

RSI

Royal Signals
Institution

JOURNAL

Volume 33
Issue 2
Winter 2015



One mission, one team, one direction.



www.airbusdefenceandspace.com

PIONEERING THE FUTURE TOGETHER



AIRBUS
DEFENCE & SPACE

CONTENTS

Cenotaph 2015	3	AFCEA European	37
.....		TECHNET Conference	
		2015	
Corps Guest Night	5	Maj Jon Heaton	
.....		
Institute of	6	A Stay Behind	38
Telcommunications		Detachment in Malaya	
Professionals		Maj Tom Johnstone	
.....		
Apprentice of the Year	6	Champagne - Worth the	46
.....		Label ?	
RSI London Lecture and	8	
Dinner		New Corps Painting	51
.....		Zeitgeist - The Spirit of	
RSI Seminar at the RUSI	12	the Times	
.....		
Encryption for	14	UK Mobile Force (UKMF)	52
Communication Security -		Lt Col Peter Richards	
A Fresh Look		
Lt Col Guy Meakin		Honours and Awards	54
.....		
Net Gains -	17	Book Reviews	56
The Internet of Things		
.....		Letters	59
USA Advanced Course in	20	
Engineering (ACE) Cyber		Remembrance	60
Internship 2015		
Lt Lindsey Wood		RSI Events 2016	64
.....		HQ Royal Signals	
Cyber Electromagnetic	23		
Activity (CEMA)			
- Supporting the			
Information Age			
Lt Col Ian Buchanan			

IN THIS ISSUE.....



14 Encryption for Communication Security



23 Cyber Electromagnetic Activity (CEMA)



38 A Stay Behind Jungle Detachment in Malaya



46 Champagne - Worth the label ?



51 New Corps Painting



52 UK Mobile Force (UKMF)

This issue's cover *Exercise ARRCAD E CHARGER. Image of the ARRCs deployed headquarters in October 2014. Exercise ARRCAD E CHARGER was a warm-up event at RAF St Mawgan that primed this UK-based NATO Rapid Deployment Corps for future training and testing as a Joint Task Force.*

JOURNAL

Volume 33
Issue 2
Winter 2015



Tom Moncur

EDITORIAL

Welcome to the second Journal of 2015, with something of a seasonal feel. I have returned for a time as your editor to allow Nigel Harrison to concentrate on other aspects of the fast growing organisation that is the Royal Signals Institution. As you can see from our articles on the Seminar and London Dinner, he has been busy!

The focus this month is on cyberspace and its ramifications. The articles are aimed at all levels of knowledge and serve to underline our need to embrace fully the issues raised. The focus of the Corps is changing to produce the specialists and knowledge we will need to support the Army's interests in this most important of fields. The quality of the awards notified in this issue are testimony to the fact that we have the quality which is needed! Note that commanders should be giving consideration now to worthwhile candidates for the 2016 awards process. Full guidelines are set out in this issue.

Articles and letters for the Journal are solicited from our readers. These may be technical or equipment related, historical or general interest in nature, and must be unclassified. The Journal is read by all senior officers in the Corps, so it is the ideal medium for giving your views some exposure. Prudence dictates that the chain of command is at least informed in advance of your views!

This issue sees the return of our book review section, notable for featuring books by two former Corps officers. We welcome also the return of an article by one of our regular contributors, Major Tom Johnstone, on a fascinating historical episode, and one on the lighter side of life, appropriate for the festive season! We wish everyone a happy Christmas, and a healthy and prosperous New Year in 2016.

*Best Wishes,
Tom*

E-mail: journal@royalsignals.org
Post: RSI Secretary, HQ Royal Signals, Griffin House,
Blandford Camp, BLANDFORD FORUM
Dorset DT11 8RH
Phone: 01258 482647

THE ROYAL CORPS OF SIGNALS



CORPS COUNCIL

Chairman	Lt Gen NAW Pope CBE
Controller, Royal Signals Trustees Ltd	Maj Gen TG Inshaw CB
Chairman, Royal Signals Association	Brig DA Hargreaves
Chairman, Royal Signals Institution	Brig M Lithgow CBE
Chairman, Royal Signals Museum Trustees	Brig CJ Burton OBE
Colonel Commandant Heritage	Brig EM Flint
Chairman, Royal Signals Games Club	Brig SJ Vickery
President, Royal Signals Dinner Club	Brig JE Richardson MBE
Colonel Commandant	Maj Gen I Hooper
Colonel Commandant	Maj Gen J Crackett CB TD
Colonel Commandant	Brig HJ Robertson QVRM TD
Comd 1 Sig Bde	Brig SPM Nesmith
Comd 11 Sig Bde	Brig R Anderton-Brown
Corps Colonel Royal Signals	Col SG Hutchinson ADC
Secretary	Col TW Canham

RSI COUNCIL

President	Lt Gen NAW Pope CBE
Chairman	Brig M Lithgow CBE
Vice-Chairman	Brig DB Warne
Corps Colonel Royal Signals	Col SG Hutchinson MBE ADC
Commandant, Defence School of CIS	Col MJ Fensom
Representative Corps Supervisor	WO1 (CFofS) T Searle
Joint Forces Member	post vacant
Reserve Forces Member	post vacant
Retired Member	Brig DE Rowlinson
Regimental Secretary	Col TW Canham
Secretary	Lt Col NP Harrison MBE

RSI COMMUNICATION COMMITTEE

Chairman	Lt Col OTB Courage
Wider Defence Representative	Maj Gen WJP Robins CB OBE
Industry Representative	Brig PJ Davies
Reserve Forces Member & Marketing Advisor	Brig NC Beacom QVRM TD
Journal Editor	Col TF Moncur
SO1 Comm & Heritage, HQ Royal Signals	Maj J Fradley
Representative Corps Supervisor	WO1 (CYofS(EW)) JP Seaton
Secretary	Lt Col NP Harrison MBE

Authors alone are responsible for the contents of their articles.

The opinions expressed in the articles are those of the authors and do not reflect necessarily the policy and views, official or otherwise, of the Royal Corps of Signals or the Ministry of Defence. This publication should be treated with discretion by the recipient.

© Crown Copyright Disclaimer: No responsibility for the quality of goods or services advertised in this magazine can be accepted by the Publishers or Advertising Agents. Advertisements are included in good faith.

*Design and Photoshop Mr Adam Forty
Printed by Holbrooks Printers Ltd, Hilssea, Portsmouth PO3 5HX*



THE CENOTAPH 2015

By Colonel Terry Canham – Regimental Secretary



For reasons which are not entirely clear, RHQ Royal Signals has not concentrated on the Cenotaph each November but has focused instead on Remembrance events at Blandford as the Home of the Corps. This seems strange, as there has long been a contingent of largely London-based stalwarts who have marched, and many other Corps and Regiments put a far greater effort into this national event.

Following some internal discussion, the Assistant Regimental Secretary, Major Mark Tivey and the SO1 Communication & Heritage, Major John Fradley, decided to investigate and took part in the Cenotaph service and march-past in 2013. They persuaded me to take part in 2014 and I, in turn, suggested to the Corps Council that the Corps should try to

build on the event with a view to being the lead contingent for the march-past for the Corps Centenary in 2020. To that effect, the Representative Colonel Commandant, Brigadier Jim Richardson, marched with the Royal Signals Contingent this year. Moreover RHQ has, since 2013, persuaded the Royal British Legion to increase our allocation of spaces to 48. They were all filled again this year, and we would like to increase the numbers further if we can.

The format of the day is relatively straight-forward. Contingents from across the Services congregate on Horse Guards Parade before marching to Whitehall where they then take part in the Remembrance service before marching past the Cenotaph. The positions of contingents are changed each year and, for 2015, we were lucky enough to be located in the first column so relatively close to the Cenotaph itself. Although we could not see the Remembrance service directly, we were right beside one of the many giant TV screens provided for the veterans on parade. This part of the day is not as solemn as might be thought as there is a certain amount of banter in the ranks – not to mention with the many spectators lining the route! Hip flasks seem to be plentiful and we were even treated to sweets by a delightful young lady in the crowd!



Top: The Cenotaph contingent

Above: Assembling on Horse Guards Parade

Once the Act of Remembrance is over and Her Majesty and the various VIPs have departed, the march past starts. It is not a long route, but goes past the Cenotaph, turns right on Parliament

Square and then back to Horse Guards Parade. As we marched, we received incredible support from the spectators who were cheering and thanking the veterans for their service and what they had done for the country; I doubt that any of us had ever felt quite so appreciated by the general public before!



Cenotaph March Past captured from TV

What many people probably do not realise is that there is always a member of the Royal Family to take the veterans' salutes from a small dais before the various contingents march back on to Horse Guards parade; this year it was Prince William. Once back on Horse Guards, our contingent joined together spontaneously to say the magnificent words of our Corps Collect before dispersing after the playing of the National Anthem.

The Cenotaph is a moving event which, at the same time, allows veterans to remember those who have fallen whilst enjoying comradeship with fellow servicemen from across the years. There is no complicated drill and much of the day is quite informal but it is, I believe, something which every Signaller might want to put on his bucket list and RHQ would be delighted to hear from you if you would like to march. If you would like to bid for a place then please contact the RSA Admin Officer, Caroline Addison, on rsa@royalsignals.org or 01258 482090. I hope that, if responses are good, we can encourage the Legion to let us have even more spaces in the run up to 2020.

The Corps Collect:

“Almighty God, whose messengers go forth in every age giving light and understanding grant that we, of the Royal Corps of Signals, who speed the word of man to man, may be swift and sure in sending the message of Thy truth into all the world. May we serve Thee faithfully and, with the help of Thy Holy Spirit, make such success of our soldierly duties on this earth, that we may be found worthy to receive the Crown of Life hereafter, through Jesus Christ our Lord. Amen.”

The Corps Contingent on Whitehall



CORPS AUTUMN GUEST NIGHT



The Corps Autumn Guest night was held at the Headquarters Officers Mess on Thursday 1 October, and saw the formal presentation of the BAE Systems 'Falcon' Award to the Corps. The trophy was notified to Journal readers in the Summer 2015 issue of the Journal. The photograph below shows the Master accepting the trophy from Mr Daren Brown, the leader of the Systems business stream within the Defence Information business at BAE Systems.

As ever, the event was an occasion where the Corps bid a formal farewell to its retiring officers, and welcomed those newly commissioned, as follows:

Officers Dining Out

Col J Vosper
 Lt Col I Blower
 Lt Col N Coatsworth
 Lt Col D Macaulay
 Lt Col R Janes
 Maj M Schofield

Officers Dining In

Capt T G Woodall	Capt S Morris
Capt P J Mason	2Lt A Balfour
Capt D Mears	2Lt A Boyes
Capt N Butler	2Lt B Cauldwell
Capt K Langan	2Lt O Franklin
Capt W J Little	2Lt B Heslop-Charman
Capt R S Murray	2Lt D Keegan
Capt I D Shaw	2Lt P Kerrigan
Capt D G Randall	2Lt D Maclachlan
Capt C M White	2Lt A Miller
Capt D J Edkins	2Lt M Shrubb



"And another thing...." The Corps RSM makes a point



The Master congratulates artist Stuart Brown on "Zeitgeist"

THE INSTITUTE OF TELECOMMUNICATIONS PROFESSIONALS



The Corps is delighted to reproduce the following testimony on Staff Sergeant Rebecca Taylor, currently serving with 299 Signal Squadron. She has our very sincere congratulations.

The judges were unable to settle on just one winner for this award. So, the Judges introduced a Runner up category – we are delighted to say that the runner up for this award is Staff Sergeant Rebecca Taylor.

RUNNER UP - SSgt Rebecca Taylor, The Royal Corps of Signals, British Army.

Sergeant Taylor is employed by the Army Royal Signals. Her senior officers detailed her achieved over a career of 14 years, exhibiting leadership, management and technical excellence and exemplary performance.

SSgt Taylor consistently demonstrates a desire to undertake more demanding and senior roles. It is this tenacity, combined with her inherent talent that led to her becoming the de facto subject matter expert in the life-saving area of Electronic Counter Measures, indeed trialing, and then instructing on a new Electronic Counter Measures equipment. Her contribution in this regard cannot be overstated, be it on operations to ensure public safety in the UK or on the frontline of countering improvised explosive devices in Afghanistan.

She serves in sometimes harsh and dangerous conditions but maintains operational effectiveness and a professional standard that is exemplary. Congratulations to Staff Sergeant Rebecca Taylor on being runner up for the Chris Seymour Award for Women in Telecoms.

Crissi Williams MITP

Senior Commercial Manager

The Institute of Telecommunications Professionals (ITP)

APPRENTICE OF THE YEAR 2015

The Royal Signals Institution in partnership with the Apprenticeship Training Provider and Professional Institutions has recognised the value of our apprentices with the award to the R SIGNALS Apprentice of the year 2015. These awards recognise the excellence and commitment of R SIGNALS soldiers enrolled on or having completed their Apprenticeship reflected in their contribution to their Unit. The award will reveal the personnel journey conducted by our Apprentices during the concurrent progression of their Military Career and R SIGNALS Apprenticeship.

The RSI, Wiltshire & Somerset Colleges Partnership Ltd, Institute Engineering & Technology and the Chartered Institute Logistics & Transport (UK) have agreed to co-sponsor the award of R SIGNALS Apprentice of the year. The award will identify the top Apprentice of each R SIGNALS Career Employment Group with a prize of £250 for the top Apprentice Logistician, Electrician, Operator, EW Operator, Technician and Engineer. From the 6 CEG Apprentices of the year, one award will be presented to the Corps Apprentice of the year with a total prize of £1000. This year by kind donation of BAE Systems the overall Royal Signals Apprentice of the year will receive the Falcon Trophy.

The Corps Colonel chaired the selection panel in Oct attended by representation from The RSI, Apprenticeship Training Provider and Professional Institutions. The panel selected the following six Royal Signals soldier Career Employment Group winners:

Engineer. Lance Corporal H Harris, Support Squadron, 2 Signal Regiment.

Technician. Signaller L C Molyneux, 241 Signal Squadron, 10 Signal Regiment.

Logistician. Signaller C L Lewin, unit withheld.

Electrician. Lance Corporal A Brabbs, Support Squadron, 2 Signal Regiment.

Operator. Signaller H R Morris, 219 Signal Squadron, 2 Signal Regiment.

EW Operator. Lance Corporal J Thomson, 223 Signal Squadron, 14 Signal Regiment (EW).

The overall winner is Signaller Morris, who was presented with the award at a ceremony at Regimental Headquarters Griffin House on 3 December 2015 hosted by the Corps Colonel.



Cisco is proud to be a corporate member of the Royal Signals Institution

Solutions to Support Your Global Mission

Global pressures and new technologies are changing the way Governments protect their national interests. Cisco deliver defence and intelligence solutions which unite legacy systems, improve agility, build your virtual presence and meet your most demanding C4ISR requirements to achieve mission success.

For more information please visit www.cisco.com/go/defence or email uki-defence@cisco.com



RSI LONDON LECTURE & DINNER 2015



Institute of Directors, Pall Mall.

The annual Royal Signals Institution London Lecture and Dinner was held this year on Thursday 19 November in the usual premises of the Institute of Directors, Pall Mall, London. The Chairman was Brigadier Mike Lithgow, and the speaker was the Master of Signals, Major General Nick Pope, who was rounding off in fine style a year which saw him selected for promotion to the rank of Lieutenant General.

Once again the event was well supported by colleagues in industry, despite the attractions of competing events elsewhere, and the staff of the Institute of Directors yet again produced a faultless menu and level of service of a kind which are too seldom seen in our present times. Attendees enjoyed a thought-provoking after dinner address which was relevant, topical, humorous and serious by turn, and stimulated much discussion and subsequent questions.

As ever, the event is also an appropriate occasion to celebrate the accomplishments and endeavours of our prizewinners, and who received Institution awards, details of which are set out elsewhere in this issue. As sometimes happens, one individual was totally unaware that he was being honoured, and Colonel Graham Norton was thus very pleasantly surprised when his name was announced!

Royal Signals Institution Prizewinners 2015

Colonel Graham Norton

Princess Mary Medal



Lieutenant Colonel Ian Buchanan

Silver Medal

Ian Buchanan is the SO1 EW and Cyber in Capability Directorate Information at Army Headquarters. He is responsible for the development and delivery of a range of capabilities that includes Electronic Counter Measures (Force Protection), Spectrum Management, Electronic Warfare, Signals Intelligence and Cyber. Each of these areas is not without its own very significant challenges; nevertheless throughout his three years in post he has shown superb leadership in carefully managing his team to successfully deliver results across the board. In particular, the Army's Cyber capability, while still nascent, has developed at an impressive pace but only as a result of his selfless commitment and sheer hard work.



As the principal staff officer leading the development and delivery of the Army Cyber capability Lt Col Buchanan has effected change with a considered, but coherent approach, ensuring that best practice from our allies and the other Services was harnessed. As an example, he introduced the US 'CEMA' (Cyber and Electro-Magnetic Activities) concept to UK doctrine, and has maintained a steady drumbeat of education to the many senior officers whom he is regularly called upon to brief, ensuring that progress is considered in a holistic, capability-wide manner. It would be easy to allow the growing focus and consequent escalating demand for cyber capability to develop disparately but Lt Col Buchanan has not taken the easy path; instead he has used his expertise to counsel wisely, and robustly when necessary, not simply to maintain momentum, but instead to gather pace.

What he and his team have achieved with only the bare minimum of resource has been remarkable. He has directed Cyber Vulnerability Investigations into potential weaknesses in Army major platforms. He has also led the Army's contribution to the creation and growth of cyber Reservist capability; developing a process to enable civilian specialists to join the Army without meeting the mandated entry standards. With single-minded perseverance he overcame policy and procedural hurdles, including significant cultural resistance at very senior levels, creating revised policies and a system of waivers to enable critical civilian expertise to be brought into the Army, the

initial tranches of whom are already delivering effect. His team has also created, without any additional resource, a pilot Cyber Protect Team that will act as a proof of concept from which to build cyber defence at the tactical level, and is in the early stages of developing a similar Cyber Mission Team that will deliver offensive effects to Commanders at the tactical level. To underpin the broader development of cyber as a capability he has made sure that the foundation doctrine and basic training is in place to set the conditions for long term success.

Lt Col Buchanan has worked tirelessly to develop the Army's cyber capability; persuading and convincing allies, seniors in the Army and those across wider Defence to engage and provide support. He is widely acknowledged as the driving force, and as having achieved remarkable progress in this area of vital and growing importance. He has put the Corps in the vanguard of the Army's contribution to Defence cyber capability. In recognition of his efforts Lt Col Buchanan is awarded the Royal Signals Institution Silver Medal.

A handwritten signature in black ink, appearing to read 'N. A. W. Pope'.

Major General N A W Pope CBE
Master of Signals
19th November 2015

Sergeant Alex Mitchell

Silver Medal

Sergeant Alex Mitchell was deployed to the Occupied Palestinian Territories (OPTs) in the rank of acting Staff Sergeant as the SNCO Instructor for the nascent Palestinian Officers' Academy. This Combat training advisory role was the first of its kind, requiring the design and implementation of culturally sensitive yet innovative methods of training delivery in an enormously difficult international environment.

As the first SNCO to be deployed into the US Security Coordinator (USSC) mission, SSgt Mitchell slipped seamlessly into a very senior multinational and multi-agency team to help deliver a landmark Palestinian Officers Commissioning Course. He coordinated and briefed at two and three Star level with the US military, US State Department, and Palestinian Security Forces to ensure this complex project



His end to end approach to problem solving, patience, and ability to manage multiple workflows with ease made him a pivotal member of the team.

SSgt Mitchell's influence and example have undoubtedly shaped the future of the Palestinian Officers' Academy and enhanced the reputation of the UK Team in the West Bank. Displaying the highest calibre of military bearing and professionalism when dealing with Israeli and Palestinian Security Forces alike, he has proven himself to be a superb ambassador for the Royal Corps of Signals, and for the British Army. His ability to negotiate second and third order consequences set him leagues ahead of his US and Canadian peers (Captains and Majors), allowing the team to progress UK Foreign & Commonwealth Office and MOD objectives in one of the most complex political environments in the world.

SSgt Mitchell's impact and delivery on this 9 month long operational tour in the OPTs was exceptional; he led his US, Canadian, Dutch and Palestinian military colleagues in the way that only the highest quality British Army SNCOs can. Lieutenant General Rudesheim US Army, the US Security Coordinator for Israel and the OPTs, was extremely impressed by SSgt Mitchell's performance and strongly endorsed the case for him to receive formal recognition for his work.

For his exemplary professionalism and excellence as an ambassador for his country, the British Army and the Royal Signals Sergeant Mitchell is awarded the Royal Signals Institution Silver Medal.

Major General N A W Pope CBE
Master of Signals
19th November 2015

was well understood and properly supported at the highest levels. Simultaneously, his consistent and high quality grass roots engagement with Palestinian stakeholders had an enormous impact, aided by learning to speak Arabic in his spare time.

SSgt Mitchell's quality and experience was highlighted when he took the lead for the procurement of the entire Academy's Equipment Table. His thorough research of suitable equipment and marked ability to balance value for money and utility was first class as he immersed himself in an opaque international bureaucratic procurement process. He was very successful on all counts, delivering critical UK input and guidance on the ground against a multinational backdrop that was fraught with challenges.

Lieutenant Colonel Dorian Seabrook, Royal Engineers

Master of Signals Award

Dorian Seabrook's contribution to the Army Software House has greatly enhanced the Army's reputation, the credibility of the Royal Signals and the development of the Corps' soldiers in areas and skills that directly support the future evolution of information professionalism. Virtualisation; agile; automation; DevOps; Continuous Integration; IaaS, PaaS, SaaS platforms are all aspirations of the MOD's Chief Digital Information Officer (CDIO) that are being delivered now by the Army Software House for which he has been the sole SO1 for the last 12 months and de facto Chief Operating Officer. It is the Royal Signals that benefits the most, both directly and indirectly, from this in-house transformation programme that reached initial operating capability during the Summer. It is Lt Col Seabrook's selfless commitment, dedication, technical expertise and sheer professionalism that lie behind this transformation success.

Building on the foundations laid by his predecessor, he has personally driven forward and been the tireless architect for the technical refresh of the Army Hosting Environment and in particular the changes to the Army Software House

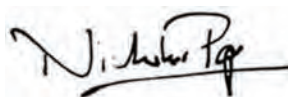


operating model. Director Information can now claim to be delivering and exploiting virtualisation cloud technologies at the forefront of technical currency and a 'DevOps' culture embracing agile development methods which is being recognised by CDIO as "an island of excellence in a sea of fudge". Of particular relevance to Royal Signals is the fact that he is bringing 243 Signal Squadron on that journey with him; the Squadron hierarchy have learned enduring skills in designing an ITIL/Agile led model which will be carried forward into other areas of the Corps.

Lt Col Seabrook has also established a contractor-supported mentoring system to develop deep application skill-sets into Royal Signals soldiers both in terms of application lifecycle management and in the administration of cloud enterprise services. This has a direct read-across into operational effectiveness as it offers a secure base from which to develop key skills that are essential in supporting our ever increasing reliance on information and data in the deployed space. As the Army move to tactical clouds the Corps will have a cohort of soldiers who understand the technology through their time in 243 Sig Sqn and Army Information Services (AIS). Lt Col Seabrook has also upped

AIS's engagement with the FofS(IS) and CISM courses during his time in post – both in terms of providing a whole day of practical examples around the theory they are learning but also in supporting a number of projects and dissertations. The credible capital of the Army Software House amongst the Navy, RAF and ISS is very high and directly reflects on the Royal Signals brand.

It is immediately obvious to all who meet Lt Col Seabrook that he is an Information Superiority role model; as well as mentoring members of 243 Sig Sqn he is an inspiration to a wider community of the Corps' officers and soldiers. He embodies the excellence, the professionalism and the array of skills that we aspire to find in members of the Corps. For his outstanding contribution to Defence, to the Army and to the Corps, Lt Col Seabrook is presented the Master of Signals Award.



Major General N A W Pope CBE
Master of Signals
19th November 2015

Staff Sergeant (Foreman of Signals) Lindsay Thorburn

Silver Medal



Left to Right:
Colonel Simon Hutchinson, Sergeant Alex Mitchell, Staff Sergeant (FoS) Lindsay Thorburn, Major General Nick Pope CBE, Lieutenant Colonel Ian Buchanan, Lieutenant Colonel Dorian Seabrooke and Colonel Graham Norton

THE ROYAL SIGNALS INSTITUTION SEMINAR

THE ROYAL UNITED SERVICES INSTITUTE
20 OCTOBER 2015

The above event was intended to create a common understanding of the potential problems with which Royal Signals will be faced drawing on the experiences of the commercial and public sectors who are successfully navigating the digitalisation revolution. The RSI events in 2016 will create a forum for discussion of the potential solutions to these challenges.

*“It is not the strongest of the species, nor the most intelligent which survives... it is the one that is **most adaptable** to change.” – Charles Darwin*

“When you come to a fork in the road, take it.” – Yogi Berra

EXECUTIVE SUMMARY

- Whilst Defence may be decreasing in physical size, the level of investment in technology at 6.1% is on a par with global technology based organisations. Those that deliver and manage this investment require a mind-set of enterprise growth, innovation and exploitation of IT/OT for a re-envisioned and demanding global security environment.
- However Defence is at risk that the benefits that should accrue at this level of investment will not be realised due to its inherent culture of being risk-averse, slow to innovate, over-burdensome governance and a mind-set of cost reduction.
- The current CDIO is charged with leading this change. Royal Signals is in a position to support, but if it fails to take advantage of this window of opportunity, evidence from other enterprises would indicate that it will be bypassed by others more attuned and ready to take on the shaping of the future.
- The redefined and demanding future will be characterised by:
 - » An acceptance and embracing of the rate of change of technology and the consequent need to continually develop and adapt the way that we work in UK and in the field.
 - » An understanding of how far current and potential opponents have come in harnessing such change: ISS and the Russian Federation are examples.
 - » A realisation that the pace of acquisition must reflect this and that this will involve some risk.
- Current Defence industry partners adapting to the new environment and for Defence to find and encourage as yet unknown innovative players.
- Competition for top young talent, who will want to be part of dynamic and “cool” organisation; talent without which we will flounder.
- An understanding that the traditional IT and hard system boundaries to this initiative have already evaporated: the Internet of Things, robotics, big data, cloud, mobile working as a norm, all lead to a new world in which the Corps must lead or be led.
- The Corps must learn new skills of modal working, strategic development and advocacy to support the CDIO.
- It must also match best in class enterprises for delivering the basis – Service and Demand Management plus Integration.
- The result of inaction will be the Corps becoming an army of people who deliver Defence Utility Services for Technology (DUST).
- This profound change in mind-set is required at every level – from managing corporate Defence down to Brigade and lower. It affects everyone in the Corps.
- The RSI is offering to lead a series of workshops to help map out a Future Corps based on the arguments above. This will require an investment in time and resource from a cross-section of the Corps who are able and willing to think beyond the current neatly defined boundaries, able to envision the future for Defence and the Corps.

Michael Lithgow, Brigadier

Chairman, The Royal Signals
Institution



Communication is everything



General Dynamics UK is proud to be a Corporate Member
of the Royal Signals Institution

ENCRYPTION FOR COMMUNICATION SECURITY - A FRESH LOOK

EDITOR'S NOTE

Lieutenant Colonel Guy Meakin MA CEng MIET

Guy Meakin had a full career in Royal Signals, passing as a communications systems engineer on his many tours in London, before transferring to the MOD Civil Service, where he spent his last five years of service as Departmental COMSEC Officer.



I seem to have missed the International Standards Organisation (ISO) 7-Layer Model for Open Systems Interconnection (OSI) during my formal R SIGNALS education, probably because it was first published in 1980 – sometime after my formal education finished. Another missed topic was the engineering design of online encryption systems, probably because that sort of work was confined to CESG in those days and R SIGNALS just took their deliverables as “given”. So it was with some puzzlement that, in the early 90s in LSOR8 (now subsumed into Equipment Capability), I read a NATO policy for the use of different types of encryption at the various layers of the 7-Layer Model. It took several years of involvement in modern electronic encryption systems for me to understand the significance of that NATO policy for secure communication systems.

Today, the relevance of the ISO 7-Layer Model has been partly overtaken by the pragmatic use of the Transmission

Control Protocol/Internet Protocol (TCP/IP) 5-Layer Model in the engineering design and adoption of online encryption systems, particularly for communication over the Internet. However, the ISO terminology is still useful in some cases.

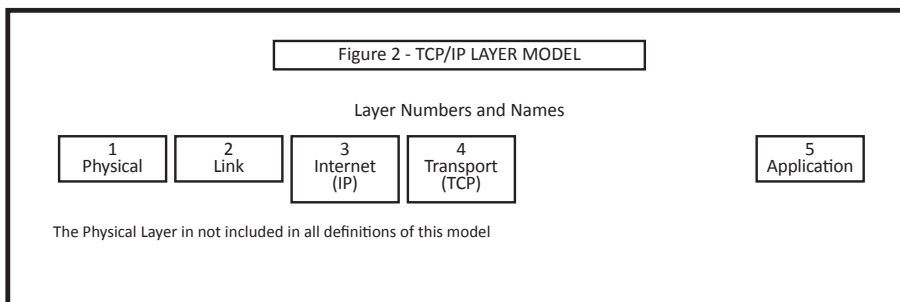
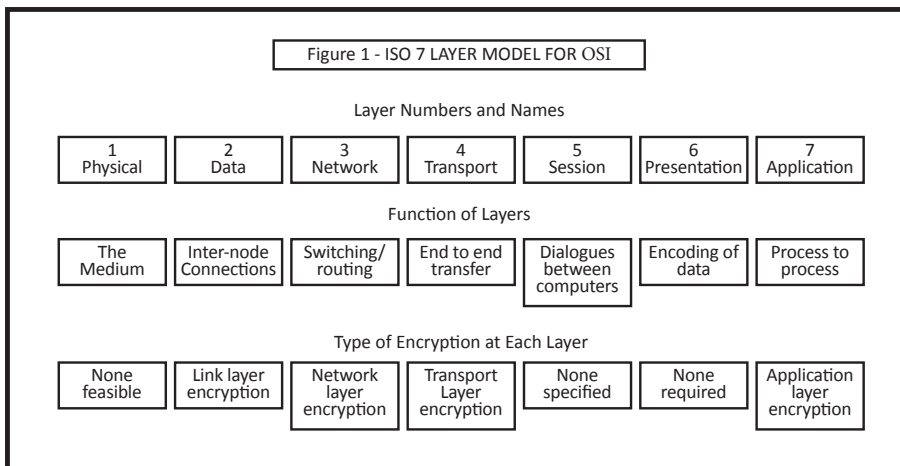
This article explores the applicability of these Layered Models to the adoption of various encryption systems. For those less familiar with the communications technology, it also presents the layered approach to an analogous parallel model of railway security. This parallelism leads to some speculation over the improvement of future policy in this area.

THE LAYERED MODELS

Figure 1 shows the ISO 7-Layer Model for OSI (ISO 7498), together with the functions of each Layer and the name of the type of encryption (if any) which is applied at the Layers. Figure 2 shows how the TCP/IP 5-Layer Model (as defined by the Internet Engineering Task Force (IETF) in its Requests for Comment (RFC) 1122 and 1123) differs from the ISO Model: the functions of each Layer and the types of encryption are the same in both Models. Since the difference between the two Models lies only in the Session and Presentation Layers and since no encryption is provided for these Layers in the ISO Model, the difference is not important in this article.

TYPICAL ENCRYPTION SYSTEMS

A wide variety of Government developed and Government approved encryption systems have been used or are still in use for securing Government, including MOD, communication systems. A few are listed below against the Layer at which they are operated.



station to terminal station through nodes called intermediate stations: in this model, all intermediate stations are railway junctions, ie have three or more routes connected. Passengers are packed into compartments; there are several compartments in each carriage. Carriages are assembled into trains at terminal stations for journeys from a terminal station to the nearest intermediate station, then the journey between intermediate stations and, finally, from the last intermediate station to the destination terminal station. Sometimes carriages may remain in the same train for the whole journey between terminal stations.

PHYSICAL LAYER

At the Physical Layer, no electronic communication security measures are feasible. Only physical security measures are available, eg secure areas, secure conduits or fibre optic cables with tamper-evident techniques.

It is important to understand that it is the Layer at which the Plain Language (Red traffic) enters and leaves the encryptor, which determines the Layer at which the encryptor operates. For example, just because an encryptor operates point to point, ie it uses a "link", over the medium of cable or radio, it is not necessarily a Link Layer encryptor. Unless it is determined by the protocols of the Layer at which it is operating, the ability of an encryptor to operate point-to-point or point-to-multipoint is largely a matter of crypto synchronisation.

Link Layer Encryption. LAKIN, ANWELL, PERTH, Asynchronous Transfer Mode (ATM) CATAPAN. Network Layer Encryption. BEAUTY, IP CATAPAN, Thales Datacryptor, IPsec in accordance with RFC 4301.

Transport Layer Encryption. No Government approved systems, but low-grade security from Transport Layer protocols: the IETF Transport Layer Security (TLS) protocol (RFC 5246) and the proprietary Secure Sockets Layer (SSL) protocol.

Application Layer Encryption. Secure data or telegraph: HORA, TRUNCHEON. Secure voice: LAMBERTON, PRITCHEL, BRENT. Secure messaging: low-grade security from the Application Layer protocol Secure/Multipurpose Internet Mail Extension (S/MIME) (RFC 3851).

PARALLEL MODELS OF COMMUNICATION NETWORKS AND RAILWAY NETWORKS

Communication networks transfer data from host to host (terminal nodes) through switching nodes (switches or routers). Data may be serial or may be packed into Protocol Data Units (PDU), eg Datagrams, Internet Protocol (IP) packets or High-Level Data Link Control (HDLC) frames. Railway networks transfer passengers from terminal

In the railway analogue, the Physical Layer is the railway track and the equivalent Physical Layer security would be achieved by stationing guards along tracks.

LINK LAYER ENCRYPTION

At the Data Link Layer, encryption is normally achieved by encrypting each link separately with hardware encryptors. (The exception is ATM encryption, of which more later.) Although all encryptors may use the same encryption key, cryptosecurity is enhanced by using different keys on each link. Inside switches traffic is in clear (unencrypted).

In the railway security analogue for this Layer, carriages are locked before departure and unlocked on arrival at each intermediate station and at the destination terminal station. Although all trains on a network may use the same lock and key, security is enhanced if each train has its own specific lock and key. Passengers change trains at each intermediate station.

NETWORK LAYER ENCRYPTION

At the Network Layer, IP packets are encrypted at the sending terminal and decrypted at the receiving terminal. Different data encryption keys are used for each pair of terminals. Switches route encrypted traffic, ie they are "black" routers.

In the railway security analogue for this Layer, carriages are locked before departure from the terminal station and unlocked on arrival at the destination terminal station, but they are sorted into appropriate trains at each intermediate station. All carriages on one route have the same lock and key. Passengers remain in the same carriage for their whole journey.

TRANSPORT LAYER ENCRYPTION

At the Transport Layer, terminals establish Virtual Private Networks (VPN) between each other in pairs for each end-to-end traffic route: so a terminal may be running many VPNs simultaneously. Datagrams are encrypted at the sending terminal and decrypted at the receiving terminal. Each VPN will use a separate data encryption key. Switches route encrypted traffic.

In the railway security analogue for this Layer, carriages are locked before departure from the terminal station and unlocked on arrival at the destination terminal station, but in this case they remain in the same train for the whole journey. As for the Network Layer, all carriages on one route have the same lock and key and passengers remain in the same carriage for their whole journey.

APPLICATION LAYER ENCRYPTION

At the Application Layer, we need to discriminate between the different types of network that will carry the traffic.

For circuit switched circuits, which are to carry traffic between secure telephones, a dedicated circuit is established between the terminals for each conversation. Key management policy may require different data encryption keys for each specific multi-party community, for each pair of telephones or even for each conversation. Switches carry encrypted traffic.

In the railway security analogue of circuit-switched communications, it is as if single locked carriages are dispatched along dedicated routes to their respective destinations, achieving special clearance through intermediate stations and being unlocked on arrival at their destinations.

For permanent circuits, which are to carry traffic between secure telegraph or secure serial data terminals, a special permanent connection is procured: this bypasses any switches in the network. Separate data encryption keys may be used on each link, or if a number of links form part of a community of interest, eg a tape-relay network, the same keys may be used on many links.

In the railway security analogue of permanent circuits, it is as if dedicated tracks, bypasses as it were, are laid around all intermediate stations.

For radio nets, the necessary circuit is established over a specific frequency and transmissions are encrypted and decrypted at terminals. There are no switches as such, but rebroadcast stations may be used to connect nets together physically, transmissions being decrypted and re-encrypted at each rebro. Because it is impossible to deliver railway passengers to more than one destination, this mode of transmission and encryption has no analogue in the railway model.

In packet-switched networks, messages are encrypted in host terminals at the Application Layer and decrypted at the destination host terminal. Each message is encrypted in a separate data encryption key. Each copy

of a message for destination addressees is encrypted in the same data encryption key: however, cryptosecurity is ensured, because the sending terminal also sends the data encryption key to each recipient encrypted in the recipient's own Public Key. Switches route encrypted traffic.

In the railway security analogue for this Layer, it is the compartment of a carriage that is locked with its own key before departure and unlocked on arrival at the destination terminal station. Passengers remain in the same compartment for the whole journey.

ATM ENCRYPTION

In ATM encryption, ATM cells are encrypted in a hardware encryptor at one terminal with data encryption keys shared with a similar encryptor at the destination terminal. These pairs of encryptors establish between each other Virtual Paths, which are in some ways similar to the VPNs used at the Transport Layer. One encryptor may establish many tens or hundreds of pair-wise Virtual Paths. ATM switches in the network route encrypted cells.

In the railway security analogue, the equivalent security functionality is very similar to that described for the Transport Layer above.

CONCLUSIONS

In the railway security model, it appears that some types of security are either costly for the network provider or inconvenient for passengers. The provision of guards along tracks and the laying of bypasses round intermediate stations are two examples of high cost. Or, in the Link Layer analogue, requiring passengers to change trains at every intermediate station is highly inconvenient. (It should be noted that parcel goods are often conveyed like this – goods trucks being sorted into new trains at railway junctions.) The expense of physical communication security is obvious and shows a good parallel with the expense in the railway model. Perhaps the expense of providing so many encryptors and the time taken for successive encryption and decryption processes for Link Layer encryption show parallels in cost and “inconvenience” of equal note.

On the other hand, the gradual reduction in the use of permanent circuits and the migration of circuit switched telephone services onto IP services show how expense has already driven the adoption of more modern communications technology. The railway model analogues above do seem to provide equally realistic examples.

So, the analogues for Network Layer, Transport Layer and Application Layer encryption - all for packet-switched networks – and ATM encryption appear to show economic and convenient services in the railway model. Indeed, in my estimation, all four types of encryption are economic and cost-effective. However, my railway analogues for Transport Layer and ATM encryption show a slight edge over the other two and my speculation is that it would be worth exploiting these two types of encryption more in the future.



NET GAINS - THE INTERNET OF THINGS

This article is reprinted from Director magazine, by kind permission of the Institute of Directors.

First there was the steam age, followed by the ages of electricity and information technology. But the biggest change – the driving force behind an imminent fourth industrial revolution – is now on our doorstep.

So crucial is it considered to Britain's future that the Prime Minister has pledged an extra £45M to its development in the UK, bringing total public sector investment to around £73M. As an emerging sector, it is on track to grow by 17.5% per year, reaching a value of \$7trn or £4.3trn in 2020 according to IT research agency IDC. Analysts at US banking giant Morgan Stanley suggest there may be as many as 75 billion interconnected devices in the world by 2020.

To call the Internet of Things (IoT) the next big thing would be an understatement. So, what exactly is this phenomenon that has proactive thinkers rubbing their hands with glee – but reactionary technophobes feeling the cold hand of Big Brother on their shoulder?

For the uninitiated, the IoT is the emerging scenario whereby familiar objects contain miniature hardware which transfers data over the web without any human intervention taking place. "Internet of Things" seems rather a woolly name for it, but "things" is the only word vague enough to cover the frankly enormous range of objects under consideration – anything from office bins to thermostats, coffee makers, washing machines, headphones, lamps, oil-rig drills, heart monitors, plants, cattle, jet engines, nuclear reactors and space probes.

The list becomes noticeably progressively outlandish – because the possibilities appear infinite. "It's the biggest change, the biggest opportunity since perhaps the introduction of the mobile phone" says William Higham of future-gazing strategic consultancy Next Big Thing. "It's a genuine revolution. And it's already started to an extent. Even things like sat-navs, GPS

museum guides – at the David Bowie exhibition at the V&A, you turned on a device and it knew where you were in the space, and changed the soundtrack and script accordingly – all these things are, to an extent, early examples of the Internet of Things in action" Higham believes that understanding of the IoT starts with an understanding of the word "smart". "The word is bandied about" he argues, "but what it really refers to is devices that are genuinely intelligent: that can, in effect, make decisions. A smart appliance realises that when X happens, it should do Y." Google Glass, exercise aid Nike + FuelBand and Apple's indoor position system iBeacon are good examples of what he is talking about, and demonstrate the extent to which behemoth global enterprises are cottoning on to the potential of IoT.

But, says Higham, the IoT is set not just to make gizmos from the world's most famous brands, but the everyday objects around us part of a network of hyper-efficiency – and throughout society at large. "Imagine there is enough rubbish in an office waste basket to reach a certain height" he says. "A sensor could send a tweet to the office management telling them to empty it. On a much larger scale, it could activate the entire building's recycling centre, which could ultimately notify the collectors when the trucks need to come and so on."

EARLY ADOPTERS

Other simple scenarios that look likely in the near future include straightforward matters of convenience – your car's satnav informing your boiler that you will be home an hour earlier, or being able to rectify the fact that you have gone out without setting your entertainment system to record the football match.

But there is far more potential to the IoT than that – not least in the area of retail. A case in point is British start-up Evrything, whose ambitious plans to change the face of UK shopping received a shot in the arm in April last year; a £4M investment from US networking giant Cisco.

In simple terms, Everything's plan is to give a unique URL to pretty much every object in existence. In practical terms, the company's vision includes concepts such as promotions tailored to the time and place an item is purchased and fridges that tell owners when food is about to go off. "With just one per cent of the physical world connected at this time, this is just the beginning of an amazing future," as Cisco's UK & Ireland Chief Executive Phil Smith put it at the time of the cash injection: "As connections become faster, smarter and more insightful, we will only see more imaginative and ambitious applications of the IoT which will, quite literally, change the world."

Higham is equally passionate about the potential that lies in the retail area alone. "The IoT is a sign of things getting a bit like the film 'Minority Report', where the star walks into the shopping mall and every store recognises him and starts telling him what goods he might want to buy" he says. "That seems a little dystopian in the film, but actually a lot of retailers are realising the IoT is a huge opportunity for them to create closer relationships with their customers. A senior supermarket chain is now trying to move towards

"We will only see more imaginative and ambitious applications of the internet of everything which will, quite literally, change the world"

Phil Smith, Chief Executive, Cisco UK & Ireland

recreating the positives of the old school retail – the old butcher's or greengrocers shop which personally knows the customers and so on. The IoT can really help fulfil this."

Meanwhile, London City Airport became last year the first major international gravel hub to implement



Pilot Scheme: London City airport is set to trial-run an interconnected IoT network.

an IoT scheme. Ideas include retailers monitoring passenger behaviour so they can customise offers and advertisements when a specific passenger arrives at the airport and luggage tracking systems which ensure the belongings of those who miss flights do not end up in the hold.

Outside UK, Xerox Research Centre Europe recently deployed 7,000 sensors around Los Angeles city centre to detect which parking meters were occupied, then adjusted prices accordingly, thereby maintain a situation whereby 20% of spaces were always available. Needless to say, there is a quirky side. Chinese tech company Baidu, at its annual conference in Beijing last year, unveiled a pair of smart chopsticks which gauge food's PH, temperature, calories, salt levels and hygiene levels (given China's growing food sanitation issues, there is more to this project than just a gimmick). In the West, the French equivalent to the smart chopstick – HASPIfork – monitors how many mouthfuls of food one eats at a sitting, as well as the intervals between them, with a view to making users' dining habits more healthy.

On a far more prosaic front, what the IoT promises is far greater, and instant, powers of analysis and therefore efficiency. "IoT enabled devices are becoming a key method for providing 'right-now' visibility into supply chains," explains Ashley Ford, vice president and General Manager of Zebra Technologies EMEA. "These devices are also prevalent in very process-driven tasks where feedback and control are essential, especially within the energy sector. Businesses can use this deep visibility to eliminate inefficiencies on industries such as manufacturing, healthcare, transportation and retail."



Right direction: sat-navs are an early example of the "Internet of Things" in action.

LOOK BEFORE YOU LEAP

Whoever coined the phrase may well have had a premonition of the exponential technological progress of the 21st century. Because wherever there is a great leap forward in information technology, it follows that there will be threats, obstacles and legal implications. The first that springs to mind in the case of the IoT is the potential for damage, disruption and fraud

perpetrated by cyber-criminals. “Will people be able,” the technophobic reader might be permitted to ask, “to access my bank account via my rice cooker?”

Banal though it sounds, it is a legitimate question. Jim Carlsson, chief executive of Swedish network security company Clavister, already has an example of the IoT being exploited for nefarious means. “In December 2013, more than 100,000 consumer devices, including an internet-connected refrigerator, smart TVs and multi-media hubs, were exploited to send more than 750,000 spam and phishing e-mails,” he stated. “The majority of the devices used in the attack were not infected by malware, but were simply left open so that attackers were able to use their IP capabilities to relay spam and infected e-mails. This incident indicates just how resourceful attackers have become in using unconventional, but effective, attack vectors.”

Proliferation of connectivity, he points out, can only create a cyber-criminal-friendly playing field. “The more smart devices are connected to the internet, the more information becomes available – creating more opportunities for people to intercept data and steal personal data, such as financial records, health information and more. They could even take control of devices for their own purposes.”



Even more concerning, it seems that our existing measures against cyber-crime will be made to look woefully archaic once the IoT really takes off. “As things stand, security relies on users changing passwords and other settings away from defaults, and ensuring the devices are not left open,” says Carlsson. “But relying on such primitive security measures is likely to become futile in the battle against cyber-crime. A new generation of security measure will be required to protect our connected lives, and manufacturers will be tasked with adopting a new generation of protection – embedded security, which actively protects devices against interception of data and data theft.”

The other issue is the legal ramifications. “Companies considering it will need to think about the draft EU Data Protection Regulations which will provide an even more robust legal framework than the existing directive,”

says Kim Walker, partner and technology specialist at Thomas Eggar, a leading law firm, with a key specialism in technology and retail. “It is under consideration, but is expected to be in place by 2017.”

Of course, while the proliferation of the IoT will add reams to the already vast repository that is Big Data, a potential pitfall that legislators are addressing is the illicit re-purposing of data. “The EU Commissioner has recommended that IoT should be designed from the start to meet detailed requirements that underpin the right to deletion, the right to be forgotten, data portability, privacy and data protection principles,” says Walker.

Early adopters, he predicts, will have been keeping a very close eye on the recent ‘Right to be Forgotten’ case, whereby Google was ordered by the EU Court of Justice to delete ‘inadequate, irrelevant or no longer relevant’ data from its results at the request of a member of the public. “Consumer-facing issues must be addressed at the outset – including privacy by design, consent, use of customer profiling and privacy policies,” says Walker, adding that stiff financial penalties are expected for those who fall foul of the EU Data Protection regulations, once enacted.

Higham, on the other hand believes that the legal difficulties are easily surmountable. “It has to be all about opt-in; you need to give legal permission to interact with your devices,” he says. “From a legislative point of view, it should not be too complex beyond that.”

All these issues considered, the word on the legislative street is, don’t be put off. The basic reality is, the IoT is exceptionally suited to the zeitgeist – the growing trend towards more personalised service; markets becoming less supply-driven and more demand driven, and increasing public (emotional) and government (financial) investment in connectivity. “It is a great opportunity for UK businesses to compete globally,” says Higham. “But in order for it to happen, government and business need to invest in digital and virtual infrastructure, rather than physical infrastructure like HS2.”

A half-hearted or fearful approach is anathema to Higham. “We have been afraid of intelligent computing since HAL and ‘2001 – A Space Odyssey’ Isaac Asimov and ‘I, Robot’ and so on,” he says. “Fears of this stuff is instilled into our psyches now. But some of it actually has the potential to free things up, rather than impose Big Brother style threats.”

Happily, he says, scepticism is waning – especially across the pond. “A survey by US software solution company Janrain recently found that 60% of Americans would be happy to lose some privacy in order to be offered more personalised marketing and offers,” he says. “It is about a trade-off. If people can see that what they are gaining is much more than what they are losing, they are going to snap it up. It has to be about understanding the opportunities and worrying less about the threat.”

THE USA ADVANCED COURSE IN ENGINEERING (ACE) CYBER INTERNSHIP 2015

By Lieutenant Lindsey Wood Royal Signals

EDITOR'S NOTE

Lieutenant Lindsey Wood is currently a Troop Commander at 21 Signal Regiment. She was commissioned into Royal Signals in 2013, and completed a six month attachment at 14 Signal Regiment (Electronic Warfare) before posting to 21 Signal Regiment as a Troop Commander. She attended the above course earlier this year and earned the accolade of top student in a class of 35 - an excellent performance.



The United States Air Force (USAF) Advanced Course in Engineering (ACE) runs annually in Rome, New York. An intense technical internship run by the Air Force Research Laboratory, it combines mission assurance education, cyber tradecraft training, leadership development, and research and development of solutions to real world problems.

The internship is aimed at Air Force Reserve Officers' Training Corps (AFROTC) cadets about to start their final year at college before they graduate into technical officer roles within the USAF. They also take a small selection of USAF junior officers from the cyber and developmental engineering branches. The course has been running since 2003 and three years ago offered a small number of places to British officers. This year saw six officers and officer cadets from across the three services and MOD attend the course.

The internship covered a wide range of topics, from building a network through to mathematics and its application to cyber. Teams also worked on a real life project; this project enhanced the skills learnt throughout the internship as students saw the practical applications of their lessons. The focus was predominantly on self-learning; the internship staff expected the students to find the information for themselves rather than just coming to them for answers.

This was particularly prominent during the networking tasks, where students were given a task to complete throughout the week but with no direction as to how to accomplish it. Throughout

the internship, interns were expected to brief on complex scientific and technological concepts to audiences that included bench-level engineers, managers and senior Air Force leadership.

A key element of the internship was leadership development. Colonel (Retd) Fred Wieners, a retired USAF officer, held weekly leadership seminars for the interns. These seminars differed from the typical military campaigns we cover at Sandhurst; instead they targeted technical events and crises, for example Apollo 13 and the Challenger space shuttle disaster.

The focus of these seminars was on how one engineer, even a low rank, could make difference and could lead not just subordinates but their commanders. This key lesson was highlighted throughout the internship, it was pressed upon us that commanders may not always understand the effect that could be provided or the risks they may be taking, as the technical expert you must be able to articulate this clearly and concisely to them and offer solutions to these problems.

The leadership lessons were a key part of the internship, as without the necessary interpersonal and leadership skills the technical lessons alone are not enough. The internship is not solely about creating technical excellence, the focus is on technically excellent leaders of consequence.

The culmination of the internship saw the interns deployed into a field environment to test the skills they had developed over the previous 10 weeks. The interns were split into two teams and for 12 hours battled to complete their set missions and disrupt those of the enemy force. These missions ranged from overwatch of a convoy through to kinetic strikes on high value targets. The focus of the exercise was on mission assurance rather than on cyber purely for cyber's sake. This highlighted a key thread impressed upon us throughout the internship; cyber should be used to generate military effects, not as a standalone asset.

The internship ended with a graduation dinner to celebrate the achievements of the interns. Each intern was presented with a certificate, coin, and cadet cyber wings for the AFROTC cadets. The top ten per cent of the course, this year three

interns, were also presented with a distinguished graduate award. This award was for those the staff felt had excelled in all areas of the course. The distinguished graduates of 2015 were

Lieutenant L Wood, Royal Signals,

Officer Cadet S Pentecost, AFROTC

Mr J Schaefer, Scholarship for Service (SFS).

The internship had huge benefits to all those who attended, every intern learnt lessons they will never forget, whether those be technical or leadership based or a combination of the two. The interns also made friendships and connections spanning America and the globe, building a network of technical experts to utilise in the future.

Following the internship the interns were expected to brief a multitude of personalities, including Major General Hockenhill and Air Vice Marshall Brecht, on their experiences. Lt Wood also attended a lunch at Army HQ where she was presented with a certificate and a coin for excellence from US Army CIO Lieutenant General Ferrell.



Lieutenant General Ferrell and Major General Semple with Lieutenant Wood

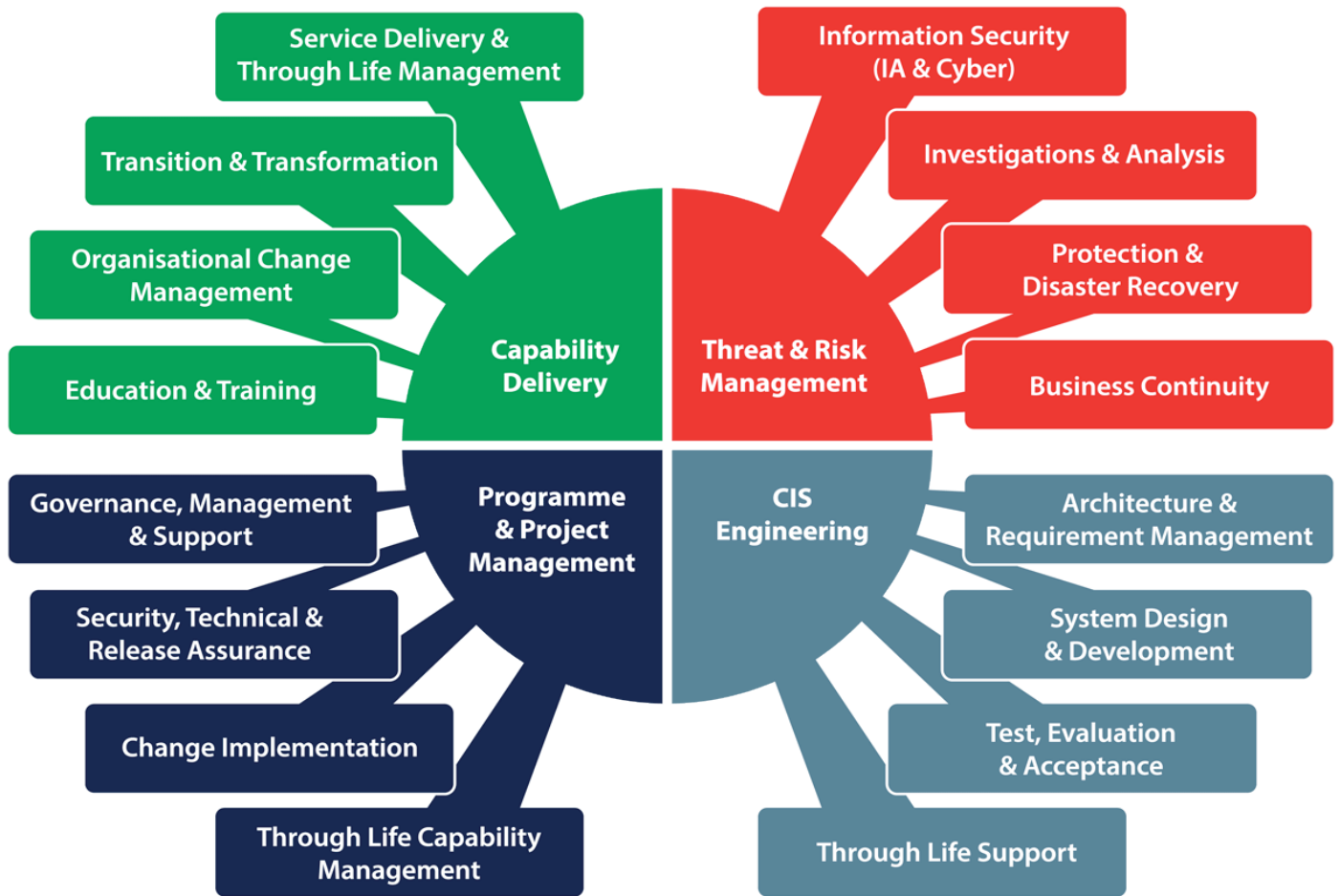
This course was advertised across the Corps. Lieutenant Wood had to complete an application and write a personal statement, supported by the chain of command. All applications were considered by a UK board and filtered before submission to the US board for final selection. Truly a splendid achievement.

Lieutenant General Ferrell presents Lieutenant Wood with her course coin.





Our customers are security sensitive decision makers who know what is important to them. Through education and experience they have learnt to work within and manage their appetite for risk. Their preferred way of working is through establishing a partnership with their security service provider. This relationship relies on trust and mutual confidence. Together we tackle challenges for which technology alone is not the answer. Solutions are tailored by team members with the knowledge, skills and experience to signpost the best route to take together.



Benefit Assured, Security Assured, Value Assured

C3IA Solutions is the partner of choice for the delivery of accredited security and technical services. Please get in touch in order to hear how we take a holistic approach to the delivery of managed security services.

We are proud to be a Member of the Royal Signals Institution and to be the sponsors of Royal Signals Rugby.

CYBER ELECTROMAGNETIC ACTIVITY (CEMA) – SUPPORTING THE NEW WORLD ORDER IN THE INFORMATION AGE

EDITOR'S NOTE

Lt Col Ian Buchanan was commissioned into the Green Howards in 1984. His technical training started with the Regimental Signals Officer (RSO) Course at Warminster in 1991 followed by the Combat Arms Fighting Systems Course (CAFS) at Shrivenham in 1994. Following a staff appointment as an SO2 in Project Management Special Projects (PMSP) in the Procurement Executive, he returned to Regimental Duty and commanded a Warrior Company serving in Germany and on operations in Bosnia. In 2000 he undertook the Design of Information Systems MSc course at RMCS, followed by an IS staff job in HQ DSF, London. He transferred to the Corps in 2003 and was posted to 2 Signal Regiment in 2004 as Second-in-Command. Promoted Lieutenant Colonel in 2005, he became the Senior J5 Plans Officer in the NATO HQ, Sarajevo. In June 2006, he was posted to the Logistics Applications IPT as the SO1 JAMES Programme Manager. He was short-toured to become the Chief Operations Officer in the UN Integrated Office in Sierra Leone, returning in July 2008 to take up post in DSTL as the SO1 Cyber and Influence. Whilst at DSTL he undertook a PG Cert in Information Operations from Cranfield University achieving Top Student. In 2010 he was short-toured again to the Defence Cyber Security Programme Office in London where he was involved in establishing the Defence Cyber Programme. In January 2013 he was posted to Army HQ as the SO1 Cyber/EWSI where he managed Army cyber capability development, EWSI, ECM FP, Spectrum Dominance and introduced the US Army concept of Cyber Electromagnetic Activities (CEMA) into the UK Army Doctrine. In November 2015 he was awarded the RSI Silver Medal.



JFC Commander's Intent

In 2014, Commander, Joint Forces Command (Comd JFC) published his thoughts on the future of Warfare in the Information Age. In the paper he articulated both the threats and opportunities that modern technology present to the UK Military. Whilst he explicitly discussed the potential of "emerging Information Technology" and cyberspace, he also clearly stated that "first consideration of commanders is how to dominate the Electromagnetic Environment (EME) as Critical Terrain". The intention of his paper was to highlight the challenges but to also throw down the gauntlet to the UK Military to come up with ideas and strategies as to how to address those challenges.

Aim of this Article

This article will aim to highlight some options that the British Army in general and the Royal Corps of Signals in particular may wish consider. It may also apply to other cap badges, such as the Intelligence Corps given its close association with us. It will examine the growth

of modern technologies considering and the threats and opportunities they present when used by state and non-state actors. Consideration will be given to the US Army who have adopted the comprehensive Cyber Electromagnetic Activity (CEMA) approach to operating in these emerging operational environments. The paper will finally consider the utility of a similar approach within the British Army and the impact at the Corps level asking if we need to become a much more agile "technology driven - people centric" organisation that can adapt quickly. The question remains whether we are bold enough to break away from our traditional mind-set and face up to the challenges presented by Warfare in the Information Age.

The Information Domain now hitting the Corps

In 2010, I wrote an article for the RSI Journal outlining developments in cyberspace and specifically the threats presented by various forms of malware along with a review of State and Non-State activities. The focus of the article was primarily upon desktop and SCADA computer systems and whilst the threats to these systems have continued

to increase, other technological developments have moved forward at breathtaking speed. According to recent academic and industry research, Moore's Law is still holding true and will do so for at least another 5 years (Brazil, 2015), noting that processing speeds have increased by at least 2 – 3 times since 2010 and will do so again by 2020. However, by then we will have reached the physical capacity for current silicon technology. In addition, there have been major developments in miniaturisation, software development (Apps), cryptography, storage, cloud computing, screen and sensor technology, Wi-Fi availability and mesh networking along with 3G/4G network connectivity. These technologies have come together into capabilities that have almost imperceptibly become central to our lives – such as the use of the smartphone and other smart / non-smart mobile devices. As Fig 1 from Cisco (2015) suggests, the demand for these devices is growing with half a billion (497 million) mobile devices and connections added in 2014, smartphones accounting for 88% of that growth. It is expected that the increase for mobile data traffic will grow at compound annual growth rate (CAGR) of 57 percent from 2.5 Exabytes per month in 2014 to 24.3 Exabytes per month by 2019 as per Fig 2.

While the Cisco report focuses on mobile and tablet devices, many other devices are being connected to what is now termed the "Internet of Things" (IoT). The drivers for the IoT include smart homes, wearables, healthcare mobile devices, TVs, cars, Business to Business (B2B), Cloud Computing and Data Analytics (Moskvitch 2015). Products include home security systems, lighting systems, smoke alarms, fridges, ovens, multimedia players, fitness trackers, street lighting and cars to name but a few. Many of these IoT devices will be linked to human users via their smartphone or other mobile devices. Although the growth and capability of these devices will continue at a dramatic pace (SRI Consulting Business Intelligence) it is also clear that they remain vulnerable to exploitation and attack. HP Security Research (2015) states that the threat to the more traditional home / office computing systems continues to grow, but so do the threats to mobile and IoT devices. They

show that Android is particularly vulnerable due to its more open architecture used for App development. However, as reported by Chin in the Wall Street Journal (2015), many researchers noted that Apple has had a vulnerability in the iOS mobile platform exploited in China. As Fig 3 from Sophos (2014) shows, once a smart device is compromised does it represent a complete liability or an opportunity? HP suggests that as the IoT brings the physical and the virtual world together, the "consequences of unethical or malicious use becomes increasingly "real".

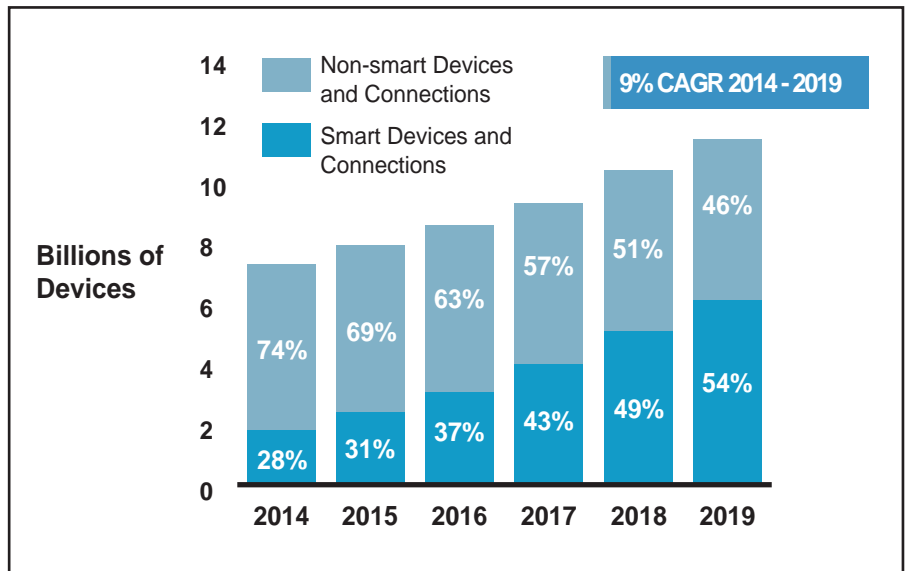


Fig 1 - Global Growth of Smart Mobile Devices and Connections

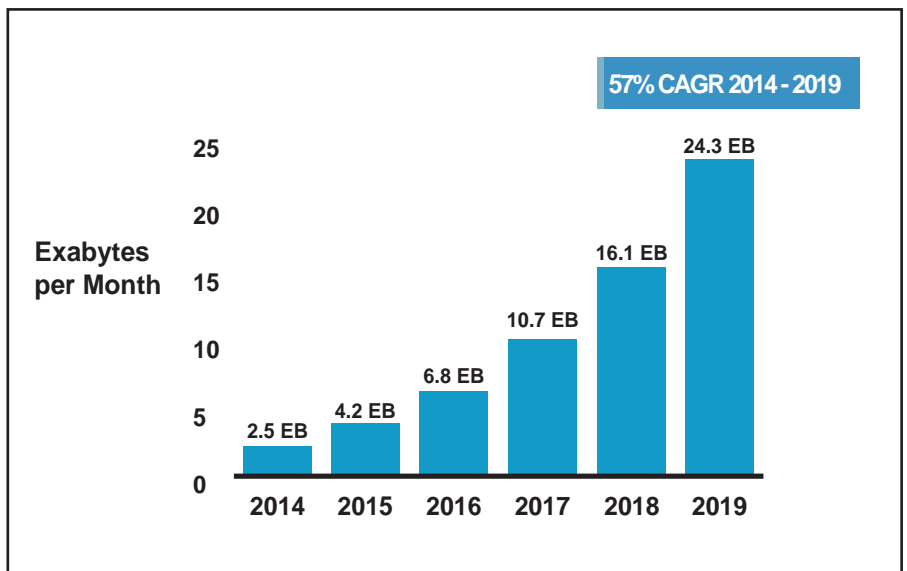


Fig 2 - Cisco Forecasts 24.3 Exabytes per Month of Mobile Data Traffic by 2019

¹ 1 Exabyte (EB) = 1000 petabytes = 1million terabytes = 1billion gigabytes.

² IoT - network of physical objects or "things" embedded with electronics, software, sensors, and network connectivity, which enables these objects to collect and exchange data.

³ [http://iotlist.co./](http://iotlist.co/)

⁴ Free Anti-malware is available for Android Phones – see <http://www.androidauthority.com/best-antivirus-android-apps-269696/>

Anatomy of a Hacked Mobile Device: How a hacker can profit from your smartphone

Your Android smartphone may look innocent. But when compromised by malware, it can illegally watch and impersonate you, participate in dangerous botnet activities, capture your personal data, and even steal your money.²⁰

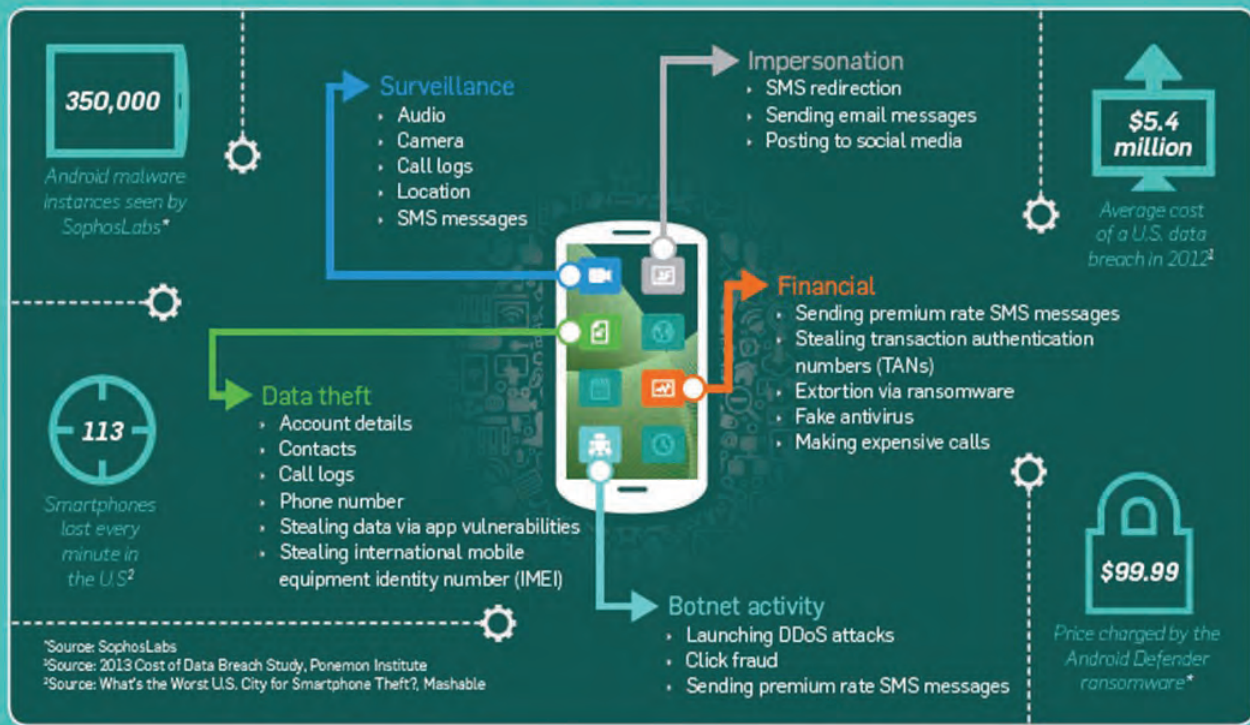


Fig 3 - Anatomy of a Hacked Mobile Device

Placing the facts and figures of technology aside, it is essential we consider is the socio-cultural-military impact this technology is having. Some examples include:

- According to Ofcom (2015), the UK is now a smartphone society. Some 33% of internet users see their smartphone as the most important device for going online, compared to 30% who are still sticking with their laptop. The rise in smartphone surfing marks a clear shift since 2014, when just 22% turned to their phone first, and 40% preferred their laptop. Although some 90% of 16-24 year olds own one (61% of whom are “hooked” on their devices), the ownership by the 55-64 year olds (many with little knowledge of vulnerabilities) has now gone from 19% in 2012 to 50%. The overall surge is being driven by the take-up of 4G mobile broadband, with subscriptions having leapt from 2.7 million to 23.6 million by the end of 2014. On average, adult mobile users spent nearly two hours online each day using a smartphone in March 2015. Ofcom also reports that more than seven in ten adult Internet users (72%) have a social media profile, and social media use is correlated to age. A majority of internet users aged 16 – 24 (93%), 25 - 34 (90%), 35 - 44 (80%) and 45 - 54 (68%) have a social media profile. The likelihood is that this shift will be reflected across the world as devices and access becomes more widespread.
- African users consume the most mobile data supporting the notion of Africa as the “mobile continent” (Alcatel-Lucent, 2015). Somalia has

frequently led in the consumption of mobile data. Hersman (2013) suggests that the mobile device “has cracked open the world to a billion new people” and impacts “every fibre of the fabric of life” becoming the driving force for innovation across Africa. Smith (2014) states “that internet use on mobile phones will increase 20-fold in the next five years – double the rate of growth in the rest of the world”.

- Lawson (2015) reports it is the smartphone that is helping to fuel the exodus of refugees from Africa and Syria. These devices allow the migrants to navigate, communicate with people smugglers, keep up to date on international developments and importantly, maintain close links with home therefore reducing the intense sense of loneliness they suffer on their journey. In his opinion the smartphone “is the untold accelerator of mass migration”.
- Although the Arab Spring took place sometime ago, Ingram (2011) suggests that it was the network, the mobile device and social media that helped maintained the momentum. However, as he points out, other observers such as Morozov (2012) states this is not true and in fact enabled the State to track down the key conspirators in the 2009 Iranian ‘Green Movement’ uprisings.
- The Libyan uprisings were described by Pollock (2013) as an Information war and it was information that “made the revolution succeed”. He quotes examples where insurgents were able

to get advice over mobile phone and skype on the weapons characteristics of a Grad 122-millimeter multiple-rocket and were then able to successfully attack and destroy the weapon system. Insurgent groups were able to set up their own independent mobile communications systems by cutting links to the Government controlled systems. External supporters set and ran the online TV channel Libya Alhurra, set up Twitter feeds and Facebook accounts to provide significant support to their war effort. Eventually these groups had the potential to supply intelligence feeds to NATO Forces on the movements of Government troops. However, it is suggested that NATO was wary of these linkages and more could have been done to take advantage of them. The implication is that there are information resources available to exploit that are several magnitudes greater than anything government systems can provide. As Pollock observes “cheap handheld technology is making citizen networks an inevitable feature of the information battle space”.

- Rafal Rohozinski of the Canadian based SecDev Foundation (<http://new.secdev-foundation.org/>) has described Syria as the “Poster Child” of future wars. He notes the massive increase in mobile subscribers during 2011 – 13 as the mobile device became an essential survival tool for the civilian population. However, both Government and opposition forces have taken to cyberspace to fight the war using social media botnets, Twitter accounts, video feeds and Skype. The Government uses censorship to crack down on the insurgent while the insurgents use tools such as TOR ⁵ to evade surveillance and censorship (2012).
- The concept of “Sousveillance” ⁶ first mooted by Mann, Nolan and Wellman (2003) is now turning into practical reality as seen in Libya but also Syria and in the US where “citizen video” has captured Police Officers killing unarmed civilians (Wright 2015). In an environment where every civilian is now a potential ‘sensor’ what are the implications for maintaining OPSEC during military operations on the ground? This potentially also adds a new dimension and added complexity to the Idea of the “Strategic Corporal” whose every action can be scrutinised by an international audience.

Snowden

Any review of modern technology and the possible threats / opportunities presented is not complete without a brief examination of the Snowden disclosures (Guardian Newspaper (2015)), Electronic Frontier

⁵ TOR – ‘The Onion Router’ is free software for enabling anonymous online communication. <https://www.torproject.org/>

⁶ Sousveillance is the recording of an activity by a participant in the activity, typically by way of small wearable or portable personal technologies.

Foundation, CJFE Snowden Archive). Whatever the truth behind these revelations a few key points are clear. Firstly, the power of state level surveillance and other capabilities enabled by technology is immense. Secondly, there is significant public concern in western countries over the legal basis of the State to conduct such surveillance which resulted in the publication of the Anderson report here in the UK in Jun 15. Thirdly, and as will be examined later and made clear in the Anderson report, there has been a significant impact on National Security. The irony for Mr Snowden is that he has ended up sheltering in one of the most internet suppressive regimes in the world.

Russian Ambiguous Warfare

In 2012, at the Atlantic Council Global Trends 2030 Symposium, Jared Cohen made the observation that we are entering a “multidimensional moment where the world is as much virtual as it is physical. Understanding a state’s power will be determined by what they do in cyberspace and what they do in the physical world”. The US Secretary of Defense, Ashton Carter certainly echoes this point when he said in 2015 “Russia and China have been pursuing long-term and comprehensive military modernisation programs to close the gap with the US and have been working on new counter space, cyber, new electronic warfare capabilities that challenge our own”. For Russia, these capabilities are aligned with their 2010 Military Doctrine in which “Information Confrontation” is regarded as key military strategy, used to impact public opinion, both nationally and internationally (Global Voices 2010). The Russians take information control seriously and may even be preparing to cut Russian cyberspace off from the rest of the internet in the event of national emergency (Harding 2014) potentially having conducted experiments to do that earlier this year (BBC Monitoring (2015)). This enables control of the strategic narrative to be maintained regardless, placing a premium on delivery of soft effect, which may have been planned in detail in advance.

Firstly in Crimea and now Ukraine, the Russians have clearly built on the experience of the Georgian confrontation in 2008 where a lot of effort was put in to disrupting networks, phone systems but minimal effort was put into social media activities and messaging. Although these Russian Information Operations

⁷ Hybrid warfare – “both covert and overt acts in an effort to destabilise a country or territory as well as attack its troops ... combines conventional attacks with electronic disruptions, cyber-attacks propaganda, information warfare and economic activities. The idea is to sow confusion and doubt as much as deliver bombs”. <http://digital.defensesystems.com/?iid=128201&startpage=page0000011#folio=10>

⁸ Reflexive control causes a stronger adversary voluntarily to choose the actions most advantageous to Russian objectives by shaping the adversary’s perceptions of the situation decisively. See more at: <http://understandingwar.org/report/putins-information-warfare-ukraine-soviet-origins-russias-hybrid-warfare#sthash.40qaqRYL.dpuf>

concepts are not new, the use of Hybrid Warfare ⁷ and Reflexive Control ⁸ in Crimea and Ukraine has been taken to new heights of sophistication. As with Georgia there have been numerous Denial-of-Service attacks and defacing of websites (both Ukrainian and NATO) as well as the physical seizure and disabling of state internet and communication infrastructure, augmented by use of malware (Channel 4 Report 2014, Fireeye 2014, Infosec Institute 2014).

However, it is the massive effort into what might be termed 'propaganda' and disinformation through the use of State TV and Social media in combination that makes this current confrontation different to previous events. The Russians put significant effort into engineering dissent and revolt among the Russian speaking minorities of Crimea and Eastern Ukraine whilst also promoting the concept of "Novorossiia" (New Russia). Social media was also used to spread fear and uncertainty in the Ukrainian population, government, military and security services by showing the power of the Russian military influence (Seaboyer, Jolicoeur, 2014). It is arguably now a well-entrenched tool of their foreign policy. As noted by Peter Pomerantsev (2015), previously it would have taken time to plan and undertake such operations but this new dezinformatsiya "is cheap, crass and quick: created in a few seconds and thrown online" with an aim "less to establish alternative truths than to spread confusion about the status of truth". How do intelligence staffs in particular then determine the truth from the half-truths and lies? The impact on ability to analyse information and create a Common Intelligence Picture that is as accurate as far as is practicably possible is immense. Disinformation can therefore potentially be seen as a new operating norm that increases the 'fog of war' and adds further to the levels of friction we can expect from both state and non-state actors. Responding to this is also not straightforward. The Ukrainians have tried to fight back online with efforts such as the StopFake⁹ website which continuously highlights Russian misinformation but this is a minor effort compared with that undertaken by the Russians. Within Russia the Authorities have also taken active steps to surpass on-line dissent with legal measures being introduced to block any "websites hosting "extremist" content or calls to protest" (Kelly, Earp, Reed, Shahbaz, and Truong (2014)). According to some observers (but not all) the impact of all this hybrid warfare and propaganda effort at the Intentional level has been to prevent the Western powers from reaching a clear unified position to deal with Russian aggression.

Potentially as important, is the fact that Russian information efforts domestically continue to portray Putin as heroic, providing him with widespread approval ratings (89%) and strong Nationalist support across the country for his actions in Ukraine (Simes (2015)). This reflects not only the effect that state-

⁹ <http://www.stopfake.org/en/news>

¹⁰ *Is Putin developing a Personality Cult particularly amongst the young? Worth catching the following at <http://www.bbc.co.uk/iplayer/episode/b05r844j/reggie-yates-extreme-russia-1-far-right-proud>*

controlled disinformation can generate, but also how such effects can – across a population as a whole – be forecast in advance. Remember, the population's use of social media will emphasise trends in thinking and perspectives held, potentially underpinned by Janus' concept of 'group think', that express and identify or sentiment which the state can then use to its advantage. In this respect, new-style Information operations are a not-so-subtle brand of psychological warfare that nonetheless presents a return on investment – sometimes almost intangible in nature – that is out of all proportion to the effort put into enabling them.

It is not only in conducting operations in and through cyberspaces where the Russians are showing considerable skill and capability. They have clearly not forgotten although arguably we may have, that on the battlefield you need to dominate the EME and are using EW capabilities to good effect in Ukraine. The Organisation for Cooperation and Security in Europe (OSCE 2014) reported that their observation drones have been subject to "military grade GPS jamming" that was not emanating from the Ukrainians. It is also on the ground that Russian EW is proving effective by not only targeting with accurate artillery fire anyone using a radio but also suppressing communication capabilities almost at will, reducing the Ukrainians to passing battlefield reports by hand (Gibbons-Neff, (2015)). Russian EW capabilities have been specifically noted by Lt Gen Ben Hodges (Commanding General, US Forces Europe) where he describes the quality and sophistication of Russian electronic warfare as "eye watering" and suggests that the US is learning a lot from the experience of the Ukrainian military (Gould 2015). Interestingly in the same article Laurie Buckhout, former chief of the US Army's Electronic Warfare Division states that the US Army could not currently "shut them down one-tenth to the degree they can us". She further notes "we are very unprotected from their attacks on our network." The EW capabilities of the Russians and their domination of the EME in Ukraine has been a 'wake-up' call for the US Army. It could be suggested that this is equally relevant to the British Army, but we may well have all but forgotten the hard learned lessons of the Cold War.

China and Others

Other state actors are also allegedly developing or improving their cyber based activities. The Chinese Government continues deny undertaking any nefarious cyber activities though credible and well documented evidence would seem to suggest otherwise. The Mandiant Report (2013) is a good example that shows the scale and sophistication of one organisation they call APT1. They state that it is in fact the 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department, which is most commonly known by its Military Unit Cover Designator (MUCD) as Unit 61398. Mandiant suggests that APT1 consists of at least dozens, and potentially hundreds of human operators, maintains an extensive infrastructure of computer systems around the world and has systematically stolen hundreds of terabytes

WANTED BY THE FBI



Fig 4 - From left, Chinese military officers Gu Chunhui, Huang Zhenyu, Sun Kailiang, Wang Dong, and Wen Xinyu have been indicted on cyber espionage charges.

of data from at least 141 organizations. In 2014 the US Justice Department actually charged 5 members of Unit 61389 (see Fig 4) with a series of Hacking offences but the chances of them standing trial are remote.

Two other emerging state actors are also worth noting. Firstly, North Korea which was clearly implicated in the well-publicised Sony Hack of Nov 2014. It is alleged that a North Korean Military organisation known as Unit 121, was behind this hack (Markowitz 2014) with members of this unit being trained in China. Such was the scale and impact of the Sony Hack that the US Government took the unusual steps of naming North Korea as the culprit and then in Jan 15 President Obama signed an executive order allowing sanctions on three North Korean organisations and 10 individuals (BBC 2015). North Korea has allegedly undertaken numerous attack on South Korean National Infrastructure including an attack in Dec 14 on a South Korean Nuclear facility (Sky News 2015). It would appear however that North Korea does not go it alone when undertaking cyber active: in 2012 it signed a Technology Cooperation Agreement with Iran that included IT and security (Cylance 2014).

This brings up the other State Actor worth noting – Iran. In 2009 – 2010, the Iranian Nuclear programme was attacked by the highly sophisticated STUXNET malware. Subsequently other facilities were attacked by the DUQU (2009 – 2011) and the FLAME (2012) malware. Although the impacts of the attacks are debated, one thing would seem to be clear which is that following these attacks, Iran went into what could only be described as “post attack mode”. It recognised it had been hurt but with a generally young and highly educated work force it decided to hit back. It has consequently developed its cyber capabilities to the extent that according to the Cylance report “Iran should now be considered as a first tier cyber power”. This demonstrates that the ability to act effectively in cyberspace is not necessarily tied to a countries size or material resource. It is access to technologies, specialist skills and a workforce able to adapt to the demands

of this operating domain at speed whilst being hide-bound by outmoded thinking.

It is assessed that one of the primary demonstrations of Iranian capability was in 2012 when Aramco, the Saudi state owned oil firm was attacked resulting in over 30,000 computers being wiped and all data being replaced with a picture of a burning US Flag. Fortunately, the internal communication networks were not connected to the oil engineering control systems, so a greater catastrophe was avoided. Within the Cylance report, the Israeli Prime Minister is quoted as saying that Iran is behind ‘non-stop’ attacks on {Israel’s} vital national systems including “water, power and banking”. The “so what” of all this is that with the right motivation, training, people resources, some internet access and a lot of determination, even those countries not considered first world powers can become effective players in cyberspace.

It is however, not only state actors who use modern technology to further their objectives and leading the non-state actors appears to be ISIS / Daesh. Although experts agree that it is unlikely that Daesh will develop an “offensive” cyber capability, they have developed a highly effective and sophisticated social media presence to deliver its narrative to supporters, encourage recruitment, justify activities and challenge criticism to spread terror and fear to adversaries. This is where we again must remain cognisant of separating out the technical, coding-based aspect of Cyber operations – which fixate some minds - vice that of web-based operations which have a particular influence and strategic narrative bent. That means being able to assess where and why an effect must be generated. Cyber-based activity doesn’t just materialise – it happens for a reason, specifically based on the judgments and desires formed in a human mind. There are a number of UK military staffs who need to bear this principle in mind.

In 2014 Daesh developed the “The Dawn of Glad Tidings” for the Google Play store that when

downloaded enabled Twitter feeds to be automatically retweeted to/from supporters. When the insurgents overcame the northern Iraqi city of Mosul, the Dawn of Glad Tidings app posted almost 40,000 tweets in a single day (Cuthbertson 2014). This adversary regards this sort of capability as key not only to its survival but as the Jhadist wife Sally Jones states “I’m gonna prove to you how social media will be your downfall” (Bhutia 2015).

However, by using Social Media and modern technology such adversaries risk exposing themselves to Intelligence gathering from Western agencies and military organisations. Unfortunately, as suggested earlier, the Snowden revelations appear to have had a significant impact on the TTPs of these adversaries who now go to great lengths to protect themselves through the use of encryption and other secure means (Stalinsky and Sosnow 2015). These authors quote senior commentators including US Rep Mike Rogers, who chaired the House Permanent Select Committee on Intelligence, Mike Morell, former deputy CIA director and John Sawers, former head of Britain’s Secret Service MI6. All state that the impact of the revelations has been detrimental to their ability to collect intelligence. Most recently Andrew Parker, the Head of MI5 stated “an increasing proportion of such communications are now beyond our reach – in particular with the growing prevalence of sophisticated encryption” (2015). So what does this tell us about this modern-day non-state adversary? It can be summarised thus:

- They are a learning organisation that quickly adapts to survive or mitigate the impact of targeting.
- They are networked and openly communicate with unfamiliar allies to share TTPs and knowledge.
- They seek to evolve and employ state of the art technology (banking grade encryption) to hide it’s C4I from the West.
- In order to collect on the adversary C4I we may (indeed will??) need to push high quality collection capabilities to lower tactical levels within the military environment.

The Electromagnetic Environment and Contemporary Operations

While most of this article has focussed on cyberspace and some EW capabilities, it must not be forgotten that most of the modern civilian and military technologies discussed are utterly dependent upon a single shared, but generally ignored resource – the Electromagnetic Environment (EME). If cyberspace is the new ‘blue eyed golden haired child’ on the block that everyone loves (but rarely understands), then the EME is the unloved ‘ugly kid’ with whom no one wants to engage. However, a quote often used to summarise the importance of the EME is from Sergei Gorshkov, former Admiral of the Fleet of the Soviet Union, who once allegedly remarked

that “the next war will be won by the side that best exploits the electromagnetic spectrum” and it would appear from the discussion so far that Russians have not forgotten that point. More recently Admiral Jonathan Greenert, the Chief of US Naval Operations stated that “future wars will not be won simply by effective use of the EMS and cyberspace, they will be conducted and won within the EMS {and cyberspace} domain” (Vitaliev, 2015).

As long ago as 2000 the US authors Lucchese, Golliday and Joglekar (2000) recognised that the increasing dependency on the EME by military capabilities was rendering them vulnerable to ‘blue on blue’ fratricide. Incidents such as the engine of a jamming aircraft shutting down when it began to transmit jamming signals, UAV’s not configured correctly and losing ground control links due to interference, jamming aircraft interfering with artillery radar and Global Hawk UAVs being lost also due to interference are but a few examples. Since 2000, the EME has become only more ‘congested’ and ‘contested’ with the demands from our military systems ever increasing, alongside the increased risks to such capabilities and military operations as a whole. This is compounded by the vast demands being placed upon the EME by the civil sector and the potential damage that a ‘near peer’ or ‘near peer+’ adversaries could cause using some form of Electronic Attack (EA), as seen in the Ukraine.

In Afghanistan, the British Army was in a relatively uncontested information space and benign connectivity environment but we still had significant ‘blue on blue’ issues such as FP ECM capabilities interfering with communications, which may well have contributed to the death of Major Alexis Roberts in 2007 (Tibbetts 2008). This raises an interesting point – a relatively unsophisticated adversary was almost able to ‘fix’ the British Army through the use of cheap improvised Radio Controlled IED’s against which we had to spend £100m’s on FP ECM to counter just this single threat. It makes you wonder what they could have done with a little more knowledge and competence! This therefore brings us to one rather unsurprising conclusion, as suggested by Comd JFC, the EME must be regarded as ‘vital terrain’ by Military Commanders, their G3/5 staffs as well as the G6 staffs and therefore active Spectrum Management is required to enable SA in the EME. G2 staffs must also be acutely aware of the effects that an adversary may seek to generate against our own forces, so that they can advise when enemy efforts may be concentrated and allow us to pre-empt, defend against or deny such activity. However, I would also argue the British Army has forgotten about the importance of the EME, the lessons learned during the Cold War and the fact that this resource must be actively managed. This issue was most recently highlighted by RUSI (2015) when they said “mutual interference will therefore exist and dynamic spectrum management for ISR, indeed for all military uses, is almost certainly going to be required” (Roberts, Payne 2015).

The US Army Approach

If the complexity of Cyberspace and the EME is increasing, how has the US Army for example faced up to the challenges? In 2013 the US Army TRADOC published The Enabling Operations in Cyberspace Through Institutional and Operational Unity of Effort White Paper and The US Army Landcyber White Paper 2018 – 2030. The former developed the logic for establishing unity of effort in developing and employing cyberspace capabilities to enable mission command explaining how Army commanders must integrate cyberspace operations in all warfighting functions. The latter describes Army cyberspace operations in the 2018-2030 timeframe being consistent with evolving joint cyber doctrine and directives. In effect they set out a clear plan for the US Army to fight in Cyberspace and the EME through the use of Cyber Electromagnetic Activities (CEMA). In Feb 2014 The Army published the Field Manual (FM) 3-38 which for the first time brought together the disparate operational activities of Cyberspace, Electronic Warfare and Spectrum Management into a single concept – see Fig 5. The US Army has defined CEMA as:

“Cyber electromagnetic activities are activities leveraged to seize, retain, and exploit an advantage over adversaries and enemies in both cyberspace and the electromagnetic spectrum, while simultaneously denying and degrading adversary and enemy use of the same and protecting the mission command system (ADRP 3-0). CEMA consist of Cyberspace Operations (CO), Electronic Warfare (EW), and Spectrum Management Operations (SMO)”

The interesting point about the way in which FM 3-38 is written is that the first part is aimed squarely at Commanders and their military planning Staffs to ensure that CEMA is understood, integrated and synchronised into military operations in the same manner as any other activities within the Land, Air or Maritime environments. There is, in layman’s term, nothing ‘special’ about the capability per se which causes it to be regarded as a ‘geeky’ afterthought – it enables one line of activity amongst many others, albeit using technically specialised means. To enable this, the FM describes in detail the staff functions and the various process through which the synchronisation of CEMA effects can be achieved at both the Operational and Tactical levels. It is made absolutely clear that if done correctly “CEMA provides commanders with the ability to gain and maintain an advantage in cyberspace and the EMS”. It may not have a turret, a big gun and go ‘bang’ but it is seen as having an equal potential to be battle-winning as anything else available in the Commander’s armoury.

The scale to which CEMA has been integrated into the US Army can be seen from the following illustrations. Firstly, there is an extract from a presentation given by Maj Murray (2014) at the AFCEA TechNet Symposium. At Fig 6, it is clearly articulated that CEMA is a thread running from the Battalion all the way through to Army level. In a subsequent slide he states that Commanders must understand “how the cyber domain and EMS influences and impacts their operational environment”, and that Staffs must “Integrate Cyber and EW in manoeuvre” and know “how to call for support, reach-back capabilities”. One might be tempted to suggest that this is the over enthusiasm of a junior field officer. However, the Keynote Speaker was LTG Cardon and knowing the American military staff system, I would respond by saying that nothing would be stated by any junior staff if it were not endorsed by the Senior Commanders – which this most definitely is! Other slides packs work noting cover EW and EMS operations under the CEMA banner and can be found here <http://www.afcea.org/events/augusta/14/tracks.asp#Cybwed815>.

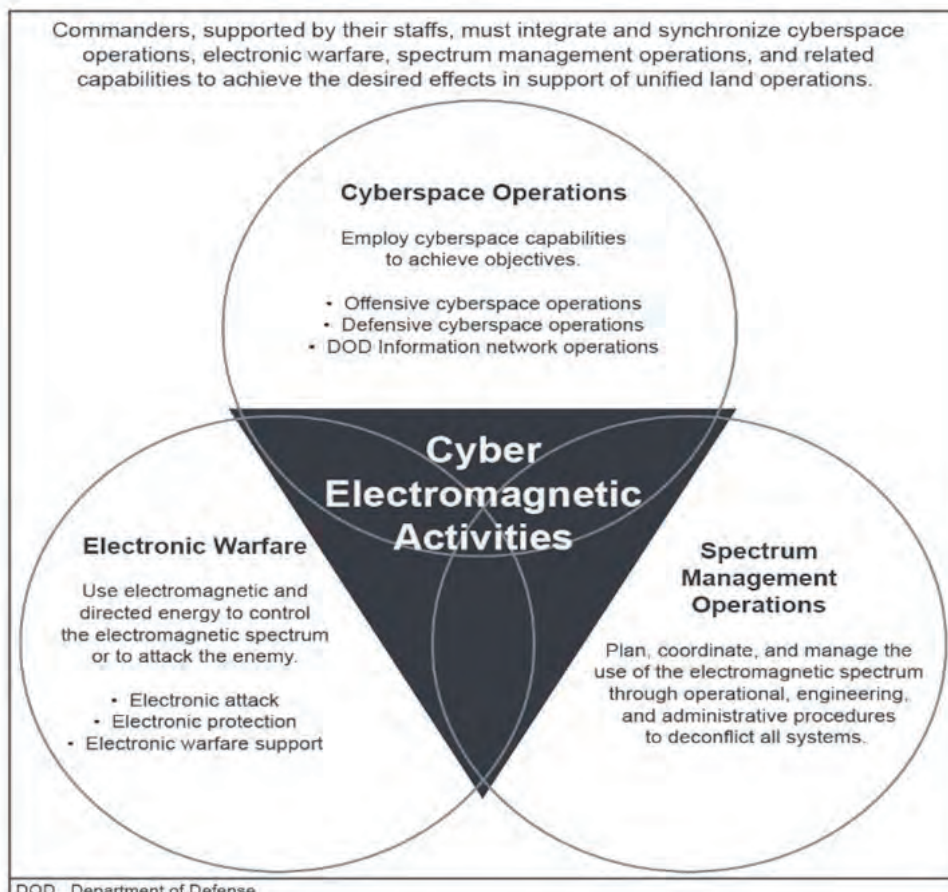


Fig 5 – FM3-38 Cyber Electromagnetic Activities



UNCLASS

FORT GORDON • GEORGIA

Army Cyber Required Capabilities

Required Capabilities: 2018-2030

- Each echelon requires the ability to access capabilities resident at other echelons
- Task + Condition + Standard (metrics)

Conduct: to direct or take part in the operation or management of (administer, control, direct, lead, operate, order, organize).

Perform: to carry out an action or pattern of behavior complete, move, observe, operate, react

Deliver: to send to an intended target or destination

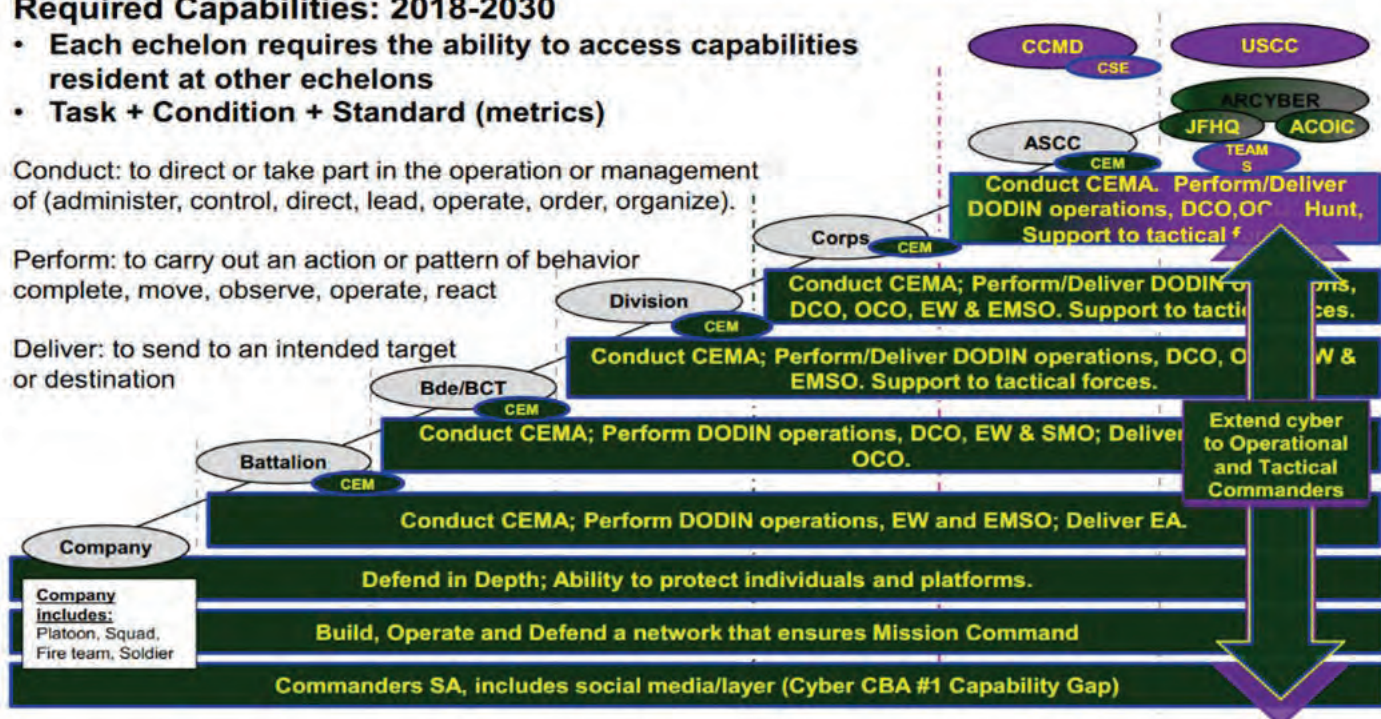


Fig 6 – The Thread of CEMA across the US Army

The second illustration is that during the COS 3 (UK) Div visit to 3 US Corps in late 2014 he was given a two-hour brief on CEMA and how it is integrated throughout the Corps, reinforcing further how the US Army takes this seriously.

The US Army has supported the development of CEMA with the creation of the Army Cyber Centre of Excellence in Ft Gordon, Georgia, bringing together 1-Star Commandants for Cyber and Signals under a 2-Star, who in turn reports to current COE Commander, LTG Cardon (Ackerman 2015). He is also dual hatted as Commander Army Cyber Command (ARCYBER) (2nd Army) whose mission is “to plan, coordinate, integrate, synchronize, direct, and conduct network operations and defense of all Army networks. When directed, Second Army will conduct cyberspace operations in support of full spectrum operations to ensure U.S. and allied freedom of action in cyberspace, and to deny the same to adversaries”. The intent is to move ARCYBER from its current location in Ft Belvoir in Washington to Ft Gordon to create a powerhouse of CEMA excellence that will drive the US Army forward as it faces the technological challenges of the 21st Century.

The US Army is also seeking to thoroughly overhaul its CEMA capabilities. It openly acknowledges that the EW cupboard is empty (Freedberg, 2015, Jul) but is investing in developing the Electronic Warfare Planning & Management Tool (EWPMT – to include EME management) and then seeking to grow its EW program. However, they acknowledge they are seriously behind other state actors. The Army has further recognised the convergence between Cyber / EW and is seeking to develop cyber capabilities

within its EW program (Freedberg, 2014). This sort of capability will build on the UASF C-130 Compass Call demonstration where they conducted a wireless attack from the plane that can “touch a network that in most cases might be closed’ to traditional means” (Freedberg, 2015, Sep).

However, the US have long realised that CEMA is “technology driven, people centric” and without the appropriately recruited, trained, managed and therefore retained personnel, it simply is not ‘going to happen. Ashton Carter (2015) spells this out when he says “our cyber strategy starts with our people – its first strategic goal is building and training our Cyber Mission Forces” (CMF). To support this development, the US Army approved the creation of the Cyber Branch in Sep 14. This was the first official step in establishing a Military Occupational Specialist 17-series (MOS - 17) career field specifically dedicated to managing the careers and professional development of officers, and subsequently in 2015 for enlisted personnel and Warrant Officers (Fort Gordon Public Affairs Office 2014)¹¹. They have actively sought to encourage transfers of personnel from other trades to the MOS-17 subject to qualifications and approval as well as offering significant financial inducements (Tice 2015).

For those in the UK EWSI community reading this and think it is all cyber then fear not – the US plan is to further develop the EW Soldiers in the 29-series Military Occupational Specialty from 2016 as well as

¹¹ This is the US Army's first new career branch since Special Forces nearly 30 years ago!

25E (Electromagnetic Spectrum Managers). However, the Cyber Mission Forces (CMF) are starting from nothing and the intent is to quickly develop an initial 41 CMF Teams (approx. 45 personnel each fully operationally by FY17) with other personnel in Cyber Protect Teams (CPT), the latter forming a Brigade working out of Ft Gordon. There is also significant effort going into training at Ft Gordon with the Cyber School developing technical courses for Officers (4-year time bar post qualification) and other technical qualifications for Enlisted operators (e.g. SANS). The same can also be said for EW with \$5.6m invested in a state of the art EW training facility at Fort Sill, the US Army EW School (Oatman, 2014). Nonetheless, with regard to the creation of MOS-17, as LTG Cardon states, the intent is for this field to “encompass accessions, career management, and retention” (Vergun, 2015). A significant focus must be on the latter as these will be expensive assets to lose.

Are the Brits stepping up to the Mark?

Here in the UK in 2010, General Sir David Richards, as CGS made the statement that future wars “will require fewer tanks and ships but more high-tech troops” (Sunday Times, 2010). However, since then it would appear that the British Army has reverted to its comfort zone to focus on large green boxes on tracks (speaking as a former Infantry Warrior Company Commander) without giving enough serious consideration to key technical enablers (tactical level Intelligence analysis included). It is true that 77 Bde was created by bringing together a number of disparate units but they deliver Influence Activity and Outreach (IA&O) in which they focus on cultural understanding, the strategic narrative and delivery of messaging. It may so happen that one of the mediums through which they deliver that messaging is cyberspace but this is an operation **through** cyberspace not an operation **in** cyberspace. They do not have technical cyberspace operators and have to rely upon others for accesses to take advantage of the technology discussed earlier. We also created 1ISR Bde which does include our own 14 Signal Regiment (EW) but arguably our current capabilities are in as poor a state as those of the US. The key focus within 1ISR Bde may well be Watchkeeper which is regarded as a strategic programme but it only provides a relatively narrow ISR coverage (admittedly in high resolution). However, as events in Ukraine suggest there is a fair chance that a near peer adversary may well quickly and successfully target it with EA or some form of cyber-attack.

In my last article I quoted a commented how “the man on the scene with a gun will continue to be the ultimate arbiter in war”. However, when entering Warfare in the Information Age, if that man is electronically deaf and blind and has an adversary capable of also making him electronically dumb, then I would suggest that the man with the gun has limited usefulness. I would also go further by saying this is all part of a “system of systems” (EW → ES → Intelligence feeds → access for cyber to counter state and non-state actors as discussed above). In this case it must be underpinned by appropriate intelligence analysis capabilities at the tactical level but at present these

are sadly deficient as the user community has thought in stovepipes and not on an enterprise level. I would therefore argue that the ‘man’ does not have functioning brain either, which renders him utterly useless.

When we design networks we have to start thinking not just of the ‘tin and string’ requirements, but what information flows across the networks, why, for whom? Information Handling Models enable the utility of information to be readily linked with our decision-making, going way beyond the mechanistic IER development we are accustomed to. However, this is an issue that is only now starting to resonate with Army staffs following some painful ISR wargames and exercise with allied forces. Moreover, the Intelligence Database Management skills once owned and developed by the Intelligence Corps have been allowed to wane and they have far fewer technically-trained staffs in their ranks now than ever before. Is that something we too should be concerned about given how closely we work with that cap badge? Efforts are being made to grow such skills once more through introduction of the Operator Technical Intelligence field, though matching this with a career management stream to retain and develop extant SME does not appear to have happened.

Given that one of our key drivers is interoperability with the US and I would suggest that if we cannot operate in the EME and Cyberspace or contribute to or access the same level of EWSI and other intelligence feeds, then they may well regard us as a somewhat over equipped Guard Force, special relationship or not.

Nonetheless, we have started to make some progress for. During the recent 3 (UK) Div Exercise Iron Resolve, a version of the CEMA construct was tested alongside the Land Cyber Operating Concept. At the end of the exercise the GOC made two observations which were CEMA seemed to be the correct way to proceed and we must dominate the EME (which is why the future EWSI / LANDSEEKER programme is so critical).

So what next for the British Army? Firstly, the Executive Committee of the Army Board (ECAB) needs to decide to what extent it wishes to develop its capabilities for Warfare in the Information Age but I would argue that a version of the CEMA construct should be right at the very centre. Once decided or in parallel, I would then suggest that the Army HQ AGILE WARRIOR (2015) report spells it out quite neatly when it says:

- The Army must seek to develop its own version of the CEMA concept, nested within a Joint Framework, with a clear understanding of the distinction between Strategic Operational and Tactical level capabilities.
- Staffs need to be educated, trained and organised to plan and synchronise complex CEMA within military operations.
- Appropriate capabilities need to be developed to provide Commanders with the necessary tools and specialists to be able exploit CEMA appropriately.

Does the Corps have a duty to Lead the Army on CEMA?

Having already noted impacts on cap badges with whom we regularly work, the latter point brings me nicely on to the 'so what' for the Royal Corps of Signals. Clearly the EME and Cyberspace should be regarded as a significant opportunity for the Corps to seize. As seen in the US, the underpinning technical personnel are key to the delivery of the CEMA construct. However, here is my controversial point to engender debate and discussion, my concern is that the Corps does not focus enough on managing its highly technical personnel. The Corps tends to be a 'Regimentally driven, people centric' organisation whereas in the 21st Century it needs to be much more a "technology driven, people centric" organisation in which personnel are managed by their KSE and competencies, rather than merely being sent to fill slots in a Regiment. Admittedly, I may be a little extreme here but all too often there are stories of highly qualified IT/IS/Cyber personnel being posted to job for which their skills are an irrelevance but a slot in a Regiment had to be filled. The net effect is for such individuals to leave for jobs in industry where their skills are better utilised. It is likely the same story in other cap badges if anecdotal evidence is to be believed on the Army rumour mill.

Should ECAB make a decision to develop CEMA capabilities then I would argue that a fundamental review of our whole technical Cyber-Electromagnetic personnel career structure and management is required (eg Cyber, IA, EWSI, Spectrum Managers, IS operators). The Intelligence Corps needs to be bought into this in order to appropriately integrate its IX and analytical capability development staffs, for the problems we face and the capabilities used to resolve them are all inextricably interlinked. As ISTAR DPD staffs in Army HQ state, such is the scale of IX challenge and the information/ intelligence feeds to be assimilated that there is a need for librarians and data scientists to join our ranks if we are to gain any semblance of information superiority in using the resources at our disposal to best effect. Which cap badge will employ such specialists (which can no longer remain a dirty word in the Army's lexicon). It is almost a moot point, for cap badge divisions and suspicions will, if they remain, lead to our collective detriment, so we must work together. Stand fast, therefore, our conducting Warfare in the Information Age as defined by JFC. From a Single Service perspective, we will not be able to support CGS' concept of Information Manoeuvre.

Clearly we are not in the same scale or league as the US Army, so we will need a cleverer and agile approach to how we manage our people potentially including Officers who can become technically streamed specialists without suffering career fouls for promotion (one for the New Employment Model perhaps?). The objective would be to ensure that we develop our personnel across the CEMA construct at the Army level (start small and grow - Cyber Mission Forces at 14 (EW) Signal Regiment, Cyber Protect Teams elsewhere, Spectrum Managers as well??) to then feed in to the Joint Force Cyber Group (JFCyG) and the newly formed 1* Joint CEMA Group (JCG) and they then have appropriate roles to come back to in the Army (Spectrum

Managers included!!). We must learn the lessons from the EWSI / Single SIGINT Battlespace world and incorporate them where appropriate as "Best Practise".

Am I being entirely unfair and out of order? Possibly not, as Roberts and Payne from RUSI suggest "The post 2035 training for ISR operators will need to be far more attuned to the personnel it is training and the technology they will be using than has been the case." I would argue – why wait for 2035 but are we brave enough? We already place people on a number of post-graduate training courses at leading UK universities, yet this is often only for the individual's edification. How often do we readily utilise their skills when they return to a military role after full-time study or complete their part-time endeavours? It is often representing wasted opportunities. For example, the Army is sponsoring a number of IX-related PhDs for serving officers, yet some of them have not had their research shaped by the very service in which they serve. Does it actually care what their research reveals? If not, is this a mindset we can afford in an information-intensive operating environment that is challenging our very doctrinal foundations?

Given how technology across the cyberspace and the EME is developing at pace, our adversaries and near peer rivals have recognised this fact and are using resultant capabilities now to great effect. The US Army has come up with the CEMA construct which could be argued is a technological and operational sweet-spot. It is now investing significantly in its CEMA doctrine, concepts and capabilities but most especially in its people resources. Is this something we can get from Reservists? Possibly, but recruitment is very slow in spite of rhetoric to the contrary and we must remember that people sometimes join the Reserves to do something different to their day jobs, so we cannot necessarily expect them to do the same in uniform.

The Future

The British Army has for too long not looked favourably upon its key technical and Information related enablers - go back to post-operation reports from the early 1980s to witness the prevailing mind set - we have had, but if we are to face up to the challenges of Warfare in the Information Age as discussed by Comd JFC, then this will need to change significantly. The British Army wishes to work alongside the US but if we are not matching their capabilities in both Cyberspace and the EME as well as the supporting / supported Intelligence capabilities, then they will regard us as a second tier military capability, and it would be very unlikely to consider a UK Brigade working under a US Division, for example. Should the Army begin to embrace these concepts and capabilities, then the Corps will need to step up to the mark and manage its technical people resource in an effective manner that encourages retention at all levels. Furthermore, it is also not something we can rush – it has to be planned properly for the long-term, else abusing further the goodwill of the few experts we do have will cause them to vote with their feet. The challenges are significant but failure to address them will in all likelihood lead to failure in future operations.

References:

- Ackerman, R. K. (2015), Army Modernizes With an Eye Toward Defense wide Efforts, - Signal Magazine, 1 Aug, <http://www.afcea.org/content/?q=Article-army-modernizes-eye-toward-defensewide-efforts>
- Alcatel-Lucent (2015), Mobile Device Report, June, p18, <http://www2.alcatel-lucent.com/landing/mobile-devices-report/>
- Anderson, D. (2015) A Question of Trust, Report of the Investigatory Powers Review, Independent Reviewer of Terrorism Legislation, UK Government https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/434399/IPR-Report-Web-Accessible1.pdf
- Army HQ, (2015), AGILE WARRIOR Report 2014/2015, Jun p 46
- Barrons, R. L. (2014) Warfare in the Information Age, JFC
- BBC News, (2015), Sony cyber-attack: North Korea faces new US sanctions, 3 Jan <http://www.bbc.co.uk/news/world-us-canada-30661973>
- BBC Monitoring (2015), Russia denies internet switch-off experiment, 15 Oct, <http://www.bbc.co.uk/monitoring/russia-denies-internet-switchoff-experiment>
- Brazil, R. (2015), Putting a Spin on it: Spintronics and Superfast Computing, E&T Magazine, 10 Nov, The Institute of Engineering and Technology, p74
- Buchanan, I. A. (2010) Cyber Space and Cyber War: Science Fiction Or Science Fact? The Journal of the Royal Signals Institution, Vol XXIX, Spring, Vol 1, p15. <http://www.royalsignals.org/files/RSI/Journal/PDF/JournalSpring10.pdf>
- Bhutia, J. (2015), Sally Jones: Widow of jihadist Junaid Hussain warns of attacks on US military targets, International Business Times 25 Oct.
- <http://www.ibtimes.co.uk/sally-jones-widow-jihadist-junaid-hussain-warns-attacks-us-military-targets-1525640>
- Canadian Journalists for Free Expression (CJFE), The Snowden Surveillance Archive, <https://snowdenarchive.cjfe.org/greenstone/cgi-bin/library.cgi>
- Carter, A. (2015), Rewiring the Pentagon: Charting a New Path on Innovation and Cybersecurity, Stanford University, April 23, <http://www.defense.gov/News/Speeches/Speech-View/Article/606666>
- Channel 4, (2014), Russian cyber attacks on Ukraine: the Georgia template, 3 May <http://www.channel4.com/news/ukraine-cyber-warfare-russia-attacks-georgia>
- Chin, J. (2015), Apple Targeted as Malware Infects China Mobile Apps, Wall Street Journal, Sept. 20, 2015 8:18 p.m. ET <http://www.wsj.com/articles/apple-targeted-as-hackers-infect-popular-chinese-mobile-apps-with-malware-1442750168>
- Cisco, (2015), Visual Networking Index: Global Mobile Data Traffic Forecast Update 2014–2019 White Paper, http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.pdf
- Cohen, J. (2012), Global Trends 2030: The Individual vs. The State: Who Will Have the Upper Hand in 2030?, Atlantic Council <http://www.atlanticcouncil.org/events/past-events/global-trends-2030-the-individual-vs-the-state-who-will-have-the-upper-hand-in-2030-transcript>
- Cuthbertson, A (2014), Iraq Crisis: Isis Launch Twitter App to Recruit, Radicalise and Raise Funds, 18 Jun <http://www.ibtimes.co.uk/iraq-crisis-isis-launch-twitter-app-recruit-radicalise-raise-funds-1453154>
- Cylance 2014, Operation Cleaver Report, http://www.cylance.com/assets/Cleaver/Cylance_Operation_Cleaver_Report.pdf
- Electronic Frontier Foundation, NSA Primary Sources, <https://www.eff.org/nsa-spying/nsadocs>
- FireEye (2014), Intelligence Analysts Dissect the Headlines: Russia, Hackers, cyberwar! Not So Fast, 12 Mar <https://www.fireeye.com/blog/executive-perspective/2014/03/intel-analysts-dissect-the-headlines-russia-hackers-cyberwar-not-so-fast.html>
- Fort Gordon Public Affairs Office (2014), Army Cyber branch offers Soldiers new challenges, opportunities, 24 Nov http://www.army.mil/article/138883/Army_Cyber_branch_offers_Soldiers_new_challenges__opportunities/
- Freedberg S. J. (2014), Army Electronic Warfare ‘Is A Weapon’ – But Cyber Is Sexier, Breaking Defense, 16 Oct. <http://breakingdefense.com/2014/10/army-electronic-warfare-is-a-weapon-but-cyber-is-sexier/>
- Freedberg S. J. (2015), Army’s Electronic Warfare Cupboard Is Bare: No Jammer Until 2023, Breaking Defense, 20 Jul, <http://breakingdefense.com/2015/07/armys-electronic-warfare-cupboard-is-bare-no-jammer-until-2023/>
- Freedberg S. J. (2015), Wireless Hacking In Flight: Air Force Demos Cyber EC-130, , Breaking Defense, 15 Sep, <http://breakingdefense.com/2015/09/wireless-hacking-in-flight-air-force-demos-cyber-ec-130/>
- Gibbons-Neff, T (2015), On the frontlines in Ukraine, a technological gap, Washington Post, 31 Aug, https://www.washingtonpost.com/world/national-security/on-the-frontlines-in-ukraine-a-technological-gap/2015/08/31/8a62a94c-4b7c-11e5-84df-923b3ef1a64b_story.html
- Global Voices (2010), Russia: New Military Doctrine and Information Security, <https://globalvoices.org/2010/02/23/russian-military-doctrine/>
- Gould J (2015) Electronic Warfare: What US Army Can Learn From Ukraine, Defense News, August 2, <http://www.defensenews.com/story/defense/policy-budget/warfare/2015/08/02/us-army-ukraine-russia-electronic-warfare/30913397/>
- Harding, L. (2014) Putin considers plan to unplug Russia from the internet ‘in an emergency, The Guardian Newspaper, Sep 19. <http://www.theguardian.com/world/2014/sep/19/vladimir-putin-plan-unplug-russia-internet-emergency-kremlin-moscow>
- Headquarters, Department of the Army (2014), Field Manual 3-38 Cyber Electromagnetic Activities, Feb, http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/fm3_38.pdf
- Hersman, E. (2013), The Mobile Continent, Stanford Social Innovation Review, Spring http://ssir.org/articles/entry/the_mobile_continent
- HP Security Research (2015), Cyber Risk Report, <http://www8.hp.com/uk/en/software-solutions/cyber-risk-report-security-vulnerability/>
- Ingram, M. (2011), It’s Not Twitter or Facebook, It’s the Power of the Network, Gigaom Research, 29 Jan, <https://gigaom.com/2011/01/29/twitter-facebook-egypt-tunisia/>
- InfoSec Institute (2014), Crimea – The Russian Cyber Strategy to Hit Ukraine, 11 Mar <http://resources.infosecinstitute.com/crimea-russian-cyber-strategy-hit-ukraine/>
- US Department of Justice, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage, 19 May, <http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor>
- Kelly, S. Earp, M, Reed, L. Shahbaz, A. and Truong, M. (2014), Tightening the Net: Governments Expand Online Controls, Freedom on the Internet 2014, Freedom House, <https://freedomhouse.org/report/freedom-net/2014/tightening-net-governments>
- Lawson, D. (2015) Smartphones are the secret weapon fuelling the great migrant invasion, Daily Mail, 28th Sep <http://www.dailymail.co.uk/debate/article-3251475/DOMINIC-LAWSON-Smartphones-secret-weapon-fuelling-great-migrant-invasion.html#ixzz3oGRVMeIC>
- Lucchese, M. Golliday C. L. Joglekar A. N. (2000) Operational Evaluation of

- Electromagnetic Environmental Effects (E3), New DOT&E Policy Calls for More
- Systematic Assessment of E3, <http://www.dau.mil/pubscats/PubsCats/PM/articles00/lucm-j.pdf>
- Mandiant (2013), APT1 Exposing One of China's Cyber Espionage Units, <http://intelreport.mandiant.com> / <http://intelreport.mandiant.com>
- Mann, S, Nolan, J. Wellman, B. (2003) *Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments*, Surveillance & Society Organisation, <http://www.surveillance-and-society.org/articles%283%29/sousveillance.pdf>
- Markowitz, E (2014), Inside Unit 121: The North Korean Hackers That Took Down Sony, *Vocativ*, 4 Dec, <http://www.vocativ.com/world/north-korea/unit-121-the-north-korea-hack-sony/>
- Morozov, E. (2012), *The Net Delusion: How Not to Liberate The World*,
- Moskvitch, K. (2015), Is our World Really Getting Smart?, *E&T Magazine*, 10 Nov, The Institute of Engineering and Technology, p66
- Murray, H. Maj (2014) - Cyber Requirements, AFCEA Technet, Augusta Marriot Convention Centre, 10 Sep
<http://www.afcea.org/events/augusta/14/documents/T2S2AFCEATechnetCyberRequirements.pdf>
- Ofcom (2015), *The Communications Market Report*, published 6th August, <http://stakeholders.ofcom.org.uk/market-data-research/market-data/communications-market-reports/cmr15/uk/>
- OSCE (2014), Latest from OSCE Special Monitoring Mission (SMM) to Ukraine based on information received as of 18:00 (Kyiv time), 3 November 2014, <http://www.osce.org/ukraine-smm/126364>
- Oatman, S. LTC, US Army EW Training Overview, AFCEA Technet, Augusta Marriot Convention Centre, 10 Sep <http://www.afcea.org/events/augusta/14/documents/AFCEAEWTrainingbriefFinalv2.pdf>
- Parker, A. (2015), Lord Mayor's Defence and Security Lecture - A Modern MI5, 28 Oct, <https://www.mi5.gov.uk/home/about-us/who-we-are/staff-and-management/director-general/speeches-by-the-director-general/a-modern-mi5.html>
- Pollock, P. (2012) *People Power 2.0 How civilians helped win the Libyan information war*, *Technology Review*, April 20, <http://www.technologyreview.com/featuredstory/427640/people-power-20/>
- Pomerantsev, P. (2015), Inside the Kremlin's Hall of Mirrors, *The Guardian Newspaper*, 9 Apr <http://www.theguardian.com/news/2015/apr/09/kremlin-hall-of-mirrors-military-information-psychology>
- Roberts, P. Payne, A. (2015), *Intelligence Surveillance and Reconnaissance in 2035 and beyond*, Royal United Services Institute,
- Seaboyer, A. Jolicoeur, P. (2014) *The Evolution of Russian Cyber Influence Activity: A comparison of Russian Cyber ops in Georgia (2008) and Ukraine*. Royal Military College of Canada, Department of Political Science, DRDC-RDDC-2014-C119
- SecDev (2012), *Syria Cyber Watch 1*, <http://new.secdev-foundation.org/wp-content/uploads/2014/08/Syria-Cyber-Watch-1.pdf>
- Sims, D. (2015), 5 Things You Need to Know about Putin's Popularity in Russia, *The National Interest*, 21 Jul, <http://nationalinterest.org/feature/5-things-you-need-know-about-putins-popularity-russia-13380>
- Sky News (2015), North Korea Accused Of 'Nuclear Cyberattack', 17 Mar,
<http://news.sky.com/story/1446629/north-korea-accused-of-nuclear-cyberattack>
- Smith, D. (2014), Internet use on mobile phones in Africa predicted to increase 20-fold, *The Guardian*, 5th Jun, <http://www.theguardian.com/world/2014/jun/05/internet-use-mobile-phones-africa-predicted-increase-20-fold>
- Sophos (2014), *Security Threat Report*, <https://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf>
- SRI Consulting Business Intelligence, *Disruptive Technologies Global Trends 2025*, Appendix F, Background: The Internet of Things
<http://www.internet-of-things.eu/resources/documents/appendix-f.pdf>
- Stalinsky, S. Sosnow, R (2015) *Al-Qaeda's Embrace Of Encryption Technology – Part II: 2011-2014, And The Impact Of Edward Snowden*, *The Cyber & Jihad Lab*, 28 Apr
<http://cjlabs.memri.org/lab-projects/tracking-jihadi-terrorist-use-of-social-media/al-qaedas-embrace-of-encryption-technology-part-ii-2011-2014-and-the-impact-of-edward-snowden/>
- Stalinsky, S. Sosnow, R (2015), *Al-Qaeda's Embrace Of Encryption Technology Part III – July 2014-January 2015: Islamic State (ISIS) And Other Jihadis Continue To Develop Their Cyber And Encryption Capabilities; Post-Snowden Fears Lead Them To Test New, More Secure Technologies And Social Media* *The Cyber & Jihad Lab*, 5 Feb. <http://cjlabs.memri.org/analysis-and-special-reports/al-qaedas-embrace-of-encryption-technology-part-iii-july-2014-january-2015-islamic-state-isis-and-other-jihadis-continue-to-develop-their-cyber-and-encryption-capabilities-post-snowden/>
- Stalinsky, S. Sosnow, R (2015) *Encryption Technology Embraced By ISIS, Al-Qaeda, Other Jihadis Reaches New Level With Increased Dependence On Apps, Software – Kik, Surespot, Telegram, Wickr, Detekt, TOR: Part IV – February-June 2015*, 16 Jun, *The Cyber & Jihad Lab*, <http://cjlabs.memri.org/analysis-and-special-reports/encryption-technology-embraced-by-isis-al-qaeda-other-jihadis-reaches-new-level-with-increased-dependence-on-apps-software-kik-surespot-telegram-wickr-detekt-tor-part-iv-f/>
- Sunday Times, General Sir David Richards calls for new Cyber-Army, 17 Jan,
<http://www.timesonline.co.uk/tol/news/uk/article6991030.ece>
- The Guardian (2015), *The NSA Files* <http://www.theguardian.com/us-news/the-nsa-files>
- Tibbetts, G. (2008). Prince William's Sandhurst instructor killed after communications failure, *The Telegraph*, 17 Jul. <http://www.telegraph.co.uk/news/newstopping/onthe frontline/2420042/Prince-Williams-Sandhurst-instructor-killed-after-communications-failure.html>
- Tice, T. (2015), New re-up bonuses and reclass calls take effect Oct. 9, *Army Times*, 28 Sep, <http://www.armytimes.com/story/military/benefits/pay/2015/09/28/new-re-up-bonuses-and-reclass-calls-take-effect-oct-9-nc0/72748682/>
- TRADOC, (2013), *The Enabling Operations In Cyberspace Through Institutional And Operational Unity Of Effort White Paper*, US Army, www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA592330
- TRADOC (2013), *The U.S. Army Landcyber White Paper 2018 – 2030 US Army TRADOC*
- Vergun, D (2015), Cyber chief: Army cyber force growing 'exponentially', *US Army*, 5 Mar, http://www.army.mil/article/143948/Cyber_chief__Army_cyber_force_growing__exponentially
- Vitaliev V, (2015), *Old Crows Fly to Stockholm*, *E&T Magazine*, Volume 10, Issue 7/8, August / September, The Institute of Engineering and Technology, p78
- Wright, B. (2015) *Police Shooting Videos: 6 Times Unarmed Black Men Were Killed By White Officers And What It Means For Social Justice*, *International Business Times*, Apr 9, <http://www.ibtimes.com/police-shooting-videos-6-times-unarmed-black-men-were-killed-white-officers-what-it-1876156>

Defence solutions

Wherever safety and security matter, we deliver

PRECISION STRIKE

Deliver precision effects within the battlespace while avoiding collateral damage

THREAT DETECTION

Provide early detection, prioritisation and faster reaction to threats

CYBER DEFENCE

Provide active defence of cyberspace

SITUATIONAL AWARENESS

Increase operational tempo through shared intelligence

NETWORKED COMMUNICATIONS

Enable the rapid escalation of decision making in the heat of the battle

MISSION OPTIMISATION

Reduce crew workload during complex tasks to shorten reaction time

POWER PROJECTION

Supply logistical solutions for the deployment and direction of forces

Millions of critical decisions are made every day in defence to protect people, infrastructure and nations. Thales is at the heart of this. We serve all branches of the armed forces for air, land, naval, space and joint operations as well as urban security and cyberspace. Our integrated smart technologies provide end-to-end solutions, giving decision makers the information, equipment, control and services they need to make more effective responses in critical environments. Every moment of every day, wherever safety and security are critical, Thales delivers.

THALES

Together • Safer • Everywhere

THE ARMED FORCES COMMUNICATIONS AND ELECTRONICS AGENCY EUROPEAN TECHNET CONFERENCE 2015



By Major Jon Heaton MSc CITP CEng

EDITOR'S NOTE

Maj Heaton is currently serving in Army HQ, within the newly established Cyber and Security organisation as the SO2 Cyber. He joined the Royal Signals at the Army Apprentices College in 1980 and completed 22 years of service as a soldier, spending extended periods of time in Northern Ireland and within the Special Communications environment. In 2003, as a Supervisor IS, he was selected for a commission and has subsequently served as an Operations Officer in 10 Signal Regiment, at the Command Support Development Centre and within the DE&S Network Technical Authority, prior to arriving in Andover last summer.



AFCEA, or the Association for Communications, Electronics, Intelligence & Information Systems Professionals, recently held their annual TechNet Europe conference in Berlin. The conference was hosted jointly by AFCEA Europe, the Bundeswehr Geoinformation Centre and the AFCEA Bonn chapter with broad participation from several government departments. For the sixth time, the conference incorporated the AFCEA Student Conference with Major Heaton acting as the Conference Director.

The student conference was opened by Major General Klaus-Peter Treche, formerly of the German Air Force, and was attended by students and their respective professors from throughout Europe, including Germany, Greece, the Czech Republic, Italy, and Romania. The conference provided an opportunity for AFCEAN undergraduate, MSc and PhD students to present short papers on the overarching TechNet conference theme to a Scientific Committee, chaired by Petr Jirásek (Head of Cyber for the Czech Republic National Cyber & Security Centre). This year, papers ranged from Biometric methods for facial recognition to Coastal Surveillance with Autonomous Sailing Boats and Workplace monitoring for Human Factors Risk Mitigation.

The student conference received financial support from a number of sponsors, which allowed prizes to be awarded and for the costs to the student social and cultural events to be offset. These included a visit to the German MOD HQ, a guided

tour of the German Bundestag's Reichstag building and an evening of gastronomy at Berlin's renowned Alte Pump.

Pictured below are the Student Conference delegates and the Scientific Committee taken in the former RAF Military airbase in Gatow.

AFCEA currently has two active UK branches, in London and Cheltenham with events running throughout the year on a monthly basis; further details can be found at <https://www.afcea.org.uk/>

I have now acted as the Conference Director for three out of the last four years. However, if there is a volunteer who would like to take on this immensely enjoyable and rewarding task in the future, he would be willing to step aside and is contactable at jon.heaton152@mod.uk. Finally, I would like to express my gratitude to the RSI for their financial support which enabled me to attend this event.

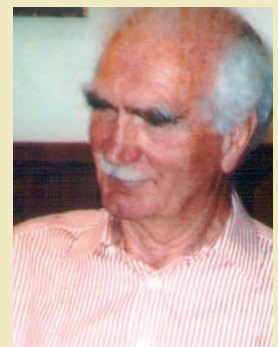


A STAY BEHIND JUNGLE DETACHMENT IN MALAYA

By Major Tom Johnstone

EDITOR'S NOTE

Tom Johnstone served with the RAF in the Middle and Far East before joining Royal Signals in 1949. After an initial tour in the War Office, he embarked for Korea in 1951. He then spent the next thirty years serving at every level of command from Brigade upwards, at home and overseas. This included SHAPE Signal Group, HMS Tyne during Suez, COMCAN Boddington and the KAR in East Africa. Three tours in BAOR followed, interspersed with ACE COMSEC, HQ UNFICYP, and finally 9 Signal Regiment (Radio). Following retirement in 1983 he realized his life's ambition by producing three historical works set in Dublin, London and Australia, where he now lives, close to Melbourne.



The pre-war military thought at Far East Command Headquarters in Singapore was that the Malayan jungle was impenetrable; therefore an invasion of Malaya was unlikely. Notwithstanding this, on the orders of the War Office in 1941 a miniscule organization had been dispatched from UK to Burma and Malaya to plan and establish training schools for irregular warfare. Following the arrival of the Singapore detachment, 101 Special Training School was established, under command of Lt-Col J.M. Gavin, RE. Later that year he was joined by Lt-Col A. Warren, RM and Maj F Spencer Chapman; both the latter had been trained in Britain for 'special operations' and had recently been in Australia as part of a team training "Special Companies." They were now in Malaya specifically to organise and train stay-behind volunteers for sabotage and guerrilla operations in the event of a Japanese attack on Malaya. Spencer Chapman became Gavin's second in command and later took over command of 101 STS when Gavin went on tour in Malay organizing potential recruits.

Following the Japanese attack, the Governor at first refused to allow 101 STS to train Chinese specially selected by the Malayan Communist Party (MCP), but after bad news from the front, he relented. Following their induction, Spencer Chapman considered them the best material that 101 STS ever had.

Communications had to be organized from the jungle to other British headquarters in Far East Command, and the search for volunteers among Royal Signals began. The first to be approached was Corporal John Cross, a company secretary in civilian life, and now a Royal Signals wireless operator. He had arrived in Singapore with 18 Division Signals during September 1941 and was posted to III Indian Signal Corps in Kuala Lumpur. He was part of HQ Company, and as such remained in Kuala Lumpur when the rest of regiment deployed, so when asked to volunteer "blind" for special work, he accepted. When interviewed at RHQ by a Maj Rosher, he was advised that he would be posted to the extra regimental employment list without pay and allowances – even in wartime, the correct form had to be followed! (1)

The detachment he joined was known as Station A, the control station on a forward net with outstations in close proximity to the enemy, and extending rearwards to GHQ Far East in Kranji Barracks, Singapore. The Chinese operators manning the forward stations had been recruited in Hong Kong and Singapore, and trained as agents and saboteurs in 101 STS. The outstations were supplied with suitcase transceivers on which they sent their traffic to Station A, who then relayed it to GHQ. Cross's catchment consisted of Sig David Mortimer, a former Cable and Wireless operator, LCpl Frederick Wagstaff, an instrument mechanic, and a Chinese operator Liu Chin Hung. Their set was a Signals issue 'mobile' station usually fitted in a vehicle, complete with batteries and a "char horse" two stroke charging engine.

Cross met James Barry, a Colonial official working with Rosher on his return from operations on the Malaya-Siam border, where together with his interpreter assistant Lee Boon, he had positioned the forward stations manned by locally recruited Chinese who had been selected and trained at 101 STS as stay at home agents. Barry always encrypted his own messages ready for transmission, and was to be associated with the signals detachment for some time. Barry was away visiting Kranji when the Japanese onslaught forced the retirement of 3 Indian Corps.

Through the help of Chapman, Cross was able to requisition a dilapidated Chinese lorry and with all their kit and equipment loaded board, they joined the convoy of HQ 3rd Corps. On reaching Kluang, they established their station in a bungalow, opened communications with Kranji, and requested instructions from Barry. The bungalow was close to a mixed police and military commando-type unit under command of Colonel Dalley, known as DALCO, one of a number of private armies established by Colonel Warren. They had no communications with Kranji, and Station A passed their message traffic. In addition, Cross helped DALCO establish a jungle resupply base 12 miles along the Kluang – Mersing Road. Here for the first time Cross saw the real Malayan jungle, and at once realized its potential for a concealed base area. Just as Kluang was being evacuated, Barry signaled Cross telling him to rendezvous at Kluang Police Station. From Kluang 3rd Corps HQ retreated to Johore Bahru, where once again Barry left them to visit Kranji. He duly returned having been appointed Major, and given command of a Chinese Special Party (CSP), consisting of seventeen operatives selected by the Malaya Communist Party, together with the Royal Signals detachment. They were to be detached on the mainland behind Japanese lines to provide intelligence for the Allied Command. Barry and the whole signals detachment returned to Kranji for a full briefing.

At Kranji, Cross and his fellows learned for the first time how desperate the situation in Far East Command was. They were issued with 12,000 Malaya dollars from Special Branch funds, European food for six Europeans and twenty-five Asians for two months, in addition to petrol, oil, arms and ammunition from 101 STS. Cross arranged a Signal plan with Kranji - station 'B' - that if Singapore fell they were to establish communications with station 'Y' – Java, and if that fell, Station 'R' – Rangoon. On 29 January 1942, L/Cpl John Cross was promoted to company quartermaster sergeant, or CQMS, and second-in-command to Major Barry. They Kranji

that same day, crossed the causeway into Johore, and took the Mersing road until they reached a point just past Ulu Tram, where they entered the jungle from which they would not emerge for over three years.

What survived operationally of the Allied forces in Malaya following the Japanese conquest was several isolated detachments, mostly in northern and central Malaya, operating independently with the assistance of what was essentially a Malayan Chinese Communist organization, grandly called the Malayan Peoples anti-Japanese Army or MPAJA. It was essentially a Chinese organization of eight autonomous provincial groups divided into patrols. All were loosely controlled by the Central Committee of the Malayan Chinese Communist Party, but with little direction or coordination. Throughout the occupation this lack of central coordination and failure to respond caused delays and engendered much frustration to the stay-behind parties and the soldiers left behind.

Cross's detachment and the CSP operated with 4th Independent Regiment MPAJA in southern Johore State, which they entered on 29 January 1942. All the stores were carried by coolies who were dismissed long before they reached the final destination, so as not to compromise the eventual location. The 4th Independent Regiment undertook the task of bringing forward the stores to their camp. With their assistance Cross and his party carried the transmitter, receiver, batteries, charging engine, supplies of petrol and acid to the camp as quickly as possible. On arrival at what was to become their first jungle camp they experienced for the first time what would soon become second nature; building a sleeping platform, roofed with atap and making mattresses of leaves, just in time to protect them from rain which fell on their third night. Behind this they established the radio station and went on calling and listening watch for Station Y – Rangoon, without response. They would endure this for three months before assuming they had been 'officially abandoned.'

Until they learned a smattering of Mandarin, communication with the CSP was by smiles and sign language. Close contact quickly disabused them of the Hollywood concept of Chinese, and saw them instead as individuals and nicknamed them in accordance with the demeanor of each. The Bank Clerk, a quiet individual with a precise manner who, whenever he was going outside the camp donned a pair of neat trousers, jacket, collar and tie and felt hat; the American Bloke – square-faced with a perpetual toothy smile, like an advertisement in the New Yorker magazine; Jungle Rat – very slight stooped shouldered with serious features and small very bright eyes; the Elephant a large lumbering playful person who became Little Elephant, when an even larger version of the same joined the group and became Big Elephant. (2) Camp followed camp in quick succession, and the British soon mastered Chinese names and the language. By this time they were all accustomed to hours of travel, but the going was so hard in places that eight hours travel covered only a mile on their map. On some jungle tracks however, although no more than two feet wide, and carrying a back pack, personal weapons and ammunition, with five minutes break every hour, fast marches covering eight miles could be achieved. Their sixth camp was situated on the banks of a tributary of the Sungei Pengeli, they dubbed it Riverside.

By this time they had discovered that the 'sparking' from their unsuppressed charging engine might be heard by Japanese. To counter this, Cross had a pit dug for the charging engine at each new location. Discovering that daytime radio listening was unsatisfactory because of interference from close local Japanese transmissions, they restricted their watch to night hours, when long range radio propagation was at its best. In the dank jungle conditions their standby suitcase transceiver became heavily mildewed, and the 'char horse' was giving trouble. To make matters worse, petrol was becoming very scarce. Often it required ten minutes of pulling and re-pulling the starting cord before the engine started. On every pull, some petrol was spilled on the ground, and passed unnoticed until a backfire caused an explosion and fire in which Cross was badly burned and Morter less so. Cross's burns turned septic and Barry had to perform rudimentary surgery with a razor blade to cut away rotten flesh before Cross's burns began to respond to the only antiseptic they had, Dettol.



The operators had been monitoring Allied stations and considered breaking-into an Allied net, eventually deciding that a one to one link would be their best choice. When Morter was well enough to transmit, they attempt a break-in on a two stations link which seemed the most promising - CNWH and VNDN. Waiting until both had finishing sending and going onto listening watch, Morter tap out a message 'en clair' "TELL LONDON BARRY SAFE. ASK COLONEL ----- TO SIGNAL DSJ ON 13720 AT 1800 AND 0200 GMT. URGENT AND VITAL. DON'T IGNORE. He sent the message to both stations twice before switching to receive. Naturally neither station acknowledged the message, they were not expected to, but it was hoped that at least one of the operators would pass on the message. For security reasons Cross did not divulge the name of the Colonel in his memoirs. For whatever reason, the message was never acted upon. Lesser men might have despaired, but not this detachment.

In April Cross realized that the six months European rations they had had been given would have to be conserved so as to last as long as possible; especially cigarettes, tobacco, glucose sweets and chocolate. They were also tempted to try and escape to Sumatra, from where they might hope to be evacuated to India; this too was rejected in favour of continuing their mission in Malaya.

It was the technician who conceived the idea of a miniature hydro-electric scheme. Doubtless the idea of a water wheel originated while contemplating the nearby river and considering how it could be used. Much work would have to be done, however. The Chinese under the leadership of Ah Kow quickly grasped the potential of the scheme and its fundamentals, and set to work in harnessing the water and constructing the wheel. No easy task. Cross and his two companions designed and the Chinese constructed a paddlewheel 68 inches in diameter, consisting of a framing with box paddles around an eight inch by eight inch octagonal hardwood shaft.

Ah Kow and his helpers fairly interpreted Cross's brain-child. Working with infinite patience, skill and craftsmanship they made the wheel and other parts out of trees felled and cut up on the spot with a handsaw. The stream was dammed and diverted into a wooden trough seventy feet long, held aloft by gantries fashioned from saplings. It was nailed and braced together at five feet intervals each length fitted to the next with a rough rebated joint. (3) The trough delivered a thirty inch head of water onto the wheel boxes turning it at 40 revolutions a minute. Meanwhile Cross, Morter and Wagstaff worked on the driving system for the dynamo. Of the three, Wagstaff did most, toiling from morning to night, and at times Cross wished he had never thought of the project.

Eventually, the main belt was fashioned from their webbing haversack straps. An improved dynamo drive belt was made from an old bicycle tyre, using the pedal wheel from the bicycle as a bearing at one end of the paddle wheel drive shaft, and the handlebar swivel as the bearing at the other end. With these rudimentary elements the wheel turned with sufficient speed to charge a battery in thirty-four hours. The first battery was completely charged by his method on 18th October 1942. With the batteries fully charged they could extend their 'listening watch' for four hours a day seven days a week. (4)

Consulting the Chinese in their own party, Lee Boon and Liu Chin Hung wanted news about China, the special Chinese party wanted Radio Moscow Chinese news. Cross therefore set up listening watches for:

- 06.15 – 06.30 – San Francisco (news in Chinese)
- 06.30 – 07.00 – Moscow (news in Chinese)
- 08.30 – 09.00 – London (news in English)
- 09.45 – 10.00 – Chungking (news in Chinese)
- 10.00 – 10.15 – San Francisco (news in English)
- 10.00 – 11.30 – Listening watch for Station 'F'

This arrangement left the British party one and quarter hours for other news and entertainment. Barry, Morter and Wagstaff preferred the comedian Tommy Handley. They all wanted Mail Call. All were satisfied with this schedule. The Chinese rigged a speaker for their bulletins, the four British personnel, including Barry, would crowd close to the set and share three head-sets amongst them. They also

found messages being broadcast from New Delhi, London and Melbourne, for internees and prisoners of war in Japanese hands, and wrote down the messages in case the opportunity to pass them on presented itself.

In the jungle the CSP discovered a considerable quantity of Allied arms and equipment. The arms were sometimes without essential parts such as rifle bolts, but some were in working order and were cleaned and reused. Among the equipment were some low powered Australian radio sets. Cross conceived the idea of training additional Chinese as operators, and using these on an internal net in S. Johore. Another item was a duplicator, and at Christmas a few weeks later, he conceived a use for this, using Barry's typewriter to cut the necessary stencils for duplicating. An idea began to form in John Cross's active mind. (5)

Pressure from Japanese patrols forced a move of the Special Party further into the hinterland near Durain, but they had to hack a track through the jungle to yet another location known as Hilltop Camp, and allow the jungle to reclaim the path before they could really feel safe. At the end of October 1942, their food situation reached a critically low point. This was due to a new slothful Chinese cook, who instead of obtaining food from outside sources with money provided by the British, had used their emergency provisions. Cross decided that what emergency rations remained had to be husbanded, and they would all have to subsist on what they had. Thus, when rice was served, each person received one cupful per two meals a day. The rice was augmented by sweet potatoes with boiled green potato stalks; what protein they received was from occasional additions of black beans.

As their first Christmas approached, the thoughts of the British party turned to a celebration. This was explained to the communist party leader, whose cooperation was necessary. He was enthusiastic and wished to have it turned into a communist affair. Cross, imagining speeches, party songs, and parades, hurriedly and diplomatically explained that in Europe it was a quiet, family-oriented, peaceful and contemplative celebration. Moreover they had been in the jungle a long time without any celebrations of their own. Comrade Mee Tek reluctantly accepted this and for the event produced two chickens, some coconut sugar, fresh pineapple and papaya, three quarters of a tin of animal cracker biscuits plus enough cigarettes to give everyone twenty-four each. With this bounty they had a merry jungle Christmas. (6)

Early in January 1943, one of their scouting parties stumbled on the isolated tin-mining village community of Tengkil, surrounded by jungle and only easily approached by river. The inhabitants were self-sufficient, producing potatoes, vegetables, rice, tobacco and raising pigs and chickens. Only small consumer items such as cloth were needed to sustain them, but when a party had visited Kota Tinggi by river to purchase these items they had been imprisoned, and released only on condition they supplied tin to the Japanese. Now they agreed to provide the Special Party with potatoes and vegetables. A search of the deserted bungalows, once inhabited by European mining engineers, yielded a very welcome small library of books with authors ranging from Shakespeare to Edgar Wallace, in addition to a typewriter and a supply of paper; it seemed heaven sent.

JOHN CROSS DCM

Born in North London in 1910, John Cross lost his half-Danish father when two years old. He lived with his mother and maternal grandparents until his mother's remarriage in 1916 when he moved with her to Hampshire. After a year or so he returned to the care of his grandparents in London. He remained with them until his early twenties and was much influenced by his liberal minded grandfather. During these years he was a voracious reader of political philosophy and biography.

Between 1926 and 1940 he trained as a commercial accountant, filling a number of posts mostly in the building and woodworking industries and including a spell with a firm of chartered accountants.

In 1940 he left his job as a company secretary to join the Royal Corps of Signals. Within five months of leaving England in 1941 he found himself in the thick of the Malayan Campaign. In Kuala Lumpur on Christmas Day 1941 he volunteered for special service. Just before the fall of Singapore Island he returned to the mainland as second-in-command of a small radio / intelligence unit and lived with Asians more or less as an Asian until the unit emerged under his command three-and-a-quarter years later. His orderly outlook stood him in good stead in these harrowing conditions, in which a

sense of purpose was essential to survival. During these years with Asians he developed a fondness and respect for them and an understanding of their desire to raise their material life to Western standards. His efforts to achieve friendship and a meeting of minds with Chinese communist leaders he found frustrating for, as he writes in Red Jungle: "It seemed just impossible to have a one-hundred-per-cent friendship with anyone who, in the final analysis, subjects everything to political considerations." He is intensely interested in people and feels that he was fortunate in that the war gave him this first-hand experience of the Far East.

In 1946, demobilized and completely restored to health, he became restless. Disappointed by London, to which he had longed to return, he went to work and live in Northern Ireland. But in 1948, he returned to start a small manufacturing business in England. He bought an old cottage in a village near Aylesbury in Buckinghamshire and interested himself in modernising it. There, too, he found that his years in the Malayan jungle had left him with a preference for life in the country. There, too, with his wife and stepson, and between his work and his hobby of gardening, he found the leisure to begin writing Red Jungle story about which he felt that, if it was ever to be written at all, it must be in his own words.

Just before Christmas 1942, Cross had suggested producing a news sheet to counteract Japanese propaganda on the progress of the war, which Cross and the others knew to be false. Real news was kept from the people of Malaya because a ban had been placed by the Japanese on radio sets with short wave reception, thus leaving the airwaves free for their own propaganda broadcasts. Now, with a typewriter, paper, and a duplicator they could produce a newsheet to counteract Japanese propaganda, and raise the hopes of the people for eventual liberation. With the failure to contact and communicate to Allied Command in India, Cross had given up any idea of passing intelligence about the Japanese in Malaya. Now, his overriding intention became the founding of an English language newsheet to reach the better educated Chinese and Malays, in the hope of winning them away from Japanese. Not that that he had he any illusions about communists aims in Malaya. He knew that in Malaya as in UK, the Communist Party had directed propaganda against the Allied cause favouring the Hitler-Stalin non-aggression pact of 1939. This only changed in June 1941 when the Germans invaded the Soviet Union. Their ultimate aim was the expulsion of the British and creation of a communist republic in Malaya. For the moment, they cooperated with the Allies for their own ends.

In January 1943 a central committee member (CCM) was received with all the preceding 'bull' Cross had experienced in preparation for a General's visit to Catterick Camp in Yorkshire during his training there. On his arrival, Cross recognized the CCM as Ah Chai, who he had been introduced to as a 'courier' in Swamp Camp in March 1942. Indeed he had carried Cross's pack and blanket on the march to Durian Camp, and his smile when Cross had voiced his suspicion that he was a person of rank. They had four conferences during the third week of January 1943, during which Cross considered much was achieved. Belatedly, Cross heard news of a plan of his to send two couriers to India to inform Allied Command of their survival and submitting a new Signal plan, for which he had provided three thousand Malayan dollars. Apparently one had reached Sumatra, from whence he hoped to get passage to Colombo; but nothing further had been heard from him. The second, disguised as a merchant, and with most of the money, had reached Bangkok. Cross was also assured that once signal communications were in place, a representative of Central with responsibility for intelligence forwarding would be attached to them. Cross would be sent a sample for current information purposes. Cross liked Ah Chai chiefly because he 'did not declaim, but discussed'. (7)

During Ah Chai's visit the rations had improved, but following his departure they plummeted, and for the next two months a most unpalatable diet of dried potatoes made up most of it. Barry took up hunting to improve matters, but only succeeded in bagging various types of monkey, against which their stomachs rebelled in various ways. Nevertheless, Barry's temperament was improved by his jungle forays at Hilltop Camp. All the party now developed an irritating skin rash. Cross was forced to wear a sarong for several weeks because his rash broke out on his buttocks. Ten dollars of dwindling personal cash invested in a traditional Chinese medicine had no benefit.

When the sores turned septic, only treatment with the precious M&B powder had any beneficial effect. Deciding their bodies badly needed protein, they purchased a cockerel and hens. In the following eight months each had seventy-eight eggs in turn and their health improved, although they never became robust. They also derived a certain amusement in the hens' behaviour.

Ah Chai returned at the end of February and they discussed Cross's ideal of a Newspaper at some length. Central had been impressed by the idea, and decided to move their Party newspaper, 'Emancipation News' to their camp, together with the editorial staff. In return for the help with radio news, the British were able to produce their own newspaper with a staff of an English speaking Chinese and two British. They also planned to open a school in the camp to train leaders for other groups throughout Malaya. To maintain the secrecy of the radio staff, the students would have no contact with the British. Doubtless Cross was pleased to be told that that Ah Chai planned to take Mee Tek and Gook Poh away with him on his departure, and send in a new leader. Cross's last request, that they be allowed to take in a small party of sick British and Australian soldiers who had been deserted by their more fit comrades, fell on deaf ears.

The new leader arrived shortly after Ah Chai's departure. He called himself Chai Chieh and was instantly dubbed Charlie by the British. He was also the Chinese member on their editorial committee. Charlie was young and had a "thoroughly attractive personality". Sometime after this change, around Mee Tek and Gook Poh defected to the enemy, and compromised the location of Hill Top Camp. They were hunted by the 'traitor killers' and had many narrow escapes before they were eventually dealt with; but not before the damage had been done.

Once more Cross returned to his idea of reaching out to the educated English speaking Malay and Eurasian population. Cross's newsheet's first edition debuted on 25 May 1943. In small print with the bold headline 'On the Eve of the Second Front', it briefly gave news of guerrilla activity in Albania, Belgium, Denmark, France, Netherlands, Poland and Yugoslavia. The rest of the edition told of the Allied victory in North Africa, the Allied air offensive across the Mediterranean into southern Europe; and the south west Pacific bombing and US amphibious operations there; Chindit operations in Burma, and the conference between Churchill, Roosevelt and T.V. Soong concerning the Far East. Guaranteeing the truth of the news and promising future editions, it ended with an appeal for paper, ink and other material and requesting feed-back. Charlie informed them it was well received, and donations of paper flowed in, enabling them to spread to two sheets per edition, printed on both sides.

Japanese reaction was swift. On the night of 10/11 June they attacked in three columns converging from different directions each led by a traitor. Well informed, the guerrillas were ready, and all three columns were ambushed in the jungle and repulsed, one guide being captured alive. The attack was renewed on the 13th and another guide and eleven local supporters taken. Learning the strength of the enemy force, the guerrillas withdrew

from their forward positions, having counted seventy enemy dead. Under questioning the local prisoners revealed that the only guide to have escaped was Mee Tek. He managed to evade several attempts on his life by the traitor killers before meeting his just deserts.

Realizing they were now on borrowed time in Hill Top Camp, the British Party prepared to move. The hens and cockerel could not all be taken, so sparing one hen who had a clutch of chickens which they placed in a wicker cage for easy carriage, the entire party feasted on the others to give themselves strength for the journey ahead. Additionally, in a carefully prepared well concealed 'dump' they placed selected spares plus two wireless sets they had 'acquired' since taking to the Jungle. When the Durian Camp, only three hours march away, was attacked, the enemy was held off by tommy-gunners of the rearguard, and most of the guerillas escaped. Hill Top was evacuated next day at first light, abandoning the waterwheel but saving the remainder of the charging equipment. Cross calculated that in ten months it had completed 2,500 hours of battery charging, enabling 1,200 hours of radio listening time, and providing morale boosting news not only to the detachment but to the MPAJF and Malaya's civilian population as well.

A tenth, temporary camp was made on the side of a ridge where they remained for six weeks while a permanent camp was erected. After the Japanese withdrew, it was found that the enemy, for whatever reason, had not burned and destroyed everything there, as they usually did, so a large party of guerillas returned and removed the atap panels to be used at the new camp. While the new camp was being created, everyone slept together, crowded into one hut while rain poured down night after night. Adding to the British party's misery was the discovery that the whisky, held for months against such an occasion, was undrinkable because the glass lining of their small Chinese vacuum flask had broken. All were 'speechless'. (8), Everyone, British and Chinese were now on famine rations. They determined not to break into their carefully hoarded emergency tinned rations, believing that there was worse to come.

On 11 September 1943, their eleventh camp was ready for occupation, in a lovely location dominated by a scenic waterfall and obviously called Waterfall Camp. Under Charlie's leadership all now ate together, British and Chinese, and all shared what was available. The British had by now acquired enough Malay and Chinese to engage in conversation with the comrades and good fellowship generally ensued, but they never liked the squatting eating posture of their companions, as it would take their thigh muscles a long time to adapt, meanwhile suffering agonies of cramp. The pleasure they notably enjoyed was the daily contact with the 'comrades' - it was a delight to escape from oratory to conversation, which was mainly concerned each other's family life before the war. (8)

Another waterwheel was crafted, and on 17 September battery charging recommenced, and soon they were back in the newspaper business. As a reward, HQ MPAJA sent them each a new shirt and shorts, to replace the rags they now wore. The new clothes had been 'run-up'

out of russet brown canvas made from a sail taken from a captured Malay vessel, which also provided the camp with a sack of rice; a remarkable 'thank you' gift from headquarters.

Barry, who had always been temperamental, now began to act strangely, and even attempted to pull rank on Cross on a trivial matter, Cross responded vigorously, and Barry dropped the matter. By November they had settled into a daily rhythm of listening watch, newsgathering and keeping the set on the air. Morter had a narrow escape from serious injury when a spark from the charging engine ignited 'gassing' around a battery on charge, which exploded, spraying him with sulphuric acid mixture. Luckily, the 'acid' had been so diluted with 'topping up' with rain water which passed as distilled water in the jungle that it did him little harm. That same afternoon, they received warning the Japanese had reoccupied both Durian and Hilltop Camps, and had even widened the track to within a mile of their present camp and established two jungle bases. It was time to move again. After a long march to the lowlands then through swamps, they reached open country for the first time in nearly two years. Here they holed up until late afternoon; they were to travel mainly by night.

The first section was by bogie on an old narrow gauge railway, whizzing along at what seemed to them remarkable speed before resuming the march through jungle to the headquarters of the 4th Regiment of the Anti Japanese Army. The guerrilla headquarters was located in a vast hutted camp near Tenkil lit by a diesel generator. Here they made contact for the first time with the Allied cut-offs in Johore. There were four of them, all British, the last of sixteen Australians having died on the way to this camp. The most vigorous of those present was Brian Smith, 2nd Loyals, only twenty years old. Two years previously he had enlisted in Hong Kong, was moved to Singapore and had just reached his battalion in Malaya when disaster struck. Jim Wright was also 2nd Loyals, while the other two were privates of the 6th Royal Norfolks. Wright was just 'skin over bone'. One of his feet had been wounded in the fighting but he had been fed by Chinese and had managed to survive.

At the headquarters the detachment resumed its news gathering and dissemination; they remained here for several months during which time Barry's moodiness increased. He asked Cross to assist him in drawing up his Will, and voiced his suspicions of being 'fobbed off' by the Chinese hierarchy. (9)

So active had the guerrillas become, the Japanese command launched a major offensive to clear Johore of guerillas. On 20 February 1944 a sentinel party of on the fringe of the jungle was surprised and six killed. The survivors retired carrying the wounded. Cross and his party now moved often, and it was in their 18th camp where Barry reached his decision to leave, but not alone. Barry claimed his reason for leaving was to win support of the Johore Malays for Anti-Japanese activity. Cross doubted all of this, but did not wish to quarrel with Barry; then came the bombshell, he wished them to give up their weapons to the unarmed four British of the cut-offs who were to accompany him on his trek to north Malaya. There he hoped to regain contact with India, and he promised to help the Signals detachment gain communications with the Allied command. Cross doubted the feasibility of any of this but kept quiet; he did insist however that his companions

should make up their own minds concerning their weapons. At a combined meeting, it was agreed to split the rations, money and medical supplies on a per capita basis. The Signalers agreed to pass a Tommy gun, a shot gun and two hunting rifles to the infantrymen. They left during the early hours of 17 April 1944, leaving Cross to explain the whys and wherefores as best as he might.

In Barry's letter to Ta Tu, the 4th Regiment's representative with the Special Party, explaining his purpose in leaving, he formally handed over command of the British Party to CQMS Cross, and it was on this basis Cross spoke to both Charlie and Ta Yu, and he took a hard line, maintaining that the Special Party had originally been created by an agreement between his government in Singapore and the Secretary General of the Malaya Communist Party. The sole purpose of this was to maintain radio contact with the Allied command overseas after the fall of Malaya; news gathering had been a sideline. Also that Central had delegated day to day access to HQ 4th Regiment for emergency assistance. He then handed Ta Yu a written request for a meeting with Communist headquarters at which Cross promised a full statement.

Afterwards Cross felt that Ta Yu had been pleased with this line, as it placed the onus on HQ 4th Regiment for a decision on the matter. On the question of arms, Cross stated that his detachment had handed over to the Special Party four Tommy guns, three service rifles and three revolvers, and asked for three weapons back. Ta Yu replied that this was not possible, however if any were travelling, weapons could be drawn from a pool.

Cross and his companions enjoyed a short period of tranquility before disaster struck again. Japanese pressure bottled up the Special group and they were extricated by the fortunate presence of a non-communist Chinese engineer, a former employee of the Malaya government. It was he who had rigged up the diesel generator for HQ 4th Regiment, and knew the location of a Sakai community north of Tengkil where he duly led them.

The Sakais made them welcome, and allocated them two areas of ground for cultivation on which the guerillas grew sweet potato and green vegetables. Continuous trouble with the charging engine however forced a decision to return to the stores dump near the 11th Camp. Wagstaff volunteered to go, and was allocated a Chinese carrying party of five. They returned on 3rd June 1944, and had a battery on charge shortly afterwards, just in time for them to receive the news of the D-Day landings in Normandy. An edition of the news paper was rushed into print, and a courier took 300 copies to HQ. Cross had no doubt but that thousands of Chinese, Malays, and others, would shortly be digesting this exhilarating news.

Cross and Lee Bon fell ill with fever shortly afterwards, Cross becoming so ill that he was sent to a guerrilla jungle 'hospital' for a week's rest. The 'doctor' was a Singaporean chemist, who immediately injected Cross with a double dose of Australian quinine. (10) Shortly after Cross's return to duty, a runner from HQ arrived with a present for them of tobacco, cigarettes and a couple of bottles of Japanese wine, together with a fulsome note of thanks and appreciation in English addressed to 'Dear comrades of the News Press'.

On 17th July they had a letter from Brian Smith explaining that everyone had been very ill, and gave news of Barry's suicide. Smith asked if the surviving three might return to the Special Party. Cross immediately wrote to HQ and succeeded in obtaining permission when they were well enough to travel. On 10 August a sampan pulled into to the bank and Brian Smith and EJ Wright alighted, the third man having died. They told a story of dreadful privations and suffering, which lead to the death to three of their companions. At one of their jungle camps Barry had gone out alone in the night and had cut his wrists with an open razor. He had been buried with the full honours the guerrillas gave their own dead; salutes, bugle call and lowered flag. It was a tragic end to a promising young man.

The new arrivals arrived in time to share the most satisfying meal they were to have for four months. The Sakais had trapped a bear, but they had not checked the trap for some time so the bear was far from being fresh when its carcass was reclaimed. However, by cutting the worst rotting part away and heavily lacing the remains with chili, their share 'cooked up to taste like the finest English beef.' (11) It is remarkable how years of deprivation and near starvation in a jungle fastness alters taste buds.

Meanwhile, in their 20th Camp, Charlie insisted on the two camp system, primarily for the safety of the irreplaceable equipment of the newspaper's equipment. Once again it was located in the jungle. Here, the first edition of the Victory Herald appeared with the headline 'Paris Freed- An Example to Malaya'. The MPAJF had agreed to distribute the newspaper in north and south Johore, Pahang, Selangor and Perak. (12) Unfortunately the charging engine on which so much depended, was out of order. On stripping it down Wagstaff found a broken connecting rod. A spare had previously been requested, together with other items some time previously from HQ 4th Regiment, and had been delivered to Tenkil just before its occupation by the Japs and could not be collected. The delay forced Wagstaff to perform a near miracle in carving a perfect wooden model, from which he fashioned a cast, then smelted metal which he poured into the cast to produce a perfect replica of a connecting rod. The rod worked sufficiently well to charge their batteries and keep the station operational until the end of January 1945.

Over Christmas 1944 Cross, Wagstaff and Morter took stock of their situation. As they saw it, they had a station no one used and a newspaper the MPAJF seemed not to wish distributed, as it did not conform to their own paper's slant towards Soviet Russia. However, they had a good camp in clear country, on which they grew fresh vegetables. There was every possibility of the war ending in 1945. 'On balance, things didn't seem too bad'. (13) They improved again in January when HQ MPAJA finally put them in contact with a British commando party in Johore under the command of Major BA Martin, who would see them in February. At the end of January, 'Charlie' informed them that the next, 31st edition, of The Victory Herald would be their last, because of shortage of paper. Had this occurred before Christmas '44 it would have been a devastating blow, now however, with visions of a change to their personal fortunes, it hardly mattered, chiefly because it was accompanied by a letter from Martin's Chinese radio operator, requesting details of their party. He had been operating remotely from Major Martin's party when it had

been suddenly attacked and scattered, and Martin killed. The good news was that he was still in communications with India.

On 20th March Cross was summoned to a meeting with a Major Sime, who had taken over command when Major Martin was killed. After a relatively easy journey to HQ 4th Regiment they met on 23rd March. Sime had expected to find physical wrecks and was visibly surprised by the appearance of Cross and Wagstaff. Having seen them, he undertook to report to India and he expected them, together with the cut-offs, to be exfiltrated at the next submarine rendezvous; until then they would be under command of Major John Hart, Intelligence Corps. Meantime, they were to base themselves with him until called forward. (14)

Following their return to camp 21, the combined British Party prepared to move, and on the morning of 1st April they pushed off from the landing stage with a Sakai girls singing class under Lee Boon singing 'Will Ye No Come Back Again', changing to 'Auld Lang Syne'. That simple gesture spoke volumes. After two hours on the river, the guide signaled the Sakai paddlers to pull into the bank and after a five hour trek to their 23rd Camp next morning they marched to the 24th Camp on 24th April where 'Charlie' greeted them with the words 'I think you are going back to England'.

Here they spent ten days, and met the three survivors of a B29 bomber shot down three months previously; two others had been captured and publically beheaded by the enemy. The survivors were Maj Harvey Wilson the pilot, the co-pilot Lieut Fitzgerald, and Sgt Roberts the radio operator. The leader greeted Cross with the words "You Cross? I'm Wilson." Cross replied 'Yes, how long have you been in here?' Wilson answered 'Three months, how long have you guys?' Cross told him, 'Three and a quarter years.' 'Jesus Christ' the American exclaimed. The incredulous intonation in the utterance of those two words can well be imagined.

In the days which followed camp followed camp as they carefully made their way from the Jungle through Japanese patrolled territory to the east coast of Malaya to the rendezvous on a beach between Tanjong Lompat and Tanjong Siang, an area isolated by mangrove swamps and unlikely to be patrolled by the enemy. Nearby was their 30th and last camp, reached on 29th May. On the morning of the 30th, the recognition signal, a large rectangular flag was hoisted in the vertical; were it in the horizontal position it would signal to the submariners 'abort, enemy close, try tomorrow'. Cross was carrying a report written by Maj John Hart giving details of his debrief of Cross and addressed to HQ, Allied South East Asia Command, Ceylon. (15)

A landing party of Royal Marines, in rubber dinghies appeared quite suddenly, and all the waiting troops boarded the submarine without mishap. The commander of HMS Thule, Lt-Cdr Alistair Mars, DSO, DSC R.N., greeted his passengers and explained their route to Fremantle on the west coast of Australia where they would land. Six weeks of travel by submarine and aircraft, lengthy debriefings and thorough medical checks followed, until their final debriefing at the War Office.

During their three years and four months cut off in the Malayan jungle Cross and his two fellow Signalers' Morter

and Wagstaff, had moved to thirty different camps in the face of Japanese harassment. They suffered repeated attacks of malaria, dengue fever, dysentery, weeping jungle sores and malnutrition. Despite this they never lost sight of their mission, and whatever the hardship strove to accomplish every task necessary to achieve their aim with commendable determination and fortitude. John Cross well deserved his Distinguished Conduct Medal as did David Morter and Frederick Wagstaff their Military Medals. Doubtless they would also have been 'mentioned' in the dispatches of the CinC SEAC, Admiral of the Fleet Lord Louis Mountbatten, in one of his reports to London. In the Foreword to Cross's memoirs Lord Louis wrote "



The book written by Cross about his experiences.

"This is an account of one of the parties left behind after the fall of Singapore – it is a tale of fortitude, courage and endurance which I unhesitatingly commend. To live and work behind the enemy lines for well over three years calls for qualities quite out of the ordinary; and as Supreme Allied Commander South East Asia at the time I had personal knowledge of what these gallant men achieved. . . I was proud to have such men as these under my command."

Some fifty odd years after the publication of John Cross's book, Professor Keith Jeffery in his monumental history of the SIS included a two page account of Cross's stay-behind party and their operations, in which he named James Barry as the SIS agent Louis Cauvin, who prior to the Japanese invasion Cauvin had been a Colonial Immigration official at Padang Besar on the Malay-Thailand border. He had recruited some mixed race local people and operated in Thailand. Forced to withdraw in the face of the Japanese onslaught he joined the Chinese guerrillas in the way described by Cross. Jeffery failed to credit the production of the morale boosting newspapers to Cross and his fellow signalers. (16) It would appear that John Cross changed Cauvin's name to James Barry because of the manner of his death to avoid embarrassment to the dead man's family; which was also described as suicide by Jeffery.

References:

1. John Cross DCM. Red Jungle. Robert Hale Ltd, London; p 14.
2. Ibid 41
3. Ibid 86
4. Ibid 85-7
5. Ibid 88
6. Ibid 93
7. Ibid 101
8. Ibid 129
9. Ibid 131
10. Ibid 148
11. Ibid 175
12. Ibid 183
13. Ibid 185
14. Ibid 205
15. Ibid 225
16. Keith Jeffery, MI6 – The History of the Secret Intelligence Service 1909-1949. Bloomsbury, London 2010; p580-1.



Champagne - Worth the label ?

By Tastevin

As a newly arrived subaltern, I was once advised by a knowing senior officer always to woo young ladies with champagne – “It’s like Double Diamond,” he considered. “It works wonders”.

True or not, the role of champagne always had for your correspondent something of a question mark around it. The price was usually unaffordable outside of duty-free areas, and the taste was either too subtle for my rude palate or (my opinion) non-existent.

Given the advent of the festive season, and in the spirit of offering some guidance to our readers, your correspondent therefore selflessly launched into a full investigation of the subject, at no small cost to the personal exchequer, it should be added.

Champagne was discovered accidentally by a near-blind Benedictine monk, Dom Pierre Perignon, who in 1688 had been appointed cellar-master at Hautvilliers Abbey, near Reims. He found that wine bottled during the cold winter started to re-ferment in the bottles during the warmer spring weather. Having established that the new bubbly wine was rather pleasant, he quickly developed bottles made of heavier glass to stop them exploding under the pressure, and perfected a means of sealing the bottles with an improved cork and wire cage.

The procedure was refined by a young woman called Nicole Clicquot, who took over her husband’s champagne business after being widowed at the age of 27. She perfected the riddling and disgorgement processes described below, and proved herself a business woman ahead of her time, and the first grande dame of champagne. Today, Reims remains as the centre of the champagne business, in the region now known as Champagne.

This region of Northern France is home to some 19,000 growers and nearly 300 Champagne Houses who account for 67% of the champagne produced. Two thirds of this is produced by a small number of these producers. By law, however, they are only entitled to hold 12% of the vineyard area, and are thus reliant on the growers for their produce.

At first sight, the Champagne region might be thought a less than ideal area for grape cultivation. With a cool continental climate and an average temperature of only 16 degrees C during the growing season, the climate is marginal for healthy growth. Winter freezes, spring frosts and sheer bad weather can all upset the vines during the season.

Vines are therefore planted on slopes, on the basis that the colder frosty air will descend to the bottom, and the vines are trained high, above the frosty ground levels. The predominately chalky soil of the region provides good drainage, albeit requiring regular



applications of fertiliser, and there is a developing trend to minimise the use of synthetic varieties.

Three main grape types are used in champagne, and it might be surprising to note that two of them are black. Chardonnay is widely planted in the sub-regions of Cote des Blancs and Cote de Sezanne, Pinot Noir in Montagne de Reims and Cote des Bar, and Meunier in the Vallee de la Marne, where it thrives particularly well, as it buds late and thus escapes the spring frosts. The intention of the grower is to produce a white wine, and care has thus to be exercised at all stages of the wine-making process to avoid colouring the grape juice. Mechanical harvesting is not permitted, grapes are not destemmed or crushed, and pressing takes place quickly, often in the vineyard itself. The pressing is as gentle as possible, and in order to maintain quality only 102 litres of juice can be extracted from 150 kilos of grapes. The first 82 litres is called the cuvee and the remaining 20 litres the taille. The best champagnes are only made from the cuvee.

The best producers will store and ferment the cuvee and taille from each grape variety and each grower separately, another example of the care which surrounds the production. Fermentation of the juice takes place after sedimentation, normally in large steel vessels, where the temperature can be controlled, although sometimes in oak vats or barrels. The eventual base wine produced is very dry, and neutral tasting with high acidity and medium alcohol. Most of this base wine is used to make up blends in the year following harvest, but some is kept in reserve in inert containers for use in future years.

At this stage, most wines will undergo a process called malolactic fermentation, something of a misnomer, as

it does not involve fermentation as such, but rather a procedure during which the harsh malic acids present in the wine are converted by bacterial action into the softer lactic acids. The choice of whether or not to opt for this lies with the grower, and will be determined by the style of wine he eventually wishes to produce. In the Champagne region, where so much depends on the uncertainties of the climate, blending is essential if the quality of the champagne is to remain consistent from year to year. This is where the reserve wines play their part, by smoothing out vintage variations and adding some complexity to the blend.

In achieving a house style, it is obviously best if the blender has access to as many base and reserve wines as possible. It is not unknown for the large producers to include as many as 70 in their final blend. Even vintage champagnes are blended, albeit not with reserve wines. The next phase is secondary fermentation, which takes place in the bottle, known as the Methode Champenoise. Some stabilisation takes place before this to remove tartrates, which might otherwise produce unwanted deposits.

Once the blend is finalised, a small amount of liqueur de tirage is added. This consists of some wine, yeast, yeast nutrients and a clarifying agent to facilitate deposition of particles in the wine. The bottles are then sealed with a crown cap and a plastic insert and stored horizontally in a cellar at a temperature of 10–12 degrees C. The secondary fermentation at this temperature is necessarily slow, and takes place over six to eight weeks. This encourages flavour development, and allows the carbon dioxide from the fermentation to permeate the wine, thus producing the eventual sparkle, and a bottle pressure of about six atmospheres.



On completion of fermentation, the yeast dies and forms a sediment of lees in the bottle. Over a period of months or years the dead yeast cells break down in a process called autolysis, which releases proteins and other compounds into the wine, contributing to the eventual bread, toast and biscuit tastes of all sparkling wines made in in this fashion.

Once maturation is considered complete, the sediment of lees is removed by the processes of riddling and disgorgement. Traditionally, riddling was done manually over a period of up to eight weeks, and involved successive movements to incline the bottles slowly from the horizontal to a vertical position. Present day automated processes using gyropalettes accomplish this in eight days, but the traditional method is still employed for bottles of unusual size or shape.

In disgorgement, the neck of the bottle is submerged in very cold brine solution to freeze the neck of the bottle. The bottle is then restored to the normal upright position, the crown cap seal removed and the bottle pressure allowed to eject the frozen wine, sediment and plastic insert. The bottle is topped up with liqueur d'expédition and sealed with the traditional cork and wire cage. The complete process is now fully mechanised, and takes only a few seconds from disgorgement to corking the bottle.

The liqueur d'expédition is a mixture of wine and cane sugar in solution, and is critical in further maturation and in determining the eventual sweetness of the wine. The amount of sugar added is called the dosage, and is important in balancing the acidity of the champagne as well as assisting in flavour development. Modern styles of champagne are usually off-dry or dry, although they can be found ranging from the very dry Brut Nature with minimum sugar levels, through Brut and Extra Sec at the off-dry level, to Sec which is medium dry. Demi-Sec, despite the name, is classed as sweet. A century ago, most champagne sold was sweet, an indication of how tastes have altered.

Quality champagne is allowed to mature for a further few months to allow the liqueur d'expédition to fully integrate with the wine. The sugar in the dosage continues to react with the proteins arising from the autolysis to develop new flavours of walnut, honey and toast, thus adding to the complexity of the wine. To the serious wine buyer, this makes the date of disgorgement important, and a number of producers do show this on the label.

Non-vintage champagne accounts for the great majority produced, and each producer seeks to develop an individual house style, ranging from dry and crisp to rich, yeasty and full-bodied. By law, non-vintage champagnes must remain on the lees for twelve months, and have a total ageing time of fifteen months. Vintage champagne is only made in the best years, and only from grapes of that vintage. Only 80% of the grapes produced in the harvest can be used, in order to maintain stocks of reserve wine. Vintage

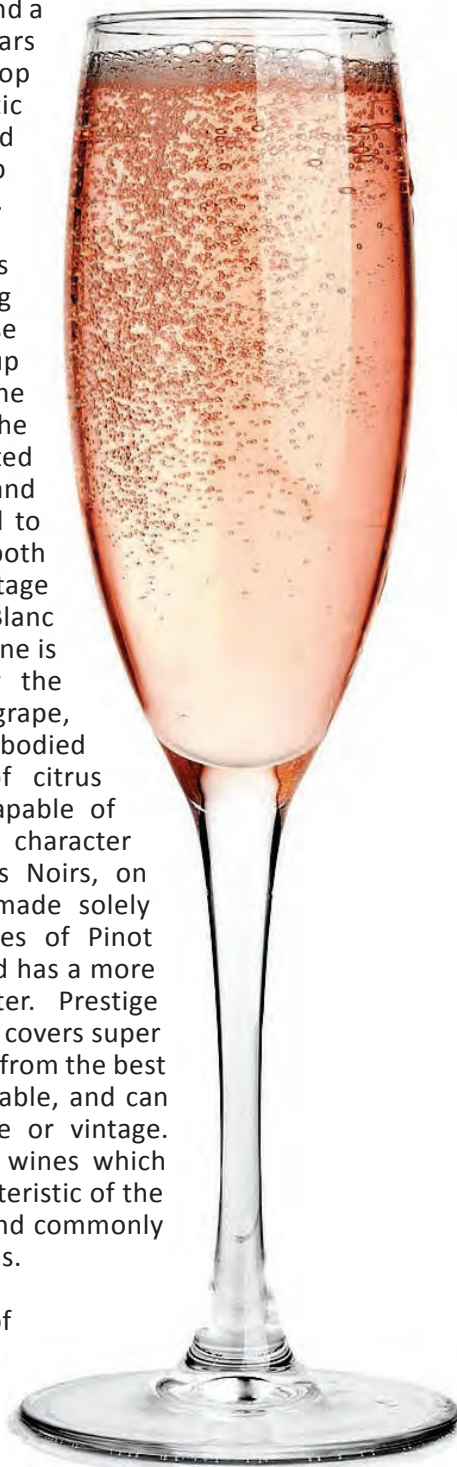
champagne must spend a minimum of three years on the lees to develop the characteristic yeasty quality, and some producers keep them for much longer.

Rose champagne is produced by blending red and white base wines at any stage up to the addition of the liqueur de tirage. The fruity tastes imparted fade with time, and such wine is unsuited to ageing, although both vintage and non-vintage styles are produced. Blanc de Blancs sparkling wine is produced using only the white Chardonnay grape, and produces light bodied wines with notes of citrus and green apples, capable of developing a buttery character with age. Blanc des Noirs, on the other hand, is made solely from the black grapes of Pinot Noir and Meunier, and has a more obvious fruity character. Prestige Cuvee is a term which covers super premium wines made from the best parcels of wines available, and can be either non-vintage or vintage. They are exceptional wines which should be very characteristic of the individual vineyard, and commonly sell for very high prices.

Other areas of France also produce sparkling wines, all made by the Methode Champenoise.

The term Cremant covers seven sparkling wine Appellations Controlles, the most important being Cremant d'Alsace, Cremant de Limoux, Cremant de Bourgogne, and Cremant de Loire. They are all limited to an extraction rate of 100 litres of juice to 150 kilos of grapes, and must spend nine months on the lees. In general, all these wines are made using regionally grown grapes, although the aromatic varieties such as Gewurztraminer and Muscat are not used. These wines can be of high quality, and are usually reasonably priced.

The Loire valley is the biggest producer of sparkling wines in France after the Champagne region, and as well as Cremant de Loire, it includes Saumur Mousseux and Vouvray AC. The former can be made from a range of local grape varieties, including a sparkling red using





Cabernet Franc. Vouvray AC can only be made from Chenin Blanc.

Elsewhere in Europe, Cava sparkling wine is made in several regions throughout Spain using the Methode Champenoise, although the majority is produced in the Catalan area around Penedes. The production rate is similar to Cremant at 100 litres per 150 kilos of grapes, with the wines spending nine months on the lees. Local grape varieties are used, although Chardonnay and Pinot Noir are now permitted. Few Cavas are intended for long term ageing, and most are available at modest prices.

Italian Prosecco is enjoying an upsurge in popularity as an affordable, fresh, slightly sweet sparkling wine with distinct apple and melon flavours. It is produced by the tank fermentation method, which does not allow for long term storage on the lees, and can be bottled relatively quickly for immediate consumption. There are two delimited regions: Prosecco DOC, which covers a wide area of the Veneto and Friuli in North East Italy, and the higher rated region of Conegliano-Valdobbiadeno DOCG. The grape variety was formerly known as Prosecco, but has latterly been changed to Glera to prevent confusion.

Sekt is the sparkling wine of Germany, also produced by the tank fermentation method. The term Sekt on its own on the label indicates wine made from grapes grown in Europe, whereas the term Deutscher Sekt indicates grapes grown exclusively in Germany. Further up the quality scale, Sekt made from one of the 13 designated wine areas will bear the title of Deutscher Sekt b.A. The best Sekt is made from Riesling grapes, and some premium Sekts are made from the top vineyards.

Asti sparkling wine is produced by a method which does not involve the production of dry wine. Instead,

the unfermented grape juice or must is stored at near freezing temperature until it is needed, and then warmed to allow fermentation to take place in pressurised tanks. The carbon dioxide produced is allowed to escape until the alcohol concentration reaches about 6%, when it is retained and the fermentation continues until a concentration of about 7.5% is attained, and the pressure is close to five atmospheres. The fermentation is then stopped by chill filtration and the wine bottled for immediate sale.

The cheapest method of producing sparkling wine is simply to bubble carbon dioxide through still dry wine, a method which certainly imparts the bubbles, but does nothing to alter the taste of the wine. This is not considered to be a satisfactory method of producing quality wine.

Excellent sparkling wines are made in the New World countries, with Australia, New Zealand, South Africa, and the USA all producing highly regarded wines – to do them full justice would be the basis of another article!

Those whose interest has taken them this far will be impressed to learn that good quality champagne is also made in the United Kingdom. It happens that 2014 was a bumper year, with over four million bottles produced, using the classic champagne grapes of Pinot Noir, Meunier and Chardonnay. Top vintages can be had at the affordable prices of £20-£30 a bottle from the better supermarkets. Camel Valley, Leckford Estate, Jenkyn Place and Nyetimber are among the foremost producers.

For completeness, a word about the storage and treatment of champagne is appropriate, on the premise that not many of us can or would wish to use our sword to slice off the cork in swash-buckling cavalry fashion, or keep the odd crate in the back of the car for eventualities.

Champagne should be stored long term at a constant temperature of about 10-12 degrees C, away from strong light and vibration, and served well chilled at 6 – 10 degrees C. The pain-free method of opening the bottle is to be aware of the considerable pressure in the bottle, and carefully remove the foil, loosen the wire cage, and holding the bottle away from the body, grip the cork with one hand, the base of the bottle with the other, and turn the bottle, not the cork. The gas should be allowed to escape quietly, not with an explosion and flying cork.


The wine should then be served in a flute shape glass, which will allow the bubbles to keep flowing and concentrate the aromas. The glass should not be cooled, as this inhibits the bubble formation, nor should it be swirled – champagne is not a cocktail! Any temptation to shake the bottle and cause a fountain of wine to spray your friends should be resisted and left to Formula One drivers and euphoric sportsmen celebrating victories.

So there we have it – compared to normal wine production, champagne involves a protracted and lengthy process, with much attention to detail at every stage. The grower may not see a return on his labours for some time, such are the periods spent in maturation at various stages, and when packaging, distribution and sales costs are added, perhaps the price should come as no surprise.

Given this lapidarian care which surrounds its production, it is probably impious or even downright sacrilegious to think of mixing the true champagne with additives to produce Buck's Fizz, Bellinis, Black Velvet or whatever, when less costly and more neutral

tasting alternatives are available. It has however been contended by certain retailers conscious of their status in society that the high price we pay is all part of the champagne experience. We leave it to the reader to judge!





SELL / BUY YOUR UNIFORM!

Have you any unwanted Army uniforms cluttering up your accommodation?
Or
Have you outgrown your present uniform and wish to upgrade?
The please contact me:

Major John Barrett MBE
Corps Uniform Dress Hire
Headquarters Mess Royal Signals
Blandford Camp, Dorset DT11 8RH

Tel/Fax 01258 481999; Mil 94371 3999;
Mobile 0777 095 8870; Home 01963 23375.
EMAIL: jbrectory@aol.com

We also hire accoutrements including:

Swords, Silver Scabbards, Sashes, Sword Sling, Gold Knot, White Gloves, Epaulettes

Uniforms for sale may be brought to me personally, or sent by post. We return you 70% of the proceeds, remainder goes to Corps funds.



Zeitgeist

- The Spirit of the Times

The task of sponsoring the BAOR picture commission was accepted in January 2014 by 1ADSR (now 1 Sig Regt) then under the command of Lieutenant Colonel Jules Hill. The lead was taken by the Second in Command, Major (now Lieutenant Colonel) Alan Garrett, with Captain David Malortie as project officer. The task of representing such a long period of service in Germany was a challenge, and the concept adopted was that of representing the changes in equipment and uniform through time to the present day. The eventual painting produced by the selected artist Stuart Brown, is shown above.

The approach chosen was to create a single scene, at first sight looking quite natural, but on closer inspection revealing the chronology and significant landmarks of our presence in BAOR. The former Soviet listening station on the Brocken is shown in rather sinister low cloud, redolent of the all-pervasive Soviet threat of the time. Just visible through the trees is the Bismarck tower, named after the Iron Chancellor who played a key role in the development of modern Germany, with the Schloss at Bisperode, the focus of many exercises, indicated left. Flying above the forest are a pair of RAF Harrier ground attack aircraft, for which Royal Signals provided tactical field communications.

The first element (left) is a Bruin communications vehicle, with soldiers erecting the radio mast, wearing 1950s battle dress. The next element depicts an armoured headquarters with interconnecting penthouse tents. The vehicle on the left is an AFV 439; the figures wear

58 pattern webbing and carry the SLR personal weapon. The third element shows a BOWMAN Landrover with operator, the foreground figures wearing CS95, and carrying original pattern SA80 rifles. The final scene reveals a modern day operator on TAC SAT, wearing Osprey body armour and carrying the SA80 with the new fore grip attachments. A female soldier is included in this group, which is complemented by a MAN truck with communications mast.

The Rhine defines Germany both physically and emotionally, and identified the role of so many signallers, namely those of the British Army of the Rhine. It has featured prominently in the consciousness of Royal Signals, bisecting the rear and forward zones, in which so many of the Corps operated, exercised and lived. The progression of equipment and soldiers demonstrates the evolving role of the Corps, from NATO defence to Out of Area operations, and exemplifies the combination of our Corps ethos with the environment and soul of our hosts across the decades – the Spirit of the Times, or in German, Zeitgeist.

Limited edition prints of the painting are available in high resolution digital capture from the original painting, with layout into print artwork with border, caption and unit badges as required. The lithographic print run is on heavy 350 gsm art board, approximately 70 x 50 cm signed by the artist and numbered in flat packs of 100, supplied with certificates of authenticity. Anyone interested in purchasing a limited edition print should contact: zeitgeist@royalsignals.org

UK Mobile Force (UKMF)



By Lieutenant Colonel Peter Richards

In 1978 the World was a different place. In Europe the Iron Curtain had been in place since 1945 and the Berlin Wall since 1961. The US and Western Europe formed NATO. The Soviet Union and Eastern Europe responded with the Warsaw Pact. Both sides had thousands of nuclear weapons ranging from multi-warhead strategic missiles down to “tactical nuclear weapons” fired from heavy artillery.

After 1945 the West mainly disbanded its armies but relied upon its nuclear weapons as a deterrent to Soviet aggression. There was a “trip-wire” philosophy whereby any attack would be met with an immediate nuclear response. During the 70s it was felt that this plan lacked credibility so it was replaced with “graduated response”. Any aggression was deemed to be a “mistake”. Our response would be to initially meet the aggression with conventional forces to buy time. If the politicians were unable to resolve the situation then NATO would “go nuclear” after, for planning purposes, some seven days. In the 1st British Corps we guarded the “sites” where the tactical nuclear weapons were meant to be, although none of us knew whether the sites held anything or not, we practised “outloading” them and spent many a night trundling around West Germany in the dark, guarded by mechanised infantry, to set up Nuclear Ammunition Supply Points. Major exercises always included “nuclear release” practise by the heavy howitzers after which it was ENDEX and everyone “went home”. We all knew that if/when they were fired for real then it would be “the end” for the survivors of the “conventional phase”.

The Warsaw Pact was one huge military camp. Ordinary people lived like slaves so that a massive part of the GDP could be spent on the military. There was universal conscription. The secret police were

everywhere, the East German STAZI, being particularly notorious, and the Gulag beckoned for dissenters.

The Warsaw Pact had a massive conventional superiority. Their first echelon of Russian and East German Armies, the Group of Soviet Forces Germany (GSFG), had the very best equipment and numbered tens of thousands of armoured vehicles. They were formidable in every area; air defence, EW, Airborne, amphibious assault, and there was their “SAS” the Spetznaz. Our exercises always included the assumption that the Warsaw Pact had air superiority. It is hardly surprising that some NATO members felt intimidated! The Danes, in particular, watched routine massive “live firing” Warsaw Pact exercises in the Baltic, on their doorstep, by truly impressive naval, amphibious and airborne forces.

It was decided to form a UK Mobile Force (UKMF) which could be rapidly deployed to the flanks of NATO, particularly Denmark and Italy, at “times of tension”. This was a political gesture of solidarity. The UKMF was a “light” brigade with a PARA Battalion forming the Lead PARA Bn Battle Group (LPBG). SH, Chinook and Puma, would be in support. The plan was that the LPBG would go in by C130 with the balance getting there as quickly as was possible. The UKMF would “dig in” on arrival –and wait. It was clear that if anything happened “for real” that we would only last for a couple of hours.

It is a good maxim that you should hope for the best but plan for the worst. If the worst happened then we needed a plan. Being a prisoner of the WP was unlikely to be softened by the Geneva Convention and the opportunity to form an escape committee! Stalin’s secret police had exterminated all the officers of the

Polish Army in 1939/40 with a pistol shot in the back of the head; all 30,000 of them. Of the survivors of the German Army at Stalingrad, about 100,000, only 6000 returned to Germany alive. UN prisoners, captured by the North Koreans, 1950-53, had been treated brutally and had suffered the infamous "brain washing".

We had no armoured vehicles and our "soft" wheeled vehicles were very unlikely to survive. In any case, a war was likely to start the biggest traffic jam in history as tens of millions of people across Europe tried to flee. The WP boasted that they would be at the Rhine in 24 hours but the German Chancellor responded that only if they could get past the traffic jams. The reality would have been much, much worse with WP ground attack aircraft making the destruction of Iraqi forces fleeing Kuwait look like child's play.

The simple plan was that we would all train to cover 40 miles on foot across country as fast as was possible but in not less than 24 hours. Armoured forces need to stop to resupply with ammunition and POL, normally each night, and it was hoped that we could get ahead and break clean. Each man would carry a weapon (of course) and a load of 30lbs including ammo, water, a 24 hour ration pack and his NBC kit. The training was an "individual event" because everyone had to learn that they held the key to their own survival. March or die!

In Denmark/Schleswig Holstein the prospects were bleak. We came under command 6 German Panzer Grenadier Division. There was going to be hard fighting. Forty miles would get you to the North Sea

and then what? In Italy the prospects were better. The attack would be by "lower grade" WP formations, channelled by the Gorizia Gap between the Dolomites and the Aegean Sea. The break clean would be into the Dolomite Mountains where there was greater opportunity for escape.

As it happened, President Reagan and PM Thatcher did not blink. They deployed cruise missiles. The task of building defences against this unique threat broke the economy of the Soviet Union. Michael Gorbachev recognised this. He knew that it was all over. In December 1987, Mathias Rust landed his light plane in Red Square having successfully evaded, at low level, all the Soviet Air Defence systems. Gorbachev seized the opportunity to sack swathes of the Soviet High Command. In 1989 he declined to support the East Germans against their own people and the Berlin Wall fell. The rest is history.....

But what of the 40mile march? In 1982 the Argentinians seized the Falklands. This was totally unexpected. Further, it was not going to be the armoured war for which everyone had trained. There were only a handful of vehicles and most Chinook helicopters had been lost on the Atlantic Conveyor. Everyone was going to have to "tab" from San Carlos to Port Stanley a distance in excess of 40 miles. Nobody had trained for this...except those men from the UKMF.

The 40 mile march is still going today. No matter what the doctrine or the technology the fact is that, sooner or later, determined men will have to march or "tab" a long way carrying a heavy load.....





ROYAL SIGNALS HONOURS AND AWARDS

There are a number of ways in which the remarkable deeds and truly outstanding abilities of Royal Signals officers and soldiers can be recognised:

- The State Honours process (for New Year Honours, Queen’s Birthday Honours and Operational Honours Lists),
- The Corps’ own annual awards process (for Princess Mary Medal, RSI Silver Medal, Master of Signals Award and the Medal for Adventurous Endeavour),
- An annual process of nomination for awards from external bodies and
- A rolling process of nominations and awards for the Master of Signals Commendation.

Sadly, but almost inevitably, the timeline for each of the honours and awards processes is different. The State Honours process is well documented elsewhere; this article gives the key details of the remaining three awards processes.

Royal Signals Annual Awards. The Corps own annual awards process culminates in an awards ceremony at the Royal Signals Institution (RSI) London Lecture and Dinner each November where typically six to eight individuals are recognised through the award of the Princess Mary Medal, the RSI Silver Medal, the Master of Signals Award and the RSI Medal for Adventurous Endeavour. The selection of worthy individuals is made by the RSI Awards Committee on the basis of citations submitted by the chain of command covering the previous year (April to March). The details of each of these awards are as follows:

Princess Mary Medal. This is the highest RSI Award and may only be presented to serving or recently retired members of the Corps who are full members of the Institution. It must be regarded as a rare honour given to mark an individual achievement, contribution or service of the highest order that is considered to have enhanced greatly the performance, reputation or status of the Royal Corps of Signals, or a prolonged period of dedicated service. Up to one medal may be awarded in any year.

RSI Silver Medal. This is an award to mark the attainment of an outstanding individual professional achievement in the Corps. This award may also be made to an individual for conduct or achievement in an operational theatre, where such conduct does not match the standard of the Princess Mary Medal. In addition, those attaining an exemplary standard on higher level professional courses may also be considered for the award. Typically three or four of these awards are made each year.

Master of Signals Award. This award is a formal recognition of a special contribution or service to the Corps made by an individual or corporate body which cannot be properly accommodated by either the Princess Mary Medal or the RSI Silver Medal. This award is open to individuals outside the Corps who have contributed significantly to the performance, status or reputation of Royal Signals. Typically, two awards are made each year.

Medal for Adventurous Endeavour. This award is intended to recognise outstanding achievement or service by a member of the serving Corps arising from exploration, expeditions or adventurous endeavour. Normally, up to one award is made each year.

Timings. The annual timeline for the Royal Signals Annual Awards process is as follows:

- 31 Mar End of (12 month) reporting period
- 1 May Names of nominees (but not citations) to HQ Royal Signals
- 1 Jul All citations to HQ Royal Signals
- 1st Thursday in October Awards announced
- 3rd Thursday in November Awards presented at RSI London Lecture and Dinner

Whistler Trophy. The Whistler Trophy for excellence at Regimental Duty is open to all subalterns and junior captains and is awarded annually. For simplicity, the Whistler Trophy nominations and selection procedures for the period follow the same process and timeline shown for the Royal Signals Annual Awards except that the award will be presented at the Corps Guest Night following the announcement.

External Awards. Each year the Royal Signals is asked by three external bodies to identify suitable individuals to receive recognition and an award for their operational signalling and operational engineering prowess over the previous 12 months. Details of the three awards in question are shown below:

The Churchill Medal. This is the premier prize awarded annually by the Professional Engineering Institutions for Defence engineering achievement. The award is for an individual or a small team (the majority of whom are serving members of the Armed Forces or were serving at the time) for “achievement in Engineering and Technical Advancement in support of Military Operations”. This award is open to all three services and to all cap-badges within the Army. Whilst any CO or line manager across the MoD can independently submit a citation direct to the Institute of Engineering and Technology, HQ Royal Signals runs its own ‘filter board’; giving added endorsement to what it judges to be the best citation from across the Corps. Citations should not exceed 1000 words and can include a maximum of one diagram and one photograph.

The WCE Royal Signals Operational Engineering Award. This medal is awarded annually by the Worshipful Company of Engineers (WCE) to the Royal Signals officer who has “best applied professional engineering judgement or technical innovation to contribute significantly to the maintenance or enhancement of operational capability or effectiveness in any theatre of operations, including the UK”. This recipient of this award will be decided by the RSI Awards Sub-Committee. Citations should be roughly 500 words (1 page of A4) in length.

The WCIT ‘Through’ Award for Operational Military Signalling. This award was inaugurated in 2012 by the Worshipful Company of Information Technologists (WCIT) to recognise the 20th anniversary of the formal affiliation between the Royal Signals and WCIT. Eligibility for the ‘Through’ Award is restricted to Royal Signals soldiers, non-commissioned officers and warrant officers who have made “an exceptional contribution to the provision of information services on operations, in support of operations or in supporting the training of others preparing for operations”. The eligibility criterion goes on to say that “a successful recipient will, in particular, thereby have displayed conspicuous levels of innovation and determination”. Once again, this award will be decided by the RSI Awards Sub-Committee. Citations should be roughly 500 words (1 page of A4) in length.

Timings. The annual timeline for the External Awards process is as follows:

- 31 Mar End of (12 month) reporting period
- mid-April Full citations to HQ Royal Signals
- late-April Winning citations passed to IET, WCE and WCIT
- mid-May Awards Announced
- mid-July Awards Presented

Master of Signals Commendation. Whilst a prestigious award, the Master of Signals Commendation is intended to be given to a greater number of recipients and for achievements that do not merit a higher award. It is therefore recognised as the lesser of the RSI awards. Nominations can be submitted at any time. If agreed by the Corps Colonel and the Master of Signals a suitable presentation can then be made under local arrangements. An absolute minimum of four weeks should be allowed between receipt of the citation and the intended presentation date. Typically about thirty commendations would be awarded each year.

Citations. The template to be used for all citations can be found on the HQ Royal Signals pages of the Defence Intranet or is available from the Corps Adjutant or the RSI Secretary (see page 81 for contact details). Where appropriate a single form can be used to nominate an individual for multiple awards. All nominations and citations must be sent electronically to the Corps Adjutant or the RSI Secretary.

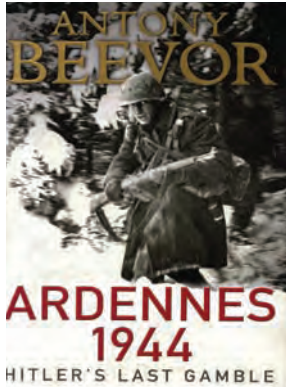
Awards Committee. The RSI Awards Committee reserves the right to consider nominees for an alternative award. Any unsuccessful nominations for the Royal Signals Annual Awards will be automatically reconsidered for a Master of Signals Commendation.



BOOK REVIEWS

ARDENNES 1944

By Antony Beevor



Antony Beevor is a renowned military historian and a former 11th Hussar. His gripping review of the ArdenNES battle is satisfying both for the professional soldier and for the historian. He has an impressive gift for describing the chaos and savagery of battle, whilst still conveying a strategic sense of events.

Here he gives a fresh view of Hitler's last desperate attempt to mount a counter-offensive to stem the final onslaught on Germany. In August 1944, the Allies were euphoric. On the Eastern Front, the Red Army was at the gates of Warsaw. In the West, Allied forces surged through Belgium. Hitler had only narrowly escaped the Stauffenberg bomb. It looked as if German disintegration had begun.

But Operation Market Garden deflated allied expectations and harmed the Alliance. Beevor writes of US irritation at poor British leadership in the September operation to seize the Rhine bridges and at British arrogance and condescension. "General Montgomery, the grandstanding and egocentric 21st Army Group Commander exacerbated this, noisily supported by the jingoistic British press."

Into this prickly alliance, Hitler conjured up a vision for an offensive through the thickly wooded and hilly ArdenNES region. His surprised generals pointed out their lack of fuel and the priority of stopping the Red Army advance in the East. Hitler would not hear of it: personally marking his final orders "Not to be altered". Army commanders were told merely to pass his orders downwards.

The Allies refused to believe in a German offensive, but they underestimated Hitler's manic grasp of the levers of military power. And as at Arnhem, the few warnings by worried allied intelligence officers of unwelcome enemy activity were ignored.

So on 16 December 1944, the Germans gained almost complete surprise: shocked US troops called for fire on their own positions as they were overrun. For the most part the inexperienced forward US units fought

well, buying time for US and British reinforcements to arrive. The fighting was savage. The fanatical Joachim Peiper's SS Panzergrenadiers described "wading through American corpses". The US 82nd Airborne used German dead as sandbags. Prisoners were murdered on both sides, first by the SS, then in retaliation by US soldiers, sometimes with the tacit approval of their officers.

The speed of the US recovery was impressive; in the opinion of some German generals their operation was doomed by the end of the first week, having failed to achieve a breakthrough. By Christmas Day it was clear to all except Hitler that the offensive had run out of steam.

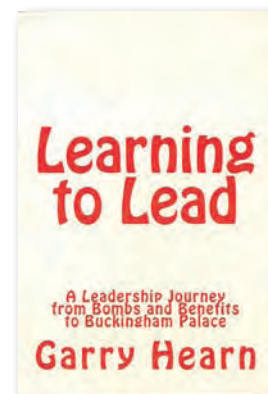
The lessons drawn by Beevor are familiar and no less powerful for being forgotten several times since 1944: the danger of ignoring inconvenient intelligence, the need for leaders to control retaliatory savagery and finally, the need for allied commanders to show respect for each other.

The lasting theme of this excellent book is the gallantry of the untried US formations who took the shock of the initial attack. In 1944 the battle-hardened German Army affected to despise the relatively green US soldier. But, says Beevor, "Isolated US infantry companies defended key villages against overwhelming odds, bought the time needed to reinforce and so destroyed Hitler's dream. Maybe the German leadership's greatest mistake was to have misjudged the US Army."

Major General Bill Robins

LEARNING TO LEAD - A Leadership Journey

By Garry Hearn OBE



Garry Hearn indicates elsewhere that this book offers insights into 35 years of leadership and the lessons that he has learnt. He is perhaps uniquely qualified to write about leadership, having been born to parents who travelled the world with the Army. He joined the Army as a private soldier, subsequently serving in several countries, including two operational theatres, and was made an OBE for his services to military leadership and education. Becoming a CIS Engineer, he nevertheless sought and achieved experience in

a broad range of challenging and diverse military roles. 'Learning to Lead' encapsulates the relevant transferable knowledge and experience gained from an unusual and distinguished career, but in a manner which is down-to-earth, unpretentious and, above all, entertaining. His positive belief that 'all people have potential all the time' is heart warming and shines through the narrative from beginning to end.

His 'leadership journey' begins with engaging, humorous but relevant examples of day-to-day leadership experiences, initially from the perspective of being 'led' and later developing into a junior leader building upon modest educational achievements. Throughout, he provides a deceptively thoughtful narrative with summary 'lessons', which relate directly to the examples and a surrounding story. This approach provides the reader with a range of pointers, all of which address the challenging and formative aspects of early leadership. For example, he covers the importance of resilience with (inevitable) personal failure and disappointment; and the perils of blurring friendship and leadership ('familiarity breeds contempt'). Most aspects will be familiar to military readers, but may well be of value to those who are new to leadership roles or who wish to evaluate their performance as a leader - whether it be a military or civilian role. Many heavyweight works have been written on leadership, but this book puts the subject refreshingly into context with a revealing analysis - beginning with the viewpoint of a private soldier.

The theme emphasises the importance of judging people on performance, not on background, and points up various pitfalls - including that of 'first impressions'. He covers the formative 1980s period with several amusing but highly relevant vignettes of BAOR, together with comments on the anachronisms of military life of the time and the complementary frailties of human nature, much of which will strike a chord with many readers. Resigning his Commission in 1988, he entered civilian life for two years, thus gaining an unique opportunity to review a varied career and decide how best to develop into the future. Re-joining and eventually moving into more senior roles, commencing with regimental command, he covers a range of leadership issues - from handling trade union challenges, through to grievance and disciplinary matters. Further experience at a senior level enabled him to develop and implement his particular brand of empowered decision-making, including that of encouraging pro-active challenge to out-dated policies and making improvements, and constructing the necessary 'vision' to take a major organisation forward as a whole, underpinned by the concept of 'continuous development'.

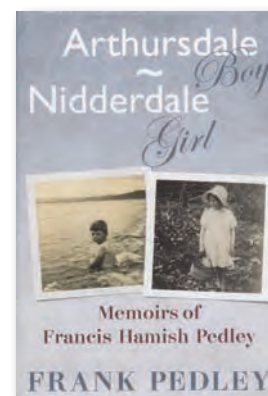
Rounding off the 'journey', it is clear that the author's high point was his penultimate role in the Army: commanding and transforming the Defence College of Communications and Information Systems. Since retirement he has continued his own academic and professional development with three Masters level degrees, including an MBA, together with

two professional fellowships to support his current leadership and educational roles. This is therefore a book that has much to offer to those wishing to follow a similar, successful career path. There is little to dislike about the book; a few may disagree with some of the views, but leadership is a dynamic concept that needs to be adapted to different situations, personalities and roles - both profit and non-profit. Some may find the contents of a few of the examples challenging. Others may be frustrated by the vagaries of digital typesetting and the lack of a traditional proofreader! But these are trivial points in what is otherwise a thoughtful, valuable and highly readable book which provides a wealth of relevant signposts for those who aspire to become successful leaders.

Brigadier Mike Taylor CBE DL
ISBN 978-1-5087-0338-9 Published by Amazon

ARTHURSDALE BOY – NIDDERDALE GIRL **The Memoirs of Francis Hamish Pedley**

By Frank Pedley



There many reasons why people choose to write memoirs: to set a record straight, give one's own version of events, stake a claim for individual glory, or just occasionally there are other, higher motives.

This book is a celebration of a military career, an exceptionally happy marriage, and a life well spent. It is intended as an account to inform present and future descendants, and as such is an unusually complete, revealing and compelling narrative. It much deserves a wider audience.

Both the author and his wife kept extensive diaries, records, cards, notes, e-mails and other material relating to their lives, and when set against the background of contemporary international events, constitute a story which is as uplifting as it is enlivening and compelling.

Lieutenant Colonel Frank Hamish Pedley rose above the circumstances of his birth through the support of his grandparents to attend grammar school and undergo officer training at RMA Sandhurst. He describes his youth growing up in the war years in

Yorkshire, his years at Tadcaster Grammar School, where he was able to give full vent to his love of sport and outdoor activities, especially cricket. His early meetings with his future wife Ruth showed much promise, but this early contact ended abruptly when her father died and she had to leave school shortly afterwards.

After leaving, and a short time as a supply teacher, he was accepted for RMA Sandhurst, and following success at the Regular Commissions Board, underwent four months infantry training with the Green Howards, before reporting to RMAS in April 1953. A concentrated sixteen months of applied effort saw him graduate very creditably in August 1954, to start his career with the Corps.

Shortly before departing on his first posting to 18 Army Group Signal Regiment, in Essen, he made contact again with Ruth, and arranged to meet. This short encounter confirmed that they still had feelings for each other, and it was with an undertaking to stay in contact that he departed for his first unit.

Their romance took its inevitable but gradual course, and following their marriage they settled into military life, which saw them move to Germany, Catterick, and on secondment to the Malayan Army. Success in the Staff College entrance examination (taken in Malaya) followed, and a subsequent posting to 6 Infantry Brigade Group, from where he was to obtain the essential recommendations needed to ensure selection to attend Camberley.

Post Staff College tours to Yorkshire, NORTHAG Air Support Signal Squadron, the Ministry of Defence and 21 Signal Regiment followed, before his selection for promotion and command of 38 Signal Regiment in Sheffield. This tour confirmed their resolve to remain if possible in their native Yorkshire, even if it meant a career limiting decision - a situation which many have had to contend with.

After a successful tour in command, he was able to remain in the North by his appointment as head of the Recruiting and Liaison Staff in North East District. By this time Ruth and he were the parents of three talented sons, the desire to put down roots was strong, and when the opportunity came to purchase a Grade 2 listed building and land in the village of Hunton, they seized the chance.

They took up the challenge of a project house with gusto, estimating that five years would be needed to turn it into the home they desired. Contact with local farmers awakened their interest in utilising their land, and it was not long before hens, goslings and sheep were to feature prominently. This tempo of life continued through his final Army appointment as OC White Helmets, during which time their knowledge and expertise in sheep rearing increased steadily.

On retirement, he took up the appointment of Army Careers Officer for West and North Yorkshire, and

shortly afterwards Ruth discovered Wensleydale Longwool sheep, and her interest was kindled. They subsequently joined one of the oldest sheep breed societies in the world, to learn more about this impressive breed, one of the best quality wool providers, and with a fascinating history.

Ruth's interest and commitment to her flock developed and grew, and she steadily acquired a reputation as a champion breeder at shows throughout the North of England as well the Royal Highland Show in Edinburgh. Her reputation soon led to her being appointed as a judge in these same competitions. This settled existence was complemented by a growing family, including grandchildren, who were to enjoy many happy times in Hunton.

After his second retirement, he accepted an invitation to be Chairman of the Rare Breeds Survival Trust, an endeavour in which he became very busy. In 2001 there took place the Foot and Mouth Disease outbreak, and although their animals escaped the epidemic, it was a close call, and a tense time, with many nearby flocks having to be put down.

Although able to take well-earned breaks by cruising and travel overseas throughout this period, by the time both were in their early seventies it was clear that Ruth and Frank's highly active life-style could not be sustained, and in mid-2006 they reluctantly decided to sell off their stock, which took place in stages over the next year.

Shortly after this, the unthinkable happened. Ruth was admitted to hospital for examination and treatment of a digestive complication. Sadly, shortly after returning home following optimistic prognoses, Ruth died. The health authorities admitted that they had made mistakes, and owned up to negligence charges. Their letters of apology were of little comfort.

Thus ends a volume which is by turns happy, funny, sad, subjective and uplifting, chronicling as it does the pleasures, pains, vicissitudes and triumphs of a military family, following a successful career all the while maintaining a happy and balanced family life. There are many who will see parallels with their own military experiences, and identify with the situations they had to deal with.

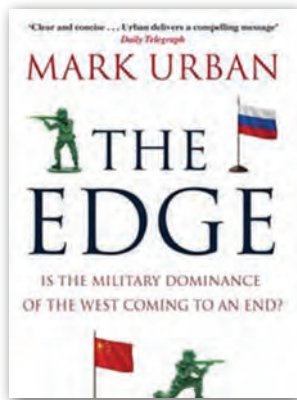
The book is well written and illustrated, and meticulously researched. It is thoroughly recommended.

Colonel Tom Moncur

Published by the Book Guild, 435 pages, ISBN978 1 910508 58 9. £17.99.

THE EDGE - Is the military dominance of the West coming to an end ?

By Mark Urban



Newsnight defence editor Mark Urban has produced a short, readable though inevitably journalistic assessment of reductions in Western military capability and the increasing reluctance to use what remains to shape international events and outcomes. He sees growing nationalism, the decline in the influence of supra-national bodies and post Cold War disarmament in NATO continuing whilst Vladimir Putin's resurgent Russia and the rise of Islamic fundamentalism threaten the existence of liberal Europe. Whilst hoping this will serve as a 'wake up' call he hints of little faith that anything more substantial than rhetoric will be forth coming. The recent UK Strategic Security and Defence Review largely bears out this bleak assessment.

Urban illustrates how, since the end of the Cold War and despite embarking on an almost continuous series of military adventures, the West has continued to pursue 'the Peace Dividend'. Whilst the events of 9/11 caused a brief pause, the impact of the 2008 economic crisis accelerated the process. He notes not only the fall in spending in absolute terms but also the increasing inefficiency of the spend as the overhead of Defence management takes up a relatively increasing proportion of the available resources. He suggests that precipitate reductions have often been based on conveniently optimistic strategic assumptions and those of us who worked on 'Options for Change' in 1990 may recall

the comment of a very senior MoD official who opined in July 1990 that it was inconceivable that in the next 10 years British armoured forces would be deployed to The Middle East in any substantial numbers!

Urban challenges the myth of technology as a 'force multiplier' or at least questions the size of the multiplication, particularly given the proliferation of military technology encouraged by the governments not least to ensure the survival of national and multi-national arms manufacturers. This has been a convenient presentational fig leaf to enable further economy whilst apparently preserving a greater measure of capability. These techniques of 'smoke and mirrors' appear now, at least in the UK, to embrace financial engineering to an extent that might make many respectable auditors feel uncomfortable!

But it is not only the reduction in capability that concerns Urban. He points to the risk averse culture which has grown up as a result of the strategic and operational failure of the West's interventions since 9/11 and the rise of 'terrorist' asymmetric warfare practiced by both state and non-state actors. He believes that the decline of western capability and will has effectively undermined the ability of supra-national organisations to manage events and that the rise in both relative and absolute terms of military capability in major states including Russia, makes regional conflict more likely and more dangerous particularly given nuclear weapons in the hands of regional powers

Urban's book, as one might expect from a defence journalist, is strong on facts and figures. It is lighter on analysis though he concludes that the reduction in military capability encouraged by the ending of a bi-polar world has sent a message that the 'West' is no longer willing or capable of sustaining the previous broad consensus in favour of liberal democracy however imperfect the reality. Whilst this may encourage the resumption of 'real politik' in international affairs, albeit with higher risk of conflict, its potential impact on western domestic politics may be even more malign.

Brigadier Cedric Burton

Obtainable from Amazon £5.99

LETTERS

Dear Sir

I write to report a strong sense of déjà vu, brought about by the report of the RSI Spring seminar in the latest Journal: The Brigade HQ as a "Platform", Journal Vol 33 Spring 2015, regarding a 'platform approach' to understanding, fulfilling and integrating the systems requirements of a Brigade HQ.

In 1984 I was an SO1 in the Defence Commitments staff, under Colonel Stan Gordon, AD EW/JW. The branch was developing a range of policies arising from the Falklands War's lessons learned. Despite considerable opposition from several quarters in the army staff, the Brigade HQ was identified as likely suitable for consideration in

policy development as a 'platform', similar to a carrier or an advanced destroyer, while the brigade and all its systems could be regarded in similar broad terms as a Carrier Task Group or Flotilla when considering weapons, surveillance, CIS and EW systems' integration and their further relationships with strategic and allies' systems, air and maritime support.

So, 31 years on, I wish my successors every good fortune in attempting to gain broad acceptance of the concept of 'Brigade HQ as a platform' in the pious hope that one of them doesn't get a déjà-vu, like mine, in 2045!

Yours Faithfully, Colonel John Roberts



REMEMBRANCE



Major General Peter A C Baldwin CBE



Peter Baldwin, who died on 15 September 2015, is notable for being the first Army Apprentice to reach two star rank.

He enlisted 20th January 1942 and joined the Army Technical School which, in those days before the WRAC, had the unfortunate shoulder title 'ATS'.

He was to the Sudan in 1946 with a contemporary former apprentice to be the only two radio mechanics in the theatre - such was the state of the army in those days!

He was commissioned into Royal Signals (1947) seeking an active life in telecommunications rather than be tied to a REME workshop environment.

An early posting to Berlin in 1947 to command an independent High Speed Wireless Troop coincided with the period of tension preceding the Airlift, lasting into the operation itself. These were exciting times for a young Signal Officer.

The Communist takeover of Nationalist China in 1949 called for a reinforcement of Hong Kong by a Heavy Anti Aircraft Regiment with all its Fire Command arrangements. As

Regimental Signal Officer he was despatched (by BOAC flying boat from Southampton Water) with the advance party to prepare the communications from scratch at strategic points around the Colony.

While in Hong Kong the Korean War erupted in 1950 and he was immediately sent to 27 Infantry Brigade as the second Royal Signals Officer (Nigel Pidsley was the OC Sig Tp) and within days the Brigade arrived in Korea as Britain's first land contribution to the UN force. The Brigade saw the 'movement' phase of that war and after a distinguished period of nearly a year the 'Cinderella' Brigade returned to Hong Kong.

The next posting was to No 1 Wireless Regiment in Munster, West Germany where he became Adjutant to Sidney Dagg and Peter Lonnon. In later years he also commanded the Regiment (then 13th Signal Regiment) at Birgelen.

A spell at HQ Eastern Command Hounslow was interrupted by a nine month stint in hospital. Notification of this admission into 'dock' came in the middle of the seven paper Staff College examination. The remaining four papers were taken (and passed) from a corner of a ward in Woolwich!

At the Staff College in 1960 he produced the pantomime, normally a recipe for a reasonable grading in the absence of any academic or tactical brilliance.

On leaving Camberley he was due for regimental duty and went to 7th Signal Regiment as Lieutenant Colonel Peter Pentreath's Adjutant and later, one of the highlights of his career, to command a squadron of 140 linemen. In Ex Spearpoint in 1962 some 700 drums of cable were laid and 699 picked up.

A second spell in the War Office followed and then to the Joint Services Staff College at Latimer, Bucks. This was put to good use in his next posting to Station Infantry Brigade as part of the Strategic Reserve, which included a year in Sibul, Borneo during confrontation. This was marked by an incident when, having been out of communication for 36 hours, the General in Labuan sent the Brigadier a rocket - by Cable & Wireless.

Back in Britain he was selected in 1967 as a member of the Directing Staff at Camberley, working under Major General Hugh Beach. After three exhilarating years he was appointed to command 13th Signal Regiment in Germany - as one would imagine, another 'highlight'. Undoubtedly the best barracks in the theatre, he was to witness later as CSO BAOR the continuation of the development of the Regiment as the nearest Royal Signals has to be the equivalent of the infantry battalion's 'family'.

On promotion to Colonel he went as Secretary for Studies at the NATO Defence College in Rome. The six months courses boasted the finest lecturer list in the defence world; it was an environment where senior officers or diplomats from the then) 14 nations offered their views on putting the world to rights.

After 30 months in Rome he went on to command 2 Signal Group (Brigade) in Aldershot, with responsibility for UK static and wartime communications from the Shetlands to Cornwall. A return to NATO followed when he was appointed Assistant Chief of Staff at AFCENT in Holland to General Dr Karl Schnell.

His last appointment involved only a move of a few miles across the border to HQ BAOR where, on promotion to Major General, he assumed the duties of Chief Signal Officer. The introduction of domestic television from the UK was one of the projects he handled, and this proved valuable when in 1979 he applied to the Independent Broadcasting Authority

for his first civilian job as Deputy Director of Radio. After seven years in that post he became Director in 1987. In 1990 he was selected to be the first Chief Executive of the Radio Authority, the regulatory body for the development and supervision of all commercial radio in the United Kingdom. He retired in 1995.

Bored by retirement he joined The Television Corporation as Company Secretary, a role he finally relinquished in 2006. He was actively involved with St James Church, Gerrards Cross and the Royal British Legion.

He was a fellow of the Radio Academy, Fellow of the Royal Society of Arts and was awarded the CBE.

He was a Trustee of the D'Oyly Carte Opera Trust and Chairman of the Eyeless Trust, a charity for children born without eyes.

He married Gail in 1982, and our sincere sympathies are extended to her and the family members.

BRIGADIER J WESTLAKE



Jack Westlake was born in Brighton, Sussex in 1934. He attended Varndean Grammar School, joined the Army in 1953 and was commissioned into the Royal Corps of Signals from RMA Sandhurst in 1955.

His first tour of duty was with the Malaysian Armed Forces where he commanded a radio troop during operations against the communist guerilla forces. In 1959 he returned to Europe to command a troop in

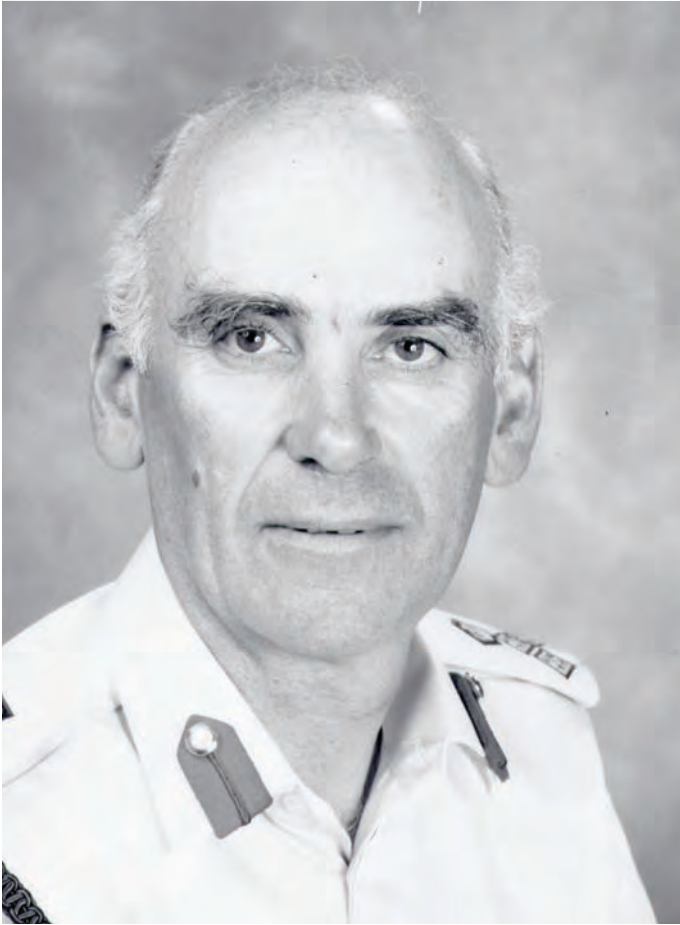
7 Signal Regiment. During his time in that Regiment he took part in the London Paris Air Race, and at one stage held the record for the journey from the Arc de Triomphe to Marble Arch with a time of 47 minutes 38 seconds.

In 1962 he moved to the Royal Signal Junior Leaders Regiment at Denbury, in Devon, to command Kukri Troop. He became a radio troop commander in 19 Airportable Infantry Brigade Signal Squadron in 1963 in Colchester, and attended the Staff College Camberley in 1965. From the Staff College he moved to the Ministry of Defence where he held a Grade 2 appointment in the Directorate of Military Operations. In 1968 he returned to Colchester to command 19 Infantry Brigade Signal Squadron. In 1970 he moved to BAOR to become DAA and OMG of 11 Armoured Brigade, returning to the UK in 1971 to become a member of the Directing Staff at the Staff College Camberley.

From 1973 to 1976 he commanded 4th Division Headquarters and Signal Regiment in BAOR. In 1977 he briefly filled the post of Assistant Secretary to the Chiefs of Staffs Committee in London before moving to Nigeria to take up the appointment of Chief Instructor (Army) at the Nigerian Command and Staff College. He returned to the Ministry of Defence in late 1980 to become a Colonel GS in the Signal Officer in Chief's Directorate; after two years in the post, he was promoted and appointed Deputy Signal Officer in Chief in January 1983. He assumed command of the SANGCOM Team in January 1986.

He married his wife, Georgina, in 1960, and they had four sons, eventually settling in Sevenoaks, Kent. His chief interests were fishing, running, golf and desert exploration. He died on 14 December 2014.

Brigadier S G M Gordon



in 1965 he was posted to Queen's Gurkha Signals in Malaysia, served in Borneo during Confrontation and completed his tour in Singapore. After a tour on the teaching staff at the School of Signals he went on to attend No 6 ASC in 1971/1972 at RMCS Shrivenham and Camberley. He was then attached to the staff of the Defence Operational Analysis Establishment as GS02(W) with responsibility for C3 and EW.

Between 1975 and 1977 he commanded 48 Gurkha Infantry Brigade Headquarters and Signal Squadron in Hong Kong and after spells as a GS02 in MOD and GS01 at the School of Signals, returned to Hong Kong in 1980 as Commander QG SIGNALS/Head of Joint Service Signal Staff. In 1983 he was appointed Colonel Plans at the School of Signals until February 1985 when he joined the Defence Commitments Staff as Assistant Director EW/JW. The post was retitled Director Joint Warfare in October 1986. In September 1987 he joined 2 Signal Brigade as Colonel G3 Comms NATO/ROW. In 1991 he was appointed Deputy Signal Officer in Chief (Army) in his final post and retired from the Active List in 1993.

He and his wife Gil settled in Essex and raised two children, one of whom was commissioned into the Corps. Throughout his career he was a keen sportsman with particular interest in hockey, football, tennis and golf, and was a member of the Army Lawn Tennis Association Executive Committee and Chairman of Royal Signals Football. Stan Gordon died on 16 September, and the sympathies and condolences of his many friends in the Corps are extended to Gil and his family.

Brigadier Stanley Gerald McKenzie Gordon was commissioned into Royal Signals from RMA Sandhurst in 1960. After early service with 2 Signal Regiment in BAOR and as Adjutant in 8 Signal Regiment in Catterick,

BRIGADIER M G TAYLOR CBE DL

Michael (Mike) Gordon Taylor was born in Canterbury, Kent on 6th March 1943 and, after being educated at Bickley Park School (where for 'games' he was reported on as "avoiding any form of unnecessary movement") and Aldenham School, where he became a Bisley-level rifle shot. He joined the Army in June 1961 and trained at Mons Officer Cadet School, Aldershot, later at the Army School of Education, Beaconsfield, and then the Royal Military Academy Sandhurst. In his inimitably self-deprecating manner, he recounted the times with mischievous humour, recalling how he and others at Beaconsfield (some rising to star rank) enjoyed 'defeating the system with passive resistance'. Commissioned into Royal Signals in December 1963 - despite being colour blind - he attended 55 'Q' Course in Catterick.

His first posting in 1964 to 229 Signal Squadron (Berlin) was at a time of much international political tension, with continuous harassment by the Soviet and East German regimes. He later found an entry in his Confidential

Report for 1966/67 where a one star officer had remarked "I have much respect for this officer. There is a lot in him, and he is useful to have about the place in an emergency. He was recently used to locate and bring out of East Berlin a British officer who had been arrested by the East German Police, and he achieved this despite alleged 'lack of presence' by cool-headedness, bluff and personal courage." After his 3 years in Berlin, Mike attended No 14 Telecommunications Course at Blandford, later to No 6 Communications Course, during which - most importantly - he met and married Mary.

Newly married, he was posted to 24th Signal Regiment, Catterick, as Adjutant to the (later, Major General) Lieutenant Colonel Jimmie Hellier. Mike learnt from Jimmie and attributed much of his later success to this 'formative period'. A tour as GSO3(SD) in HQ 1(BR) Corps, Bielefeld, was followed by a posting as Second-in-Command of 20th Armoured Brigade HQ & Signal Squadron, Detmold. He then became OC 633 Signal Troop (Belize), awaiting



transition to 2nd Division Signal Regiment and moving it to York. This was a challenging period, albeit being superbly supported by his Divisional Commander, the (then) Major General Peter Inge - who had very firm views about signals support.

There followed a posting to United Kingdom Land Forces, Wilton, as SO1 O&D. It was not a happy tour, but he was soon promoted from it to become Col O&D, HQ BAOR, which again carried many challenges. He then became Commander 1st Signal Brigade, Bielefeld, which he much enjoyed - especially being supported by a strong and loyal team. During this, he was selected to attend the Royal College of Defence Studies for the 1992 course and later to be Deputy Signal-Officer-in-Chief (Army) - in which he felt misplaced. But relief was at hand when he was short-toured and appointed as Chief of Staff to the 'soon to be formed' United Kingdom Support Command (Germany) - the successor to Headquarters, British Army of the Rhine. He also became 'double-hatted' as Commander Rhine Troops.

For Mike, this last four years of service in Rheindahlen, under three different GOCs, was the high point of his career. He enjoyed it immensely, as did his family. It was hugely interesting and varied work, which set him well for retirement. But he did not 'wind down'; indeed, he was amused to read, years later, a three star reporting officer's comments that "Any who take him for a rotund and jovial old buffer are quickly disabused - for he stands no nonsense, tackles difficult issues head on, and is a tough cookie." After being made a CBE and retiring into civilian life directly from Germany, he set up his own limited company, mainly undertaking consultancy work on the BOWMAN project. Fortunately, he chose the winning consortium, which then provided a further ten years of gainful and very enjoyable employment.

After retirement, Mike also became a lay member of the Immigration Appeal Tribunal, the Solicitors' Disciplinary Tribunal and a General Commissioner of Income Tax (later being selected into the Tax Tribunal). But few were aware that he also carried out highly classified judicial functions for the Ministry of Justice in regard to non-UK citizens suspected under the Prevention of Terrorism Acts. Further, he was an Independent Member of the Dorset Police Authority from 1999, becoming its Chairman from 2002 until its demise in November 2012. Away from such duties, he was President of the Old Aldenhamian Society for eight years until 2010, a Trustee of the Royal Signals Museum, a lifelong Member of the Radio Society of Great Britain and the Royal Signals Amateur Radio Society, holding the amateur callsign 'G3UCT'. He was delighted to be appointed a Deputy Lieutenant of Dorset in July 2009 and, later, to achieve re-appointment to age 75 on the Solicitors Disciplinary Tribunal.

Brigadier Mike Taylor died on 25 November, aged 72. Retaining a mischievous sense of humour to the last, he will be much missed not only by his family, but also by his many close friends, colleagues and comrades, both professional and social, past and present. He leaves his wife Mary, daughter Juliet, son Robin, daughter-in-law Lucie and a grandchild Tom.

the outcome of the staff selection process. This was a challenging 18 months with many inherited problems writing off lost stores - including two 'missing' K9 trucks (one of which was found as an ice cream van in Belize City), but supported - thankfully from afar - by Commander 1 Signal Group, the (later, Major General) Colonel Henry Hild, who became a friend.

Mike attended Division 3 of the Army Staff College at Shrivenham & Camberley. On telling Henry Hild that he was pleased to be on Division 3, Henry remarked "There is no reason to make a virtue out of necessity!" After Staff College, he joined the Defence Intelligence Staff (DIS), where he spent a fulfilling tour in a politico-military branch, in which he came close to leaving the Army and becoming a Crown Servant. After four years in post, he was selected to command 3 Squadron, 13th Signal Regiment in Berlin. In some respects this was a reminder of his time in Belize, with significant problems to resolve about the unit's acceptance within an American site, a RAF building and, most importantly, the British Garrison itself. But by the end of his 18-month tour, he had successfully resolved all of these sensitive issues.

He was surprised to be unexpectedly posted back from Berlin to be Military Assistant to the Deputy Chief of the Defence Staff (Intelligence), then Lieutenant General Sir James Glover, who had known Mike from his earlier tour in the DIS. This proved to be another formative period, during which he was made a MBE in Margaret Thatcher's 'Falklands List' for his private office work and involvement in the inevitable enquiries after the campaign. He was then selected to be Commanding Officer of 2nd Division Headquarters & Signal Regiment in Bunde, finalising its

RSI DIARY DATES

The definitive list of known RSI dates for 2016 are as follows:

- **Thu 17 Mar 16** RSI Blandford Spring Lecture
- **Thu 8 Jun 16** WCIT Employment Panel
- **Thu 8 Jun 16** RSI Blandford Summer Lecture
- **Thu 13 Oct 16** RSI Blandford Autumn Lecture
- **Thu 17 Nov 16** RSI Annual London Lecture & Dinner
- **Thu 8 Dec 16** Royal Signals Apprentice of the Year Awards

The dates of the RSI Annual London Seminar and two RSI Workshops have yet to be decided.

Below is a reminder of the contact details for the key individuals within Headquarters Royal Signals.

HEADQUARTERS ROYAL SIGNALS

Corps Colonel Royal Signals	Col Simon Hutchinson	01258 482151	rsignalshq-corps-colonel@mod.uk
Corps Adjutant	Capt Rosie Bonner	01258 482082	rsignalshq-corps-adjt@mod.uk
Corps Regimental Sergeant Major	WO1 (CRSM) Rob Luke	01258 482871	rsignalshq-corps-rsm@mod.uk
SO1 Royal Signals	Lt Col Al Balsdon	01258 482130	rsignalshq-so1@mod.uk
SO1 Reserves	Lt Col Mike Smith	01258 482083	rsignalshq-reserves-so1@mod.uk
SO2 Royal Signals	Maj Rachel Clayton	01258 482168	rsignalshq-so2@mod.uk
SO2 Commitments	Maj Paul Kelly	01258 482085	rsignalshq-so2b@mod.uk
C2 Whole Life Development	Mr Dave Barlow	01258 482098	rsignalshq-wld-c2@mod.uk
Regimental Secretary	Col (Retd) Terry Canham	01258 482081	rsignalshq-regtsec@mod.uk
Assistant Regimental Secretary	Maj (Retd) Mark Tivey	01258 482082	rsignalshq-regtsec-asst@mod.uk
Secretary, Royal Signals Association	Mrs Caroline Addison	01258 482090	rsa@royalsignals.org
Welfare Secretary	Mrs Linda Sizeland	01258 482089	rsbfgrantscoord@royalsignals.org
Corps Accountant	Mr Michael Fisher	01258 482086	accountant@royalsignals.org
SO1 Communication & Heritage	Maj (Retd) John Fradley	01258 482077	rsignalshq-commheritage-so1@mod.uk
Head of Publications	Maj (Retd) Keith Pritchard	01258 482817	wire@royalsignals.org
C2 Business Support	Mrs Becky Hollands	01258 482076	rsignalshq-bus-sp-c2@mod.uk
Subscriptions	Mrs Jess Lawson	01258 482087	subscriptions@royalsignals.org
Chief Clerk	Mrs Emma Harper	01258 482161	rsignalshq-chclk-e1@mod.uk
Secretary, Royal Signals Institution	Lt Col (Retd) Nigel Harrison	01258 482647	rsi@royalsignals.org
RSI Journal Editor	Col (Retd) Tom Moncur	01258 482647	journal@royalsignals.org
Museum Director	Mr Nick Kendall-Carpenter	01258 482267	director@royalsignalsmuseum.co.uk
Museum Business Manager	Mr Adam Forty	01258 482329	adam@royalsignalsmuseum.co.uk
Museum Shop Manager	Mr Mark Cozens	01258 482248	shop@royalsignalsmuseum.co.uk

Headquarters Royal Signals, Griffin House, Blandford Camp, Blandford Forum, Dorset, DT11 8RH



The Royal Signals Association
and
The Royal Signals Benevolent Fund
Swift and Sure Help for Signallers in Need



Your Legacy can help us

Did you ever benefit from a welfare grant from Corps Funds or maybe one of your mates received help with a welfare problem where the Royal Signals Benevolent Fund stepped in to help him or her in their time of need? There has been a long-standing saying that the "Corps looks after its own" and Royal Signals has a proud history of care for its people, supported by the one day's pay scheme and generous donations from serving and retired Signallers.

... help others in their time of need

That work continues today and every year we help hundreds of those who have fallen on hard times whether it be a serving Signaller who has been injured on operations, the families of those who have made the ultimate sacrifice, members of the Corps who need help with specialist medical care for their children or veterans who need help in maintaining their mobility and independence.

We don't distinguish between Regular, Reserve, National Service, ex-ATS or WRAC who served with the Corps, officer or soldier and their dependants; any case brought to us will be considered with expert support from SSAFA, The Royal British Legion and the Army Benevolent Fund. We will help whenever we can and you can help too, by leaving a legacy in your will. Its simple to do and can make all the difference to someone who has worn the same capbadge and who may not have been as lucky as you. If you would like to make a difference, please contact the Association who will tell you how to leave a legacy so that others from the Corps might benefit from your generosity.





SUPPORTING SERVICE PERSONNEL AND VETERANS

CSC

As a Next Generation ICT services provider to Government, CSC is proud to be a corporate member of the Royal Signals Institute, providing JPA services to Defence. www.csc.com