of micro-mini UAV and related technologies have made available very affordable off-the-shelf solutions - that can be customised easily - to perform various operations against a range of targets beyond those normally associated with the battlefield (e.g. critical national infrastructure, cultural heritage sites, and large events). These operations could be undertaken to perform direct attacks (e.g. using explosives or NBC agents) or to create panic and confusion (e.g. by spreading some form of powder, or simply by landing in the middle of the crowd at an event).

There are many types of micro- and mini- UAV available, broadly sub-divided into fixed-wing and multi-copters. Some can be purchased fully configured, but there is a growing market for component parts that can be purchased separately. This means that the control systems and datalinks may be specific to an individual UAV, even though the body and motors may be from a COTS system. In general, these "hobby UAV" will be capable of a maximum speed that is less than 100 knots, with a maximum endurance of ~1 hour. The maximum payload capacity of most hobby UAV will probably be less than 2kg, which is sufficient to carry a good quality camera and a small payload, while commercial cargo drones can carry up to 30kg for about 20km.

Early hobby UAV were controlled by fully 'human-in-the-loop' modes, where the controller must maintain visual contact with the UAV and imagine that they are on-board the UAV - making them limited to short range and hard to control in difficult air conditions. The majority of the smaller UAV are now equipped with video cameras, GPS and various gyro-controlled inertial reference systems that make the task of flying the

UAV very simple. These allow the UAV to fly pre-programmed routes, without operator intervention, and have a "return to home" capability.

In most cases, some form of up-link is required for the operator to control flight control and sensor/payload management functions, with one or more down-links to carry video, pictures and telemetry data; obviously these usually need line-of-sight to the receiving station (of which there could be more than one). The nature of the links is changing towards the increasing use of wi-fi frequencies, although these do not always follow any form of standardisation of data content or protocols. The majority are now digital with full encryption; analogue interfaces are becoming obsolete.

In terms of addressing a comprehensive solution to counter the micro-mini UAV threat in specific missions, the following aspects may have to be considered:

1. Detection of UAV in flight;
2. Detection of the datalinks;
3. Localisation of the UAV;
4. Localisation of the controller or remote command & control (C2) site;
5. Identification of datalink characteristics used to perform command and control of the UAV (radio, laser etc.) and to transmit video / telemetry data from the UAV;
6. Jamming of the navigation system (e.g. defeat of GPS or other electronic capability to deceive UAV and divert it from remotely controlled / pre-programmed navigation)
7. Hacking or jamming the various datalinks associated with the UAV
8. Soft-kill systems to neutralise/degrade the sensors used on the UAV
9. Hard-kill systems to engage and destroy the mini-micro UAV threat (kinetic or laser DEW)
10. Systems to catch the UAV and remove it to a safe location

Items 1, 2, 3, 4 & 5 fall into the category of Situation Awareness capabilities, including ELINT and Cyber.

Items 6, 7 & 8 fall into the general category of ECM or Cyber Attack capabilities.

Items 9 & 10 fall into the category of Physical Effectors.

Taken at one level, the obvious solution is a radar or EO sensor with a control sub-system and a hard-kill effector - in essence something similar to a VSHORAD capability. However, given the range of mission scenarios noted, a hard-kill system might create more collateral damage and panic than a system using a different form of effector. This could be the case in an urban or civil environment where crowds might be expected (airports and events, for example). Consequently, many of the CUAS systems in development or already deployed claim to be modular and scalable using a mixture of sensors and effectors. Most of the technologies are available, particularly for Situation Awareness, ELINT and ECM, while some of the possible Cyber and DEW Effectors would require development from current capabilities. Searches on Google will reveal many different solutions and some wonderful publicity.

There is an overlap in functions and technologies between EW, CUAS and DEW, so the next part of the jigsaw to look at will be the situation awareness elements. More to follow next time...

AOC UK Chapter Awards

The John M. Clifford OBE Award

The John Clifford OBE Trophy is awarded to the top EW student going through Weapon Systems Operator (WSOP) training at RAF Cranwell. Sgt Tom Yates was the proud recipient of the award for 2022, accompanied by an AOC certificate and cheque for £250. The award was presented by Gp Capt T J Lindsay, Commandant No. 3 Flying Training School, at Tom's graduation. BZ to Tom.

The No. 52 AeroSystems Course Award 2023

The AOC UK sponsored the "Best EW Related Personal Project" award for the No. 52 AeroSystems Course was awarded to Flying Officer Charlotte Pauling (RAF) at the graduation ceremony at the Defence Academy on 27th July 2023. UK Chapter Vice President Jonathan Bramley had the privilege of attending the ceremony and presenting the award trophy to Charlotte. A UK Chapter AOC certificate and cheque for £250 accompanied the award. BZ to Charlotte.

Imperial War Museum - "Lifesavers" Museum Pieces

Tom Withington, our regular contributor on current EW affairs, also has an interest in the history of EW. He has provided this request for information from the IWM.
Tom's interesting PhD thesis on Bomber Command EW Policy can be found here:
https://etheses.bham.ac.uk/id/eprint/8076/1/Withington18PhD.pdf

Is your company, organisation or even your good self in possession of some electronic warfare or radar history that had an impact far beyond the military domain? Did that black box or circuit board proudly displayed in your office cabinet change our everyday lives in some unsung, yet pivotal, way? Perhaps you have a similar story to share about your work? If so, the United Kingdom’s Imperial War Museums (IWM) want to hear from you.

The IWM and Lloyd’s Register Foundation are collaborating on a five-year project entitled "Lifesavers" to explore how conflict has driven innovation in science and technology. The project will look at how innovation affects safety today on land, at sea and in the air. From tiny personal possessions and insignia to aircraft and warships, IWM’s collections span all major British and Commonwealth conflicts since 1914. The collections provide a rich resource for examining the connection between conflict and innovation. If it was not for warfare, would we have much of the science and technology we take for granted today?

From advances in aviation technology during the Second World War, to modern air travel. From the rescue of downed wartime pilots to modern air-sea rescue and air ambulances. Safety equipment at sea, ejector seats, radar, radio and communications technology, the list of wartime innovation goes on.

Nonetheless, it is not just about the gadgets and machines in the IWM’s collections, fascinating as they are. Lifesavers also encompasses the social history of technological innovation. From the people who developed technology, those who used it in the field, to those who continued to innovate once peace was declared. IWM’s collections include many of the personal stories and voices of those who were there.

Lifesavers is a truly international project. As well as possible collaboration with British institutions such as the Science Museum, the Royal Navy and Lloyd's Register Foundation themselves, the initiative aims to share collections and knowledge with museums around the world. The IWM already has links with museums in Canada, continental Europe, the Republic of Korea, Singapore and the United States.

One of the project’s deliverables will be a digital exhibition of objects, literature and stories relating to Lifesavers’ core themes. If you have something to exhibit such as a photographed object, infographics, literature or even just a great story to share please get in touch with Robert Rumble, the project curator in the IWM’s Cold War narrative team. Mr. Rumble can be contacted at rrumble@iwm.org.uk.

AOC UK Chapter visit to Y Squadron

On Friday 3rd November a Chapter visit took place to Royal Marines Y Squadron at their base, Stonehouse Barracks in Plymouth.Y Squadron is part of the 30 Commando Information Exploitation Group, providing Electronic Warfare and Signals Intelligence (EWSI) capability for the group.

The visit started with a Welcome brief with OC Y Squadron followed by a brief on Y SQN Orbat and mission. An equipment demo followed with a description of a recent exercise. The visit included a look around the historic Eastern Kings Fort, HQ Y Squadron, with spectacular views of Plymouth harbour on a sunny morning.

Unfortunately the effects of Storm Ciaran the day before the visit had taken its toll on the travel plans of some of the attendees, but those that did manage to make it to Plymouth had a very worthwhile experience with much fruitful discussion with Y Squadron personnel and with the other AOC members.

Future Events/Visits

- **UK Chapter Xmas Dinner -** RAF Club, London - 8 December
  - **Book now if you haven't already!**
- **Electromagnetic Warfare 2024**- Shrivenham, CANCELLED
  - *I am working with Shrivenham and others for an event later in the year.*
- **AOC Europe 2024 –** Oslo, 13 - 15 May 2024
  - *https://www.aoceurope.org/*

Bottom Line

Stay well and enjoy the last few weeks of 2023. I'll be in touch again in the New Year.

Steve Roberts
AOC UK Chapter - President - Email: *steve.vespasian@gmail.com*

Keep Checking out the UK Chapter website at: www.ukaoc.org

Bletchley Park and Bomber Command - 1943

John Stubbington, Wg Cdr, ret'd for RAF Historical Society

1. Signals Intelligence Dissemination - Obstacles

The rigidity of pre-war policy within the Air Ministry denied contact for several years between the producers of 'intelligence' and the operational users of that 'intelligence'. Part of the problem arose from the departmental organisation within the Air Ministry, where 'Signals' were regarded as 'Communication' and nothing to do with Intelligence. The Air Section at Bletchley was allowed to report information only to the Air Ministry.[1] The RAF Home Commands were deprived of Intelligence which they could have had and which may have avoided many operational losses.[2]

2. Signals Intelligence Dissemination - Successes

In the face of the Security policy and the various obstacles to informed timely dissemination of the SIGINT product, there were outstanding successes which contributed substantially to the conduct of the Bombing Offensive, including:

- The Hook-Up and Operational Interaction.
- BMP Reports.
- Liaison with the 8th USAAF
- Contribution to Raid Planning.

3. Liaison with the 8th USAAF

The successful application of Y-Service ground-based intercepts of German R/T together with airborne intercepts by the 8th AAF called for a high degree of judgement in real-time. This was to lead to a close working relationship between the German Air Section at Bletchley and the 8th USAAF Fighter Command, using the Hook-Up facility.

4. Raid Planning

The Command Intelligence staff advised the C-in-C on the choice of targets in areas suitable for bombing within the forecast weather conditions; and assisted the navigation staff in planning the outbound and return routes. The timing of indirect routes, diversionary raids and counter-measures were all part of the process. A despatch rider from Bletchley delivered the maps of the preceding night raids and night-fighter responses to Bomber Command HQ before the 0900 daily morning briefing to Sir Arthur Harris. The maps were attached to narrative on the main points of interest and formed the 'Preliminary Version (PV)' of the daily BMP. [3]

Summary

There was practically no initiative or guidance from the Air Ministry. There was serious obstruction between the originators of the intelligence product and the operational users of that product for at least three years. Fortunately, the German Air Section achieved the distinction of being accepted by the Allied Air Commands as a reliable source of advice on the Intelligence and operational tactics that they should consider.

[1] The Bletchley Park War Diaries, page 42/05B

[2] Official History of British Sigint, 1914-45, page 88

[3] PRO, HW 3/105, p61

Women in British Intelligence – WW2

John Stubbington, Wg Cdr, ret'd for Defence Electronics History Society (DEHS)

Introduction

The talk highlighted specific activities by women who were working either with the RAF Y-Service, or at Bletchley, Malvern, Bomber Command or RAF 100 Group (a small, but vital, piece of British Intelligence at large). Through the last nine months of the war there were typically 10,000 people working at Bletchley and the Outstations; nearly 7,000 of whom were women.

The RAF Y-Service

The Y-Service was the "ears" of Bletchley Park and, without it, all would have been lost. Many of the personnel were WAAFs. 'Mike' Morris was one of those young women – later becoming **Squadron Officer Morris, MBE** – having served at Kingsdown, the Middle East, the Western Desert and Italy.

Decryption and Decoding

The history of British cryptography and codebreaking is often portrayed as a men-only preserve. Actually, the majority of the people involved were women and foremost among them was **Emily Anderson, OBE**. A leading member of British intelligence for over three decades, she played key roles in both World Wars, at Bletchley Park and in the Middle East. She became Head of the Italian Diplomatic Section. Emily was awarded an OBE in 1943, for Services to the Armed Forces in connection with Military operations. Later, in 1961, she was awarded the Order of Merit, First Class, by the Federal Republic of Germany for her research and ground-breaking translations of the correspondence of Beethoven and Mozart

Countermeasures

By the time Pearl Harbor was attacked in December 1941, **Joan Curran** was nearly a year into painstaking experiments on using metals to reflect radar signals. In 1942, Curran finally settled on reflectors that were about 25 cm long and 1.5 cm wide. In 1943, the reflector strips were put to a serious military test when the Allies launched the strategic bombing attack Operation Gomorrah on Hamburg. Bomber Command lost only 12 aircraft out of 791despatched. Joan's invention of 'window' is still in use today but has become internationally recognised and named as 'chaff'.

SIGINT for Bomber Command and the USAAF

The German Air Section BMPs became a daily event from June 1942 until the end of the war, providing an increasingly comprehensive picture of the German Air Defence System in action.

- In March 1943, **Dorothy Gunn, MBE,** became Head of the German Air Section/Day Fighter sub-section, developing an effective liaison with the 8th USAAF Fighter Command.
- **Flight Officer Shirley Peek** was an Intelligence Officer in Bomber Command, initially at RAF Marham; then at HQBC as Int1b studying Bomb Damage assessments and updating the Blue Books (Damage Diagram Albums) for the King, the Prime Minister and Chief of Air Staff; finally with HQ 100 Group debriefing crews and generating Immediate Raid Analysis Reports.