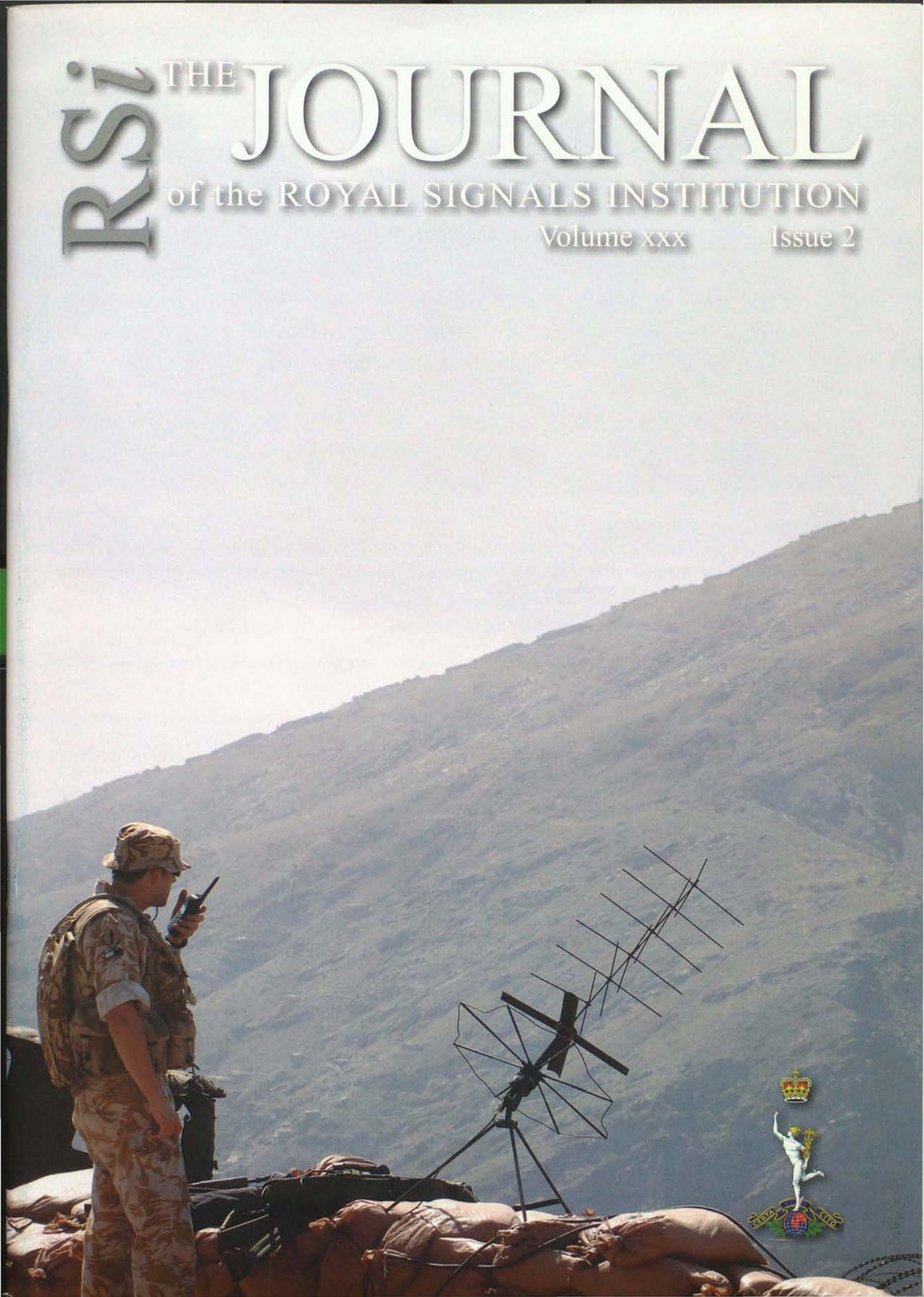
RSI

THE JOURNAL

of the ROYAL SIGNALS INSTITUTION

Volume xxx Issue 2



PROFESSIONAL SECRETARY, THE ROYAL SIGNALS INSTITUTION

Applications are invited from serving or recently retired Royal Signals officers of the rank of Colonel or Lieutenant Colonel for the post of Professional Secretary of the Royal Signals Institution (RSI) to replace Colonel (Retired) Tom Moncur in September 2012.

The purpose of the RSI is to maintain strong professional links between the Royal Corps of Signals, industry, professional bodies and other relevant areas of Defence, in order to foster the well-being of the Corps and to contribute to the delivery of Information and Communications Services within the domains of Defence and Security.

The RSI Secretary is the only person engaged full time in assisting the Chairman of the RSI to fulfil its purpose. As such, applicants should have a proven record of successfully working unsupervised and using their initiative to achieve a vision. Reporting to the Chairman of the RSI, the Secretary is guided by the Charter of the RSI and serves the requirements of the RSI Council and its Executive Committee in furthering the professional interests of the Corps. The Secretary is responsible for: generating ideas and proposals that support progress towards achieving the purpose of the RSI; planning and managing the RSI programme of activity, including lectures at Blandford and elsewhere; organising the annual RSI Seminar, the bi-annual RSI/BCS Lecture and the the annual RSI London Lecture and Dinner; editorship and production of the RSI Journal; administration of RSI prizes; maintaining the records of RSI honorary membership and of non-members who have influence in this area; the provision of material and amendments for the RSI website; liaison with other professional bodies such as AFCEA, BCS, IET, WCIT, specified universities and RMCS to share professional experience and arrange joint events where appropriate. In particular, the Secretary acts as liaison with the AFCEA UK Southern Chapter, its Blandford Sub-Chapter and as Secretary/Treasurer to the AFCEA UK Academic Trust.

Based at RHQ Royal Signals as a Corps employee, the post enjoys terms and conditions comparable with a Civil Service C1 grade, including salary and hours of employment. No pension is payable, but a terminal gratuity based on the period of employment is payable on departure. Further details are obtainable from the Regimental Secretary.

Applicants should have a technical background in communications and information systems theory and practice, and be capable of writing fluently on technical and military subjects. Membership of one or more of the above professional bodies is highly desirable, and essential within six months of employment. Full IT facilities are provided, including desk-top publishing software, as well as administrative support from RHQ Royal Signals.

Application forms can be obtained from the Regimental Secretary or the Secretary, the Royal Signals Institution. The closing date for receipt of applications at RHQ Royal Signals is 30 April 2012.

THE JOURNAL of the ROYAL SIGNALS INSTITUTION

Volume xxx Issue 2

The second Journal of 2011 comes at the end of a busy and significant year for the Corps, as the article by the SO-in-C (A) in this issue makes clear. I am particularly pleased in this issue to be able to include the top two winning entries in the 2011 Deane-Drummond Prize Essay competition, which this year addressed the topical subject of cyber warfare. This year's competition attracted an increased number of submissions, many from the non-commissioned ranks, and the overall standard was very high. The end of 2011 has been a busy one for the Institution, with our Seminar for Industry taking place just two weeks before our annual London Lecture and Dinner, for which attendance this year was at an all-time high. In between, the Blandford lecture by former Ambassador Sir Sherard Cowper-Coles on Britain in Afghanistan was one of the highlights of the year. Finally, acknowledging that all good things come to an end, this issue contains the vacancy notice for a new Secretary of the Royal Signals Institution to take up office next year, and submissions should be made to the Regimental Secretary soonest.

Tom Moncur

CONTENTS

THE ROYAL SIGNALS INSTITUTION LONDON LECTURE AND DINNER

Company tables at the Dinner

The Master

Mr Bernard Gray, the Speaker

Maj Peter Griffiths

WO Bruce Paterson

Maj Gen Nick Pope

Major General Tim Inshaw with the prizewinners

STOP PRESS ITEMS

CORPS PIPES AND DRUMS AT THE EDINBURGH TATTOO

Next year the Corps Pipes and Drums have been once more invited to take part in the world famous Edinburgh Military Tattoo under Pipe Major Jimmy Scott, thus reprising our first appearance in 2007. This is a major undertaking, not only for all our performers but for the units who support us by releasing personnel to play and practice. This is already showing dividends, with our current trainees already leading their intakes at the Army School of Bagpipe Music and Highland Drumming. Book your trip to Edinburgh in August 2012 now!

CORPS CEMENTS RELATIONSHIP WITH THE WORSHIPFUL COMPANY OF INFORMATION TECHNOLOGISTS

This year the first Corps personnel will join the Journeyman Scheme inaugurated with the WCIT by virtue of having come top of their courses at the Defence College of CCIS. Members of the CIS Management course, the Foreman of Signals and Foreman of Signals (IS) courses,the Yeoman of Signals and the Yeoman of Signals (EW) courses and the Troop Commanders course are all eligible, as is a selected TA officer. Personnel agreeing to take part will have their three year journey subsidised by the Corps, after which they will be able to become full members of the WCIT, with all the career and professional advantages that offers, not to mention the strengthening of links between the two organisations.

THE ROYAL CORPS OF SIGNALS

CORPS COMMITTEE

Chairman	Lieutenant General R Baxter CBE
President, Royal Signals Institution	Major General TG Inshaw CB
President, Dinner Club	Brigadier JE Thomas MBE
Chairman, Finance Committee	Major General AEG Truluck CB CBE
Chairman, Museum Trustees	Brigadier CJ Burton OBE
Signal Officer-in-Chief (Army)	Brigadier TJP Watts OBE ADC
Commander, 2 (NC) Signal Brigade	Brigadier SJ Vickery
Chairman, Royal Signals Association	Brigadier NF Wood DL
Representative Colonel Commandant	Brigadier EM Flint
Colonel Commandant	Colonel KJ Bruce-Smith TD
Secretary	Colonel TW Canham

COUNCIL OF THE ROYAL SIGNALS INSTITUTION

President	Lieutenant General R Baxter CBE
Chairman	Major General TG Inshaw CB
Vice-Chairman	Brigadier SJ Vickery
Signal Officer-in-Chief (Army)	Brigadier TJP Watts OBE ADC
DCOS HQ Signal Officer-in-Chief (Army)	Colonel DG Halstead
AD CSD Networks HQ Signal Officer-in-Chief (Army)	Colonel P Drew
Commandant DCCIS	Colonel G Hearn
TA Member	Colonel H Robertson
A serving Comanding Officer	As nominated
Retired Member	Brigadier DG Rowlinson
Retired Member	Brigadier NC Jackson MBE
Retired Member	Colonel AC Cunningham TD
Corps Regimental Sergeant Major	WO1 (CRSM) A McBean
Corps Foreman of Signals	WO1 (FofS) D Tibbetts
Corps Yeoman of Signals	WO1 (YofS) K Heaton
Secretary	Colonel TF Moncur

EXECUTIVE COMMITTEE OF THE RSI COUNCIL

Chairman	Major General TG Inshaw CB
Vice-Chairman	Brigadier SJ Vickery
Signal Officer-in-Chief (Army)	Brigadier TJP Watts OBE ADC
DCOS HQ Signal Officer-in-Chief (Army)	Colonel DG Halstead
AD CSD Networks HQ Signal Officer-in-Chief (Army)	Colonel P Drew
TA Member	Colonel H Robertson
Senior Corps Techical Officer Telecommunications	Lieutenant Colonel T Waites
Secretary	Colonel TF Moncur

REGIMENTAL HEADQUARTERS STAFF

Regimental Secretary	Colonel TW Canham	01258 482081
Assistant Regimental Secretary	Major IN Greig	01258 482082
Secretary, RSI and Editor, The Journal	Colonel TF Moncur	01258 482647
Secretary, Royal Signals Association	Mr P Cuckow	01258 482090
Corps Heritage Officer	Major I Seraph	01258 485837
Editor, The Wire	Major K Pritchard	01258 485248
Assistant Editor, The Wire	Mrs Amy Peterson	01258 485249
Secretary, Welfare	Mrs L Sizeland	01258 482089
Corps Accountant	Mr M Fisher	01258 482086
Administration	Miss R Fuller	01258 482161
Museum Director	Mr Nick Kendall-Carpenter	01258 482267
Museum Business Manager	Mr Adam Forty	01258 482329
Museum Shop Manager	Mr Mark Cozens	01258 482248

THE ROYAL CORPS OF SIGNALS - FORCE DEVELOPMENT AGENDA

By Brigadier TJP Watts OBE ADC, Signal Officer-in-Chief (Army)

Commissioned in 1980, Tim Watts commanded a signal squadron in the 1991 Gulf War, and then the Airmobile Brigade Signal Squadron in Colchester. He was on the staff of the new Joint Services Command and Staff College, and then Commanding Officer of 1st (UK) Armoured Division Headquarters and Signal Regiment in Germany. He then served as Chief of Staff of the UN Mission in the Democratic Republic of the Congo in the rank of Colonel. From 2005 to 2007 he was the Defence Attache in the Sudan, before returning on promotion to command the Defence College of Communications and Information Systems in January 2008. He took up the appointment of Signal Officer-in-Chief (Army) and Director Command Support Development Centre in September 2010.

As I write, the Corps has some 650 regular and TA personnel deployed on operations, and many more providing live, operational support from the home base. It is running at least 10 force generation cycles, from Campaign Signal Regiments, to close support to the infantry, Special Forces, Signals Intelligence, Air Support, Explosive Ordnance Disposal, Other Government Departments and Front Line Commands. And we have earmarked forces at readiness for national operations in the UK and for national and NATO operations abroad, some at very high readiness. We are busy. The technical and military challenges we are facing and defeating are like none before, particularly in terms of complexity and the pace of change.

This is my intent as the Corps' head of profession that, alongside our support to operations, we develop quickly to be ready for the next set of challenges. You will see that I am not varying significantly from the clear and forward-looking direction set by my predecessor, Brigadier Ted Flint, nor do I seek to trump any direction from the chain of command, but I do want to set out some specific actions and changes in the way we need to operate and think as a profession. So this is not, I am afraid, a short piece. Here goes.

Context

The context in which we shall operate is well described in the Future Character of Conflict (FCOC) paper, easily available online. Our operations will be conducted in a "super-joint" environment, that will include our sister Services, other parts of the MOD, including special forces, intelligence, DE&S / ISS, other government departments, allies and coalition members, the United Nations and other International Organisations, as well as NGOs and parts of the indigenous administration where we are serving.

The future will see a series of Defence and Security reviews, and major studies into the way the Ministry of Defence and the Army operate. There will be a great deal of change, and we shall not for the foreseeable future have enough money or people to do all the things we know we should. We can therefore expect to remain very busy on complex, information-rich operations and we will have fewer resources overall than now. Picking through these influences there are a number of common themes to which we must attend.

Our role has traditionally been the delivery of communications and life support, as elements of command support, and electronic warfare. In many ways this has not changed, but neither the words nor the approach they imply properly reflects the current needs of commanders, or the rapidly expanding opportunities and threats provided by technology in the information age.

Command Support

In the command support part of our role, our emphasis has shifted from communications to the information itself – we need to deliver an overall Information Service in the deployed environment that supports commanders and their staff at all levels:

a. In their understanding of the situation, the environment and their mission

b. By providing and supporting Information Exploitation and management tools that assist them in reaching decisions that enable them to disseminate those decisions and fresh understanding, as part of a continuous process.

This means, in effect, that delivering and managing applications (the tools used to support this process), and that includes securing access to the data they use, is now our command support main effort. We design and deliver the rest of command support around this.

We also deliver deployed Life Support where it makes sense for us to do so. That is, where it would be inefficient to separate it from delivery of the information service element of command support.

So, the elements of command support delivered by the Corps are:

a. First: Application Services, including:

(1) Interpersonal communications and feeds: Point to point and conferenced or netted voice and video, Full Motion Video.
(2) Messaging: CHAT, email.
(3) Common Operating Picture, positional and situational awareness and tracks.
(4) Collaborative planning, dissemination, assessment and control tools.
(5) Intelligence databases and tools that access intelligence sources.
(6) Combat Support and Service Support calculators, control and planning tools.
(7) Underlying geo and reference databases and viewing tools.
(8) Internet.

. . . *and, therefore:*

b. The underpinning Information Infrastructure and Network Services;

c. Information Assurance and Cyber Defence;

d. Electrical power; and,

e. Deployed Life Support Services.

The services we deliver must meet those needs of the FCOC environment, enabling commanders to bring a national and coalition, "integrated response" to bear. So we need to be equipped and trained to deliver:

a. National and coalition services simultaneously; that is, application services at the Secret UK Eyes and Mission Secret levels. In line with MoD direction, our "configurable mission secret" services will be based on NATO services for training and as a start state for deployment – "train and get-you-in". It is from this baseline that we shall adjust for coalitions and for the specific information needs of an operation. Our UK Secret services are based on BCIP and JC2SP/DII LD.

b. Above Secret services, so that national and Alliance capabilities including intelligence and cyber can be brought to bear where required.

c. Access to services, Restricted and Unclassified.

We do not do this alone. Specialist applications will sometimes need vocational specialists – intelligence, air, engineer, fires etc – but responsibility for providing the overall service, and as many of the individual elements as possible, including close support to the staff in their use of the application service, is ours. So, while other specialists need to be in our team, the default setting must be that Royal Signals provides deployed application support in all but the most specialized areas.

To deliver and manage these services, the Corps has adopted the government and industry standard Information Technology Infrastructure Library (ITIL) v3 framework, incorporating the continuous process of Strategy, Design, Transition, Operation and Service Improvement. This is a guide to applying strategic thinking to IT service management, the ultimate goal being to design, develop, and implement service management as both an organizational capability and a strategic asset.

Working with the key players, DE&S, PJHQ and the other Services, we have led on developing the Joint Information and Communications Services Operating Framework, JICSOF, based on ITIL. It is our core doctrine for command support delivery.

Electronic Warfare

As before, we assist commanders in their understanding by exploiting others' use of the electromagnetic spectrum through intercept, location etc. We can then shape and disrupt them by denying information services to our adversaries or by a range of other effects.

But we can only carry out these functions on our own against relatively simple systems - what most think of as "electronic warfare". This remains useful, particularly in support to the close battle, but very much greater overall effect is achieved by exploiting the Single Signals Intelligence (SIGINT) Battlespace, or SSB. This can only be done in close cooperation with other areas of Defence, other Government Departments and with allies.

Intelligence derived from SIGINT, fused where appropriate with that from more traditional electronic warfare and other sources, is critical to current and future operations. Our people are playing an increasing role in the analysis of SIGINT and in advising commanders – it is no exaggeration to say that our contribution in this area has re-defined operations. This trend is here to stay, and we must train for it. So what we call "electronic warfare" has already changed greatly.

But as the internet and mobile computing expand, any boundary between SIGINT and cyber operations is disappearing; these two elements being simply parts of our exploitation of the electromagnetic spectrum. Cyber operations will, again, rely heavily on and contribute to the work of other areas of Defence and Government, and our relationships in these areas, and with colleagues in the other

Services, as with SIGINT, need sustaining and strengthening.

Every member of the Corps has a responsibility to understand, in varying degrees of detail, the nature of cyber threats and vulnerabilities. Each must understand his or her role in dealing with them – their part in cyber defence – and form part of Defence's 'cyber police', explaining to others what this is about and enforcing discipline and information hygiene. Very few individuals will not need to be engaged continuously in this – it is one of a number of 21st Century Basic Signalling Skills, a term that will increase in importance in this coming year.

In order to be effective at cyber defence, and to enable Land Forces to utilise exploit and attack opportunities in the future, we need to grow and sustain expertise in these specialist areas. We will do this initially through expanding the training already provided, and by committing the right people to the new Defence Cyber Operations Group. We will also reinforce our existing SIGINT capability as the foundation on which to build our cyber capability. This will entail some people staying in this field for extended periods to build up the necessary skills and the trust of other organizations.

Our operations beyond command support will need to include other areas of exploitation of the electromagnetic spectrum, including spectrum management, force protection counter-measures, ELINT and other non-comms exploitation. So, while our role can still accurately be described as the delivery of 'Command Support and EW', and for now we will continue describing it this way, we must all understand that this is now more about information support, SIGINT and Cyber.

Developing the profession

Command support and EW are delivered by Royal Signals brigades, units, independent squadrons, troops and personnel deployed individually in Corps appointments and outside. Our role at the HQ here in Blandford, the home of the Corps, is to ensure, with the support of others, that there is:

> *a military, command support and electronic warfare profession with the right ethos, individual education and skills, doctrine, services and equip ment, and in the right structure and numbers, available to the Army, Defence and wider Govern ment, now and in the future.*

This means that we must constantly redesign the profession and drive change, against a backdrop of great change across Defence, Government, the nature of operations and technology. I'll deal now with some specifics.

Structures and Basing

The Corps did well in getting ahead on the Operation ENTIRETY initiative and then keeping up its high rate of change with success in Afghanistan in mind. This continues and the Corps is held in higher regard than anyone serving can remember – just look at what has been achieved in Afghanistan, and how our force preparation for that operation has improved. Many of the drivers for change have come from these operations in Afghanistan, and we know that several of the 'information' features will endure. But we have had to manage support to other operations and concurrent contingency during this period, and in addition to making sure we achieve success in Afghanistan – our Main Effort - we need to address now how we shall be designed when that particular fighting stops, how we intend being ready.

The shape and size of the Corps will rightly depend on how the Army and Defence develop – we are in support - but we can no longer afford the luxury of organic support to any but the very highest readiness headquarters. So we are creating as part of our part of Transformational Army Structures, five new "theatre" Signal Regiments, based on our Campaign Signal Regiments. These will provide close support to brigades and battlegroups, and other points of information presence, using satcom and terrestrial bearers (largely Skynet and FALCON), information infrastructure (principally DII), and suites of applications. Support to other HQs, such as aviation, Joint Force Support and two star HQs will be provided from within these regiments, although it is likely that some adjustments will be made as our thinking on the future of divisional HQs develops. There are other changes, designed both to meet our manpower reduction targets and balance us for the future.

As well as this, support to the ARRC and the Joint Rapid Reaction Force will be adjusted and, on current plans, one of our ARRC regiments, 7th Signal Regiment, will disband. These are all major changes for the Corps, and for the Army. The Corps will return from Germany and we are well provided for, with two regiments moving into new, purpose-built facilities at Stafford alongside 22nd Signal Regiment under project BORONA, in 2015/16. Other moves back from Germany will take place as part of the wider SDSR basing plan.

The Army is changing the way its Regiments and Corps are led. Current capbadges are not under threat, but the post of Signal Officer-in-Chief (Army), along with all the Arms and Services Directors, will change significantly over the next two years, and many of the functions of HQ Officer-in-Chief (Army) and the Command Support and C2 Development Centres will be subsumed into the work of one of four 'Capability Directors', with some Corps-specific functions falling to a more empowered Regimental Colonel. So, in a year's time the Signal Officer-in-Chief (Army) as we currently know him is likely to be a

matter of history, but the new structure will ensure that our essential professional characteristics remain, and we must treat this as an important opportunity.

Training

The demand for command and EW support now exists close to the contact, "kinetic" battle. Our people must be able to operate not only while surviving alongside the infantry, armour, special forces, Explosive Ordnance Disposal and intelligence specialists and others, but they must be able to take on combat tasks as integral parts of those teams and in their own right. We are specialists, but we are military specialists, and our fitness and military skills must be of a high standard.

We cannot provide all the technical training people need through residential DCCIS courses; that is manifestly so from the special-to-arm training burden that already exists. But even if there is a return principally to contingency after Afghanistan this feature will endure. Phase 2 and 3 career training will need to concentrate on basics and principles. We must structure and resource ourselves to manage and deliver specific-to-role individual technical and military training in units and brigades. No unit can afford to be without its own technical and military training facilities, or access to these reasonably locally. It will not be possible even to provide all the up-to-date principles training needed, call it technical education, in a rapidly changing operational and technological environment, at DCCIS. For most there are no more than two technical "career courses" during one's service, and for Direct Entry officers there is only one. So:

a. First, officers and soldiers must take more responsibility for self development – keeping up with technology and other elements of our profession by reading, study and courses.

b. Second, some training and education will need to be delivered in smaller modules, frequently updated, delivered when required (so that it is as up to date as possible) and usually delivered or made available by DCCIS. In fact, while Phase 2 training should remain residential and based on cohorts of students from Phase 1 living and working together, thereafter training should, wherever possible, be delivered just in time to those who need it, minimizing residential courses away from units. Maximum use will need to be made of distance learning, and the time people need to study and train must be made available.

c. Third, we must continue to pursue accreditation and recognition by the Professional Institutions and academic bodies. These provide additional validation that what we teach is modern and commercially relevant and allow our skills and experience to be recognized by others we work with, as well as aiding resettlement.

d. Fourth, we must rapidly develop a means of recording the training each individual has undertaken in much more detail than is currently the case. This information can then be used within units to help place the right people in the right jobs and design their training. We must then use this information as part of the selection and posting process.

We are under-training in two important areas. First, our Direct Entry officers need a new approach to technical training that will take them beyond an initial troop commanders' course, currently their only formal special-to-arm training. Second, we must professionalize the Regimental Duty roster for the Warrant and Late Entry Officers who have responsibilities for military training, the Deployed Life Support Service, discipline and other G1 support, in and out of barracks.

We keep all trades under constant review and in a constant state of change – that is the way of this environment. There is a great deal going on, but the biggest changes are likely to be to the operator roster, both Communications and EW. There is also a very much reduced requirement now for a stand-alone Line trade and we shall be incorporating the skills everyone needs into the 21st Century Basic Signalling Skills programme.

Ethos

What sets us apart from our civilian counterparts is our Corps ethos. This rests on the bedrock of the Army's Values and Standards and is now taught and reinforced at Blandford. It is set out:

You are a vital member of a highly professional and technically able military team that supports our commanders and disrupts the efforts of our enemies. We are a close but welcoming family of regulars, reservists, veterans, families and friends.

Train hard to win and to conquer adversity. Strive to be tough, skilful, confident, brave and cheerful. Keep seeking out new skills and knowledge. Never ignore something you feel is wrong or that you don't understand: ask and act.

Like our predecessors have always done, fight for communications with energy and imagination, never resting until you are "through". Wear your Jimmy with pride and live up to our Corps motto, 'certa cito' – sure and swift.

Most of this is self explanatory, so 'communications' means 'information' or 'EW effect', and getting 'through' means succeeding in your information support or EW task. But I'd like to expand in a few areas. The nature of our business is that we are often dispersed and it is essential that we are welcomed and trusted by those we support. In this we must lead by example: we must warmly welcome those from other organizations serving, living and working

with us, and those who are interested in joining our Corps. Our "offer" or "unique selling point" is:

To be at the heart of the fastest moving, game-changing military capability, exploiting information technology and cyber opportunities, among highly professional and intelligent soldiers and officers, in a warmly welcoming family that stays with you for life.

None of us knows everything about the breadth and depth of our technical and military business. We must, therefore, be a team, confident in each others' support even when we are far apart. So friendship and networking are important to us operationally as well as making the Corps a good place to live and work.

This will take us so far, but we must also minimize the differences between some of our internal "tribes", not just in a social sense, but in creating as much equal opportunity and commonality of employment as we can, while recognizing and exploiting the positive differences that each brings. I would pick out here: Direct and Late Entry Officers, Gurkhas and UK soldiers, TA and Regular personnel, regional and national TA, and Warrant Officers and Officers. These are the serving Corps in its totality, and to under-involve, under-recruit, under-train, under-promote or unnecessarily segregate any part of it weakens us. Being an "equal opportunity employer" in this sense must be culturally and, wherever possible, tangibly a reality. The Army's structural requirements do not always help – we need to stay progressive and challenging.

In the same way, we know from our experience on operations that our people step up to challenges beyond what has traditionally been expected of their trade, experience or rank. I would pick out particularly our Communications Systems Operators, who have excelled in tasks previously the preserve of EW operators, engineers, application specialists and infantry signallers. In reality, everyone has stepped up a rung and we must get used to stretching our soldiers and, particularly, our junior officers; they will succeed. Demand on the Corps continues to increase – a sign of success - particularly in specialist areas such as Special Forces, ECM EOD, SIGINT and Cyber, and the Army will get smaller, so we must really make best use of our people and forget any entrenched views about who should do what.

In this area we shall need to adjust our approach to the Territorial Army. Our Specialist Group provides a unique resource of skills and we must get better at employing it and increase its capacity. Our regional TA units have specific tasks and provide significant support to operations in a number of ways. But the increasingly specialist nature of our work means that we shall find it harder to provide the necessary foundation training to those who come to the TA with no relevant technical skills. We must attract, recognise and reward those with relevant skills into the main body of our TA as well as an enhanced Specialist Group. There are likely to be big changes to the place of reservists in our armed forces in the coming years, and in Royal Signals there are many opportunities.

I would add that we must also include the contractors so essential to our business in this family. In many ways, we are the point of the information spear, that part that goes to the dangerous and difficult places. Much of the effect we are part of is delivered by contractors and our ability to work with them as a team becomes more important every day.

Why is cheerfulness important ? Well, aside from making the Corps a happier place – a vital part of leadership – we recognize that it is the commanders we support that are under the real pressure. They will make better, quicker decisions if their support is delivered by people so professional, confident and on top of their game that they have the capacity to spare to be cheerful and go the extra mile. I would add, that now, when change is everywhere and nothing seems clear other than that resources are diminishing, that the future of the Corps is very bright indeed. Senior people in Defence really do get what we do and we know that we are essential to the information battle, the battle of today and tomorrow.

Sport, and arduous and adventurous training are essential to our success. The Corps has an extraordinarily successful sporting record and the links to teamwork, selfless commitment, pride and quality of life are clear. We shall continue to strive to win at sports, as units, as a Corps and as individuals, but we shall also maintain sporting diversity and a high-participation, "sports for all culture". Arduous and adventurous training with elements of fear and physical challenge, from ambitious expeditions for the relatively few, to more local activities for as many as possible, and tough events like the Lanyard Trophy and Race the Sun, build courage, confidence, leadership and planning skills. Links to the Retired Corps, our ability to help those in need, and the maintenance and development of tradition and heritage are all part of our capability. We must keep these areas strong.

These are some of the ideas that will shape our work over the coming years, and we need to get on with the specific changes rapidly. This is an endeavour that involves everyone, for there are some important changes of overall emphasis, in our structures, equipment, training, and in many other aspects of Service life. We should only wait for direction when absolutely necessary. The Corps that I see every day is not only up for this, but in many ways is getting on with it: every one of the initiatives I describe is a live, current project. Now we need to get it into our DNA – to be sure and swift in our driving ahead with change as well as delivering every day in support of operations, and being ready for those operations we do not know are coming. **Certa Cito!**

THE INTERMEDIATE COMMAND AND STAFF COURSE (LAND) A CORPS PERSPECTIVE

By Major A Owen, Royal Signals

Major Alan Owen is currently deployed to Op HERRICK as the COS of JFCIS(A). Prior to this he spent the last two years as a member of the JSCSC Directing Staff where he was a ICSC(L) Syndicate Leader responsible for the mentoring, coaching and education of a number of student syndicates. In addition, he was a Divisional Executive Officer in the Army's Intermediate Division for the Regular and the Territorial Army courses. Major Owen graduated from ACSC 8 in 2005 and has a Masters degree in Defence Technology from Cranfield Universtity. His previous appointments include SO2 J6 in 16 AA Brigade Headquarters, an E1 SO2 in MOD and Squadron Commands in both 11 and 3 Divisional Signal Regiments.

Introduction

The Intermediate Command and Staff Course (Land) (ICSC(L)) is a key component of Army and Royal Marines Officer education. It is now in its 16th iteration and remains the first formal staff training that most officers receive. The course is mandatory for all direct entry officers on promotion to Major and is optional for professionally qualified officers and late entry officers.

The aim of this article is to share my experience having been a member of the ICSC(L) directing staff, in order to improve the awareness of the course for Royal Signals officers. This is intended to educate both future students, as well as their present and future employers about the course and how they can get the best out of it.

Background

The introduction of ICSC(L) was a 'game-changer' for Officer education. Its programme reflects the influence of both the Army Junior Division (AJD) and the Advance Command and Staff Course (ACSC), in terms of its content and emphasis. Many of the pre-ACSC 10 graduates would recognise many aspects of the course. I think it is fair to say that following ICSC(L) junior Majors are now far better, and more widely, educated than those AJD trained majors who preceded them. The syllabus has been constantly developing and changing but at its core it provides a solid grounding in:

a. The '7 Questions' Combat estimate.
b. An insight in Geo-political affairs.
c. Military Technology *(i)* based on its capability.
d. Management of Defence.
e. Staff skills.
f. British Military Doctrine.
g. The conduct of operations at the Brigade and the Divisional level.

This is by no means an exhaustive list but it does show the breadth of the topics covered. The dynamic programme has meant that the course has reflected the need to adjust to the changes in Defence but it has meant that no one ICSC course has been the same as the last.

The introduction of ICSC(L) has had some unintended consequences. The first is that Captains have a gap in their education that used to be filled by AJD. Unfortunately distance learning and MK2 have not filled the void left by AJD's removal. This is a widely known problem and there are moves to create a short residential Captains' module to provide them with an element of formal staff training.

Secondly the removal of IPSE *(ii)* has removed a hurdle to promotion for the less-able. In the past many less committed or able Captains would have left the Army because of the challenge of AJD and especially IPSE. The loss of these people was not always to the benefit of the Army. However, while the removal of IPSE has probably aided retention it does mean that the spread of ability of those attending ICSC(L) is wider than it would have been if IPSE was still in effect.

The impact for ICSC(L) has several facets. Firstly, and most significantly, each course has students who struggle to keep up with the main body of the course. While this is clearly an issue for them, it does mean that it is much harder for the DS to 'stretch' the more able students while simultaneously keeping the less-able students engaged. Secondly there are students on ICSC(L) who are not competitive with their peers. Now that the IPSE-filter has been removed, these Officers have promoted at their fourth 'look' and would probably have not made it through the IPSE filter. It is not unusual for some students on ICSC(L) to be approaching the end of their IRC commission.. This is not a good return on the Army's investment of an 8 month residential course. Understandably these students,

appreciating that they are not competitive and with little chance of conversion of their commissions, are often not well motivated individuals.

Course Reports

The ICSC(L) course report now counts as the Officer's OJAR for the year and sits on their report book in APC Glasgow. Consequently the report format is becoming closer to that of an OJAR in appearance. Students are no longer individually placed as XXX of XXX students on the course. The course report does reflect whether they sit below, on a par with or above the main pack of the student body. Those students whose performance, both subjective and objective, places them in the top 10% *(iii)*are commented on as such. In addition to the performance grades and narrative, course reports include recommendations for the students' suitability for future employment in technical, logistic, HR, Def Pol or Combat roles. Following on from this are the recommendations for student's suitability for key staff appointments such as Brigade COS, DCOS or to return as ICSC(L) DS. While the vast majority of students already know their initial Staff Appointments, the report may influence their competitiveness for Squadron Command and for subsequent staff appointments.

Royal Signals on ICSC(L)

The Corps averages 10 Royal Signals Officers per course. This is mostly DE officers. Unlike other cap badges, Royal Signals LE officers attending ICSC(L) are not drawn from the QM fraternity, but are DE converts (iv), Traffic Officers or Technical Officers Telecommunications. This is slightly disappointing, as other Arms LE officers with an RD background do find the course an eye-opening experience in many cases, and some compete very well indeed. I am not sure whether this absence is from a lack of ambition on the part of Royal Signals LE RDs, or a numbers constraint imposed upon Royal Signals Officer Wing.

In my two years the performance of Royal Signals Officers has been largely consistent. Frankly, the majority of the Corps' Officers fall into the middle third of the course. There have been a few noticeable exceptions and a few who have under-performed. It is impossible to list why this is the case but it is clear that there are a number of contributory factors. These do not apply to the Corps alone and are equally applicable to officers from other areas of the Army.

a. 'Self-selecting bottom third.' This phrase was coined by one of the Divisional Directors and is quite apt. The self-selecting bottom third encompasses those students who arrive with a self-limiting attitude. All too often this manifests itself in comments such as 'I don't do that/ I can't compete as I am a J6 specialist' or a tendency for the least able to self-situate themselves in their own comfort zone and not compete in the various exercises *(v)*. It is vital that students arrive at the course without a 'chip on their shoulders' about their ability to compete on an equal footing with Combat arm officers.

b. Lack of knowledge about Corps capability. All too often Royal Signals students have little understanding or knowledge of Corps ICS capabilities beyond what they saw as troop commanders. There is clearly a credibility issue here when Royal Signals students cannot explain even the very basics of Corps business to other Arms students. There is a problem with the Corps' professional development of our young officers when ICSC(L) students know less about G6 *(vi)* than teeth arm officers. Closely linked to this, are the students who arrive with a very limited breadth of experiences. This may be the student who has only ever touched one or two bespoke areas of comms employment or worse the Royal Signals Officer whose G1 career path has been Squadron 2IC, Adjutant, recruiting post etc. The pre-ICSC(L) briefing course at Blandford is only an update course. I was disappointed by the student who complained that it did not prepare them adequately for ICSC(L). It is naïve to expect a 2 day course to make up for one's own failure to take responsibility for one's own professional education.

J6 related courseware.

There are several areas of the course where there is J6 and Corps related input into the course:

a. *Equipment Capability Module.* This module introduces students to the principles of communications. Visiting lecturers give students an exposure to BCIP, trunk networks and Logistic IS. The element is finished with a morning confirmatory exercise based on a Divisional-level CIS planning exercise. The aim of this is not to train the students to be comms planners but to give then an understanding of the capability and constraints of G6 that they will face as non-Royal Signals headquarters staff.

b. *Land Environment Capability Module.* This module gives an exposure to Corps' capabilities and related activities. Included in this are the role and capabilities of EW, the topical subject of ECM and an understanding of deployed formation headquarters.

c. *Operations Term exercises.* While there is little formal G6 play in the exercises there is significant cross over from the knowledge developed in term 1. The exercise scenarios are all set using the ARRC Cerasia *(vii)* scenario in 2018. Consequently the ORBATs all use Brigade Signal Regiment (BSR) ORBATS and core programmes such as Falcon rather than Op HERRICK constructs. While I am conscious that the BSR construct is still under development, it has occasionally been challenging to map across the BSR construct onto Divisional-level ORBATS which is one area that may require SOinC O&D clarification.

Pre Course Preparation

Positive mental attitude. It is vital that Royal Signals students arrive with a positive mental attitude. Key to this is an understanding that they are **not** at a significant disadvantage than their teeth arm counterparts. The vast majority of the students do not come with a significant advantage from their previous jobs. That is not to say that some do not already have a superior understanding of the Combat Estimate but rather that any such advantage is short-lived. The standard of instruction is very high and all students can soon reach a high standard in every area if they apply themselves. It is worth highlighting that many teeth arm officers arrive with a very limited set of experience, mostly HERRICK focused, that does not give them any edge in the generic ICSC(L) syllabus.

Pre course development of professional knowledge. Despite the comment above, this does not mean that students should expect to arrive with out any pre-course preparation. The students who have applied themselves and completed MK2 properly, have read some of the pre course reading, are familiar with the 7 questions construct and have acquainted themselves with key publications *(viii)* will benefit from it rather than arrive on the course 'cold'. Commanding officers can contribute to this by encouraging their young officers' E2 professional development and allowing them the opportunity to expand their core knowledge. Young Officers need to be encouraged, nay mandated, to get out of the G6 tent and get involved in the key planning processes within Brigade headquarters. It is exposure to the Battlegroup and Brigade planning process, its toolsets and terminology that gives other Arms SO3s such a head-start during the Operations module at ICSC(L) and the Corps officers need to take every opportunity to match this.

E1 knowledge. It is important that Royal Signals officers expand their own knowledge in E1 matters. This is not to say that they have to delve into deep technical matter; in many ways such an approach would be unhelpful. They need enough knowledge to explain Corps' capabilities, at a level and in a vocabulary that other Arms understand, to the remainder of their syndicates. To give an idea of the level expected, there is nothing on the course that I would not expect a 2Lt fresh from his Troop Commanders course to be able to explain. It is worrying that our young majors cannot do this. There is no need for a residential course to meet this need. The existing EC module has an online package of journal articles, RSS powerpoint presentations and other material as additional reading aimed for the Corps' officers on the course. A pre-ICSC(L) dedicated page on the SOinC's website would meet the requirement for pre-course familiarisation.

Opportunities for DS

Now a sales pitch for Royal Signals instructors at ICSC(L). All of the SO2 posts are WTE *(ix)* and as such the instructors' posts are both rewarding jobs and get the recognition that a WTE-tagged post attracts. The Corps does not have any Royal Signals-tied posts but 'targets' two posts to be filled by the Corps. Unfortunately this has lapsed over the last year but there will be two Royal Signals DS from August 2011. The quality of the other SO2 DS is exceptional in many cases with a vast amount of operational experience, gallantry medals and high quality individuals in evidence. The command structure is very flat with the SO2s being given a considerable amount of leeway to tailor their delivery of the Training Objectives to best meet their syndicate's need. While there is a considerable amount of responsibility placed on each DS, it is very refreshing to be given the latitude and ability to practice genuine Mission Command in delivering the course. For those DS who have yet to attend ACSC, it is a very useful education process in its own right. The quality and rank of the visiting lectures at ICSC(L) is outstanding. This ranges from a host of senior officers, household name-academics and politicians to cutting edge military theorists and the like. Finally the role of DS at ICSC(L) gives each incumbent the opportunity to personally deliver a better prepared generation of Majors into the Army or RM.

Conclusion

ICSC(L) offers opportunities for the professional development of the Corps' officers. For any student it is important that their chain of command invests in their professional development prior to the course. For Royal Signals officers this needs to be at E1 and E2 with an emphasis on the latter. This will enable Royal Signals students themselves need to approach the course with a positive attitude and understanding that the course will impact upon their future careers. Finally Royal Signals as a whole needs to understand that a generation of Majors will make judgements about the Corps on what they see of us while they are on ICSC(L).

Finally a plea for any Royal Signals Officer who is invited to brief the course as a visiting lecturer. The performance of some visiting military lecturers is sometimes lacking and the Corps has not been immune from this. A poor performance gives a bad impression not just about that individual but reflects badly on their cap badge to a generation of newly-promoted Majors. One student inval read 'This Lieutenant Colonel was an embarrassment to Royal Signals Officers everywhere and delivered the worst lecture of the entire course.' Harsh words. The trouble was that he was right.

NOTES

(i) Now re-titled Equipment Capability to reflect the change in the approach of the module.

(ii) The Integrated Staff and Promotion Exam was taken at the end of AJD and students were required to achieve a set level to be eligible for promotion to major and a higher score to for eligibility for ACSC.

(iii) 10% is more of a subjective term for those students who are clearly performing well above the others rather than a fixed numerical quantity.

(iv) ie LE officers who have transferred to Direct Entry terms of service. These do tend to be from the supervisory rather than the RD backgrounds.

(v) Such as the Royal Signals student who always puts together the Powerpoint slides in the syndicate rather than lead on the G3/5 planning of the combat estimate.

(vi) Included in this is an understanding of BCIP, EW and how Div and Bde HQs function.

(vii) A mythical country using the Horn of Africa for source material.

(viii) JSP 101, Army Staff Handbook, ADP Ops.

(ix) Where Talent Endures

A VIEW FROM THE ARMY PERSONNEL CENTRE

By Mr Danny Powell

A note from Lieutenant Colonel Neil Stevens Royal Signals, Army Personnel Centre, SO1 Soldiers. Mr Danny Powell has worked in the Army Personnel Centre for a total of seven years as a civil servant; with three of these years having been spent as a Royal Signals Career Manager. Having seen at first hand the effect of the current changes to defence, along with the associated military manning issues, he has identified an alternative approach that might be of assistance in our efforts to build a British Army for the future. These are his own views in his own words, but the Military Secretariat, Major General AR Gregory, has sat alongside Danny at his desk on a number of occasions, has personally welcomed his analysis with its unconstrained input and has passed some of these thoughts on to the Carter Study. Readers views on these propasals are welcomed.

The Challenge

In what meaningful way can we frame the unique challenge that awaits the Army in the coming years?

Let us look at the Army as a machine; a model or device of some description. And let us look at its Soldiers as the circuitry, the internal components, the mechanical moving parts, the information carriers, the processors – everything the model encases which allow it to deliver its output. Now, imagine the latest version of the Army model is brought out. It has a sleek, streamlined and lightweight design.

What has facilitated this new economic design? It is of course an increase in the efficiency of its internal components. This increase in efficiency allows the size and weight of those components to be compacted and reduced whilst still delivering the same level, or even an improved level, of capability.

Except this unfortunately isn't the case in real life. The new economic design of the Army hasn't been facilitated through internal improvements, but rather, it has been forced on us by external circumstances – the financial constraints of the whole country, and it is a burden that just has to be shouldered and adapted to wisely, whilst still allowing us to meet our demand.

So the challenge for the Army must be to reverse engineer the traditional cause / effect relationship to make the new reduced Army seem justifiable by virtue of the improvement in efficiency of its Soldiers. From here, I will assume that this analogy captures the general viewpoint from which the restructure is being pictured, and will suggest a way in which the Royal Corps of Signals, or possibly the wider Army, could adapt.

The Royal Corps of Signals

Royal Signals, as it is now, holds variety of experience and fluidity of structure as its core philosophy.

The more varied a soldier's experience, the more employable they are deemed and consequently the more competitive they appear to promotion boards. The structure is given its fluidity through the six monthly re-evaluation of need and corresponding reallocation of manpower, known as the MDD; the Manpower Distribution Document – a document published by the Signal Officer in Chief's Directorate aimed towards a constant adaptation of Corps manning.

Is this ethos compatible with what the whole Army needs to become? If efficiency is to be the governing force of the new design, then let us quickly look at what efficiency is, and how it is brought about.

Efficiency is an increase in production, relative to effort spent. If, whilst maintaining the same level of input, you are able to increase your output in terms of quality or quantity, then you have become more efficient. Or, if whilst maintaining the same level of quality or quantity, you are able to decrease the required amount of input needed, then again you have become more efficient. The difference depends on how you use your time.

Efficiency is brought about by spending time and attention on a given task. The more time you spend doing something the better you are likely to get at it because you are able to concentrate your attention fully on it. And the less tasks that you perform, the more likely you are to get better at them, as repetition breeds dexterity. If you are required to spend a limited amount of time performing a large variety of tasks, then obviously your attention becomes diluted and the quality of your results, if they don't suffer, are at least unlikely to improve. In other words, if you try

to spread yourself too thin, holes will begin to appear in the fabric. Variety, in this sense, is almost the antithesis of strength and efficiency.

Can we carry the current philosophy into the coming era?

I don't think we can, though this is not to suggest that we should swing from extreme variety to extreme limitation, but if the Army is looking to create a more efficient machine, then we should be exploring ways in which we can strike the balance between them by becoming visibly more stable, calm and measured. I believe one way we can do this is by rethinking our perception and use of time in the career and promotion model. Below is a proposal as to how we can amend the models towards this aim. This paper has not explored ways in which we can make the structure firmer, though the proposal does imply that the MDD will, or should, be largely abandoned. It also assumes that Super Garrisons will come to be.

The Proposal

Change the Promotion Model!

The whole Army career is very much centred on promotion. There are problems with the nature of the career structure in Royal Signals and indeed the Army. It's a vacuum, it's speedy, and it perhaps helps create more imbalances than it alleviates.

What determines promotion zones and tour lengths? They are generally determined simply by the length of a Soldiers career (22 years, 24 with VEng) approximately divided by the number of ranks which exist (seven) allowing for some tweaking here or there, particularly amongst the more senior ranks. With the satisfaction of certain pre-requisites, it is possible for a Soldier to be eligible for promotion to the next rank up after only two years in their present rank.

I propose we fold back the ranks of Lance Corporal, Staff Sergeant and the two classes of Warrant Officer and instead have four core ranks, three of which are promotable. These core ranks would be Signaller, Corporal, Sergeant and Warrant Officer. Tour lengths would be extended to five years (six for WO), and one would only be eligible for promotion having spent five years in rank. This would increase the value of each rank.

What would become of the Lance Corporal, Staff Sergeant and Class 2 and 1 ranks? They would become nominal ranks only and they would merely signify a phase in development within the core rank itself.

This would provide an environment more conducive to increased efficiency, by allowing more time on which attention can be fixed on a Trade subject and role, and its knowledge exploited. It would offset the impact of relative ineffectiveness that occurs whilst a Soldier is in his 'bed in' period and when he is mentally winding down prior to leaving. The period of usefulness is thereby increased. Trade mergers, coupled with the increased demand and limited resources should mean that there is at least enough variety within a role to sustain interest for a prolonged period. In those trades and roles where there isn't enough variety to sustain interest and enthusiasm, an internal move after 2½ years could be granted within the same five year assignment.

Promotion

Although internally reported on every year, since Soldiers will now only be eligible for promotion after five years in rank, the report that goes to the promotion board will be a synthesis of the last five years progress and development. Trends in character and professional development and the unfolding of maturity will be given a more prominent place in deciding which unit will be more suitable for the Soldier to spend the next phase of his career in.

Year 1: Training.

Years 2-6: Signaller. The first year following Trade Training is spent as a Class 3. The 2nd and 3rd are spent as a Class 2 and the 4th and 5th are spent gaining a Class 1. The Soldier is awarded the nominal rank of LCpl to signify that he has attained Class 1 status or that he is currently engaged in Class 1 training. Class 1 training should be spread out over the two years so as to allow, if needed, the soldier to be recalled for the more immediate business of his unit. It would ease the pain, and threat of pain, currently imposed on units and rosters by the Class 1 vacuum, but it would depend entirely on an increased capability of the units' integral training wing. For those unfamiliar with Royal Signals, these are residential Career Courses that take anywhere from 4 to 42 weeks depending on trade. For those trades with longer courses, this is a significant time spent away and has a considerable impact on manning.

Years 6-11: Corporal. These are the years which will identify the leaders from the standard. Whilst the Signallers had to be given a hands-on approach and have visible targets to hit to keep them focussed and interested, once the Corporal completes his JCLM, he is largely given the time and space in which to demonstrate value. He will have to show leadership, create, innovate, expand his knowledge etc, unimpeded as much as possible by courses, and with his progress being witnessed more than directed, except when needed. It is during this assignment that the Soldiers raw potential is noted and reported on, allowing the stage to be set for the next phase in career, where he will be recommended for the Supervisory or Trade routes. By adopting this method, it shifts the focus away from baiting our potential Supervisors with financial gain, by instead breeding them through noticing, nurturing and exploiting their inherent supervisory potential. We meet the initiative they have already shown with initiative of our own.

Years 11-16: Sergeant. Having already identified the potential future Supervisors of the Corps, the first 3 years of this assignment are spent deliberately nurturing the leadership qualities required to become the most effective Supervisor possible, with the remaining 2 years – if they have been recommended to go forward for it – being spent doing the assessments and course. A Soldier who is engaged in the formal business of Supervisor Training should wear the nominal rank of staff sergeant to signify what he is to become. Potential RD will not wear the nominal SSgt rank.

Years 16-22(24): Warrant Officer. The rank of the Supervisors. Again, the Class distinctions are phases of development within the rank. The years spent as a Sergeant could be used to identify those with commissioning potential much in the same way as the Corporal phase was used to identify Supervisors. WO1 could signify a Soldier who is undergoing MK1 after years of having his potential maximised by his superiors.

Other thoughts

Financial Savings? Disturbance Allowance, FTOD and CEA could be made more or less obsolete, or dramatically reduced. You could save on wage bill by having less pay increments and slowing down the promotion vacuum. The role of RCMO's and the APC could be reduced by making the Army more self-determining.

Increased morale? Although not without its potential pitfalls, this way could possibly increase morale by giving soldiers the stability they want and by making them feel more valued through adopting the active mentoring and conscientious approach rather than shunting them around to fill gaps as and when they appear. Again, a more solid structure of liability is implied.

Improved efficiency? Increased capability of Training wings: If knowledge is power, it would be the equivalent – using the opening analogy – of always having your device plugged into the power socket. More time spent doing fewer things, even more time spent doing the same number of things, will naturally increase efficiency, but coupled with the mentoring approach and increased capability of Training Wings, the quality should be sped along and developed quite nicely.

This only has to be a temporary measure. The ranks are folded back, not eliminated, so there is always the option of restoring the old system once we are through the other side of the financial crisis and building the Army back up.

ROYAL SIGNALS INSTITUTION

Prizewinners in 2011

The Royal Signals Institution prizes for 2011 have been awarded as follows:

The Silver Medal

Major (TOT) H Taylor

WO2 (FofS) WP Quinn

Sgt G Thompson

Master of Signals Award

Major PF Griffiths

WO B Paterson, RAF

Mr MH Shepherd MBE

Mr A Wilkinson

Medal for Adventurous Endeavour

SSgt TW Abbott

ADVENTUROUS TRAINING - A LEADERSHIP DEVELOPMENT TOOL

By Brigadier DG Robson

Brigadier David Robson has been keenly involved with adventurous training since joining the Army, and is a qualified Rock Climbing Instructor, Advanced Mountain Leader, Klettersteig Leader and Formation Skydiving Coach. He has run mountaineering, kayaking and skiing expeditions to the Alps, Rockies and Pyrenees, skydiving expeditions to Florida and Cyprus, and numerous other exercises in Germany, Spain and the UK. He was prompted to write this article after reading the CV of Major Dan Ashton, who is currently commanding 4 Military Training Squadronn in 11 (Royal School of Signals) Signal Regiment.

Introduction

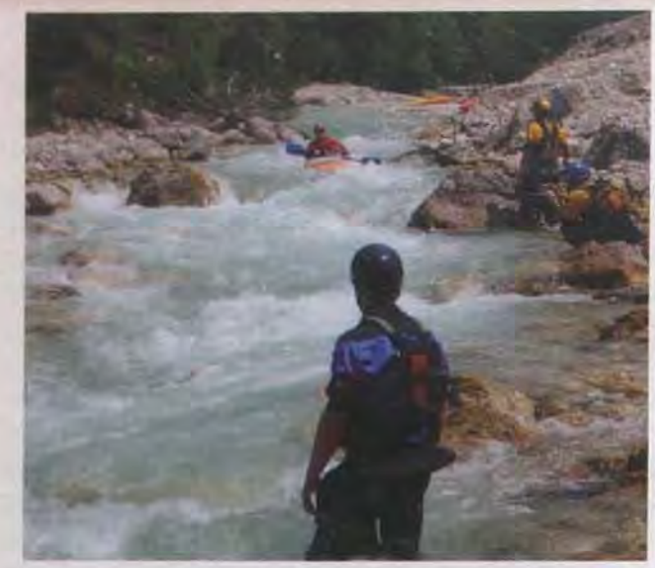
Major Dan Ashton's CV expresses his love for mountaineering, but more specifically, and related to his current role, identifies adventurous training (AT) as 'defining the qualities of effective administration, skills and leadership that is essential to success in the British Army'. I have long held the same view based on my personal experiences of AT and the evidence I have seen in the units in which I have served. So why is AT so different, indeed unique, as a training tool?

Armed Forces personnel require mental and physical robustness to withstand the rigours of military life. Out with active operations, AT is the only way in which the fundamental risk of the unknown can be used to introduce the necessary level of fear to develop adequate fortitude, rigour, robustness, initiative and leadership to deliver the resilience that military personnel require on operations. AT contributes to recuperation from the mental stress of operations, by re-introducing the concept of fear in a controlled environment. AT is therefore a core military training activity, which supports operational effectiveness and the ethos of the Armed Forces. AT has most effect when delivered as part of a wider programme of through-life personal and professional development.

The policy statement identifies a number of reasons why we use AT to improve our operational effectiveness, and cites the inducement of fear as being the essential element that is needed to derive the effect we seek. The ability to handle oneself, and in particular the critical requirement that our leaders understand themselves and how they will react when frightened or under extreme stress, is key but the value we derive from AT as a leadership development tool is much broader than that in my view. The planning and conduct of AT exercises offers a powerful medium for leadership development in our officers and NCOs. It demands the full range of practical and intellectual skills that we look for and value, and teaches other crucial lessons such as effective administration and logistics. It requires our instructors to acquire teaching and coaching skills, and nurtures self-confidence, all of which have direct read across into our mainstream military roles as I hope to demonstrate in this article.

Fear

Before I expand on the planning and development benefits of AT I want to return briefly to the subject of fear. Why is it so important that our leaders in particular experience fear in training? It is critical because we must know ourselves ahead of the point when the lives of our soldiers are dependant on our ability to think and act when the perceived risks to life and limb are high. If we analyse how we react when we are scared, or in the hands of a good coach have that analysis done with us, we will be alive to how we are likely to behave in the future when 'gripped'. This allows us to mitigate any less useful traits we may have, and devise coping strategies where necessary. Let us be absolutely clear here, fear is not a weakness , it is a fundamental human emotion that serves to enhance our chances of survival as an individual and as a species, and it affects individuals differently (not better or worse, just differently). A lack of fear when the odds are shortening is every bit as dangerous as an inability to act, if not more.



Student navigating the Upper Isjar, Austria, Grade 3

We need a level of self awareness that enables us to train ourselves. We must be able to say to ourselves 'I'm not brave, and I know it. I know that my instinct will be drop to the back but because I know it I will guard against it and drive myself to the front. I know how I will react because I have been here before and I can already visualise and rehearse what I am going to do'. It is not just about our tendencies to avoid, or rush headlong at, physical danger, we also need to understand how our cognitive processes will be affected. Do I become indecisive? Do I grasp the first idea that comes into my head because any activity is better than none? Do I stop listening? Do I withdraw to work out the next move? Do I get shouty? I have always found it is easier to spot the traits in others before we spot them in ourselves!

Exercise Planning

So fear, and more particularly our response to the sensation, is an important facet of AT but my thesis is that the practical value of AT for our leaders goes way beyond the conduct of the activity, and is as much in the planning as it is in the execution. The planning of an AT exercise, even a low level and short duration one, requires the leader to address every facet of the expedition. Unlike our military exercises, the idea for the expedition will normally be the product of the imagination and research of our junior officers and NCOs, and they then start the plan from scratch. No-one is going to issue them a set of orders from which they can extract their part. The leader will decide on his/her aims, take advice as necessary from the QMSI, RATO and others, and request copies of relevant Post Exercise Reports from Adventurous Training Group (Army).

For 'High Risk and Remote' expeditions there are additional complications and scrutiny but assuming our potential leader has more modest aspirations they will now address the various factors that will lead to tasks, freedoms, constraints or information requirements (sound familiar?) Costs and the availability of funds/grants to offset them are always high on the list and very often lead to a 'Question 4' moment. Equipment is generally available to support most aspirations but decisions on what kit to bid for need to be taken sufficiently early to meet the DSDA timelines. Transport needs to be planned whether air, road, rail, or donkeys, and is often far less simple to organise than one would imagine. The leader needs to source the necessary maps, try to find guide books printed in English, or be able to translate them. They must produce a medical plan. If freeze dried food is required it must be purchased and planned for in the baggage etc.

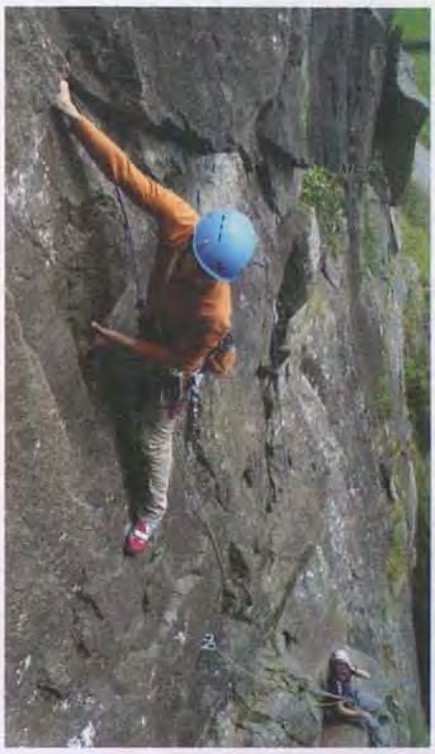
The exercise leader will seek the guidance of the MTO, RMO, Media Officer, RAO, QM(T), RCWO, and external HQs, and are way beyond their routine boundaries (this process is of course common to many such training activities including a sports team touring overseas, battlefield tours and so on, and not limited solely to AT). Once they have a plan they must also gain the necessary political clearances. During the execution phase of an expedition they are the MTO, RAO, and so on – responsible for every element of direction and administration for their soldiers, vehicles, rations and equipment across the range of G1 to G9 activity.

Type 3 AT - Expeditions, and Type 2 AT - Unit Training

The execution phase of an expedition (known as Type 3 AT in the JSAT Scheme) brings unique challenges for our young leaders as they embark into the unknown. In the extreme they will be in a foreign land that may have very limited or unreliable mapping, communications with the local people may be limited to gestures, there may be no medical support in reach, and no way of communicating with the outside world short of sending a runner back down the valley (this may sound like France to some less adventurous readers). Uncertainty becomes a fact of life, and the impact of a hole in the plan will not be rectified by a quick call on the mobile phone or popping back to camp. Big holes in the plan may have disastrous effects on the exercise participants.

We must also be cognisant of the fact that there is no discipline system to fall back on in the hills or on the rivers. Dealing with misbehaviour or an unwillingness to participate is done at the most basic level through raw leadership ability. You can't invoke the assistance of the chain of command, and the threat of formal disciplinary action (although in serious cases it may be the final result) is going to be of little help with another 2 weeks of isolation ahead of the group. The expedition members must have confidence in their leader if the exercise is to be successful. Above all the leader must lead by example and be sensitive to the needs of the group – listening is an often overlooked but essential element of leadership.

Planning and running Type 2 AT (as Unit Challenge Pursuit type camps are now defined in JSP 419) may not have the isolation, risks or foreign travel elements common in expeditions but they still demand first class organisational skills, and the planner must still navigate through the complexities of land clearance, equipment bids, ration and MT accounts. They demand effective delegation and organisational skills as you tend to be dealing with often quite large groups of individuals, which comes with its own challenges.



Lead climbing on Grim Wall, Very Severe 4c, Tremadog, North Wales

Instructor Qualifications and Coaching

Having discussed the benefits of the planning and execution of AT exercises let me now turn to the merits of our people becoming qualified as AT instructors and coaches. The reader should note that there is widespread muddling of the terms leading, instructing and coaching, and the terms are employed differently in each of the disciplines.

Leader qualifications under the JSAT Scheme are primarily about giving soldiers the opportunity to experience an activity or environment, rather than being about teaching skills. The definition is not hard and fast though, and in specific cases (for example the Joint Service Mountain Expedition Leader) qualified leaders may award Foundation level qualifications through the Distributed Training scheme (see below). We should not mistake AT Leaders for some sort of tour guide though. In fact, almost uniquely, in the mountaineering environment the safety of the leader depends in a most fundamental way on the ability of their charges to carry out the actions they have been taught quickly and effectively (belaying being the obvious example). Even relatively simple days out are, therefore, an excellent vehicle for the development of teamwork, mutual trust and self-confidence. The Instructor awards permit the holder to teach the discipline to students. They also allow for the conduct of Distributed Training on behalf of the JSAT Centres and enable the holder to assess students for Foundation Awards The syllabus for the training and associated supporting material is supplied by the lead JSAT centre.

The instructors in paddle sports are known as Coaches. This reflects the fact that you can teach strokes, how to read the river, safety drills and so on (skills) but once the leader lets his charges loose on the river there is actually precious little that can be done to prevent them from getting themselves into trouble. You can shout instructions, use hand and paddle signals, and then rescue the individual and their equipment but you never have control over their movement. Being a good paddle sport coach demands plenty of experience and the ability to read your students well. As with all AT, good judgement by the leader is fundamental to success and to safety. For the students it is about applying the skills that have been taught, managing their fear and getting themselves through the rapid (preferably the right way up) as no-one else can do it for them!

Free-fall in Cyprus

IT'S A MAN'S LIFE IN BUSINESS DEVELOPMENT!

By Lieutenant Colonel (Retired) JP Munnery MBA BSc (Eng) CEng MIET

John Munnery served for 22 years in Royal Signals, being commissioned in 1966. He served in BAOR in 6 Infantry Brigade HQ & Signal Squadron, was Adjutant of 7 Signal Regiment, and then in 7 Armoured Brigade HQ and Signal Squadron. After Staff College he took up a GSO2(W) position at AWRE Aldermaston, and commanded 39 Brigade HQ and Signal Squadronn in Belfast at the height of the troubles, where he received a MiD. Following a tour as BM of the Training Brigade in Catterick he was promoted Lieutenant Colonel and appointed to a GSO1(W) post at SHAPE, from where he went on to command 29 Berlin HQ and Signal Regiment. In civilian life he was employed by British Telecom, Cable & Wireless and the Deutsche Telecom Group. He now runs his own consultancy company (Vitosha Consultants Ltd – www.vitcons.com) and has just concluded two years work in Muscat, Oman. He and Vesselina live both in Bulgaria, and Hove, East Sussex. Visitors are always welcome.

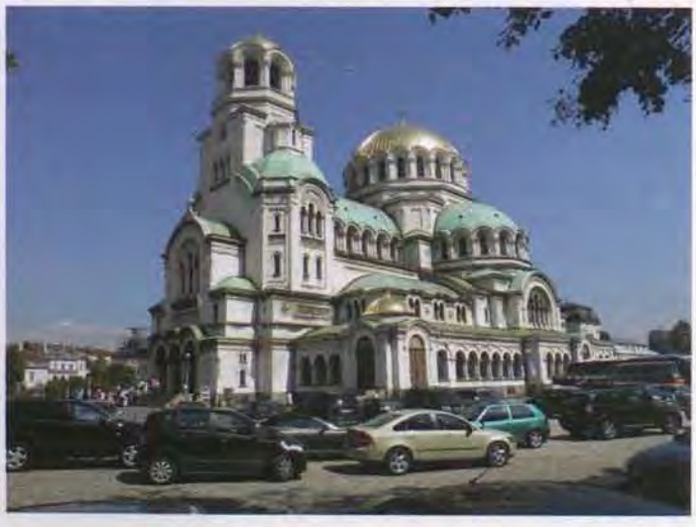
How on earth did I get here?

Flash back to a dull, muggy day in autumn 1993 in Bulgaria. We had just launched Mobile Phone Service in Sofia with a first generation cellular network (NMT-450 technology) a week or two previously with just three base stations as part of a tentative move into the Wild East by Cable & Wireless, and we were selling handsets at a rate far higher than my Marketing Manager's wildest dreams. But there I am, lying on my office floor with my arms outstretched. A senior US official (a customer from an agricultural aid initiative) has assumed the foetal position in an office chair in the corner; my secretary has locked herself in the toilet, from whence it took several hours to encourage her to emerge, and the Financial Accountant is on her knees following the CFO's 'what to do in a raid' procedure by proffering the key to the safe to the two surprise guests – two young thugs in jeans and bomber jackets wielding 9mm pistols who are assiduously paying her no attention at all.

This was a good moment for me to reflect as to how on earth did I get there (as 'Scotty, beam me up' was not an option)!

The Road Map to Bulgaria

Four years previously, almost to the day, I was sitting in the HQ Mess in Blandford with a severe case of post-command blues, and contemplating the future, when my eyes alighted on an advertisement from British Telecom which was looking for a Chief Engineer for international mobile projects. Having just completed a tour in Berlin, where I had my own budget because of the unique funding arrangements from the Federal German Government, I found that I actually understood the language of the advertisement as we had been engaged on the installation of several state-of-the art wireless systems in the city (in the words of Yosser Hughes from 'the Black Stuff' – "I could do that!"). For the first time in my life I wrote a CV, and was astonished to be invited to an interview. This was held in the BT Mobile HQ in Euston, and I was so convinced that I had made a complete mess of things I missed my underground stop at Waterloo, and did not become compos mentis until we reached Kennington Oval. I was amazed when I was told that I was the preferred candidate, and to cut a long story short early January 1989 found me reporting for duty.



The Alexander Nevski Basilica in the centre of Sofia. Built in honour of the assistance of the Russians from the 500-year Turkish occupation.

The first day of work was spent travelling to Stuttgart to take over leadership of the engineering group bidding for the German GSM licence, in a consortium including not only BT, but Daimler-Benz, Nynex (the New York New England Bell spin-off, now Verizon) and the power utility giant RWE. It really was a case of 'in at the deep end', and military experience was invaluable in the organisation of a diverse group with an understanding of technology and business process way ahead of mine to a common goal. It was a fantastic learning experience, but one where I quickly understood the limitation of military education when it

came to financial business modelling and some of the more sophisticated marketing tools both vital in the Business Development cycle, and I had to do some hard work to catch up.

A breathless two years followed with very extensive worldwide travel, and it became clear that the crumbling of the Soviet empire would open up substantial new business opportunities in Central and Eastern Europe. One day I found myself in the office of the telecommunications regulator in Prague, who was describing the country to me off a wall map in his office. "And here", he said, "Is where we used to build tanks!" He paused in mid-speech. He looked at me in shock – "if I had told you that a year ago I would have been shot!" I had to reply that if I had been there a year previously he would not have been alone in front of the firing squad. Shortly after came a call from a head-hunter (and another key difference from la vie militaire is that in civilian life you have to be your own career manager), and subsequently a move to Cable and Wireless as Regional General Manager for new business in Europe. Early movers had already established first generation mobile businesses in the three most attractive Eastern countries of Czechoslovakia, Hungary and Poland, but Bulgaria was somewhat behind in opening up and so I decided to focus there.

The parliament building in the centre of Sofia

Bulgaria is a country with about the same land area as England, but with the population density of Scotland, bordered by Romania to the North, The Black Sea and Turkey to the East, Greece to the South, and Macedonia and Serbia to the West. It has a history of not getting on with its neighbours – having been occupied by Ottoman Turkey for 500 years until 1878, getting the worst of the second Balkan War campaigns of 1913, and siding with Austria/Germany in both world wars. Since the liberation from the Turks, the country has had a history of being a divided society, unsure whether to look to the East or the West. The Cyrillic alphabet was developed in Bulgaria, and was subsequently established in other Slavic states, and there is a very strong Slavic bond which encourages the Eastern connection. However, and at the same time, there is a very strong identification with the more sophisticated role model of Austria, which historically has played a strong part in Balkan politics.

Even at the time of the liberation from the Russians, there was a division of views as to how this should be achieved, with the idealist national hero Vasil Levsik insisting oninternal revolution, whilst the soldier-poet Hristo Botev was convinced that external intervention was needed, prompting the intervention from expatriate Bulgarians, Russians and Romans. The revival architecture of the late 1800s borrows much from Vienna and Paris; and even in Communist times French was the most popular second language.

It is not a country used to ruling itself. Following the liberation from Turkey, the Bulgarians decided to appoint a monarch (Tsar). Curiously they chose a foreigner for the job (a precedent which many people think should be followed today), and appointed a member of the Battenburg line - Tsar Alexander - which tended to be Moscow looking. This did not work out well, and after a coup d'etat Prince Ferdinand of the Saxe-Coburg dynasty got the job – which was Vienna/Berlin oriented and kept power until 1944 despite a number of minor insurrections along the way.

The Saxe-Coburgs maintained a strong regime, and gravitated towards fascism. It is interesting to note that one of Churchill's objectives in the Gallipoli campaign was believed to be to encourage the Bulgarians to attack their recent enemy Turkey and to regain territory lost in the second Balkan war – which clearly did not happen (Balkan Wars for beginners – in the First BW the Balkan countries allied to throw out the remaining vestiges of Turkish occupation; in the Second they fought each other in a scrap for the newly acquired territory; Bulgaria did brilliantly in the First but heavily lost out in the Second).

In the Second World War, Bulgaria was the only member of the axis neither to send troops to the Russian Front nor to take major sanctions against its Jewish population (it took the Communists to do that later on once Israel was established, when there were massive deportations). Tsar Boris died in 1944 under suspicious circumstances following a visit to Hitler in Germany. His son, Simeon – then only a child – was crowned, but subsequently deported to Spain as a result of combined internal insurrection and Russian intervention down the Black Sea coast. Bulgaria was never occupied by the Russians, but threw itself willingly into the arms of Communism, led in the main by the partisan forces which had been involved in internal insurrection throughout the Second World War. A strong-liner-Georgi Dimitrov - was appointed Premier, but died in 1948 following a visit to Moscow (there must be a lesson for Bulgarian leaders making foreign visits.....). His body was laid to rest in a Lenin-style mausoleum in Sofia city centre, but his remains were moved following the political changes; the bizarre side to this (typical of Bulgaria) was that subsequently a 'blue' Deputy Prime Minister decided to destroy the mausoleum in a public display with a con-

trolled explosion. He pressed the button – and it fizzled. Conventional demolition techniques then had to be used.

Simeon Saxe Coburg II established his own political party, and was elected Prime Minister from 2001 to 2005, when the country had a bizarre political structure with a Moscow-educated Communist President, a former King as Prime Minister and a Jewish Minister for Foreign Affairs who gave the Pope an invitation to visit which was accepted!

October 1991 found me disembarking for the first of many, many times from an Austrian Airlines flight into Sofia, with just myself and a Queen's Messenger 'greyhound' occupying the business part of the cabin. He didn't stay very long – a quick tarmac turn round and back again. I was there for the week, and fortunately was well-prepared for what to expect having made many day-trips to East Berlin – grey Communist concrete apartment blocks, Stalinesque monolithic official buildings, and abject poverty. Empty shops, huge pollution from 2-stroke vehicles (even today the Trabant is alive and well in Sofia, although becoming something of a rare bird).

What did come as a surprise was the amazing warmth and hospitality of the Bulgarian people; and the superb climate – cold winters, but Mediterranean summers. The country is a garden, in which anything will grow, and the people did not suffer in the same way as others in the former Communist Bloc as private ownership of plots of land was permitted and everyone grows fruit and vegetables, and raises animals to supplement their diet. Even today many of the older local villagers near my house (just 20 minutes from the centre of Sofia) take their goats, sheep and cows to graze in the national park which surrounds us.

The sheer beauty of the land, which was left relatively unspoilt by the ravages of the Command Economy, although even today there are many scars left by the unbundling of former uneconomic State enterprises, with closed factories littering the suburbs of many towns. It is a land of mountains with three substantial ranges going up to some 3,000 metres. Musala, near the Borovets Ski Resort, is the highest mountain in the Balkans, topping Mount Olympus by 8 metres. Low population density has a lot of advantages - I can walk my dogs in the forest off the lead; I do not have to carry a plastic 'poop' bag; kids can go freely in the woods without fear, lighting campfires and cooking kebabchi. It reminds me of growing up in London in the early 1950s when the bomb-sites were our adventure playgrounds (no health and safely lot in those balmy days....).

Anyway, and back to the story, there followed some 14 months of solid business development activity as we (the Cable & Wireless team) got to understand the opportunity, and undertook the 'sell-in' to the telecommunications officials and their political masters. This was by no means easy; as there was a lot of competition for the single NMT-450 licence on offer, and the local regulators were terrified of making a wrong decision (a sense of individual responsibility was something that the Communist regime did not encourage). Personal sell-in was a key factor, with my team and me making it clear that we were personally committed to move into the country and to make the new mobile business happen. At the same time we were faced with the need to also sell-in the project to our London HQ, which was not always an easy job.

The signing of the partnership agreement between C&W and the Bulgarian partners; from L to R: Marian Dragustinov – President of BTC, Stefan Sofianski Chairman of the Committee for Posts and Telecommunications, author in a nervous hover, Lord Young, Executive Chairman of C&W.

A major factor in closing both sides was to arrange a visit for Lord Young, then Executive Chairman of C&W, who paid a personal role in convincing politicians that we were the act to be with, as well as carrying the message back to London that this was something that C&W should do. Official procrastination continued in Bulgaria, with a number of 'spoilers' making themselves evident. However luck was on our side and a very active and progressive Chairman of the Committee for Posts and Telecommunications (Mr. Stefan Sofianski, and an ally of ours) fell out with the Prime Minister and sensing that he would soon be replaced, presented us with our operating licence on the day before he was dismissed. (He later became Mayor of Sofia, being re-elected twice; and in addition was interim PM during a later period of political change).

We had the licence, we had a structure in which C&W owned 49% of the new Company (which was called Mobikom), and we had local partners in the form of the Bulgarian Telecommunications Company (BTC) which had a 39% stake, and a Company called Radio Electronic Systems (RES - part of the Interior Ministry industrial group) with 12%. C&W put in upfront cash equity, BTC (who had no cash) mortgaged assets such as leased base station backhaul lines and equipment sites in lieu of equity, and RES had access to funds from a local bank for their share.

It was now time to make it all work – and despite a C&W colleague telling me that as the new MD for the Company my problems were only just starting, actually it turned out to be the fun part.
We chose the NMT-450 technology, as it had become a de-facto standard for Central and Eastern Europe, due to a number of reasons;

- The 450 MHz band allowed for large cell radius essential for coverage of large areas, both for rural environments, and for coverage of cities with low cellular penetration. A cell based on the mountain above Sofia actually had a reach of 100km; but soon had to be turned off to reduce interference once customer numbers climbed and demanded smaller cell radii for capacity reasons.

- Cocom regulations initially prevented the export of advanced digital technology to the Region.

- We were able to use analogue channels for backhaul (BTC had virtually no digital channels available initially).

Building the New Company

Setting up our first-generation cellular booth at the Plovdiv International Trade Fair. A poignant picture for two reasons: firstly in the centre in the dark suit is Roger Short, the then UK Ambassador to Bulgaria who was a great supporter of ours and was later tragically assassinated in Istanbul where he was Consul (he was a great Balkan expert and planned to retire to Turkey); and secondly on the far right our first Bulgarian Head of Marketing – Vesselina Paskova – who later became Mrs. Munnery

Imagine yourself thrust into a (very slowly) emerging economy and being asked to establish what was effectively a Signal Regiment from the ground up using a management training team of about 12 people (to thin down to 5 within a year); a budget of £3 million in cash to cover both operational and capital expenditure until financial break-even; and a tough regulatory coverage requirement to be established within 18 months of licence award. Add to that layers of bureaucratic process at all levels – from company registration through to permissions and appro als for infrastructure sites, and, horror of horrors, the eagle eye of C&W Internal Audit hanging over you.

The start-up team on the day of the NMT licence award in front of our very Spartan office accommodation. Author left, Headley Hamiliton, our first CFO (who went on to the EBRD); Phil Watt deputy CTO, who also went on to do great things; Jean Oelwang who now works close to Sir Richard Branson; Bistra Hristova who excelled at keeping the regulators under control; John Carrington, our Boss from C&W; Svetla Nestoraova, who is now Svetla Potter and working for Colt in London, a visitor; Jim Courtney who set up our IT and billing systems, an LSE graduate who is now a Chief Officer in a major South African Mobile network; Jana Voinikova our Office Manager and fix-it lady; Rupert Trollope (a relative of the author Joanna Trollope), a brilliant Cambridge and INSEAD graduate who was my number 2 in the BD process, who regrettably died very young.

The core expat team was based on a number of individuals who had become personally committed to the project and had developed for differing reasons a love of the country. Over the years some 30% of the team (including myself) married Bulgarian wives, and are all living happily ever after. We had to rough it. There were no prizes to be had to be seen living in exorbitant style, at a time when the pay of our employees averaged about 400 euros per month. We shared electricity cuts, water shortages and even petrol and bread rationing in the early years of the initiative. We established a head office in a run-down row of shops belonging to our partner, BTC (part of its contribution in kind), and had what I was later told was called a 'Lenin Saturday' when we all came in, hosed the place down with the fire hydrants, and installed very second-hand furniture bought from a failed computer company. No frills at all. Our technical centre, however, required substantial investment and this was built into a nearby BTC exchange substantially rebuilt to suit the demands of a modern Ericsson AXE Mobile Switch. This was at the time the most advanced platform of its sort in Bulgaria, and was a massive leap forward from the Siemens 1920-vintage step-by-step exchanges accommodated in the other floors of the building.

Staffing the company presented some interesting challenges. Technical staff was not a problem. The standard of university education in telecommunications was high, and while we could find a lot of engineers well versed in digital technology, they had never been given a train set to play with. More difficult was the principle of establishing no-smoking rules in the office, as in Bulgaria smoking was then almost compulsory. Additionally, trying to force delegation of responsibility was a challenge, as people were simply not used to being allowed to make, and to be responsible for, their own decisions.

Rolling Out the Network. The opening of our retail centre in the ancient Bulgarian capital of Veliko Turnovo – a city now heavily settled by UK retirees.

Marketing and Sales was easier, as Bulgaria has something of a bazaar mentality and sales skills were relatively easy to upgrade to our required standard. Everyone thinks that they understand marketing, but we did have to undertake a lot of formal offshore training for key team members to impose up-to date disciplines and methods of analysis.

Most difficult of all was to find people for our Finance and Billing area. Computer-based accounting and billing were unknown outside one or two Western-based businesses; and BTC billing was still based on photos being taken of the meters attached to individual subscribers relay sets. We tried taking the best economists and bookkeepers from the market, but it just didn't work. The answer was to headhunt the best qualified software engineers from the technical university, who were confident in front of a screen and keyboard, and to teach them accounting and billing disciplines. This was a resounding success, and today many of these individuals are CFOs or equivalent in major companies, and one is in a senior position in the World Bank.

Motivation was crucial. People had to be encouraged to go the last mile, most of this being energised by example from the expat team. People were key to making things happen, and motivating the very young team of Bulgarians we took on (the older generation were past redeeming) was easy. Salaries, although higher that the Bulgarian norm, were pitifully low, and we sought to do other things to reward them; foreign training courses, good working conditions with modern equipment, but above all engendering an atmosphere of mutual respect – which was non-existent in Bulgarian-owned enterprises. I have to say that my single greatest personal achievement from the Mobikom experience was not the business success (which was substantial), but rather the life-changing opportunity we gave to our young Bulgarian team. Almost without exception they seized the opportunity given to them and the vast majority have moved on to senior executive positions nationally and internationally, both within and outside telecommunications. This did not just apply to the Bulgarians; many of my expat team benefitted from the experience and have moved on to much greater things – as just one example, my first Head of Marketing (a wonderful American lady called Jean Oelwang) is now sitting at the right hand of Sir Richard Branson running his not-for-profit initiatives.

We launched the network, and had an outrageous success on our hands. Early adopters – typically for start-up mobile networks in those days – were businessmen, film stars and criminals. There are not too many film stars in Bulgaria, and the division between the other two categories was, and remains to some extent, fairly obscure. Which brings me back to the start.....

Back to the Floor of my Office

The two thugs had things under control, and there as a pause, when they were followed into the office by men in black, wearing ski-masks, carrying automatic weapons and with the word 'POLICIA' emblazoned across their body armour. It was a raid by the anti-terrorist police, and the 'thugs' were plain clothes members. We were frisked for weapons and the offices were searched. As is often the case in Bulgaria, this was all a bit dysfunctional, as they missed one office block and our technical centre entirely. Things started to become clear. The previous evening there had been a Mafia-on-Mafia shooting downtown, and one of our new shiny phones had been found at the scene. Having heard of this the following morning, we immediately called the authorities and told them that we had certain functionalities in our technology which were lacking from the fixed network (identification of the owner of the phone, billing records, etc) that might help their enquiries. However, the more enthusiastic members of the constabulary obviously decided that we were a criminal organisation that needed stern action.

Pulse rate having subsided somewhat, I sought out the raid leader, a Colombo look-alike complete with beige raincoat and dark glasses and asked him what was going on. As he was looking down his nose at me, the Company lawyer appeared and gently explained to him that we were a foreign investment, with majority state participation, as well as a substantial shareholding from the Interior Ministry itself. His face rapidly assumed the 'Oh S**t' expression.

There were a couple of outcomes. At 6pm the Secretary General of the Interior Ministry appeared in person to offer profuse apologies. Rather sadder to relate, the same anti-terrorist team was involved in a blue-on-blue incident the following day, when two of the policemen were killed.

Mafia Moments

Organised crime has been, and still is, part of life in Bulgaria. It has moved on over recent years from Deadwood 1880s to Chicago 1930s, with many 'business' organisations now developing conventional business fronts. Corruption is endemic, but Western business simply ignores it. It makes life more difficult, but is the only way to go. Those who chose the slippery slope of compromise with local business ethics never get on well in the long run. Anyone wishing to understand more should research Wikileaks and cables from the US Ambassador, which give a good insight into what goes on. Suffice to say that the Godfathers seem to achieve a remarkable extent of untouchability; and while arrests happen, prosecutions rarely succeed. I believe that this is something that will take a generation to change.

However, it has given us some 'moments':

- I have met two 'businessmen' who have been subsequently assassinated, of whom my wife had known three. I do not seek to match her score.

- An old telecommunications story did actually happen here. A 'Mutra' (heavy wrestler type, thick neck, gold chain, dressed in black) waddled into one of our shops with a carrier bag stuffed with low-denomination banknotes (it was the height of the hyper-inflation period) and said he wanted to pay his bill. The cashier told him that it was far too much money. He the pointed at the sum on his bill, and had to be gently told that this was his phone number.....

- I was driving into the North Western town of Vratsa one day to check on arrangements for mobile service launch. I was stopped by some Mutri on the way in (our vehicles all had logos – it helped to cut down on vehicle theft), with one telling me that his phone was working. I explained that this was a pre-operational phase and that we would officially launch the following week, but that he was welcome to use his device, as billing was working. He then pressed me and asked 'BUT is the service OFFICIALLY opened here?' I told him 'No, next week'. So he switched off his phone and said 'I will wait until it is officially opened!' The bureaucratic mind even spreads into organised crime, it seems.

- The Mafia had, and to a smaller extent still do, have their major impact on the weaker members of society – such protection racketeering (now developed into conventional insurance and the private security businesses) – and in the early days we did have some approaches into our regional shops. However it was impossible for local thugs to find the right target. Approaching a junior sales assistant with some threat, they were told that such matters were dealt with in Sofia, or even maybe London. It all became too much for them, and they went off to seek softer targets.

Please don't get me wrong – Bulgaria was and remains a very nice place to live and to do business in, but just has some special environmental factors which have to be taken into consideration. On the credit side consider the geography – when you can't swim, you can ski, and vice versa. There are four main ski resorts – the usual Bulgarian dysfunctionality means that they will never be like Austria, but are otherwise quite acceptable; the nearest from my home is just 20 minutes away on Vitosha Mountain, overlooking Sofia. The northern Greek Aegean beaches are just a four hour drive away, and the Black Sea is nice when the Mediterranean is too hot. Add to that a 10% upper income tax rate and very cheap living expenses, and above all the people, and then the benefits outweigh the negatives substantially.

Moving On

The business developed well, and at its height had a turnover of some 150 million Euro per year, with some 700 employees, and network coverage of 98% of the territory. We also developed a nationwide Paging network (POCSAG), and later Internet Service Provision.

We faced competition with the mobile network from a very early stage, from a local entrepreneur who' managed' to get a bare minimum of GSM spectrum from the military (which was stated to be unavailable to us), but the NMT did us proud – we held off completion successfully for some 8 years particularly through superior network coverage and simply knowing our job better, and as well as introducing a lot of innovative features such as anti-cloning features, frequency interleaving, advanced cell repeat patterns, and adaptive power control – all of which were never part of the NMT specification. We were able to achieve separation of just 500 metres between city cell sites -something for which the 450 band was never intended. Our antennas for the final configuration caused some consternation amongst the technically minded – the directional antennas were actually tilted upwards towards the sky. The reason for this was that we used electronic downtilt in the main beam, but the uncontrolled back lobe (a major interference source) was actually being fired back into the ground. Such ideas were generated by encouraging original thought amongst our young employees.

Business success allowed us to be generous. We could not solve all the problems of Bulgaria on our own, but we did our bit by adopting an orphanage and making it a rather better place than some of the nightmare places in the country. We sponsored many concerts, bringing in performers who had never been seen in Bulgaria before (such as Sting, Vanessa Mae, Plant and Page of Led Zeppelin, Uriah Heep, Nazareth, Metallica and many others). Good advertising, but very much a fun thing

to do. We were particularly proud of our sponsorship of a combined archaeological 'dig' over some 5 years involving The Universities of Nottingham and Veliko Turnovo, which produced a great deal of unknown information about the late Roman/pre-Byzantine history of the region. Key in arranging all of this was my later Head of Marketing, Vesselina, who was so brilliant that I had no choice but to marry her.

True, but sad to say, nothing lasts forever. In 2002 Cable & Wireless had a strategy change and put up many of its businesses for sale to fund its expansion into Internet services (it has been said that it 'bet the shop' on this – and lost heavily). This meant no migration to GSM technology for us, and an inevitable decline as GSM was now starting to take a hold. At the same time I had an invitation from the Deutsche Telecom Group to become CEO of the newly-privatised Macedonia Telecom, which I accepted – an incubent fixed-line and GSM business. Skopje is just three hours from home, so easy weekend commuting. Some 5,000 employees so I was getting my Signal Brigade, and there was a war going on – but that is a story for another day.

ARTICLES FOR THE JOURNAL

Articles are sought for publication, subject to editing and the possible risk of omission if we are deluged with copy! Electronic Word format in Times New Roman 11 point type is preferred.

Original quality photographs and diagrams should where possible be used to complement the text. These can be sent as jpeg files separate from the article to the current e-mail address of rsi@royalsignals.mod.uk until the new e-mail address of Secretary@royalsignalsinstitution.co.uk comes into effect from 1 February 2012.

Please note that the deadline for submission of articles for the Spring 2012 edition is 23 March.

DATA OVER HCDR ON OPERATIONS! - TIGR, THE STORY SO FAR...

By Warrant Officer Class 2 (Foreman of Signals) WP Quinn, Royal Signals

WO2 (FofS) Warren Quinn has been the CBM(L) Trials Troop Foreman since it rebranded from the Bowman Trials Team in June 2009. Since then he has been deeply involved in the acceptance and development of BCIP 5.4 along with a myriad of smaller capabilities from batteries to manpacks and test kit. Recent developments have seen him become the UK military foremost SME on TIGR, with particular regard to extending the capability to the lower formations using BOWMAN. In 2010 he put forward a case to Land, PJHQ and CSD to be allowed to deploy with a planned TIGR Fielding Team, whose aim was to deliver a standalone capability, training and develop operating procedures in theatre, in preparation for the development of a networked solution. The Foreman argued he could do more, sooner, if allowed to try. He is an advocate and active committee member of the Armed Forces Communications and Engineering Association (AFCEA) for the southern region. His previous post as a Foreman was at 21 Signal Regiment (AS) during which period he was recognised at an award ceremony in the US as a Distinguished Young AFCEAn, for work carried out on the Foreman course project (with FofS D Gunn) and afterwards whilst at 21 Signal Regiment (AS). He has this year been presented with the Royal Signals Institution Silver Medal for his work on TIGR.

What is TIGR?

The first question I am always asked is, "is it pronounced 'tiger' or 'tigger'?" A simple question, yet you would be surprised by the amount of times it is asked. As it causes such interest, let's make it clear. TIGR is pronounced 'tiger' by the US and pictures of tigers are all over release documentation. However, we in the UK use the term Tiger Teams to refer to trouble shooters and also have a Tiger G4 team. So, by power of will alone, let's pronounce it Tigger! It does cause confusion, people thinking we had a Tiger Tiger Team and that it had something to do with bar codes or equipment accounting! Not an area a Foreman necessarily wants to be seen working in!

Tactical Integrated Ground Reporting (TIGR) is an application brought in as an Urgent Operational Requirement (UOR) to address capability gaps with tactical situation awareness (TacSA) to support the wider Counter IED (C-IED) fight. This improved SA has a primary benefit of reducing risk to patrols - it has the potential to save lives! Having been developed by Ascend Intelligence in the US it is now provided to the UK under license from the DoD's Defence Advanced Research Projects Agency (DARPA).

The core C-IED benefits of TIGR are achieved in two main ways; firstly by the identification of threat patterns, denoted by significant activities such as IED types, found in a given area and prevalent sighting locations. This serves to help identify Vulnerable Areas (VA) or Vulnerable Points (VP) prior to deploying onto the ground. Of course it is not the only aid to identifying VAs and VPs, so the normal indicators such as channeling should still be utilised. Secondly, it helps to prevent friendly forces from setting patterns, which can then be targeted by the enemy. This is done by recording patrol honesty traces and sharing this information theatre wide, to enable the next patrol routes to be selected with this information in mind.

I can understand how a reader may not immediately appreciate the benefits of exploiting these two areas of information, but rest assured, the patrol commanders I have seen go through some training scenarios appreciate it immediately.

Screen shot from the DARPA Tactical Ground Reporting (TIGR) System (synthetic data).

The secondary benefits include:

- The sharing of local information over the tactical network such as pictures of friendly or enemy personalities in a given location, including prime sleeping locations.
- The ability to carry out basic human relationship analysis.

- The means to inform limits of influence, for basic Operational Analysis.
- Providing a simple means of identifying threat patterns; for example, over a previous Herrick, x % of significant events in an AO were sharp shooters. Over the first three months of this Herrick the most frequent event is Command Wire IED at y %.

Where Are We Now?

From early 2010 CIS TDU has been supporting a CSD Apps, TacCIS initiative to exploit the capabilities of HCDR in theatre. This initially began as private venture work for the Troop and Maj Marsden of TacCIS, giving the troop the freedom to investigate what could be achieved. Concurrently Land ISTAR was developing TIGR to replace the in theatre means of recording patrol honesty traces in DataLogger. This work lead to the first TFT being formed and deployed to theatre to support TIGR for 16AAB on Herrick 13. This standalone capability would be phase one of three, moving to a maximum tactical network, gatewayed into Overtask, for Herrick 16. The multi capbadged team consisted of (see Figure 2):

The TIGR Team. OC - Maj S Finch RE, centre. Trg Lead. To support RSOI and deliver training as far forward as is required – WOII J Pearson RA, fourth from right. Exploitation Lead. To ensure best practice is delivered theatre wide and aid in the development of other J2 opportunities – Cpl M Lampett, Int Corps, third from the right. Data Manager. To address and manage the myriad of very challenging GEO and imagery tasks. Including deep database integrity management – Cpl Jones RE, second from right. Network Lead - WO2 (FofS) W Quinn, second from left.

CIS TDU grasped the opportunity to share the lessons learned on the various lab tests and trials. So after putting our case forward I was given permission to deploy as the Network Lead for the TFT. This was done in the knowledge that a BATCIS delivered networked TIGR solution was not due until Herrick 15, but with the authority to make best efforts and utilise the as yet unused HCDRs around Helmand. Immediately, it was made clear that as the official solution was in the pipeline, any advances in networking, whilst authorised, would be on a self help basis – there would be no cash from the system. Any solution therefore needed to be easily supportable while providing an appropriate level TIGR data synchronisation across theatre that could be trusted by the user.

The gains available from the development of this network were by no means trivial. It is important to understand that up until this time, any sharing of TIGR data or honesty traces was done by hand. This required the passing of secret disks by hand, around theatre and brought significant risk and delays. Ultimately that information could be up to three weeks old, if you got it at all. The use of HCDR, at company level and up, if held, reduced this time to minutes, greatly increased the audience and improved the credibility of the message. In short it passed the message swifter and more reliably - that sounds familiar - and this was achieved without any user interaction, on a system that was sat waiting to be exploited.

The Challenges for J6

Whilst no one task was particularly challenging from a technical perspective, a large number of interlocking factors, aggravated by 'theatre realities' brought quite a challenge to the J6 solution. These included, but were by no means limited to:

Information Management. The brigade information manager, Maj V McNaught, as a strong advocate and driving force for TIGR in the Bde had a very clear idea on what levels of information he needed to share amongst and within the Battlegroups. This could be achieved within TIGR as it allows for six levels of synchronisation between each location, via logical TIGR links, over the physical infrastructure. Supporting and detailed processes would still need to be developed to ensure locations without HCDRs could access the most recent data and submit their own data in support of flank units in a timely manner. More than once, the TFT deployed forward to deliver this information, whilst processes were developing, to support immediate operational planning.

Equipment Distribution. The limits at the time, of only having HCDRs in BOWMAN Deployable Ops Rooms (DOR) lead to a maximum limit on what could be achieved by the TFT. This challenge was magnified by the lack of investment in the BOWMAN data network over previous Herricks. This was somewhat understandable, as it wasn't being used and there was no known plan to do so, it did leave some locations in a position where they could not immediately operate, once authorised.

There was also a need to purchase small items such as hubs and cable heads and other miscellaneous items that were at that time un-codified. Comd JFCIS was more than willing to help here when able and the IPT also cajoled into releasing some funds to help. But all-in-all, less than £2000 was required to support the project. The challenge then, once the appropriate source were identified, was to deliver the items to theatre. The Troop supported me by driving round the UK purchasing and delivering to purple gate, and even the SO1 ISTAR at PJHQ was roped in, to deliver some items to theatre whilst on a visit! A good team effort.

Support. This is always a challenge for a UOR, as I am sure you appreciate; the policy for TIGR was to buy enough spares and replace them on failure. This may be a valid method if you are focused on delivering equipment, but when delivering a capability, a wider view is required. Here the goodwill of individuals and the CoC in JFCIS and deployed elements of the USSO enabled a model to be developed and loosely followed (Figure 3) whilst the formal recommendation of the solution was passed back to the UK. Unfortunately, a formal support package for TIGR was not achieved by the TFT.

Network Architecture. As we all know, the HCDR is a self forming and self healing network. In a Brigade AO in Europe, with HCDRs everywhere and traffic flows expected to go in any direction, that is fine. In Helmand however, where there aren't many radios and we know the flow of data is not only more hierarchal, but to be controlled, things are slightly different. One must consider the HCDR stages of Island Heads, Cluster Heads and Net Members as well as the number of channels available to data and management and how they are re-used throughout clusters; and then take this into account when carrying out bandwidth management tasks for the guest data service, in this case TIGR. Consider the three open questions below and you will start to see the many levels of challenges that need to be managed:

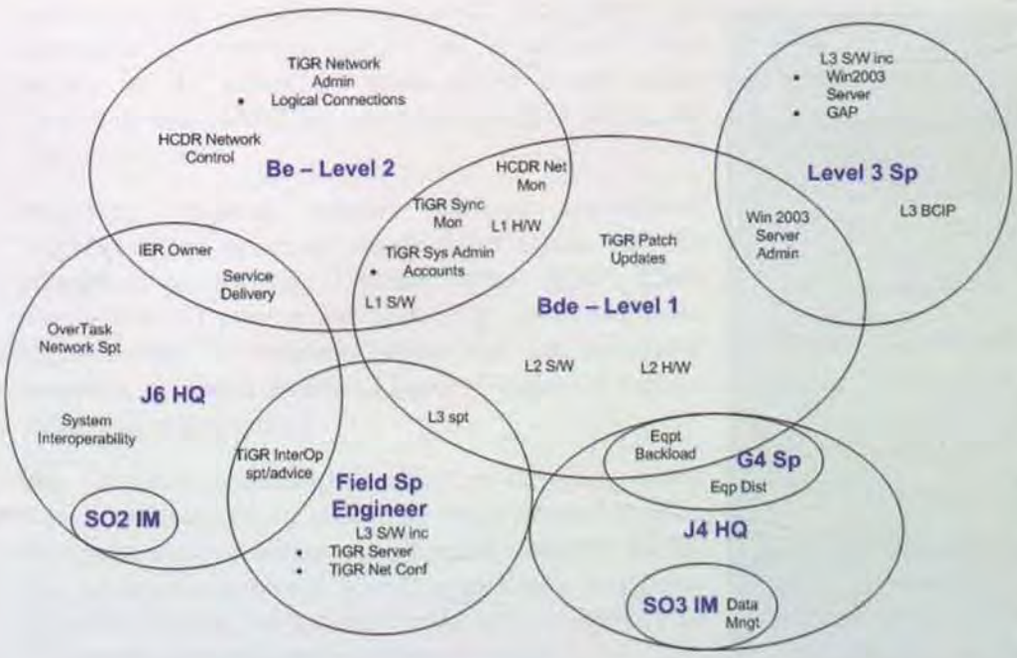
Q1. A Company server should synchronise with its Battlegroup's HQ, if we are to follow the IM plan. But what happens when the HQ is two or three HCDR hops away and in another cluster? What latency can this bring ("it can double it")? And what speed shall we configure our logical links over these multiple hops without the benefit of the BOWMAN CFP stack?

Q2. What if the Cluster Head is from an alternate Battlegroup, meaning it controls your available channels and routing, how then shall we share the data?

Q3. Are the benefits of a self healing network still a benefit, if we have balanced out the bandwidth to achieve a set QoS and then a new location comes on or moves, resulting in new or different Island or Cluster heads? How is this managed?

User Buy-In. "Hello Sir, I have come to put your TIGR over your HCDR". "Data over Bowman, I have done my RSO course, you have no chance!" The perception that accompanies conversations such as this brings some real challenges to delivering a capability, especially when the user is also focused elsewhere and that capability is being delivered on a self help basis. To counter this perception, a series of in-theatre trials were run to generate the required user buy-in. These trials served to achieve exactly that. After only a few weeks of networking TIGR, the team would receive calls from some of those same customers asking "how do we get more HCDRs?" One measure of success!

I hope this article helps BATCIS fight the good fight and get the word out that BCIP 5.4 and BOWMAN data work!



What is Next?

SSgt (FofS) Taylor of CSD Apps has recently returned from theatre after leading TFT 2, with the aim of delivering networked TIGR, using the provided formal solution. Unfortunately the UK trials of that solution identified some technical limitations that were sufficient enough to prevent it from fielding to theatre. TFT 2 were therefore tasked to expand on the self help solution, with the added value of further HCDRs being delivered with the

new Modular-DOR (M-DOR), also trialed by CIS TDU - this work is ongoing.

In the long term, BATCIS is still persevering with our industry partners to deliver a more appropriate and scalable network solution. This will undoubtedly include the ATIS protocol, which accounts for the lack of CFP stack and wraps the TCP/IP traffic in such a way as to 'play nice' in the RF environment. This feature will include the ability to auto throttle the network as congestion occurs.

Recent field trials of ATIS on the same network as BCIP data, FC-BISA and MAKEFAST BISA have shown that ATIS will bring a much improved throughput and all these data types can be handled by the BOWMAN network without the loss of a single message, even with platform mobility. ATIS is still in development, but CIS TDU and C2DC are regularly used to aid in that development. It is anticipated that formal trialing of ATIS will begin in September 2011.

Their are two deployment options when it comes to ATIS: a standalone application on the server or on a Versatile System Access Point (VSAP), which aims to reduce the management burdens felt by the first Fielding Team. The benefits and challenges of each are as different and complex as networked TIGR it self. Time and September's trial will tell which way we will go.

Prizes in the Journal

We are pleased to announce that the prizes for the best articles in the Spring 2011 edition of the RSI Journal have been won as follows:

£100 - "Mr Pepin of Marlborough" by Dr B Austin

£100 - "Traffic Engineering in the Military Environment" by Major MC Duff

£100 - "The Rev John Gamble, The First Chief Signals Officer" by Rev Roy Burley

Our congratulations go to them with the hope that other Journal readers will be inspired to send us more such high quality articles

TACTICAL COMMUNICATIONS 2011

By Major (Retired) JKC McLean

John McLean served in the Corps from 1965 to 1984, and *saw service in Northern Ireland and BAOR, interspersed with tours in an Army Youth Team, the Far East, HQ UK Land Forces and the Ministry of Defence. He commanded The White Helmets and 63 (SAS) Sig Sqn (V), and gained Corps Colours for tennis and Combined Service Colours for yachting. On retirement, he held several positions in industry, including being a Director of Unisys and participating in many Defence IT projects. He is now a freelance author and journalist at jkmaclean@btopenworld.com.*

Introduction

The Defence IQ conference on modern-day Tactical Communications was held in April at London's prestigious Dorchester Hotel and was chaired by Lieutenant General Robert Baxter, our Master of Signals. This summary is slanted towards UK communication integrators and to enlighten those who, like the author, have their signalling experiences firmly rooted in the last century!

Advertised as "enabling advanced, networked and interoperable communications", the conference dwelt largely on the extent to which armed forces within Coalitions and NATO are carrying out these echnically challenging tasks.

Presenters covered current military operations, interoperability, spectrum management issues and the emergence of Software Defined Radio (SDR). There was a heartfelt plea to 'do something' about perceived short-comings of infantry radios and for equipment suppliers, a market forecast of global values of tactical radios and radio systems.

Our Chairman observed that effective signalling meant achieving results on the ground by conveying information to a given location where it can become tactically useful. The conference explored how this challenge was being addressed within the nature, terrain and complexity of contested operational environments.

Operations in Contested Environments

In his keynote address Brigadier Alan Hill, Commander of 11 UK Signal Brigade, which sustains and supports UK field operations, highlighted the positive impact of digital radio. A variety of broadband applications are now becoming available to support mobility and situational awareness within patrol bases.

In collaborative working, it was important to ensure benefits to the troops rather than saddle them with a reporting system for higher commands. As an example he described how the map-based US Tactical Ground Reporting System (TGRS) is used for avoidance of IEDs in Afghanistan and for passing information on suspicious activity.

He related how 'Chat' services have developed along the same lines. Patrol Bases clearly feel less isolated by up-to-date exchanges informally communicated across the network. There was also a capability for transmission of images to 'look at a target for tomorrow' as well as development of FMV (Fast Moving Video) that enabled patrols with limited vision to 'see around the corner'.

Reinforcing the chairman's observations, Brigadier Hill described some of the longer standing issues. Typically, contractors had to be deployed in conflict areas to ensure equipment functionality and there was a continuing need to educate and train soldiers in making full use of their tactical digital radios.

Industry Support to Operations

Peter Steensma of ITT Defence Ltd followed the history of capabilities fielded from early UK Clansman examples in the 1980s to the multi-waveform US Joint Tactical Radio System (colloquially known as Jitters) with its possible full roll-out date around 2015. To emphasise what is now commercially possible, he gave the example of the multi-media information fusion needed to capture the unfortunate ditching of the ill-fated Airbus in the Hudson River. The full imaging sequence was up-loaded onto the World Wide Web in as little as 5 minutes after the event.

Similarly, sports broadcasts of rugby, football and golf are good examples of consolidating multi-source information. The techniques could form the basis on which to build military specifications such as those needed for air / ground and strike communication and decision making capabilities.

But the backdrop to tactical operations includes troops who routinely lose signal strength and are prone to diffracted signals in urban areas. Given the plethora of

automatic updates and a host of other reporting, management of 'all stations' in a crowded frequency spectrum provide additional technical challenges.

Variable data rates in the battlefield also present problems. To mitigate choke points, he briefly discussed the potential of smart antennas (MIMO – multiple inputs, multiple outputs), spectrum techniques ('jump in, do our business, jump out') and clever ways of embracing interference.

He mentioned that multi-hop networks such as Mobile Ad hoc NETworks (MANETs) are another emerging technology with a promising line of development together with specialist software tools for modelling network configurations.

Backroom Developments for Coalition Operations

TACOMS Dr Peter Emmett described how STANAG rules have been shaped to enable TacticalCommunication Interoperability for Coalition Operations (TACOMS). Military network interoperability can be defined in the first four layers of the OSI protocol stack and form a federated network (TFN). He showed how, using Network Element (NE) building blocks, it is theoretically possible to connect a TFN to a non-TFN (e.g., legacy tactical, strategic, and public network) or one operating at a different security levels. Later this year as a practical example, calls for fire (UK – FC-BISA and US – AFATDS) will be tested over the two respective network elements connected under TACOM protocols.

SDR Dr Phil Vigneron of the VHF/UHF standardization group, took this further by describing how engineering software protocol stacks (waveforms) into nationalsystems such as SDR, can deliver interoperability. He likened the objective to our old friends AM and FM voice. Despite different national systems and different aircraft avionics, these two common waveforms have provided reliable interoperability for commercial and military air traffic control for many years

The same degree of trust for SDR envisages a UHF component offering wideband coalition waveform designed for secure tactical battlefield IP connectivity. For VHF there is a defined narrowband waveform for secure voice, light data and messaging. It is designed to be sufficiently robust to operate in an EW environment.

The challenge to governments is to set up the conditions for standardized SDR waveforms to be a productive and profitable for industry to invest in. This may require manufacturers to forego proprietary aspects to their designs (IPR) in order to share results whilst benefitting from broader marketing opportunities arising within the public sector.

European Secure Software Defined Radio (ESSOR)

Mr. Alfonso Aiello, the ESSOR technical specialist working on SDR under a collaborative armament programme, described the anticipated results of this European version in such enthusiastic terms that it was hard to believe it was still in its prototype stage! He is working towards a common architecture shared by the participating states that defines the framework for the development of radio platform software and associated security elements - SDR across Europe perhaps?

The target waveform is called HDR WF which has advanced communication characteristics. It will be ported onto six different national radios and success will be judged on their communication capabilities running under this common HDR base. Critically, ESSOR has already passed scrutiny and is compliant with US JTRS (Jitters). Being a multi-channel waveform it can be used with other waveforms such as military links to TETRA (i.e. Police and Emergency Services).

Cognitive Radio

Cognitive radio is the term used for a future system (beyond SDR) that becomes capable of dynamically adjusting its internal state to optimize its transmission and reception, based on the current atmospheric conditions and geographic environment.

This whole subject was considered in the pre-conference workshop led by Dr David Grace, head of communications research at the University of York. Attendees concluded that if achievable, cognitive radio will be capable of interfacing to many SDR systems have improved effectiveness and be better able to cope with hostile EW.

Cognitive radio has the potential to fundamentally reshape the way communications are deployed with all sorts of positive impacts on bandwidth and spectrum usage, energy saving and improvements in communication ranges. It will clearly come at a high price, lots of risk and requiring steadfast commitment to turn the concept from its prototyping stage to reach a degree of maturity.

More from the Backroom – MoD and Radio Spectrum Management

Paul Adams, Head of UK MoD Defence Spectrum Policy, gave delegates an insight into how the radio spectrum is regulated internationally and how this supports military use within national allocations. Spectrum is a valuable national asset and the UK MoD pays £155m annually for its frequency holdings.

He elaborated on Allied Communication Publications (190 and 194) that provided chapter and verse on the way military spectrum is to be managed and co-ordinate. This included the different approach to frequency allocation between war fighting and peace-keeping situations. He noted the increasing spectrum congestion (particularly acute in the 400 MHz region), indicating that ten

projects have been earmarked to signpost the necessary developments.

Frontline Realities of Spectrum Management in an Operational Theatre.

Contrasting this, Captain Muz Murray Royal Signals gave a dynamic account of on-the-ground spectrum management in a war zone. His initial picture of a free-for-all communications area in Kandahar with various nationalities competing for space and frequencies graphically illustrated this.

He gave a telling example of what can happen if spectrum unruliness becomes endemic. His picture of the damage inflicted by an incoming missile, simply because the HQ's protective devices were obliterated by local interference, graphically illustrated this. After that incident he described how he had the full attention of all the resident staff!

He pointed out that spectrum agility costs money at the procurement stage. New systems originally specified to be wideband tunable, had been accepted into service with a fixed frequency device as a cheaper option. This type of trade-off often proves to be a costly mistake. He felt that SDR could be developed to support lessons recently learnt.

Captain Murray then dwelt on the need for this subject to gain more prominence in operational staffing since its omission could endanger complete operations. He also noted that the deployed environment was always hard to characterize. To understand the extent of any problem, let alone resolve it, it was essential to have a roper management tool so that spectrum conflict could be more easily resolved.

Frontline Realities of Infantry Radios issued to UK Forces

Before leaving HM Forces recently, Adam Hughes served as a Regimental Signals Detachment Commander in several Afghan warzones. He graphically conveyed concerns at what he perceived as the mismatch of the actual requirement of troops on operations to the technology and design of radios that are currently issued to them.

His first target of disapproval was the battery drain on personal role radios. On operations, the logistics of supplying a battalion with sufficient AA batteries (2 with 20 hours life per set) was huge. He next took aim at connectors, especially the fragile pins into which headsets had to be plugged.

He followed this up with the positioning of a dual role switch that required a soldier to take his hand off his personal weapon to activate it. Having a multitude of interconnection cables didn't help, especially when one went missing. Then he rounded on the failure to improve range of transmission despite all sorts of innovative relay designs. It was often better to shout, he concluded.

He described the process of checking battery power on a regimental VHF set. Unclipping, removal from bag and stepping through an analytical programme with four sub menus did sound rather extreme! Soldiers liked their TacSats but, with an antenna looking like an umbrella, it stood out and could not be deployed for scouting or covert assignments.

His litany continued with the inability of anyone other than a trained technician to wire a vehicle set and harness, the inability of many sets to operate above 45°C (a temperature that is frequently encountered in Afghanistan), extreme weight issues and the visibility afforded to the enemy of a coalition patrol. A line of an ennas above a poppy field was a definite giveaway!

By the time Adam had applied himself to the risks of new crypto fills, incompatibility with adjacent troop formations and skill fade, the audience was getting rather uncomfortable.

Reliance on Infantry Reports

Tim Mahon of Hawk Associates corroborated Adam's concerns. He noted for instance, the emergence of 'the Strategic Corporal' whose reports and transmissions could impact on the intelligence and targeting of many supporting assets.

The cohesion of ISR (Intelligence, Surveillance and Reconnaissance) coupled with target acquisition and counter measures required a significant network of inter-communicating devices. Given the risks, with every device needing to have untold amounts of versatility built into it to cover a multitude of inter-communication possibilities, its original purpose might somehow be lost.

To demonstrate this, he considered a step by step approach to soldier modernization embodied in the procurement of the French FELAN system to be less risky than the untested UK FIST for just about any mission that crops up. Given the considerable investments needed for information dominance and response – the roadmap we are currently following - he then dared to voice the unstated question namely: "How much difference do Staff demands for NEC (Network Enabled Capabilities) really make?"

Future Market

Mahon went on to examine the driving factors such as multi-intelligence fusion, transatlantic interoperability, the integration of TacComms with Strat Comms, soldier modernization and requirements to meet current operations. From this, he derived potential growth levels, giving predictions to 2019.

He considered SDR to be 'waiting on the sidelines' and a slight shrinkage in the Tac Comms market as some of this moves into the sphere of StratComms. Interestingly, he considered ther may be some additional radio developments using terrestrial low frequency navigation (LORAN) as a back up to satellite GPS

He noted the constraints to growth that included a lack of standards, spectrum congestion, ever-increasing budgetary pressures and spending reviews. Interoperability depended largely on building communities of trust. Eventually he suggested it may be possible to show demonstrable benefits, such as the ability to field cohesive Euro-battlegroups if required.

Other Related Presentations

Commercial Off The Shelf (COTS) Following the recent reorganisation of the Belgian Armed Forces, COTS non developmental items were replacing existing military communication systems because upgrades were judged to be unaffordable and probably ineffective.

Lt Col Peter de Picker indicated that the switch was working surprisingly well using small detachments of 6 – 8 personnel with a wide remit to support all manner of tactical systems and strategic systems. An added role of CIS support in Belgium is to provide social communications in cybercafé style, where troops stationed abroad have an allocation of airtime to talk home. The public often judged the overall effectiveness of their country's tactical military communications on whether these particular social links were working!

High Altitude Platforms (HAPs) - "No More Congestion"

Dr Grace further contributed with his presentation of research work on HAPs that could provide a front line with all the bandwidth it asked for (with a caveat on urban force operations)

He evaluated the relative potentials of the stratospheric manned plane (e.g. M55 Geophysica), an unmanned hydrogen powered global observer, an unmanned solar powered aircraft such as the NASA Pathfinder and an unmanned solar powered airship.

He is working on how it might be introduced in a commercially sensible way.

Panel Discussion and Closure

Delegates discussed a number of topics including air/ ground communications, appetite suppressants as the antidote to ever increasing spectrum demands, commercial WAN compression techniques and reduction in IP codes that are too big for military networks to handle.

It was noted with regret that such events as CWID (The Coalition Warrior Interoperability Demonstration) rarely retained funding to continue to develop ideas and solutions without moving the process into formal procurement. There was a strong feeling that prototyping methodology was under- invested.

Our Chairman brought a vibrant discussion to its conclusion. He quoted Catherine the Great, Empress of Russia in the18th Century stating "A great wind is blowing that gives either imagination or a headache!" As the conference illustrated, these two conditions clearly apply within current radio developments.

CYBER WARFARE – THE AFCEA LANDWARNET SYMPOSIUM

By Lieutenant Sam McEvoy

The author found himself in Tampa, Florida earlier this year on an Op HERRICK detachment from 30 Signal Regiment when he heard of the international convention on cyber warfare being organised locally by AFCEA. By a commenadable exercise of sinitiative he was able to persuade the AFCEA (UK) Southern Chapter to fund his atttendance. This is his conference report.

The week of 23 – 25 August 2011 saw the LandWarNet Conference arrive in Tampa, Florida. Designed to be a forum to present and learn about the recent developments in tactical and strategic communications, there was also an opportunity to hear about the US Army's take on Cyber Warfare, as presented by US Cyber Command. CYBERCOM has only been operational since October 2010, and so this was a good insight into exactly what the US' take would be on the fifth battle spectrum.

The entire conference was hosted by Lieutenant General Susan Lawrence, the US Army Chief Information Officer G6. She emphasised the importance of J6 and CyberWarfare, placing a big emphasis on how absolutely everything we did must be to support the soldier on the front line. This would be a recurring theme from many speakers.

With the conference in full swing, it became time to sit down and get to work. A number of different tracks were available for discussion, including Coalition COIN campaigns, Defence Information Systems Agency and, of course, US Army Cyber Command. The CYBERCOM talks included a number of key individuals, going right up to the top of CYBERCOM with Lieutenant General Hernandez, an interesting and lively speaker. CYBERCOM's talks had to be, for obvious reasons, somewhat vague, as a lot of what they do is still tightly guarded, but they were willing to discuss a number of key topics on the problems and challenges they had faced in their first operational year.

Perhaps most interesting was their talk on where the Cyber Warriors themselves would come from. Vincent Viola, an entrepreneur who used to serve in the US Army, was invited to talk and put across his opinion on Cyber Warriors. He said that we had to actively and aggressively recruit, and make a "Gestalt of the Geek", and that we had to "Grab the Geek" or risk losing them. In the civilian world, someone with the Cyber Warrior's knowledge of IT systems would earn somewhere between $42,000 - $60,000 a year, so a major problem would seem to be retention. Mr. Viola suggested that we put a lot of kudos on being a Cyber Warrior and really make them feel valued. Amongst these were making Cyber Warrior tabs that would be worn on uniform and, in his words, "make them feel a stud." Interestingly, this seemed to be at odds with the overall audience conception of what a Cyber Warrior would be, and how they would be recruited.

There was a feeling that the Warriors should be military, and not contracted civilian personnel, but there was a great sentiment that the ideal Cyber Warrior would not be an ideal soldier, which seems odd. There seemed to be a deep-felt belief on both sides that a Cyber Warrrior will not be able to get below 10:30 on a PFT or, indeed, be any good at any sort of PT at all. The immediate assumption was that they would have to be like doctors or lawyers, who, in the US Army, are held to different physical standards. This seemed to my mind to be a very bizarre concept, as the SFC course, as well as 216 Signal Squadron and numerous other Signals courses that are physically demanding, prove that stereotypically 'geeky' jobs such as IT and radios can be done by people who are fearsome athletes. However, I was immensely outvoted.

What was not in doubt was the obvious seriousness of Cyber Warfare and the emphasis that was put on it. Mr. Viola talked about a Cyber Manhattan Project, and that we must mobilise or be left behind. Brigadier Jeffrey Smith of US CYBERCOM gave a very informative talk where he discussed exactly what the impact of Cyber Warfare could be. He emphasised that Cyberspace must be viewed as being just as important as the land, air, sea and space battlefield spectrums, but also more far-reaching, as cyberspace permeates through each of these other domains. This necessitated a global command, as an attack in one region could be initiated on the other side of the world as easily as just down the street. The lethality of cyberspace rests in this over-arching reach, as in the modern world everything can be electrified. As technology increases and everyone becomes more and more connected, we become more and more vulnerable to a cyber attack.

One important point he brought up was that cyberspace is not just a J6 domain. It is also J3, J5 and J2 just as much as anything else. He pointed out that to operate in cyberspace we must not only understand the systems being used, but also the current environment surrounding

the attack. Cyberspace is also an artificial domain that is completely man-made, and is a "mental landscape formed by the code-based interaction of humans and their processes", so we must understand human nature as well, and that a heavy PsyOps presence would not hinder us. Brigadier Smith left us in little doubt as to what he felt about the danger we face, saying "nothing will bring this nation to its knees more."

There were also discussions on how to fight in cyberspace. It became obvious immediately that this was going to be a large problem, as it is far-reaching and complex. One of the fundamental problems with cyberspace is that it does not fit into any previous spectrum and so our existing doctrines and tactical frameworks do not fit into it either. This is compounded by the problem that it is actually very difficult to define the nature of cyberspace. For example, is it geographic or not? If we are being attacked from a server, then in cyberspace that server has no geographic location in that it is simply a link in a chain from which the attack comes. However, if you defend yourself by shutting down that router, then you shut down the router in a specific geographical location. That router could be used for many other things, such as emergency services or co-ordinating power distribution to an area. The country that the router is physically located in may not have anything to do with the country or group from which the attack originated.

The complexities of this situation means that our current Rules of Engagement do not fit particularly well with this new battlefield spectrum. The Judge Advocate Generals Corps admitted that it had no benchmark for Cyber Warfare and that a new ethos was desperately needed. These problems are ones that desperately need answers if we are to operate, and Lieutenant Colonel Terry McGraw posed two options. While he was talking about the new system architecture, it also applies to our ways of thinking. Do we accept the current architecture and try to improve it, or do we radically change our architecture to one that works? He believes that our current architecture is indefensible, and we must come up with a radical new solution. He was also quick to point out that our enemies will not wait for us to improve it.

The talks culminated with the US CYBER COMMAND panel, which the commander of CYBERCOM, Lieutenant General Hernandez presided over. This was a very informative discussion that focused on tying up unanswered questions and providing a good general view of the way ahead. Two key messages were pushed out. The first was that there was a real lack of understanding amongst the rest of the military about the potential of Cyber Warfare, in both positive and negative lights. For example, on one hand there is not an appreciation about the real world kinetic impacts of cyber warfare, such as shutting down enemy infrastructure or disrupting command and control. Likewise, there was not enough light on its ability to affect our OPSEC. If someone loses a rifle he is in serious trouble. If someone opens an email without checking it for viruses properly he gets a slap on the wrist, even though the latter could be a lot more serious. These views need to change, and quickly. The second message was that we must try to fail at Cyber Warfare, and we must embrace failure. We have to be aggressive and attack our own systems without mercy in order to defend them, and when we find a way through we should celebrate that, because then we can fix it. As Lieutenant General Hernandez said, "I learnt more when I was embarrassed and lost then when I was doing high fives on the objective."

The conference also played host to an exposition, with numerous companies showing their wares and attempting to sign up new customers with sexy new communications gear. There were a number of great new ideas coming out, highlights including radios being turned into routers, new Situational Awareness systems from Harris that allows a much greater view of the battlefield to everyone, and, amazingly a spray-on UHF antenna. It comes in a can (I didn't believe them either).

A few high-profile guest speakers also attended. Perhaps most notable was Admiral MacRaven, the new commander of US SOCOM. He praised the J6 role and stated how invaluable it was to him, giving him the ability to command and control in a way that was not even conceived when he first joined the Navy. Perhaps most refreshingly he stated his view on how the armed forces should operate in the current economic climate. While he acknowledged the greater emphasis on efficiency and financial propriety, he emphatically stated that "our job is to be effective, not efficient." It is, of course, important to be efficient with our funds, but never at the cost of operational effectiveness, pointing out that we owe it to the military men and women on the ground.

In summary, it is clear from the conference that CYBERCOM has a long way to go. Their endstate is, that by 2020, they will be the greatest Cyber Army in the world. What is obvious is that they have a long way to go before they achieve that, and a number of key questions and issues need to be addressed. A recurring theme from the speakers was that, at the moment, the US is not prepared for a Cyber War. We cannot afford a Cyber 9/11, and we must be ready, because the enemy will not wait for us.

HOW SHOULD THE CORPS ADAPT IN RESPONSE TO CYBER THREATS AND OPPORTUNITIES?

By Captain SC Church, Royal Signals

This was the winning entry in the 2011 Deane-Drummond Prize Essay competition

The National Security Strategy published by the Government in October 2010 *(i)* recognises the threat of cyber attack on the United Kingdom as enough of a danger to class it as a Tier 1 Priority Risk, alongside international terrorism, international military crises and major natural disasters, and above the risk of a CBRN attack. The risk of cyber attack has prompted the establishment of the UK Defence Cyber Operations Group (DCOG) *(ii)* who will work to counter the possibilities of attacks against the computer networks which control the nation's civil and military infrastructure. Cyberspace can be defined as:

a global domain within the information environment consisting of the interdependent network of information technology infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

The United States Army employs a useful model to break cyberspace into layers: physical, logical and social. *(iii)* These layers break down into five components: geographic, physical network, logical network, cyber persona and persona. The nature of cyberspace means that the physical geographic locations of attacker and target can be many miles apart with no physical infrastructural connection between them. The attacker may also be aloe, or part of a larger group (potentially state-sponsored) and his particular persona may differ from his, potentially multiple, cyber personae. It is the logical network layer that links the physical computer hardware to the network, thus linking personae over multiple geographic locations.

Cyber is not yet fully defined within the military context, and in examining how the Royal Corps of Signals fits into the national response to cyber threats and opportunities, it is worthy of note that nearly 80% of military network traffic is delivered by commercial service providers such as BT. *(iv)* Interoperability is a force multiplier, but also a vulnerability as there are now more entry points for cyber attack than in the past. The Corps has two avenues down which to develop its response to this growing field: in the development of doctrine and policy, and at the tactical and operational levels through development of capability to counter cyber threats and capitalise on cyber opportunities.

As well as working to defend the nation's infrastructure, DCOG will develop opportunities to exploit the cyber domain in order to allow the United Kingdom to retain its military might. DCOG is a multi-agencyorganisation which brings together the military and civilian sides of cyber development, namely the Government Communications Headquarters (GCHQ) and the Ministry of Defence (MOD), as well as recognising that the cyber threat knows no geographical boundaries so we must seek to co-operate with our allies to respond to the threats and opportunities presented by cyberspace. In examining the role of the Royal Corps of Signals in these developments, it is important to consider current and future doctrine on cyberspace, as well as how the Corps' current and projected capabilities fit into the development of that doctrine, and the wider cross-governmental response to cyber. The management and security of the digital network used by the military should not limit protection against the cyber threat to the J6 world, much like Information Management (IM), Information Assurance (IA) and Information Exploitation (IX) are J3 functions as part of the wider planning cycle. It will be important however to keep the J3 planners current in the use and capabilities of the electromagnetic spectrum, including cyberspace. This is where the Corps should ensure it has embedded staff within DCOG and the Global Operations Security Control Centre (GOSCC) in order to maintain our position at the forefront of developing doctrinal and capability responses to cyber threats and opportunities. The role on the battlefield of the Corps in response to cyber is in protecting and projecting fighting power, and in maintaining information superiority.

Definitions of 'cyber attack' vary, but centre around the hostile use of computer software to disrupt digital systems. This attack may take place to distract from other activities, gather intelligence (espionage), disrupt processes or for criminal purposes such as theft. The actors conducting such attacks could be state or non-state actors and 'attribution' is very difficult given the virtual nature of cyberspace.

Malicious software, or 'malware' takes three major forms: viruses, worms and Trojans. *(v)* Each type attacks networks in a different way, and can have extremely damaging and lasting effects. The Stuxnet worm used against the Iranian nuclear power digital support system is a recent example of the targeted use of malware to disrupt infrastructure, and is comparable to a limited military strike. *(vi)* Denial of Service (DOS) and Distributed Denial of Service (DDOS) attacks are the threats against which most strategic planning is taking place. An attack such as this would deny or disrupt the use of limited or widespread information and/ or telecommunications networks. At the operational and tactical levels, this is also relevant: disruption of air traffic control networks for RAF or AAC platforms could prevent movement of personnel and equipment, and could prevent our ability to maintain air superiority in a given theatre. Disruption to domestic military computer

networks could simultaneously impede essential rear-link communications, affecting our ability to respond in UK to operational developments in theatre. In essence a cyber attack can add to the 'fog of war' and it is against this we must defend our networks. This is reported to have successfully been used to simultaneously attack Georgia's digital infrastructure at the same time as land, sea and air invasions were launched on Georgian territory by Russia in 2008. *(vii)*

Although the UK has adopted a cross-government approach to cyber, it is of note that US CYBER COMMAND established in 2010, has brought control of cyberspace firmly into the military domain. Essential components of UK cyber capability demand reliance on our allies, not least the control of our nuclear deterrent which depends on the use of US satellites. The US also manufactures a large proportion of the hardware and software employed by the British armed forces. The Corps should seek to tap into American developments, both in concepts and doctrine, as well as taking part in multinational exercises to practise our counter-cyber capabilities. The UK Cyber Range at Fareham *(viii)* is interoperable with the American equivalent in Maryland- Royal Signals soldiers and officers should be integrated into these exercises at the technical and staff planning levels so that a more complete understanding of cyber can be brought to bear in the tactical and operational military operating environments. It is in this area that we may make best use of our Territorial Army (TA) soldiers; we are unlikely to coax well-paid cyber experts from their current employment, but they may be persuaded to add value to a national effort to counter the cyber threat by giving their time and expertise as a member of the TA. The establishment of an expert 'guild', such as in the case of the Engineer and Logistic Staff Corps, *(ix)* could harness the private sector's expertise under the umbrella of the Royal Corps of Signals.

Returning to the US Army model, it is not appropriate or possible for the military to address the cyber threat at every layer. Nor is it the role of the armed forces to provide personnel to defend against strategic threats to our infrastructure- this is GCHQ's role. However, DCOG works pan-government so the military should be called upon to provide expertise in development of network defence systems. The Corps has a major role at the tactical level and should add value to the growing Information Operations strand of modern warfare. Information Operations doctrine already includes a key Corps asset: Electronic Warfare (EW) as well as Computer Network Operations (CNO). *(x)* It is in the area of Computer Network Defence (CND) that the Corps should adapt in response to the military cyber threat.

Protecting fighting power is part of the CND battle: the interdependency of the different elements of cyberspace can be a confusing picture, however to simplify it within the context of military CNO is the most useful way to examine how the Corps should develop its role in response. In the military context, if CND is taken to mean Information Assurance (IA), ie, the protection of our information assets through OPSEC, INFOSEC and COMPUSEC, then the responsibility for this falls to all; IA includes Information Management (IM) which is an inherently J3 function. Protection of the systems which hold or process information is part of CND assuring our information superiority over an adversary, and in the tactical environment this could be a role for Corps tradesmen trained to monitor systems or update protective software. The physical integrity of communications network hardware is also at risk when there is no facility for second or third line repair within the Corps: contractor support to classified systems increases the vulnerability of those systems to attack. Communication Systems Engineers (CSE) should be re-empowered to maintain equipment up to third line.

In the Contemporary Operating Environment (COE), the military (Army, Navy and Air Force) rely very heavily on networked digital systems. These systems are by no means limited to the Corps, and the response to the cyber threat must be a J3-led part of the operational planning cycle. Network-Enabled Capability is a force multiplier in the COE; it links military and cross governmental units, as well as linking in to contractors supporting the operation. Paradoxically it is this strength which provides the greatest vulnerability the wider the logical network, the more open it is to penetration by a hostile actor. For example, Air Support to operations (from logistic lift to Close Air Support) and aerial ISTAR platforms are cyberspace dependent to the point where a successful attack could ground aircraft, potentially surrendering our air superiority. Wherever networks exist, a particular layer of cyberspace belongs to the Corps: in this example the physical network component. In a purely Land-based environment, the Corps may also 'own' the logical network component. It is in these particular areas that hardware, software and trade skills should develop to protect military networks from cyber attack. The Electronic Warfare Systems Operator should be skilled in the use of firewall software, and the ability to detect cyber attack. The CSE trade group should also develop to focus on specific hardware and software, depending on the Communications Information Systems in use in that theatre (Tactical CIS, Theatre CIS, Air Support).

Using the 3-layer model, it is impossible for any network that is not completely closed to be protected by military means alone. For a formation HQ J2 or EW cell to be able to locate and neutralise a single attacker, who may be thousands of miles away and whose primary effect is not actually in the military area of operations, but whose second order effects are disrupting operations, would be virtually impossible. GCHQ however are developing the capability to do just that.

As well as adapting to meet the threat of cyber attack, the Corps must also be ready to lead the exploitation of tactical cyber opportunities. Under CNO, the area of Computer Network Exploitation (CNE), most specifically where it overlaps with Signals Intelligence (SIGINT), is the arena in which the Corps should focus its efforts to adapt in response to the cyber opportunities presented by the COE. This is a capability to project fighting power, that is to say to multiply the effect on the ground of other force elements. There is the potential to train a new strain of EW Sys Op who is essentially a field computer hacker. This capability would require more than training, man-portable computer systems would need to be developed so that a target could be identified (by GCHQ) and then hacked by the operator. This could arguably be conducted remotely by other government agencies, but in order to capitalise on the tempo of the current battle, it might be necessary to have capability at the fingertips of the formation HQ, much like ICOM interceptors, without the delay and process of applying for sensitive information from GCHQ. Operators would have target information provided, much in the same way that enemy key leaders are identified by the J2 cell, and the exploitation of that information within cyberspace could be used to effect as part of the targeting process. Within Information Operations doctrine, this link between EW and Influence Activity already exists, but it needs to move across now into cyber exploitation. CNE has the potential to be the ultimate manoeuvrist weapon in the COE.

Computer Network Attack (CNA) is the final corner of the CNO triangle and would be another string to the targeteers' bow. The technological ability to hack into the adversary's cyber domain to conduct jamming or have a diversionary effect through the use of malware in support of the mission would be another role for the EW Sys Op.

In summary, the Royal Corps of Signals has an important role to play in the military's response to cyber threats and opportunities. As discussed, this is as an important contributor to doctrine and capability development at staff level, as well as at the tactical and operational levels as part of the wider Information Operations plan. Cyber security is 'everybody's business', and as such the Corps has a role in assuring compliance with physical security constraints for communications infrastructure. Further to this, our role on the battlefield, particularly in the field of Electronic Warfare must adapt to include cyberspace. Computer Network Defence and Computer Network Exploitation are areas where the Corps can take a lead to add to the wider Information Superiority battle.

Footnotes;

i. A Strong Britain in an Age of Uncertainty: The National Security Strategy. Presented to Parliament Oct 2010 by HM Government. P27.

ii. Cyber Space, Cyber Power, Cyber What? Lt Col I Buchanan. The British Army Review Spring 2011. LWC. p80.

iii. Cyber Space, Cyber Power, Cyber What? Lt Col I Buchanan. The British Army Review Spring 2011. p80.

iv. Spotlight 11-2. Special area of interest guide to: Cyber. June 2011. 22 (Trg) Gp Generic Education and Training Centre (RAF). P4.

v. *Spotlight 11-2. Special area of interest guide to: Cyber. June 2011. 22 (Trg) Gp Generic Education and Training Centre (RAF). P3.*

vi. Spotlight 11-2. Special area of interest guide to: Cyber. June 2011. 22 (Trg) Gp Generic Education and Training Centre (RAF). P5.

vii. Spotlight 11-2. Special area of interest guide to: Cyber. June 2011. 22 (Trg) Gp Generic Education and Training Centre (RAF). P5.

viii. http://www.mod.uk/DefenceInternet/DefenceNews/DefencePolicyAndBusiness/DefenceMinisterOpensUkCyberSecurityTestRange.htm accessed 27 Jul 2011

ix. http://www.army.mod.uk/royalengineers/units/21204.aspx accessed 29 Jul 2011.

x. Allied Joint Publication 3-10 Information Operations. Nov 2009. DCDC. p1-11.

BIBLIOGRAPHY

A Strong Britain in an Age of Uncertainty: The National Security Strategy
Presented to Parliament October 2010 by HM Government
Cyber Space, Cyber Power, Cyber What?
Lt Col I Buchanan
The British Army Review Spring 2011.
Land Warfare Centre
Army Doctrine Publication: Operations
November 2010
DCDC
Spotlight 11-2, Special Area Interest Guide to: Cyber
June 2011
22 (Trg) Gp Generic Education and Training Centre (RAF)
Allied Joint Publication 3-10: Information Operations
November 2009
DCDC
Meeting the Cyber Challenge
Speech delivered by Nick Harvey MP
November 2010
Chatham House
http://www.mod.uk/DefenceInternet/AboutDefence/People/Speeches/MinAF/20101109MeetingTheCyberChallenge.htm accessed 25 Jul 2011.
Defence Minister opens UK Cyber Security Test Range
http://www.mod.uk/DefenceInternet/DefenceNews/DefencePolicyAndBusiness/DefenceMinisterOpensUkCyberSecurityTestRange.htm accessed 27 Jul 2011
Dominant Air Power in the Information Age
Speech delivered by Chief of Air Staff
February 2010
International Institute for Strategic Studies, London
http://www.mod.uk/DefenceInternet/AboutDefence/People/Speeches/ChiefStaff/20100215DominantAirPowerInTheInformationAge.htm
The British Army Website: The Corps of Royal Engineers
http://www.army.mod.uk/royalengineers/units/21204.aspx accessed 29 Jul 2011.

HOW SHOULD THE CORPS ADAPT IN RESPONSE TO CYBER THREATS AND OPPORTUNITIES?

By Captain C Goslin, Royal Signals

This entry was the Runner-up in the 2011 Deane -Drummond Prize Essay Competition

Captain Chris Goslin was commissioned in 2006, and has served in 14 Signal Regiment (EW), the Falkland islands and with 2 Rifles. He enjoys skiing, climbing and mountaineering. This is his second success in the Essay Competition; he was the winner in 2010.

SDSR context: "over the next five years, we will develop a transformative programme for cyber security which addresses threats from states, criminals and terrorists and seizes opportunities which cyber space provides for our future prosperity and for advancing our security interests".

Introduction

In 2010 the British Government delivered the results of the Strategic Defence and Security Review (SDSR), where they laid out the threats to the UK and the how they intend to shape the security services to better tackle these threats. For the first time cyber-security was considered in earnest and "the risks emanating from cyberspace (including internet, wider telecommunications networks and computer systems) are one of the four Tier One risks to national security". *(i)*

Predictably, Hollywood has been quick to sensationalise the threat in movies like War Games (1983) and Die Hard 4.0 (2007). These may just be creative speculation but we have already witnessed significant cyber-attacks on Estonia in 2007 and Georgia in 2008. There was a 14% increase in online banking losses between 2008 and 20091 and large companies and security services have suffered significant cyber attacks, most recently Sony and SOCA.

A number of nations have begun to develop and possibly deploy cyber-attack capabilities and the NATO Cooperative Cyber Defence Centre of Excellence was created in 2008. Terrorist networks have identified cyberspace as a domain in which they can even the odds with militarily more powerful states and criminals have the potential to create economic turmoil by well targeted hacking. The military must be able to gain dominance in cyber-space and the Corps will be a key player as the military develops its own capabilities.

Defining Cyberspace

Computer networks now dominate worldwide communications and control systems; the internet is now accessible by a third of the world's population1. People now have unprecedented access to information, cheap and potentially secure international communications, as well as access to any system that is connected to the Internet including banks, industry networks, utilities control systems and military systems.

Since the term cyberspace was originally coined in the 1980s the concept has always been relatively vague. Despite being a contentious issue, a useful definition of cyberspace can be found in a report commissioned for the United States Air Force in 2009. *(ii)* It defines cyberspace as "an agglomeration of individual computing devices that are networked together" but goes further in its explanation by detailing the fundamental elements that combine to create a cyberspace. It argues that cyberspace consists of three distinct layers: a physical layer, the equipment and physical connections; a syntactic layer, containing the instructions and protocols through which devices interact with each other; and the semantic layer, the information stored on the devices. Each of these layers can be attacked or exploited using various forms of cyber-attacks.

The Threats

The aim of a cyber-attack is to exert control over a target's information system, whether that is in order to steal information, referred to as computer network exploitation (CNE), or to corrupt or disrupt a system, referred to as computer network attack (CNA). All of the three layers of cyberspace are vulnerable to attack.

On the physical layer the most obvious attack is a kinetic attack; destroying key network infrastructure (e.g. servers, mass file storage locations or key bearer links) will significantly disrupt the system. Defence against a kinetic attack is familiar territory for most organisations. Another

threat to the physical layer is supply chain attacks. Without complete control of the supply chains used to construct hardware employed on the network it could already be corrupted on delivery. There is evidence of this form of attack already being conducted: in 2008 some Chinese manufactured USB devices were identified as being supplied pre-installed with malware, these were especially prevalent in markets in Afghanistan frequented by coalition soldiers. The only defences for this type of attack are education of all users and complete control of the supply chain. Equipment like key-loggers can also provide valuable information to cyber attackers, usernames and passwords especially. The problem with this method of attack is that it relies on the equipment being installed and retrieved without detection, however this is achievable if an enemy can turn a user or administrator. Defending against this sort of attack is familiar and relatively straight forward: vetting of all personnel and good physical security significantly reduces the risk.

The syntactic layer is the one that is most vulnerable to attack. It is through the manipulation of protocols and algorithms, essentially controlling how a system interacts with other systems, that hackers can gain access to and exploit a system. Malware can be installed onto vulnerable elements of a network to facilitate access to the entire system by cyber-attackers.

Once access has been gained to a system or network the cyber-attacker can steal information, corrupt the smooth operation of a system or manipulate whatever the system is responsible for controlling. It has already been demonstrated that malware can cause a turbine to self-destruct; *(ii)* this is concerning given that a lot of new military hardware relies so heavily on software for safe operation and a network for fault diagnosis and calibration (e.g. Typhoon). Hackers can also create 'botnets', where malware turns a computer into a drone under command of a 'bot-master'. These drones are particularly used for Denial of Service (DoS) attacks where all drones on the 'botnet' will try to access the same website concurrently; the volume of traffic overloads network infrastructure causing the network to crash. *(iii)*

All that is required to conduct a cyber-attack is a computer with an internet connection. Geographical distance is meaningless, the initial financial outlay is low and the probability of an attack being traced back to its source in any meaningful way is also low. Cyberspace is the perfect asymmetric battlefield. This opens the UK up to serious threats from nations which would normally not pose a security threat, terrorist organisations, criminal organisations, political activists and industrial espionage.

These are certainly not future threats: terrorist organisations already exploit cyberspace; the internet is used as a reliable communications network for terrorist networks to control the actions of their cells. Jihadist websites are often used for recruitment and there has been some speculation that phrases posted on these sites (especially in videos) have been used to activate cells or trigger attacks. Terrorist want to cause psychological and social disruption and they want to publicise their cause; they will often target soft, civilian targets to achieve these aims. The advantage of a cyber-attack is that it is often headline grabbing without causing fatalities, allowing the terrorist to argue the moral high ground. This is particularly effective if a terrorist organisation can provoke a state to overreact, strengthening their cause considerably. *(iv)* The internet can also be used to provide ready-made target packs; social networking sites and mapping sites provide an enormous amount of information with very little effort. Criminal organisations are also exploiting cyberspace: as early as 1994 Russian cyber-criminals stole $400000 from US Citibank. *(v)* Political activists are already prevalent on the internet especially in times of conflict; access to the Internet has been a major factor in the recent viral spread of dissent throughout the Middle East and North Africa.

The world has already witnessed national level cyber-attacks, first in 2007 on Estonia. This lasted 3 weeks and virtually paralysed the country's information networks. Although it was never proved that Russia was behind the attack, the evidence suggests that there was some Russian state involvement. The second large cyber-attack was on Georgia in 2008 and coincided with the Russian occupation of South Ossetia, it consisted of large scale DoS attacks, causing virtual paralysis and confusion. Given the timings of the attacks it seems fair to suspect Russian involvement3. China is also a major cyber-power; it is suspected that they have battalions of highly trained cyber-warriors. They are suspected of significant industrial sabotage and Germany's Chancellor "felt confident enough in this attribution to complain to China's premier in person" *(ii)* in 2007.

A final, key point when considering the threat is that as we become more networked and reliant on technology to operate we also become more vulnerable to cyber-attacks.

The Role of The Corps

Given that the Royal Corps of Signals are "the leaders in Information Technology and Communications for the British Army"*(vi)* it seems that, if there is a requirement to develop cyber-warfare capability within the Army, this role would sit comfortably with the Corps. That said, there is no clear trade group that could take this task on. The recent merger of Communications System Engineers has created a large pool of generalists; cyber-warfare requires experts who are dedicated to cyber-operations. The best we can expect from the Corps is a handful of amateur enthusiasts receiving outdated training given how quickly the cyber-threat develops. If we were to train Royal Signals soldiers to conduct cyber-operations they would have to be locked into this trade; this is not a skill set that one

can dip in and out of. Also if a person is an expert in cyber-operations it is highly likely that they will not join or remain in the Army as there are far better prospects in civilian employment, especially with banks and engineering companies.

The role of cyber-operations sits far more comfortably with GCHQ; the SDSR has made the focus of cyber-operations the "UK's centre for cyber security operations at GCHQ". *(i)* GCHQ can recruit the very best people and employ them solely in trade, constantly developing and adapting to the current threat. The key to cyber-defence especially is that it must be executed using a comprehensive approach, making sure that government departments, security services, civilian organisations and the military are all equally protected. Given the amount of interaction between all of these groups it is paramount that we all protect each other. We are only as secure as the weakest link in our system. GCHQ is the ideal central node for this cooperation.

The Corps could develop and field a tactical cyber-attack capability, where a cyber-attack directly supports a military operation2. The potential for tactical cyber-attacks is massive: a well timed cyber-attack on command and control systems can freeze a headquarters, on air defence systems could disable them and on ISTAR systems could confuse them. The problem is a lack of ability to conduct battle damage assessment. There is no way to confirm that, for example, the enemy's air defence system is disabled and this presents a huge element of risk to a commander. There are also much easier ways to achieve the same effects: Electronic Warfare or kinetic attacks on key infrastructure would cause as much disruption to an enemy as a cyber-attack. Also if the enemy network is vulnerable to cyber-operations from friendly forces on the ground it can be equally vulnerable to friendly forces in the UK. If a military operation requires an effect which can be achieved through cyber-operations GCHQ could deliver this effect remotely. There is a role for the Corps in this scenario as there would be the requirement for liaison officers who understand both the technical issues and the operational picture.

The role of the Corps is more likely to be to provide technical expertise within the military. The Corps must be able to educate military personnel and monitor our systems in order to make sure all individuals are working towards a secure military cyberspace and not inadvertently creating breaches in our cyber-security. The Corps should be the first port of call for military units to go to for cyber-defence issues. We have the technical understanding of the issues and the credibility to provide advice and support.

The Corps can also influence the training of headquarters in order to allow them to adapt quickly to a cyber-attack. A headquarters staff must be able to operate without its Information Systems (IS) and on minimal communications systems; the only sure defences from cyber-attacks are either not being networked (not an option in a modern military) or being able to cope despite an attack. Royal Signals personnel should be the first line support during a cyber-attack and must therefore be competent in cyber-defence and recovery of systems once attacked.

Conclusion

In a modern, network-enabled military there is a significant risk of cyber-attack. Given the nature of the enemies we are likely to face in the near future,cyberspace will be a battlefield of choice for them as it presents complex asymmetries which work in favour of small low-tech organisations. The potential effects achievable by cyber-attacks are massive: deployments could be delayed, air defence systems could be immobilised, ISTAR or platform control systems could be disrupted or information could be stolen.

This new battle-space presents opportunities to the Corps both in the form of developing cyber-attack and cyber-defence capabilities. The argument for developing cyber-attack capabilities is not persuasive and would stretch our, constantly reducing, manpower and funding further. This role sits more comfortably with GCHQ with their expertise and global reach being exploited by the military to deliver operational effect (CNA or CNE) as required. The Corps needs to develop the expertise of its personnel to deliver robust cyber-defence capabilities and, equally importantly, the ability to recover attacked systems quickly in order to minimise operational disruption.

To achieve a credible level of cyber-defence a comprehensive approach is required; the military's IS connects to industry, foreign military and OGD IS. This will require a significant lean towards interoperability and liaison between the Corps and these agencies. It is the role of the Corps to be the Army's representative in this forum: to ensure that there is no weak link in this system and importantly that we are not that weak link. An understanding of all systems is required but ultimately the Corps cannot control the other players. A key weakness is with industry delivering IS projects to the military; by the time a system is delivered it can be almost obsolete and ther fore vulnerable, the Corps must be in a position to influence this process for the better. We are often working with aging equipment, minimal training, generalist IS engineers (as was) and we are highly reliant on being network-enabled.

Every person in the military has a role to play in cyber-defence, from the individual soldier knowing not to use a personal USB to the Divisional Commander who needs to limit his vulnerabilities by training without his full IS suite. Primarily the Corps must stick to its core role of establishing and maintaining the commanders' communications; if there is a threat to these communications we must stand ready to defend them whether that is on the physical battlefield or the emerging battlefield of cyberspace.

Bibliography:

i. "Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review" Presented to Parliament by the Prime Minister Oct 10

ii. "Cyberdeterrence and Cyberwar" Martin C. Libicki, RAND Corporation 2009.

iii. "Cyber Space and Cyber War: Science Fiction or Science Fact" Lt Col Ian Buchanan R SIGNALS, published in The Journal of the Royal Signals Institution Vol XXIX Spring 2010.

iv. "Understanding Terrorism" by Gus Martin, Third edition, SAGE Publications 2010.

v. "The Problem of Crime" edited by Eugene McLaughlin and John Muncie, Second Edition, SAGE Publications 2002.

vi. http://www.army.mod.uk/signals/signals.aspx accessed on 081530 Jul 11.

vii. "War and Power in the 21st Century" by Paul Hirst, Polity Press 2010.

THE DEANE-DRUMMOND PRIZE ESSAY COMPETITTION 2011

The Examiners Comments

This year's topic was intended to be thought provoking, and picked on an issue that is at the forefront of the Corps force development agenda. It demanded a consideration of all of the Defence Lines of Development when capturing the challenge of how the Corps should adapt within a more challenging Cyber environment. Governance was an area it was particularly important to cover, but also a recognition that we are already heavily involved in Cyber activity as a Corps even if we do not call it such.

The fact that a sensitive subject had to be written about in an unclassified article also posed a challenge to the authors who needed to capture the pertinent issues without straying into a minefield of compartmentalised information. The top essays all managed to achieve this, with the winning essay delivering the most balanced argument to the proposals that were made.

Cyber is everyone's business, and its headline in the SDSR has helped take forward a broader understanding by the entire military community of their part in defending, attacking and exploiting information. The Corps potential role alongside other stakeholders in the Cyber battlespace was captured well by Captain Church in the winning submission.

A TROOP COMMANDER'S ROLE - IN 1900

By Lieutenant Colonel (Retired) DS Mullineaux

David Mullineaux retired from the Corps in 1985 to take up a second career in industry, and subsequently developed an interest in military history, in particular signalling. He has contributed several articles to the Journal on these topics, and this is his latest.

Introduction

The previous issue of the Journal published the winning entries of the essay competition about the changing role of a Royal Signals troop commander. This seems to have become a current topic because the nature of recent army operations has led to organisational changes which have been introduced to accommodate the flexible, multi-role operational capability that is now desirable - the Contemporary Operating Environment. Also, within the Corps, changing technology and new communications systems have demanded change. But are these factors anything new? Wars produce unexpected situations, and in the past many troop commanders responsible for communications have had to undertake tasks that were not 'in the book'.

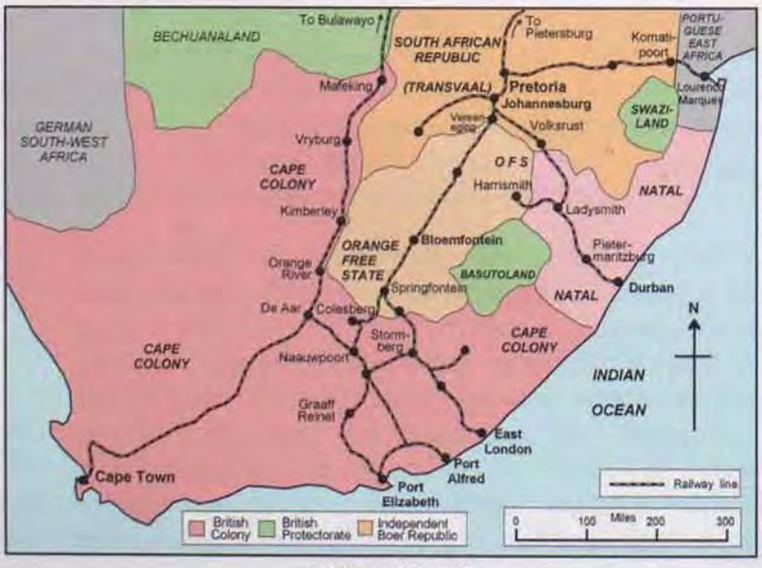
This article is the story of one such troop commander, Lieutenant Dickie Jelf, who in 1900 became responsible for field telegraph communications in support of the force attempting to relieve Ladysmith in the Anglo-Boer War, and found himself having to undertake something far beyond what might normally be expected.

The Anglo-Boer War

The war followed a long history of disputes between the British and the two Boer republics in South Africa, and started on 11 October 1899. It had been expected for some time but for political reasons, to try and avoid inflaming the situation, mobilisation was left too late. General Sir Redvers Buller, the GOC of the Army Corps based in Aldershot, was appointed in overall command. The operational plan, drawn up in England beforehand, was for a holding force to defend Natal and for the main Army Corps to advance up the line of the railway from Cape Town to Bloemfontein and then Pretoria. (Railways were then the main transport artery; otherwise, it was animal transport, with all the limitations that imposed, especially in a country where distances are great.) Having quickly reached Pretoria, that would be the end of the war, so it was complacently thought. 'Home for Christmas' was the cry. Events were soon to turn out otherwise. *(i)*

As part of the Army Corps, the Telegraph Battalion was deployed. The first detachment, comprising the headquarters and one section (a section, of about 55 men, was the equivalent of what today is a troop) were sent with the first batch of troops from England to Natal where the initial threat was greatest. They left Aldershot on 20 September 1899 and eventually, after a frustratingly slow journey through the Mediterranean, reached Durban on 27 October, the war by then having started. They reached Ladysmith on 29 October. The second detachment, consisting of a further headquarters element and the remaining four sections, one of them commanded by Lieutenant Dickie Jelf, departed belatedly on 21 October aboard the SS Gascon (by coincidence the same ship that had been used earlier that year for sea trials of wireless telegraphy in Algoa Bay, near Port Elizabeth), and arrived in Cape Town on 12 November. They moved quickly by rail to De Aar where they set up an initial base camp, their role being to provide telegraph communications for the intended advance to Pretoria.

Meanwhile, since it started on 11 October, the war had quickly taken a turn for the worse. Mafeking and Kimberley were besieged by 16 October. On 2 November, after several battles to defend it, Ladysmith was also besieged, and all telegraph lines southwards were cut by the Boers. Only four days after their arrival there, the headquarters



SOUTH AFRICA, 1899

and section of the Telegraph Battalion were entrapped, able only to provide local communications within the defended perimeter. Then, between 10 and 15 December, the so-called 'Black Week' followed, with severe British defeats at Stormberg, Magersfontein (near Kimberley), and Colenso , the battle of Colenso being General Buller's first attempt to relieve Ladysmith.

After the defeat at Colenso the Natal Field Force, as it was known, had withdrawn southwards to regroup in the area around Estcourt and Frere, and was being reinforced for a renewed attempt to relieve Ladysmith. Buller remained in command in Natal, but overall command passed to Field-Marshal Lord Roberts, who arrived at Cape Town on 10 January 1900.

Heliograph Communications Established

The helio detachment on Observation Hill, Ladysmith signalling to Buller's force on Mount Alice

Since 2 November, when the telegraph lines were cut, communication with Ladysmith had been very limited. A number of other methods were employed: native runners, carrier pigeons, flashing by searchlight reflections from the clouds at night, and eventually and most usefully, heliograph.

Ladysmith was screened from the Natal Field Force located to the south by the intervening range of hills known as the Tugela Heights, thus preventing direct visual communications. Although Ladysmith is mostly in a hollow, the area to the immediate north west of the town rises by just a few hundred feet, and two features were to become important for visual communications, Convent Hill and Observation Hill. Both gave good long-range views out over the surrounding country, Convent Hill to the east and south-east, Observation Hill to the south-west. Nowadays modern housing covers these hills, and there is a water tower on Observation Hill, the highest point in the town, but the topography is otherwise unchanged and the limited scope for visual communications to the relief force south of the Tugela river is evident. There was, however, one way into Ladysmith, to be exploited by Buller's divisional signalling officer, Captain John Cayzer, 7th Dragoon Guards. From Convent Hill in Ladysmith to the south east there is a line of sight to a prominent high mountain - Mount Umkolumba, some thirty miles away. About 5,000 feet in altitude, and 1,700 feet higher than Convent Hill, Mount Umkolumba also dominates much of the ground south of the Tugela where Buller's forces were situated around places like Frere and Estcourt twenty miles away. It became the heliograph relay station into Ladysmith. Communications between Ladysmith and Umkolumba were established on 2 December, one month after Ladysmith was besieged and the telegraph cut. General Buller was then in regular communication by heliograph with Lieutenant-General Sir George White, the commander in Ladysmith, using cipher codes when necessary. Many messages were passed.

It was well known that interception of heliograph messages was possible, even though the beam was very narrow, and with Boers all around care had to be taken. When the heliograph link from Mount Umkolumba into Ladysmith was initially established, Captain Cayzer firstly wanted to ensure he was communicating with the right people. As it happened, he had a friend who was besieged in Ladysmith. He sent a message to the distant station, addressed to his friend, asking a personal question that only he would know the answer to - what was the name of his father's estate in Scotland? When the correct answer (Gartmore) was promptly received as authentication, message traffic began. General Buller was from then on in regular communication by heliograph with General White in Ladysmith, using cipher codes when necessary.

Telegraph Section deployed to Natal

As part of his preparations for a renewed attempt to relieve Ladysmith, General Buller needed field telegraph communications and had ordered another section to be transferred from the western front to Natal. *(ii)* This task fell on No 1 section of the Telegraph Battalion, commanded by Lieutenant Dickie Jelf. His reaction on being detached to run the telegraph operation in Natal was, so he said at the time in a letter to his parents, one of 'unspeakable joy'. Sadly, as will unfold, it was not to end that way.

Lieutenant Dickie Jelf

Dickie Jelf was following in paternal footsteps, for his father, Colonel R. H. Jelf, had served in 'C' Telegraph Troop in 1871-72 and commanded the Telegraph Battalion from 1885 to 1889. Young Dickie had been born in what at the time was descriptively called the 'Adjutant's Tin Hut' in Aldershot, when his father, then a Captain, held that appointment in 1872. *(iii)* After that unpretentious arrival matters had improved, and Dickie had been educated at Cheam and Eton. He had several brothers serving in other regiments and, as it happened, one of them, Rudolf Jelf, in the King's Royal Rifle Corps, was besieged in Ladysmith – so there was a certain incentive for Dickie to assist in its relief. Dickie Jelf himself had got married in England in September, shortly before war broke out, and a few weeks later was about to return with his new wife to his post in a RE Company in, Gibraltar when he was recalled for active service with the Telegraph Battalion, having served with them in a previous posting and thus conversant in their work.

Dickie Jelf and his section left De Aar on 23 December and returned to Cape Town. After some slightly over-exuberant celebration of Christmas there, they continued by ship to Durban, which they reached on 3 January 1900. From Durban, they immediately moved up by rail to Estcourt to join the relief force. There he reported to Lieutenant-General Sir Charles Warren, Commander 5th Infantry Division. Some fifteen years earlier, in 1885, the then Lieutenant-Colonel Sir Charles Warren had commanded the Bechuanaland Expedition in which Dickie Jelf's father, then Captain Richard Jelf, had provided the communications by constructing a 200-mile telegraph line from Barkly West (near Kimberley) to Vryburg as part of an operation to deal with Boer land-grabbing in the British Protectorate. After this meeting with Warren at Estcourt, Jelf and his section moved on to Frere, the forward headquarters, served at the time by a civilian telegraph office.

At Frere preliminary discussions took place with the colonial Telegraph Department as to the working of the circuits to be established for the army and the civil-military interface. It was decided for the time being to make Frere the handover point between the army and civil telegraphs, and the army would open a military telegraph office there alongside the civil one. North of Frere the telegraph lines into Ladysmith had been cut and the country was in the hands of the Boers, so the telegraph communications for Buller's forthcoming advance were going to be Jelf's responsibility. Rearwards, the Natal system was connected through Pietermaritzburg to the Cape Colony where De Aar, like Frere, had became the handover point for the time being between civil and army systems. South Africa was also connected internationally by submarine cable from Cape Town and Durban. Generally, therefore, there was good telegraph communication between the main towns in the two British colonies, between the two separate army forces in Cape Colony and Natal, and with England.

The task facing Jelf was enormous. The resources of only one section, consisting in this case of one lieutenant, one sergeant, two corporals, four lance-corporals and fifty three men, were tasked with providing communications for an army which by early January had reached a strength of some 30,000 men, including nine officers of General rank.

Not something 'in the book', this was quite insufficient for the task and they were to be heavily over-worked in the stressful weeks ahead as Buller's field force tried to cross the Tugela and relieve Ladysmith. And what exactly they did can be gleaned from the very detailed diary kept by Dickie Jelf. *(iv)*

The Advance to the Upper Tugela - 9 to 16 January

General Buller had decided to try to cross the Tugela further upstream than the normal approach through Colenso, although several of his Generals had argued that the best route to Ladysmith was via the Hlangwane and Monte Cristo features just downstream from Colenso. His plan was to establish a forward headquarters near Springfield (nowadays called Winterton), from which to launch another attack. This strategy, and the conduct of the tactical operations in the Upper Tugela, have attracted much criticism from historians but that is not part of this story. What it meant for Dickie Jelf and his men was that there was going to be quite a long field telegraph line along an extensive left-flanking movement towards Ladysmith, well away from the civil telegraph line which followed the course of the railway.

General White in Ladysmith was appraised by heliograph signals of Buller's intentions, and on 10 January a cumbersome and overloaded column started the advance from Frere. Heavy rain had begun to fall on the previous day; wagons sank up to their axles, progress was laboriously slow, and the Tugela river was in flood. As the troops found out, summer in Natal is the rainy season, and the rain there can be very heavy. Eventually 23,000 troops moved to the Upper Tugela, leaving 7,000 at Frere, their base camp.

An intermediate depot was established at Pretorius's Farm, about seven miles from Frere. On 10 January the telegraph section built an airline to it and a telegraph office was opened there. This line, for its preservation, was kept about a mile away from the road along which the transport marched, and it worked well. It had been preceded, as was the practice for rapid laying, by a cable laid from a cable cart following a more direct route, but the cable was considerably damaged by the baggage wagons.

Also on 10 January the leading troops, a mounted Brigade, found the bridge across the Little Tugela river at Springfield undefended and intact. The Boers, fearful of being cut off by the rising river, had withdrawn. Seizing this unexpected opportunity, they pushed on and established themselves on Spearman's Hill. This hill is a dominant feature with two crests, Mount Alice on the western end, and at the eastern end, where naval guns were later emplaced, what was to become known descriptively as Signal Hill. From Mount Alice, on 11 January, the regimental signallers with the leading elements of the force established heliograph communications with Observation Hill in Ladysmith.

The airline being constructed by Jelf's section was continued to Springfield, which was to be General Buller's headquarters that night (11 January), and an office opened there working to Frere, with Pretorius's Farm as an intermediate office. On the morning of 12 January Buller pushed his headquarters further forward, to Spearman's Farm just at the base of the hill. The airline followed him there and the telegraph office at Spearman's Farm opened on 12 January, working back to Frere just over twenty miles away. Buller himself rode up to Mount Alice, 1,000 feet above the surrounding country, and enjoyed the splendid panorama it afforded northwards and eastwards over the intervening range of hills to his now visible objective, Ladysmith.

Due to the bad weather and condition of the roads it took six laborious days, until 15 January, to move all the troops and the supplies up to their positions at Springfield and Spearman's Farm, ready for the operations to follow. This done, the intermediate depot at Pretorius's Farm was no longer needed, and the telegraph office there was closed. The insufficient number of telegraphists meant that they constantly had to be redeployed to where the workload fell heaviest.

Soon after the troops had left Frere, Captain John Kennedy RE was attached to the force as the Assistant Director of Army Telegraphs (ADAT). John Kennedy had been the officer leading the experimental wireless detachment deployed around De Aar. *(v)* After it had been decided that the wireless was unable to contribute effectively to the army's operations, and the trial had ended, Kennedy was redeployed to assist the overstretched telegraph section in Natal. As ADAT, based at Frere, he was now principally acting as a coordinating officer between the army telegraph section and the colonial Telegraph Department, and dealing with such things as press traffic - something the army could well have done without at that time. It involved censorship, collection and accounting for money, and the excessive use of telegraph lines of limited traffic capacity.

Plans and Deployment - 16 to 19 January

The plan that then emerged was for two columns to cross the Tugela at two different places - Potgieter's Drift (ford), to be the crossing for General Lyttelton's Division, and a pontoon bridge constructed just upstream of Trichardt's Drift, to be the crossing for Warren's Division (see map and photograph below).

This was completed by 19 January. The Boers, from their observation posts on the hills north of the river, had seen all the movement to Springfield, and the two crossings of the Tugela, so there was absolutely no element of surprise. Buller's Chief of Staff at this time was Colonel AS Wynne - the same officer who in 1878-79, as Captain Arthur Wynne, had been the signalling officer to the then Major General Roberts in the first part of the 2nd Afghan War. *(vi)* He had also participated as a signalling officer in the 1st Anglo-Boer War of 1881, and was responsible for establishing a heliograph chain from Natal to Pretoria, the Boers having destroyed the electric telegraph route. *(vii)*

It becomes apparent from Jelf's diary that Wynne's signalling experience ensured he was well briefed about operational plans and future communication requirements.

A signalling station had been established on the eastern crest of Spearman's Hill and heliograph communications established with Ladysmith, over fifteen miles away. On 16 January a cable was laid from the headquarters at Spearman's Farm to the signalling station; it was initially a telephone circuit but on the 17th this was changed to a vibrating sounder (presumably the telephone circuit was unsatisfactory), and one of Jelf's telegraphists was attached to the signalling station.

The construction of the field telegraph from Buller's headquarters to Warren's and Lyttelton's headquarters, using field cable and airline, need not be described in detail here (although Jelf's diary explains exactly how it was done). The layout is shown on the map. Suffice to say that it was completed by 19 January with telegraph offices at each headquarters and an intermediate office on each flanking line, that it generally worked well with few outages, that all the senior commanders were in telegraph communication with each other and with the rear link at Frere. The forward communications and the line to Frere were heavily used, Jelf noting in his diary that "immense amount of work at front and main office, and Frere, but hardly any at Springfield."

He was, in fact, very short of telegraphists for the amount of traffic being passed and the number of offices being manned. At some offices there was only one telegraphist working all hours; they were rapidly becoming exhausted, and unable to stay awake. To relieve this problem Captain Kennedy back at Frere arranged for the line there to be connected directly with Pietermaritzburg. This had the effect of reducing the staff needed at the handover point at Frere, where there had been two full time offices, one civil and one army. Buller's headquarters at Spearman's Hill could now communicate directly with Pietermaritzburg, and only local traffic for Frere needed an operator. The army telegraphists thus saved were redeployed to Jelf at the sharp end. A number of the civilian telegraphists from Frere also volunteered to come forward and help. A Mr Rea was working at the headquarters near Spearman's Farm, later to be joined by Messrs McArthur and Anderson, and a Mr Banks assisted the lone army telegraphist at the telegraph office at Springfield. Banks had been assisting in the military telegraph office at Frere for some time. It was helpful that the colonial telegraph system used British procedures (most of their telegraphists had emigrated from Britain) and similar equipment, so there was a high level of compatibility.

Administrative Problems

Apart from the shortage of telegraphists, Dickie Jelf's diary describes how there were other more mundane administrative problems. The telegraph section was not an integral part of any larger organisation. Detached from their parent unit, and deployed over extended distances as required for the telegraph operations, they were 'nobody's children' when it came to responsibility for feeding and administering them. Collecting food, and distributing it around his scattered men, were all additional problems.

Spion Kop from Ladysmith

A further distraction was minor financial administration - matters normally dealt with in those days by a 'Clearing House' which formed part of the Telegraph Battalion headquarters establishment. Private use of the telegraph to send personal messages was permitted but had to be paid for, and Jelf had to deal with that. His diary shows various transactions and financial arrangements that had to be made - something he could well have done without when there was so much else to be done.

The Battle of Spion Kop

The next phase of the operation, commanded by Warren, was to attack and capture Spion Kop. It was to prove another disaster; the purpose of occupying it was questionable, and the tactics and command and control arrangements were a shambles. Many descriptions have been published and it is unnecessary to add to them here. Suffice to say that the attack failed and the hill was evacuated that night.

Graveyard at Spearman's Farm. Picture: Author, November 2002

The British suffered thirty-two officers and about 290 men killed, and there were some 560 wounded. The many graves and memorials now on the hill record the disaster. The telegraph section was not involved in the assault and maintained their communications between the headquarters of Buller, Warren, and Lyttelton. Forward of them, the tactical communications using visual methods were badly organised and ineffective, and will not be described. An extract from Jelf's diary on the 24th, the day of the battle, gives his version of events:

All working well. Fighting has been going on for several days and Sir C Warren is especially engaged. Sergeant Hawker managing left [flank] cable very well indeed.
About 10.00 am firing got very heavy on the left and pressure on the local lines was very heavy in consequence.
[Warren sent a telegram to Lyttelton at 9.53, received 9.55. 'Give every assistance you can on your side; this side is clear but the enemy are too strong on your side ... if assistance is not given at once, all is lost. I am sending up two battalions but they will take some time to get up.']
At 12 noon 'Clear Line' messages occupied local circuit for considerable time. [Clear the Line messages are authorised only by the senior commanders and immediately clear the line of all other traffic ready for operational messages of very high precedence.]
12.30. Hawker, who had stuck to Sir C Warren throughout, reported 5 shells falling within a few yards of the cable cart. No casualties among his party DG [thank God], but one orderly killed and one horse, and one man badly wounded. Cart went dis [disconnected] for ¾ hour and took up safer position.
An appeal from LF [the telegraphic address for the intermediate telegraph office on the Left Flank, on the way to Warren's headquarters] for relief of clerk but can't spare one. Have tried to arrange for a sapper to listen there and wake clerk, but seems impossible to teach them .....

So much for the telegraphic communications on the day of the battle of Spion Kop. Although there were short periods of line failure, and apparently some delay due to exhausted operators, the telegraph generally worked and the important messages were passed quickly.

Buller and Warren, the two architects of this disaster, met, and Buller decided to withdraw. The telegraph detachment that came back with Warren were, in Jelf's words, "quite done" after their exertions. The 26th and 27th saw the lines being dismantled and reeled in as the force withdrew back across the Tugela.

Meanwhile work continued for the telegraph section, repositioning lines and offices, with traffic still very heavy. More mundane matters came Jelf's way with having to settle his financial accounts - such things as payment for officers' private telegrams, to tell their family they were still alive! For three days it rained heavily; the section was becoming exhausted.

Buller next attempted to cross at Vaal Krantz, further downstream. The signalling station to Ladysmith was repositioned on Swaartz Kop. Jelf was kept very busy again laying further lines to the signalling station and to new positions downstream. This was provided by cable as the ground was too rugged for the construction of airline, and they were under observation and sporadic artillery fire from Boers on high ground north of the river. Kennedy, meanwhile, had been called to the headquarters near Spearman's Farm to run things there while Jelf was busy with the new work.

After further unsuccessful operations, it all came to nought at Vaal Krantz, and after two days, on 8 February, the newly laid cable started to be recovered. It all involved considerable work. As the withdrawal continued, more lines were dismantled and recovered. The office at Spearman's Farm was closed at 2.15 pm on 10 February. By 11 February lines had been recovered as far as Springfield. There, the office and the airline rear link back to Frere were left working, to provide communications for a Cavalry Brigade being left there. Having spent the night at Pretorius's Farm, the main body of the telegraph section marched to Chieveley, on the main railway line and just north of Frere, rejoined Buller's headquarters, pitched their tents, and rested overnight. It was a month since Buller's force had left Frere. In that time his force had suffered more than 1,750 casualties, and were no nearer to attaining their objective – the relief of Ladysmith.

Operations at the Tugela Heights

From Chieveley, Buller prepared a new plan (see map above). This time it was to advance north from Chieveley and establish a base on Hussar Hill; to capture the Boer positions south of the Tugela at Hlangwane Hill, Green Hill, and Monte Cristo; to cross the river downstream from Colenso; and then to advance generally along the line of the railway as it cut its way through the difficult and hilly country known as the Tugela Heights to Pieter's station, and once past there across the plain to Ladysmith some ten miles away. This was what several of his Generals had recommended before the futile Upper Tugela operation was decided.

The operation started on 12 February and lasted until 27 February, the details not relevant here. In summary, the Tugela river was crossed on 21 February, over a pontoon bridge built by the engineers to the west of Hlangwane. The bridge used by the Boers near the Colenso Falls had also been repaired sufficiently for infantry to cross. On the 22nd Buller transferred his own headquarters north of the river. There was hard fighting around the 24th in the area of Inniskilling Hill, and the Boers were becoming demoralised; apart from the pressure being applied they had heard of the relief of Kimberley on 15 February. By 27th the Boers defence collapsed, and at about 4:00 pm on 28 February the leading elements of Lord Dundonald's brigade rode unopposed into Ladysmith.

Communications in support of the Operation

What part did Jelf's telegraph section play in this final and eventually successful operation? On 13 February telegraph office arrangements at Chieveley were set up, so that military and civil lines were coordinated, as had been done previously at Frere. Diagrams in Jelf's diary show the detail. That evening Jelf was briefed by the Chief of Staff for the forthcoming operation. On the 14th a cable, subsequently replaced by airline, was run from Gun Hill to Hussar Hill, four miles further on and the office located near the headquarters and the signalling station. Another line was laid for a telephone to the 5th Brigade at Schutter's Hill, a few miles north-west of Chieveley. On 16 February, just after breakfast, a Boer shell burst about fifteen yards from the telegraph office at Chieveley camp, fortunately with no serious casualties. More shells arrived, and the office was moved to a more protected position in a donga (dry river bed). Civilian telegraphists helped the undermanned army telegraphists at the offices at Frere, Springfield, and Gun Hill.

During this period Jelf was impeded by further administrative problems. The system of orderlies, provided by units which had been briefed about the requirement and who were needed to deliver and collect messages from the telegraph offices did not work. Frustratingly, many messages, having been sent and received, piled up uncollected at the telegraph office. "Whole system of telegraph orderlies needs to be on a much more organised and important footing", noted Jelf in his diary. Rations, mentioned previously, and now also drinking water, had to be drawn from a central point at Chieveley and then redistributed to the section scattered at various telegraph offices and laying line all over the place. For several days the temperamental Natal weather had been very hot, so the water was essential. On 18 February the Hussar Hill line was prolonged about three miles to Green Hill, where General Buller established his headquarters on the 19th and 20th, and later on in the day it was extended another two miles to Bloy's Farm. The line was heavily used by the headquarters to the guns at Gun Hill, calling for and directing artillery fire. Various other lines were laid locally at the time. On the following morning the line was extended to Hlangwane Hill, where General Buller temporarily relocated his headquarters. On 21 February Jelf received further instructions, his diary noting: "Sir R. Buller sent for me before daylight this morning, and said he wished airline brought direct from Hussar Hill etc. ..... Was kind in what he said when I told him how short-handed we were." Later that day the line was re-routed direct from Hussar Hill to Hlangwane, and extended to the pontoon bridge over the Tugela. Buller moved his headquarters across the river on the 22nd.

On 23 February the wire was pushed across the river at the pontoon bridge to the left bank, where an office was established. The telegraph detachment was exposed to severe rifle fire from the overlooking heights, and had to seek refuge in a donga, where the office instruments were brought. Heavy rains fell suddenly, turning the donga into a rushing torrent which carried the instruments away, and before they could be saved they were nearly into the Tugela.

On the morning of the 24th Jelf got all his wagons and men across the Tugela. Finding the new headquarters position too exposed to enemy fire, and reminiscent of the Grand Old Duke of York, Buller that evening moved his headquarters back across the river to Hlangwane Hill! The heavy rain continuing, the lines and offices had to be rearranged in the darkness. Jelf was so soaked and exhausted that he went to sleep on the job and fell off his horse, fortunately without injury. The headquarters now occupied two positions, during the daytime on top of the hill, and at night just to the west of the hill, each requiring a telegraph office.

On the night of the 26th the pontoon bridge was removed to be set up in a better position further downstream, but without any warning being given to Jelf, whose cable across the river had been supported on the pontoon. The cable was, of course, carried downstream and had to be cut and replaced by another piece, heaved with difficulty across the river where it narrowed into rapids. General Lyttelton advanced down the left bank of the river and close to the railway wires, which were used to keep him in communication. On 27 February Jelf was at the headquarters at the northern tip of Hlangwane Hill when an important telegram reached them. His diary records events:

Just as the troops were going to attack, the news of Kronje's [sic] surrender to Ld Roberts [at Paardeberg] on the anniversary of Majuba was flashed through the wire to this telegraph office, and telegram handed to Military Secretary and to Sir R. Buller, who had it immediately signalled to all the Brigades and Divisions not in touch already by wire, and to Ladysmith. The Military Secretary said: 'This news is worth 100,000 men to us today.'

The Boers also heard by their telegraph about Cronje's surrender at Paardeberg, and the next day they cracked and ran, freeing the route into Ladysmith. On 28 February, the headquarters moved across the river again, this time northwards to Kitchener's Hill, not far from the railway. *(viii)* Unsure of the state of the railway telegraph line, Jelf sent one of his men across the river to test and repair it, while starting to lay a new line across the river to the headquarters' new position. Minor repairs were made to the railway telegraph line, and it was brought to working order, a cable completing the short distance to the headquarters and thus putting them in direct communication with Chieveley and Frere. Later that day the first troops rode into Ladysmith.

On 1 March General Buller moved on to Nelthorpe Station, where a telegraph office was opened. A cable was pushed on towards Ladysmith, and at about 3.30 pm the line party met a line party from Lieutenant Hildebrand's

previously besieged section running a line out from Ladysmith, and so telegraph communication with the town was restored. Thus, at last, ended the siege of Ladysmith. After the relief, the two telegraph sections, the one that originally went to Natal and had been besieged, and the other which had come from De Aar with Jelf, joined forces. They remained in Natal under Major Hawkins to continue operating there with General Buller when he later advanced into the Eastern Transvaal. The telegraph traffic passed during the operations on the Tugela river from early January until the end of February was immense, covering as it did the build-up, movement and logistics for 30,000 troops, the operations firstly to the Upper Tugela and then to the Tugela Heights, the battles and the traffic generated in their aftermath – casualty lists, and so on - handled mostly by one telegraph section with some civilian assistance. The line laying and maintenance throughout the movement and various redeployments of headquarters had also been immense.

Jelf describes in his diary how, at Nelthorpe Station on 3 March, he met up with his brother "Ru" (Rudolf), who rode out to meet him. Dickie described him as "thin, and suffering for a month from an upset inside", as many others in Ladysmith were. They met again the following day.
Dickie Jelf was known personally to General Buller, who mentioned him in his despatches from Ladysmith at the end of March, saying that:

Lieutenant R. J. Jelf, Royal Engineers, has been indefatigable in charge of the Field Telegraph, and has constantly had to work day and night. No difficulty was too great for him.

Unfortunately the strain of these operations, lasting over two months, took their toll on the unfortunate Lieutenant Dickie Jelf, aged 28. The work he had to do in Natal with a small number of men and no supporting administrative staff was overwhelming – communications ever changing, the telegraph system heavily worked, desperate fighting at the Upper Tugela and then the Tugela Heights. Once Ladysmith was relieved, and suffering from dysentery, he collapsed. He suffered mental and physical exhaustion and what would appear to have been a severe breakdown. He was taken to Pietermaritzburg hospital, kept under observation for some time, and then sent back to England to recuperate. He died on 2 June during the voyage home, and after his short marriage, leaving a young widow.

A memoir appeared later in the RE Journal, written by his father, Colonel RH Jelf CMG. *(ix)* It discreetly omitted the full story. In fact, as a sad ending, Dickie Jelf committed suicide on the ship on the way home. In Khaki Letters, a collection of letters written by civilian telegraphists from the Post Office who were sent to South Africa as reservists, the detail is exposed.

It is with much regret that we record the death of Lieut R. J. Jelf, R.E., an officer well-known to all the men of the T.B., not only in South Africa, but at home. He had been invalided home suffering from dysentery which had followed enteric fever. He embarked at Cape Town on board the transport "Dilwara". All the way home he was in very low spirits and generally despondent. About 7 o'clock in the evening of 2nd June, just before dinner time, he left his attendant and went right aft on the starboard side of the promenade deck. Without a moment's hesitation he took out a revolver from his pocket, and before he could be prevented, placed it to his temple, and pulled the trigger. ..... He was buried at sea next morning. (x)

Conclusion

Perhaps this story of one troop commander in the early days of army communications has shown that, although operational environments and technology are forever on the move, the fundamental requirements remain, embracing such old-fashioned terms as leadership, man-management, communications planning and organising ability, initiative and resourcefulness. In an operational scenario the troop commander needs to be somebody able to deal with the unexpected and unplanned, as Dickie Jelf did.

Endnotes

i. Many books about the Boer War were written in its immediate aftermath. For any reader wishing to cover the full story of the war the recommended book is The Boer War by Thomas Pakenham, published in 1979 after exhaustive research, and now easily obtainable in paperback. (Pub Abacus, ISBN 0 349 10466 2.)
ii. This depleted the Telegraph Battalion's limited resources even further, as one of their sections under the command of Lieutenant Harry Mackworth had already been transferred to the area of Colesberg to provide communications for a force being quickly assembled to counter Boer incursions in that area. The work of this section was described in the RSI Journal, Vol XXV, Spring 2004, pp 18-22. Another example of an unforeseen task not 'in the book'.
iii. On being appointed adjutant of the RE Troops at Aldershot, Jelf handed over his section in 'C' Troop to Lieutenant Herbert Kitchener, later to become Field Marshal Earl Kitchener of Khartoum, who in the Boer War went to South Africa with Field-Marshal Lord Roberts as his deputy, and later assumed command.
iv. Lieutenant Jelf's diary is held in the archives of the Royal Signals. It describes his section's work in great detail, including the names of the soldiers and their duties, as well as diagrams of the line layout and telegraph offices to support each stage of the operations.
v. A description of their experimental wireless work will be found in the RSI Journal, Vol XXV, Spring 2004, pp 23-29.
vi. The signalling operations in the 2nd Afghan War were described in the RSI Journal, Vol XXV, Spring 2006, pp 191 to 201.
vii. The telegraph line to Pretoria was subsequently restored by a combined detachment found from 'C' Troop and the Postal Telegraph Companies and sent to South Africa under the command of Lieutenant Arthur Bagnold, who described their work in the Journal of the Society of Telegraph Engineers, 1882, Vol XI, pp 312-340.
viii. The hill was named after Colonel Walter Kitchener, commander of the West Yorkshire regiment, and not to be confused with his brother, Lord Kitchener, who was at that time at the western front with Lord Roberts.
ix. Royal Engineers Journal, July 2, 1900.
x. Khaki Letters from My Colleagues in South Africa, p 195. Reported by Colour Sergeant R E Kemp.

SIGINT-THE SECRET LAND WAR 1939 – 1942: PART ONE

By Major (Retired) Tom Johnstone

Major Tom Johnstone served a full career in the Corps, including a tour with 9 Signal Regiment (Radio) in Cyprus. He now lives in Australia, where he is an active contributor of historical articles to military journals.

Introduction

In 1919 a new organisation entitled the Government Codes and Cipher School (GC&CS) was created in Britain. Attached to the Foreign Office, it was tasked with cryptanalytical attack on intercepted cipher traffic. Naval signals intelligence (Sigint or Y) remained largely as during the war years, based on the Admiralty, with outstations at Malta and Singapore. Army Y suffered most heavily, the Intelligence Corps was disbanded and the RE Signals element became part of the newly formed Royal Corps of Signals. Consisting of several wireless companies, although Royal Signals units were under SD6, they were operationally controlled by Director of Military Intelligence (DMI). In 1924 one wireless company was based at Sarafand, Palestine and another at Razmak on the Northwest frontier of India and detachments at Tientsin and Aden. The last monitored aircraft, while the others had watching briefs on Soviet Russia. Later, RAF operated detachments were dealing with Italian colonial communications in North and North-East Africa. During 1924, at the negotiations leading to the treaty of Lausanne, Sigint, in conjunction with human intelligence (Humint), furthered British political objectives by enabling negotiations with the Turks for a final peace treaty. (1)

Before the outbreak of WWII the Foreign Office refused to cooperate with the armed services in gathering intelligence in foreign countries, even when Hitler came to power in Germany and began furiously to rearm. The Service Chiefs of Staff, knowing the extent of Britain's military unpreparedness for war due to Treasury constraints, were determined on resisting British involvement in military operations. They became increasingly critical of Foreign Office initiatives in central Europe, well knowing the slow progress of British rearmament, especially in view of the Foreign Office's own estimate, that Germany would be ready for war in 1939. "In the Foreign Office some of the leading figures became increasingly incensed with the Chiefs of Staff for pessimism in their strategic assessments and took the view that they were exerting too much influence on the formulation of policy. In these circumstances, far from becoming reconciled to the need to pool intelligence and to reach agreed assessments, the two sides persisted in their right to render separate assessments." (2) This was to continue even after the outbreak of war until 1941.

After 1918, Sigint concentrated on strategic intelligence and ignored tactical intelligence, forgetting the hard won lessons of WWI. Moreover, although wireless telegraphy (W/T) continued to be developed and used, self-monitoring was neglected outside Royal Signals controlled networks. Illustrating the watch kept on Royal Signals nets is the story of an operator swearing on a net on the NW Frontier in the 1930's, and picked up by monitors in Aldershot. Reported to his CO in Peshawar; the operator was duly charged (3) On the other hand, when radio communications for armoured fighting vehicles were developed, VHF was the chosen band. Operating on voice and unfortunately called radiotelephony (R/T), it was used like a secure telephone. Outside the control of Royal Signals it was a practice dangerous to security in peace and proved disastrous in war. Conversely, since their use of tactical Sigint at Tannemberg in 1914, the Germans had never forgotten its lessons. General Heinz Guderian, founder of the German armoured forces, had begun his military career commanding the signals section of a cavalry division on the Western Front in 1914, before going on to staff appointments at division, corps and army. In addition to being a signals officer he was a cavalryman in the mould established by General Friedrich von Seydlitz, Frederick the Great's cavalry commander. Seydlitz led from the front and trained the Prussian cavalry to high and exacting standards of performance, discipline and control.

In developing the new armoured cavalry, Guderian imbued the new Arm in precisely the same mould. He insisted on commanders leading from the front in close contact with the battle. Moreover, having had a signals background, and remembering the lessons of WWI, Guderian imposed tight security on his command and control communications. All traffic had to be encrypted before transmission by radio. An extant photo shows him during the Polish campaign standing in a half-track armoured command vehicle, among signals personnel operating radios and an Enigma enciphering machine. Concurrently, the Germans developed tactical radio intercept (Nachrichten-Fernaufklarung) units, to operate in the front line. They first saw action in Poland 1939, and then in France in 1940. General Liss, head of intelligence staff of the German army 1937-43, later wrote that during the battle of France, German field Sigint was his best source of intelligence. (4).

Teething Troubles

Before the outbreak of WWII, GC&CS, now at Bletchley Park, forecast that wireless telegraphy would be little used by the Germans and this proved correct. Consequently, having little material to work on, the attack on Enigma ciphers stalled until the Norwegian campaign began, when voluminous quantities of cypher traffic transmitted by W/T gave GC&CS cryptanalysts ample scope for their talents, and a German Air Force (GAF) code was broken. Then a new problem arose. During WWI Sigint was confined to operational headquarters; in France for the Army and at the Admiralty for the Navy. Therefore no precedent existed for distribution by secure means of Sigint product to government or defence departments with source protection. (5) Nor were GC&CS and Whitehall departments prepared for the quantity of intelligence produced, and they becme swamped. Additionally, the staff of GC&CS "was quite inadequate in numbers or in its understanding of military matters" (6) However, more importantly, the Enigma decrypts flowing in enormous amounts first from Norway, and then from France enabled GC&CS and the Services intelligence and operational departments to accumulate the expertise that ensured accurate interpretation, efficient distribution and use of the product in the future. (7)

Army Tactical Sigint in France 1939-1940

Army Sigint returned to the tactical sphere when a Sigint Company, given the disingenuous title of 2 Company, 1st GHQ Signals, was attached to GHQ British Expeditionary Force (BEF). It was probably the unit which had been stationed at Aldershot. At this time Army Sigint units were still controlled by the DMI and were dealt with by a Signals section known as Intelligence Signals (IS).
Signals Branch itself was part of Staff Duties known as SD6. Not until 1941 was the SO-in-C given his own Directorate. (8)

The intercept stations for enemy nets were in the Lille-Roubaix area; other stations at Arras were monitoring own nets for security purposes and tracing clandestine radio stations. The direction finding stations were in central France positioned near Dijon and Tilleroy; and formed a baseline for triangulation on enemy stations in north-western Germany. (9) True to GC&CS's forecast, in this phase of the 'Phoney War', enemy radio stations maintained radio silence; the detachments therefore monitored other stations, including police nets, which were often the source of useful information.

During the battle of France, Sigint provided HQ BEF with much information concerning enemy movements, locations and intentions. Sigint was first to report on 24 May, a plain-language message giving Hitler's order for the attack on the line Dunkirk-Hazebrouck-Merville to be "discontinued for the present". (10) By the time the attack was resumed on 26 May, the BEF had already retired to Dunkirk. The unit not only provided superb intelligence, but identified problems maintaining communications between Y detachments and intelligence staffs in mobile warfare. (11)

Additionally, material gleaned from the transmissions of German radio nets during the battle enabled the company to amass considerable information concerning the German Army (GAR) order of battle and radio procedures. When this material was brought back to Britain, it enabled War Office operations staffs to compile an accurate GAR order of battle for the first time. (12) After the evacuation and following a period deployed on the Channel coast in an anti-invasion role, the unit moved to the Middle East, the only theatre of land operations in 1941.

Lieutenant General Sir Henry Pownall, Chief of Staff BEF 1939-1940 later wrote: "The part played by the Royal Corps of Signals in the BEF of 1939-1940 is a record of great achievement. No Commander in the field and no Staff Officer can be unaware that without an efficient signal system his personal contribution to success in battle will be crippled if not entirely frustrated. I well remember the serious anxiety of Senior Commanders in this respect when the BEF first landed in France. When it was all over their gratitude for services rendered was greater still." (13)

The Conquest of Cyrenaica January – February 1941

Just before the outbreak of war, a Middle East Intelligence Centre (MEIC) was established in Cairo in June 1939 to support the Cs-in-C Middle East and provide intelligence to London for HMG. Italy's entry into the war on 11 June 1940 saw a need by all three intelligent services to combine their resources; they prevailed upon their Cs-in-C to demand London's agreement to transfer the main cryptanalytic attack on Italian ciphers to the Middle East. At first the Chiefs of Staff rejected the request. However, on the advice of Directors of Intelligence in Whitehall, they agreed, but insisted that the effort should be a combined one. This led to the establishment of the Combined Bureau Middle East (CBME) at RAF Heliopolis. They defined the functions of the Bureau and GC&CS in such a way as to preserve GC&CS control of cryptanalysis. The Bureau, administered by the Army was composed of the cryptanalytic staff of all three service in Egypt together with cryptanalysis sent out from GC&CS. GC&CS also retained responsibility for the basic research and initial attack on the high-grade Italian ciphers. The bureau was also to work on lesser ciphers; and 'with the aid of GC&CS, to be responsible for exploiting readable high-grade ciphers for the benefit of their service intelligence staffs in the theatre'. Direct communications between GC&CS and CBME, known as the SCU/SLU link, for Ultra dissemination had opened on 13 March 1941. Probably this link was the one on which the Head of Bureau "could raise technical problems, but not change GC&CS policy decisions". (14)

Shortly after the outbreak of war with Italy on 11 June 1940, 2 Wireless Company (2 WC} in Palestine, moved its Italian section to Cairo and created four mobile sections; 1 and 2 Mobile Sections (MS) were probably despatched to Khartoum and Nairobi, 3 MS was attached to HQ Western Desert Force (WDF); 4 MS was sent forward immediately to Mersa Matruh and began operating. During the following month the Italian army in Libya moved across the Egyptian frontier and formed a series of defended boxes and 4 MS 'obtained a fairly comprehensive picture of the Italian forces from its work on their field ciphers.' The work of the forward Y detachments was backed-up by the parent unit 2 Wireless Company, shortly to become a regiment,. and by the Army section of CBME, which did the same work for the benefit of GS Int GHQ M.E. in Cairo. (15)

Following the Italian advance across the Egyptian frontier, through aggressive patrolling and raiding, armoured cars of the Western Desert Force (WDF) gained a moral superiority. At the same time 3 MS, now attached to HQ Western Desert Force, well briefed by 4 MS were able to profit from this in the operations which followed.

During December 1940, the WDF under Lieutenant General Sir Richard O'Connor struck with 7th Armoured Division and 4th Indian Division, and in a masterpiece of secret preparation, surprise and speed, routed an entrenched Italian Corps. General Wavell then replaced 4th Indian with 6th Australian Division, against the advice of O'Connor, who wanted to use the Australians as reinforcements and complete the conquest of Libya. A month later 7th Armoured Division followed closely by the motorised 6th Division overran Cyrenaica capturing the fortress towns of Bardia, Tobruk and Bengazi.

From the commencement of the battle 3 MS provided invaluable intelligence to its headquarters. But because of the Signals policy of daily destruction in forward areas, little was preserved. However, the British Sigint historian recorded some of its successes. "It is difficult not to say impossible, to document the part played by Army Intelligence in the campaign. Most reports of immediate tactical value went by word of mouth or were scribbled on message pads which have not been preserved. But it is known that 3 Mobile Section, attached to the WDF HQ, provided a steady stream of information from its decryption of Italian tactical codes and ciphers. During December alone it produced 300 valuable decrypts. Later in the campaign its decrypts included the situation reports of the Italian Corps Commander in Bardia to the Italian Supreme Command during the Australian attack on that garrison in early 1941; a full strength return of the Italian garrison before the attack on Tobruk, and despite Italian cipher changes after the fall of Bardia, details of the Italian withdrawal from Benghazi. These last played their part in O'Connor's decision to thrust south-westward across the desert to Msus. A decision the Italians had considered the British might take but dismissed it as 'impossible'." That move resulted in the destruction of an Italian army at Beda Fomm on 5-7 Feb 1941, and completed the capture of Cyrenaica. In their cryptanalytical attacks on enemy signals, the forward sections were backed up by their parent unit - 2 Wireless. (16)

Sir Harry Hinsley, the Sigint historian, has starkly outlined British Sigint's bleak future for the succeeding eighteen months in the Desert War: "Nevertheless, despite the windfalls brought by field Sigint during the advance against the Italians, its recondite character and liability to interruption prevented it from being treated by operational commands on a par with regular, orthodox, non-Sigint sources."(17)It would the cinderella of the Staff. Not until the summer of 1942 and after many defeats would Sigint be fully integrated into operational intelligence. Following this there was never a defeat.

Pre-war British Intelligence in Italy was controlled by the MI6 Vienna station, but when Germany occupied Austria in March 1938, all British agents were expelled and intelligence about Italian forces dried up. Additionally, HQ Middle East, by pre-war agreements, relied on French intelligence regarding Libya. But following the French defeat and the action taken against the French Fleet at Oran, intelligence cooperation not only ceased but became hostile. Attempts to insert agents into Libya failed, as did those to suborn Italian POWs. (18) Such was the British human intelligence situation when Rommel landed at Tripoli with his Afrika Korps, that HQ Middle East had to rely for intelligence on Sigint Air reconnaissance and the Long Range Desert Group, (LRDG) during the campaigns in North Africa and the Mediterranean. In 1940 the LRDG was raised, trained and led by Lieutenant Colonel RA Bagnold, Royal Signals in the years 1940-41. (19) Its exploits in the Western Desert behind enemy lines needs no elaboration here

East Africa

During the period March to May 1941, Middle East Command with two Indian Divisions, a South African division and a force of East and West African colonial troops, conquered the Italian colonies of Eritrea, Italian Somaliland and their newly occupied kingdom of Ethiopia. During the conquest of the Italian East African colonies such was the success of Sigint in those campaigns that the DDME in Cairo wrote he "could not believe that any commander in the field had been better served by his intelligence than the commander of the forces operating in East Africa.(20)

The Balkans

In December 1940, after the invasion of Britain had been cancelled, GC&CS broke a code of the Abwehr which revealed a switch in German intelligence priorities from Britain to the Balkans. From that time onwards considerable military activity was taking place there. German strategic thinking was directed towards Turkey, Syria, Iraq, Iran

and Egypt. In this, the movement of the RAF to Greece and the threat it might pose to. Rumania's oil fields at Poesti – essential to Germany's war effort – and the southern flank in future operations was enough. Operational planning to move into Greece began in November 1940 with the object of attacking British targets in the eastern Mediterranean and preventing British attacks on Rumanian oil fields. The British assumed it was also intended for a thrust through Turkey to the Middle East. (21) Shortly afterwards the build-up of German forces into the Balkans began. First with GAR infiltration of signals, and AA artillery and Gestapo in plain clothes were detected early on by British agents and military attaches in Bulgaria and Rumania. From January 1941 voluminous Enigma decrypts showed how advanced German preparations were for an operation code Marita, the invasion of Greece. In early February, decrypted railway timetables when analysed by the Railway Research Service in UK showed massive railway movement of warlike stores through Bulgaria on the axis of advance to Salonika. Moreover, British SIS agents gave supporting evidence on rail movements through Hungary.

These preparations could not be concealed for long, and it is probable that the Greek government as well as other Balkan governments were aware the threat Germany posed. Yet, Greece had made it clear that there was to be no intervention until German forces entered Bulgaria. On 11 February, the DMI gave a verbal presentation of the probable strength, direction and intentions of a German attack. The British Military Attache Bucharest had already reported that German troops would cross Bulgaria on 17 February, and calculated that they would reach Salonika a week later, and reach Athens with ten divisions between mid-April and mid-May. Any hopes the British might have had have for cooperating in possible advance defence planning to resist a German invasion 'were wishful thinking'. (22)

Greece – The Decision to Intervene

During the critical month of February when a decision had to be made vis-a-viz Greece and Libya, Whitehall displayed masterly indecision. From 6 February 1941 the evidence of a GAR move into Africa had been growing. On the 6th a convoy sailed from Naples; MI thought it probably portended an expedition of two or three GAR divisions. On the 9th an IAF high-grade message was passed giving special instructions for IAF and GAF escorts of convoys to Tripoli; GC&CS was reasonably sure the convoys were transporting GAR units. On 11th February during a meeting of the Defence Committee; chaired by the PM, Churchill argued that if British troops moved to northern Greece they could delay the German advance. This was agreed, and the C-in-C ME was told to give preparations for intervention in Greece priority over the continuing the advance to Tripoli. On 15th Air Intelligence (AI) was still 'unimpressed with the evidence' of enemy moves to Libya. Between 12th to 18th messages flowed between the Admiralty and C-in-C Mediterranean on the nature of the convoys, and finally on the 18th the Admiralty signalled C-in-C Mediterranean that the convoys [from Naples and Genoa to Tripoli] appear to be German'. (23) The final decision to intervene was taken on 27 February, despite a General Staff appreciation that "we must be prepared to accept the loss of all forces sent to Greece". (24) Acerbically, the official Army historian commented, "It would appear that in such matters the Norwegian campaign had taught us little" (25).

W Force in Greece

On 5th March 1941 W Force began moving to Greece. The force commander, General HW Wilson, in order to keep a low profile, met his force in mufti. The German military attaché in Athens was also there, counting the force as it arrived. This included an Australian and a New Zealand Division and a British Armoured Brigade; a second Australian division was to follow.

The Germans attacked Greece on 6 April 1941 with fifteen armoured, infantry and SS divisions, supported by dive bombers; with heavy bombers attacking strategic targets deep inside Greece. These latter wrecked the harbour of Piraeus on the night of 6/7 when the SS Clan Fraser, loaded with TNT, exploded destroying seven other ships, many lighters and wrecking the port. On the same day Wavell signalled General Blamey, commanding the Anzac Corps, telling him that 7th Australian Division could not be spared from Africa. (26)

W Force was positioned on the Aegean south of Salonica then westward to the Aliakmon River; with the New Zealanders on the flat coastal plain and 6th Division in the mountains to the west. Exposed to enemy turning movements, its positions were indefensible. 40th Motorised Corp, consisting of 3 armoured, infantry and SS divisions', advanced through Yugoslavia crossed the Monastir gap and penetrated deep into Greece using mountain tracks considered unfit for tanks, and was in danger of outflanking General Wilson's Aliakon line. Timely warning from his Sigint unit alerted his HQ to the danger, and Wilson ordered Blamey to retire to the Olympus line. (27) "If the British withdrawal had begun a day later it would have been disastrous for the British force."(28) Retirement to positions around Mount Olympus was made without air support, and the force was fortunate to reach their new positions largely unscathed after being bombed and strafed day and night. However, when warned again by Ultra concerning his precarious situation, Wilson decided on evacuation. Luckily, this probability was foreseen by Major Freddie de Guingand and preparations were already in hand for simultaneous withdrawals to seven different beaches in the Athens and Corinth areas.(29) Re-embarkation began on the night of 24/25 April and despite the GAF furious reaction the plan worked. But while a high percentage of personnel was evacuated, all heavy equip-

ment, guns, tanks and vehicles were lost. Sigint units were however able to take their precious sets and documents to Crete and with the issue of fresh vehicles, continued Sigint operations from there.

Sigint Units in Greece

On arrival in Greece, the British Sigint unit already been seasoned by service in France and England, and became operational immediately. However, this was not the case with 4 Australian Special Wireless Section (4 ASWS). This consisted of officers and men who until war was declared had been either commercial radio engineers, telegraphists or amateur radio enthusiasts. Although skilled engineers and operators, they had received only brief Sigint training in Egypt. Its two Australian Intelligence Corps corporals were as equally inexperienced in field code breaking. But what they lacked in expertise they made up for in enthusiasm. (30)

It had been intended for the British Sigint detachment to deal with low-grade Italian ciphers; but most of its personnel knew German or Italian. They were also equipped with GAF codes and bomber grids and therefore could exploit the GAF tactical and plain language traffic encountered in Greece and Crete. Working with this experienced British unit, 4 ASWS could not help but quickly assimilate the technicalities of their new role. Together they shared notable successes, such as reporting the German advance into Yugoslavia; the coup in Belgrade and indications that an invasion of Greece was imminent. They followed this by reporting the capture of Barce in Libya by the Afrika Korps (DAK). Picked up by plain language voice transmissions from tank commanders, it was disbelieved at first by headquarters intelligence staff, but the section were later commended. (31)

"It soon became evident to us that it was the help given by the British unit that made it possible for our Australian section to operate so successfully in Greece and later in Crete." (32) The two corporals, who were shortly to be commissioned, considered themselves 'privileged' to receive instruction from 'such dedicated, enthusiastic and patient officers.' (33)

Having managed to save their precious sets and documents, and on receiving vehicles on arrival in Crete, they were quickly operational as a joint Sigint unit team working near Crete Force HQ. Although the Headquarters was receiving magnificent strategic intelligence direct from Ultra, real-time tactical information was of prime importance, and was provided by Army Sigint. This included news of enemy occupation of the Greek islands astride the approaches to Crete; details of large numbers of JU52 transport aircraft moving to Greece; enemy sightings of allied naval moves in the Rhodes area. (34)
When German airborne troops attacked and suffered heavy losses, code books were found on some bodies. Using these, Sigint began decrypting German messages and reading them as quickly as the enemy. Included were reports of seaborne convoys and their progress; enemy air reconnaissance reports on convoys; and during the fierce struggle for Maleme airfield, a stream of tactical reports through enemy eyes. (35) Acting on information picked up from them, the Royal Navy intercepted an enemy convoy and destroyed it completely. (36) When Maleme fell and reinforcements were brought in by air-landings, the situation of Crete, without air cover, became untenable. Evacuation was decided upon, and an 'emergency destruction' order received from the Chief Signals Officer Crete Force, Lieutenant Colonel W.R. Smjth-Windham, Royal Signals (who as a Lieutenant had been OC Comms on the 1933 and 1935 Mount Everest expeditions). Instructions were given to move to Sphakia for priority evacuation to Egypt. Given but one hour to accomplish destruction and move, no time was lost. (36) The British unit did take the captured enemy code books back to Egypt and they later proved invaluable.

Lebanon and Syria

The operation to recover the Lebanon and Syria from the Vichy French and prevent the possible use of its airfields by the enemy began on 8 June 1941. Once again field Sigint achieved considerable successes. "The excellent order of battle and topographical information Intelligence had available must have enabled the staffs to make good use of the tactical information that came to them from sightings, POW and the field signal intelligence unit which had previously distinguished itself in Crete." (37)

Following the fall of Beirut, Sigint moved to Souq el Gharb with detachments at Aleppo, where "much better" reception of German communications from Russia was was reported. (38) Germa advances into Russia were successfully monitored, and traffic in high grade cipher was passed back to GC&CS.
When Germany invaded Russia, 2 Wireless Regt had switched targets from the Red Army to the Werhmacht's triumphant advance to the Volga. In 1943 they eavesdropped on its final messages from Stalingrad.(39)

After Pearl Harbour, the thoughts of all in 4 ASW turned towards their next target. No time was lost in preparing for this; the operators learned and practised KANA code (the Japanese version of morse - containing 76 variants instead of the 36 for Morse), and methods of recording Japanese language transmissions went ahead 'relentlessly'. Similarly, the two attached Intelligence staff (now sporting the pips of Second Lieutenants), intent on learning Japanese scoured the bookshops of Beirut and found three Japanese primers. (40) 4 ASWS left for Australia and the Pacific war in mid January 1942. The Sigint experience and invaluable expertise which the unit had gained in the Middle East and Greece was to prove of inestimable value in the Pacific War.

Meanwhile the British Sigint unit had already departed for Egypt. Their vital skills, honed during the battle of France and perfected in Greece, were desperately needed in the epic struggle unfolding in the Western Desert.

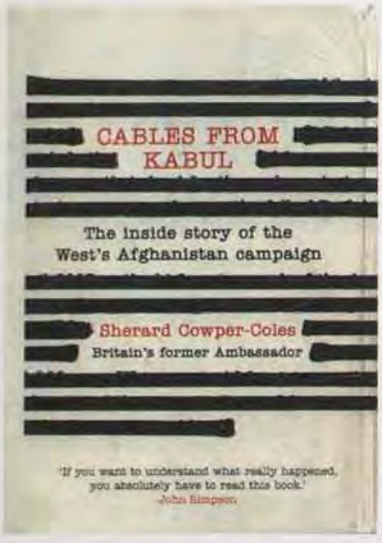
References.

1. Jeffrey, Keith. MI6 History of the Secret Service 1904-1949. Bloomsbury Publishers, London 2010, p196.
2. Hinsley, F.H. British Intelligence in the Second World War vol 1 HMSO. London 1981, p74.
3. Ex Cpl Bill Barlow. His father had been sergeant-major at Peshawar District Signals and had 'marched the man in'.
Bill was the radio 'mech' on the authors radio det in Korea.
4. Quoted in Hinsley vI p163
5. Ibid p162.
6. Ibid p148.
7. Ibid p147.
8. Royal Signals Association. A Short History of Signals in the Army(SHSA) Part 2. p6&7
9. Ibid p23.
10. Hinsley vI p148.
11. Ibid.
12 Ibid p287.
13. SHSA p1.
14. Hinsley vI pp219-20.
15. Ibid pp214-5.
16. Ibid vI p379.
17. Ibid p214-5.
18. Jeffery p424-5.
19. See SHSA (Additional) p7-8, and Lt-Col Peter Richards Brigadier Ralph Bagnold OBE FRS. The Journal Vol XXV
Summer 2005 N0 3
20. Hinsley vI p381.
21. Ibid 375.
22. Ibid 357-9.
23. Ibid 386-8.
24. Ibid 361.
25. Butler, Sir James, History of WWII. Grand Strategy. Vol II. HMSO, p549. Quoted in Hinsley vI p379.
26. Long, Gavin. Crete and Syria. AWM Canberra 1953, p39-40.
27. Hinsley, vI p407.
28. Long p81.
29. Collins, Major-General R.J. Lord Wavell, (1883-1941). A Military Biography. Hodder and Stoughton. London.1947.
p 385
30. Ballard, Geoffrey. On Ultra Active Service. The Story of Australia's Signals Intelligence Operations During WWII.
Spectrum, p49.
31. Ibid 50.
32 Ibid..
33. Ibid p74.
34. Ibid p78.
35. Ibid p79.
36. Ibid p83.
37. Hinsley vI 425.
38. Ballard p83.
39. Hinsley v II p199
40. Ballard p134-5.

CABLES FROM KABUL

The Inside Story of the West's Afghanistan Campaign

By Sir Sherard Cowper-Coles



The author was HM Ambassador to Afghanistan for three years from 2007 until 2010, and the Foreign Secretary's Special Representative for Afghanistan and Pakistan from then until his retirement earlier this year. This book sets out to identify some fundamental truths about the involvement of the West in Afghanistan, along the way acknowledging the successes our troops are enjoying, and concluding with some thoughts on how the conflict (or project, as the author terms it) can be brought to a successful conclusion.

In the manner of assignment organisations everywhere, the Foreign Office postings officer assured the author in 2006 that it would be a very worthwhile thing for him to leave his embassy in Riyadh early to assume responsibility for an increased UK presence in Helmand, following the large deployment of troops in that province, and that moreover, he was just the man for the job. Convinced there was a worthwhile task to be done, and dismissing the warnings of American friends to leave it well alone, he underwent a hectic in-depth series of briefings and meetings back in UK before assuming his appointment in May 2007.

His preparations were an inkling of what was to come, as he encountered the Afghan conference industry, a "stage army of caring and committed local and international actors, travelling from conference to conference, endlessly re-examining the entrails of the problem". Early misgivings about the wisdom of involvement in Helmand were brushed aside by a senior FCO official on the grounds that now we were there, we had to deal with things and get on with it.

The traditional limousine VIP departure for new Ambassadors was to be in sharp contrast to the chaotic tactical approach of the ancient UN aircraft chartered for the final leg of the journey from Dubai to Kabul. Met at the steps of the aircraft, he was bundled into an armoured Toyota Landcruiser, given a quick first-aid lesson, and driven off to assume office in the modest premises which were HM Embassy in Kabul. One is struck by the range of organisations he was to meet on his arrival, including HM Revenue and Customs, the Ministry of Justice, the Crown Prosecution Service, the Department for International Development (DFID), known as "tree-huggers", as well as the military, the Met and Northumbrian police and what the author terms "Men in Beards", some of which were genuine Special Forces, but others just pretending to be so.

Early impressions were not of the best. Offices were located in a block leased from the Bulgarian Embassy, and the staff lived in converted cargo containers, although the DFID staff had somehow managed to relocate to expensively leased villas. Travel out of the complex had to authorised, and the whole facility was guarded by about 100 private security guards and some 300 Gurkhas, all at an annual cost of tens of millions of pounds.

The approach was set early on when the Embassy intelligence officer advised him that his prime relationship as Ambassador would not be with the Afghanistan President, but the American Ambassador, without whom any hope of influencing the President could be remote. Fortunately he was to get on well with his American opposite number, despite the latter's predilection for aerial spraying of the poppy crop, something the author resisted, for various reasons. His first meeting with President Karzai to offer his credentials went well, even if his carefully prepared speech, delivered in Pashtu, hastily learned for the appointment, seemed to provoke great amusement. The point had been made however, that his arrival indicated an increase in support for the President and his government from the United Kingdom.

Early briefings then followed from the other key personalities: the US commanding General of ISAF, and the UN and EU Special Representatives, all of whom would be needed as allies if the Embassy mission was to be successful. The author notes wryly how often the phrase: "much has been achieved, but challenges remain" featured in these and subsequent briefings.

For those who have not been part of an Embassy staff, what follows is fascinating and enlightening, as the work of the Embassy is unfolded. The writing style is clear, honest and logical. Once established, the author had to contend with a steady flow of high level visitors, all of whom needed visit programmes to be tailored, itineraries agreed and meetings with senior Afghan government personalities arranged,

as well as appropriate security cover. Relations with the United States Embassy was as important as those with the Afghan authorities, but the constant comings and goings of Richard Holbrooke, together with his predilection for multiple mobile phones, were evidently something of a challenge when it came to having meaningful discussions.

Ironically, his eventual selection by the Foreign Secretary as Special Representative for Afghanistan and Pakistan was to involve him in almost as frenetic a schedule, and his relations with Holbrooke became even closer. Although based in London, his remit was to take him far and wide, and his dealings with the Secretary of State became more frequent and concentrated. His view that the military approach had to be complemented by an overarching political strategy became a conviction, which he steadily propounded throughout his appointment, and which is set out clearly in the latter part of the narrative. After the General Election of 2010, it became evident that his views were not meeting with official approval, and a series of snubs culminated in him being overlooked for the post of Ambassador in Paris, which he had been promised. Coming to the conclusion that his work was done, he submitted his resignation from the Diplomatic Service.

The author is evidently a man of considerable energy and formidable intelligence, which will have been evident to all who were fortunate to hear him address the RSI at Blandford in November. He has a reporter's eye for detail, and his observations of the military and diplomatic machines in action are striking in their originality and impartiality. There are places in the book where the author's diplomatic training appears to come under some strain, as he tries to deal even-handedly with the various senior personalities he had to contend with. It is clear that there are more illuminating opinions still to emerge, and we look forward with interest to seeing another version of the book, perhaps with the inclusion of some of the views which hindsight will surely have brought about.

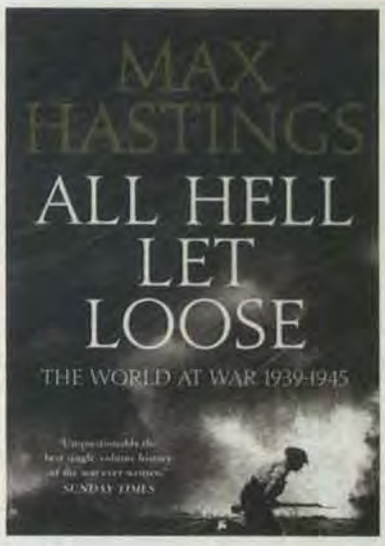
Highly recommended.

Available from Amazon £13.25. ISBN: 978-0-00-743201-1

ALL HELL LET LOOSE

The World at War 1939-45

By Max Hastings



The author has written ten books on the Second World War, reflecting some thirty-five years research into the topic, and in this his latest work he offers a single volume history of the conflict, taking into account new testimonies as well as revisiting traditional archive material.

The author's characteristically thourough approach is underlined by some thirty pages of copious references and a comprehensive index, which simplify greatly the act of tracking down particular subjects.

As always, the author tries to portray his account from a different angle - in this case what the Second World War was lrerally ike, and uses personal accounts from all sides to inform the narrative. In a book this length, any description of the subject is bound to be an overview, and this is freely acknowledged.

What seizes the reader however, is the balanced deductions which follow the accounts of each theatre and phase of the War, in many cases drawn from that careful consideration of contemporary accounts which is only possible with hindsight. It is interesting to learn that the succcess of the British in buidling and replacing aircraft during the Battle of Britain outpaced that of Germany, as did the Soviet arms construction effort during Operation Barbarossa. Another absorbing fact is that at the beginning of the War, Germany's military strength was only just greater than that of the Allies.

While the war started well for Germany, the book makes clear that hesitations, infighting, political manoeuvering and sheer wishful thinking on the part of the Allies only played into the hands of an adversary whose training, tactical awareness and tactical flair were of the highest.

The author covers areas which are less well-known, such as the immediate situation after the fall of France, which left many French servicemen now under the regime of Vichy France effectively in conflict with the British. The naval actions taken to neutralise the French fleet are well documented, as is the conflict in Lebanon, which saw over a thousand French casualties, and over 32,000 elect on capitulation to return to Vichy France, many of them to end up in Nazi slave labour camps, while some 5,000 decided to join the Free French forces of De Gaulle.

One of the benefits of this compact narrative is that the sttrategic and as well as the lower tactical intentions of the belligerents become clear, and how the intially sound plans of the Nazis and Soviets were to degenerate into horror, confusion and chaos as the leaders on each side took personal charge and inflicted much unncessary suffering on their own troops.

The book has a truly ambitious scale: all the major theatres of the conflict are covered, including Europe, the Middle and Far East as well as the war at sea. There is a final section dealing with the final fall of Germany and Japan, which is particularly illuminated by contemporary accounts, and brings hope the apocalyptic state in which the last-ditch defenders found themselves.

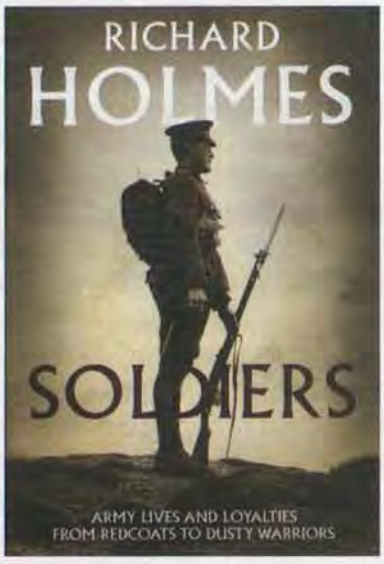
Ther are several contentions which are thought provoking and unexpected. Over ninety percent of all German soldiers who died did so on the Eastern front, and the industrial contribution of the United States was more fundamental to the success of the Allied effort than that of the British Army.

This book maintains the standard the author has set for himself with earlier more focused accounts such as *Nemesis* and *Armageddon,* beside which it fully deserves a place on every miltary historian's bookshelf.

Published by Harper Press, ISBN 978-0-00-733809-2, 747 pages, obtainable from Amazon £13.50 in hardcover.

SOLDIERS

Army Lives and Loyalties



This book was published after the author's death in April this year, and is a fitting testament to his love of the British Army and its soldiers. Already the author of 22 works on his favourite topic, as befits a former Professor of Military and Security Studies at Cranfield University and the Royal Military College of Science, this book looks at the soldier himself "warts and all", extending from the bonds of comradeship on the battlefield to the other aspects of service life: leave, courses, sport, family life, women, drink and gambling.

Exhaustively researched, and well indexed, the author's learning and passion for the subject are leavened by a keen sense of humour and a tase for the apt anecdote and epigram. In almost every situation, the capacity of the British soldier to find humour in the darkest of times is celebrated, and the whole narative is enlivened with well chosen and wittily captioned photographs.

The treatment is broadly in historical order, staring with the beginnings of the National Army in 1960, and leading up to the present day, with excursions into the officer and gentleman, the Church militant and the danger of foreign alliances. The author brings this to life by by making regular comparisons wuith the present day, and how traditional customs have evolved over the centuries.

Such potentially fraught areas as women in the service, Army cuts and regimental amalgamations, and the particlar peculiarities of certain regimental customs are addressed square on, and with an admirably even-handed treatment.

Throughout this well-written volume the author's affection for his subject comes through strongly, and he draws

extensively on his 35 year career as a TA officer for first hand experiences, particularly the Princess of Wales's Royal Regiment, of which he was Colonel-in-Chief for eight years. His readiness to shed the aloof stance of a typical academic and "muck in" has given him a real feel for what drives the British soldier and motivates him in these modern times to achieve what he does.

As he acknowledges, continuity and change are at the centre of his narrative. He believes that the great Marlborough would recognise in the present day combatants in Helmand the descendants of those he led to victory at Blenheim over three hundred years ago, but acknowledges that political, social, economic and technological factors have their effects.

Despite its length and the thorough approach, this is a highly readable volume, and is recommended for the interested reader and the serious historian alike.

Published by Harper Press, ISBN 978-0-000-722569-9, 657 pages, obtainable from Amazon £12.25 in hard-cover.

CORRESPONDENCE

From Lieutenant Colonel CM Vaudin, Royal Signals

Dear Sir,

I very much enjoyed reading the new look Journal that landed on my desk late last week. In particular I found the three winning Deane Drummond Prize essays stimulating and illuminating; please pass my congratulations to Captains Goslin, Pollit and Whillis.

As I prepare to assume command of 2nd Signal Regiment the essays were a timely reminder of the critical, and unique role of our soldiers and the young officers who command them. They were, are, and will remain our most vital asset and are our strategic edge ensuring success on operations both now and in the future.

As we adapt our young officer training and education to meet the demands of the contemporary operating environment we must continue to ensure we offer a demanding, challenging and rewarding career. Firstly we must ensure we retain the essence of what it means to be an officer: An officer must be the embodiment of leadership, character and the Army's Core Values. They must be dedicated to the essential qualities of courage, selfless commitment and self-sacrifice that are enshrined in the Ethos of the Army and which foster mutual trust. Second our young officers must then be competent in their profession; and this is no longer network focussed but requires them to have a wider understanding of the commander's information needs, the application layer, the information flow that enable the applications and then the network layer; but there is a continued requirement to include the basics such as antenna propagation and tactical siting. This level of professional knowledge is critical both for officers focussed on technical issues as well as those filling J6 staff functions advising commanders in deployed headquarters (in plain English not signalese). To be effective our young officers must be competent to span all these areas and as such we must continue to recruit from a broad church of applicants; we must not become PQOs but likewise there is no place for technical luddites.

The essay authors articulated many of the points I have raised and with far more clarity. However, having made this analysis we must be clear that it is incumbent upon Commanding Officers to ensure they train and then appoint their young officers to posts where they are fully employed both as leaders and J6 professionals. Those who know me will realise that that I am not making an altruistic point, rather we must continue to use our most vital asset in the most effective way if we are to succeed on operations. I will be looking critically at where and how I employ my young officers within 2nd Signal Regiment, especially their roles when the Regiment deploys to Afghanistan next year.

Yours Sincerely

Colin Vaudin *Shrivenham, May 2011*

MAJOR GENERAL AH BOYLE CB

Born in Kidderminster, Worcestershire on 18 January 1941, the son of Hugh and Irene, Tony Boyle had his secondary education at Forest School Snaresbrook from 1953 -1955, at Harrogate Grammar School from 1956-1957, followed by Welbeck College from 1957 - 1959. He was part of RMA Sandhurst lntake 27 from 1959 - 1961, and was commissioned into the Royal Corps of Signals in July 1961. He attended 50 Q Course at Catterick from September 1961 - February 1962 and the Whiteshod Course at the Norwegian Signal School at Jorstamoen, Lillehammer during February/March 1962.

His first posting was to 4th Divisional Signal Regiment from March-September 1962 under Lieutenant Colonel PE Hutchins before going on take the Mechanical Sciences Tripos at St Catharine's College Cambridge from September 1962 -June 1965. He was then sent to the Joint Communications Unit Borneo from June 1965 -June 1966 under OCs Major JH Hild and Major JF Blake and became OC COMCAN Bangkok (237 Signal Squadron) from June 1966-September 1967. He was selected to attend No 1 Fast TE Course at Blandford from September 1967-September 1968, before being appointed Adjutant 22nd Signal Regiment from September 1968-December 1969 under Lieutenant Colonel AL Dowell. He was Adjutant, Cambridge University Officers Training Corps {CUOTC) from Jan 1970-Dec 1971, before selection to attend Division 1 Army Staff Course No 7 from January 1972-December 1972 at Shrivenham and at Camberley from January-December 1973.

He was appointed GSO2 in the PTARMIGAN Project Office from January 1974-December 1975 under Brigadier JL Akass when DCMP. His Squadron command was OC 20 Armoured Brigade HQ & Signal Squadron (200) from January 1976-December 1977, and he eventually disbanded the Squadron to become Task Force Hotel. He was GSO2 AG11 Stanmore from January 1978–January 1981 and appointed CO 9th Signal Regiment (Radio) from February 1981-October 1983. He was a member of the Directing Staff EGW Division at Shrivenham from November 1983-March 1984 and of the Payload Specialist Team from March-September 1984 for SKYNET 5, but was removed from the team in the wake of the Cyprus spy trial. He was GSO1 (W) LSORS from October 1984-November 1985 and Colonel (W) MGO Secretariat from December 1985-December 1986. He became Commander, The School of Signals from January 1987-December 1988 and Director Military CIS Projects (DMCP) from January 1989-November 1992. On promotion to Major General, he was appointed DGCIS(A)/SO-in-C(A) from November 1992-December 1995 and retired from the Army on 17 January 1996.

lnitially barred by MOD procedures and company objections to taking paid employment, following procurement related appointments, he eventually became Bid Director for Racal Telecom and won the bid to renew telecommunications for London Underground, following which he continued in a consultancy capacity for a number of years. He followed Major General Alan Yeoman as Chairman of the RSA for five years during which he initiated a fundamental study of RSA structure and procedures, and implemented changes accordingly. He joined the West Wales Branch of the RSA and became its Treasurer in 2010. He was the Armed Services representative on the lnstitution of Electrical Engineering Membership Committee for three years, and conducted many membership interviews before the commercial approach to the lnstitution and the change to the IET persuaded him into resignation.

Having married Ann in 1964 and had three children together, in retirement he settled in Wales, and was a member of Builth Wells Golf Club for 14 years. He joined Summerhill Golf Club, Hay-on-Wye and played very happily with a strong senior section for many years and achieved a minimum handicap of 14. As a volunteer, he drove the minibus for Hay-on-Wye Dial-a-Ride once per week for some three years until his final illness was diagnosed. His two Border Collie twin sisters who arrived from Dan-y-Capel Farm in October 2004 provided plenty of exercise and joy in his last years. Possessed of a shrewd intelligence and a well developed sense of humour, he was a popular figure, and his death on 25 October 2011, was met with great sadness by all who had known him during his long and dedicated service to the Corps.

MAJOR GENERAL EJ HELLIER CBE

Major General Eric Jim (Jimmie) Hellier was born at Wedmore, Somerset on 23 July 1927. After education at Hugh Saxons School and Cardiff University, he entered the Royal Navy as a Cadet in April 1945. In May 1946, he was commissioned as a Midshipman and until June 1948 served continuously at sea in both home and overseas stations as a Navigating Officer in destroyers and minesweepers. In June 1948 he was commissioned into Royal Signals and immediately posted to the Canal Zone of Egypt where he served as a Line Troop and Detachment Commander at Fayid and later at Suez with Egypt Command Signal Regiment. He left in July 1951 to attend No. 1 Subalterns Part II Course, after which he was posted to command the Training Aids Development and Method of Instruction Troop at the School of Signals. He served there from 1952 – 1954, when he joined 18 Army Group Signal Regiment in Herford later Essen in Germany. He served with this Regiment as a Troop Commander, Squadron 21C and Adjutant until 1958. From June 1958 until December 1959 he saw service in the Far East as a Staff Officer with Commander Royal Signals, Hong Kong.

In 1960, as a Captain, he attended the Staff College at Camberley, from where he was appointed as GS02 at the War Office, dealing with All Arms Tactical Communications Systems. During this time, he was responsible for the Larkspur radio project and for establishing the Tactical Communications Committee. After two years in the War Office, he joined 1st Divisional Signal Regiment, in which he commanded 7th Armoured Brigade Signal Squadron until January 1966. During his tenure of Squadron command, the Squadron became the first to be integrated, the first to receive the AFV 432 and the first to deploy speech security on its VHF command nets.

In January to July 1966, Major Hellier attended Number 32 Joint Services Staff College Course at Latimer, from which he joined 39 Infantry Brigade as the DAA & QMG in Northern Ireland. It was whilst in this appointment he was selected to command 24 Signal Regiment at Catterick an appointment which he held from September 1967 until May 1970. He then joined the staff of General Sir William Jackson as the GS01 (plans) in Operational Requirements at the Ministry of Defence during which he was responsible for planning the major equipment programme for the Army. Subsequently, he joined the staff of Maj Gen Farrar Hockley as the Colonel AQ of the 4th Armoured Division in Germany, a post which he filled for some two years and during which he started the Ice Breake series of exercises.

In 1973, Brigadier Hellier was appointed as the Commander Training Brigade Royal Signals and Commander Catterick Garrison where, for the next two years, he was heavily concerned with the re organisation of the Brigade, the review of trade structures and dealing with the constant problem of IRA attacks in that area. In 1975 he was selected to attend the Royal College of Defence Studies as a student at the end of which he was appointed as the Brigadier AQ of the 1st British Corps. During his four years in this appointment he was heavily involved in the re structuring of the 1st British Corps, in planning and operating major FTXs and with the Army's contribution to Her Majesty's Silver Jubilee celebrations. In 1979, he joined the staff of Headquarters United Kingdom Land Forces as a Major General where, apart from his full time responsibilities in the United Kingdom, he was also responsible for overseas detachments at Belize, Turkey and in Rome. He was appointed as Colonel Commandant Royal Signals on 1 February 1981.

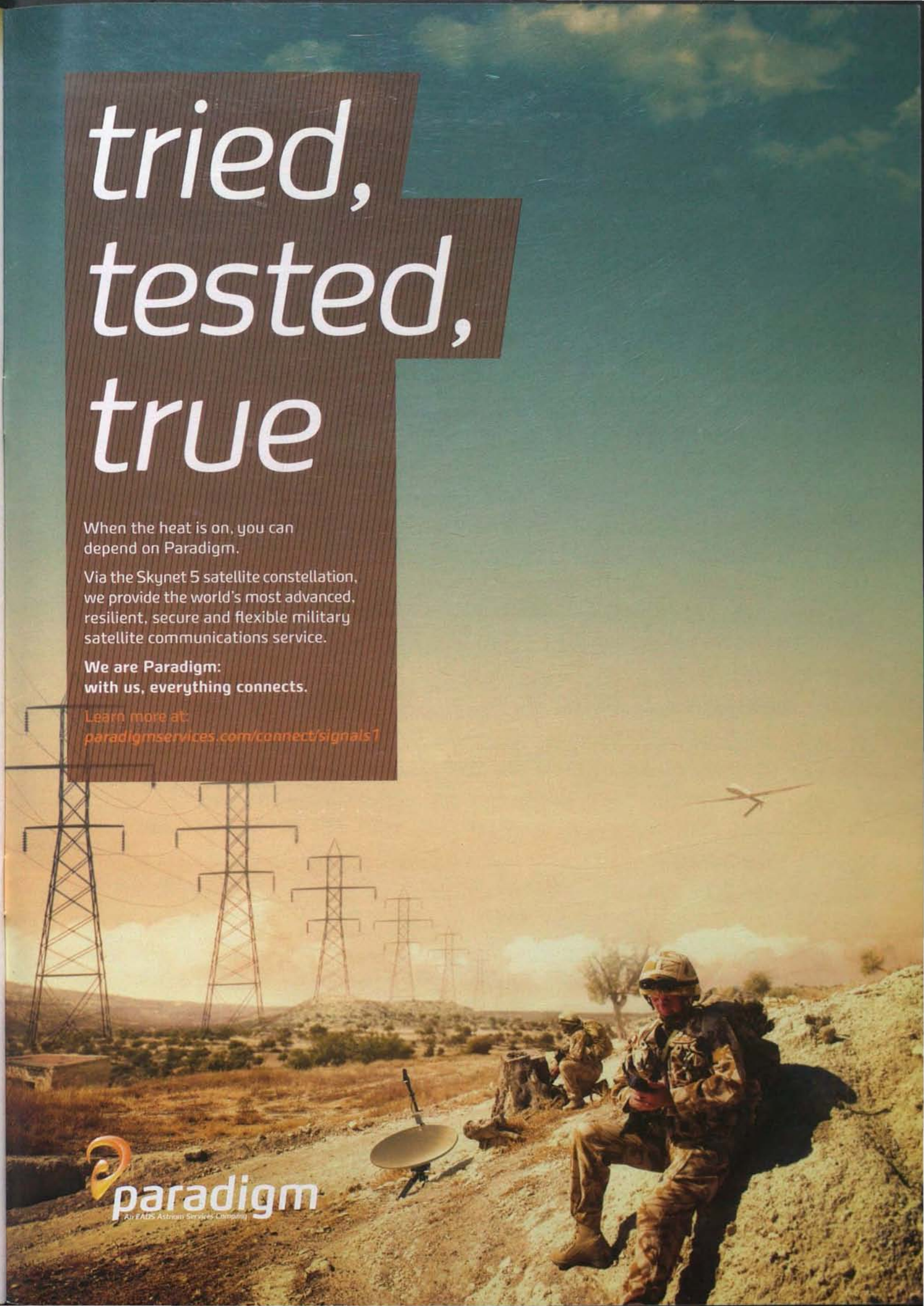
Major General Hellier was awarded the MBE in 1967, the OBE in 1970 and the CBE in 1977. Throughout his career, he was an active participant in Army sport. He won the Army Three Mile Championship in 1951 and represented both the Corps and his Regiment at hockey and squash, a game which he still enjoyed playing in the Veteran Leagues. He also continued to sail and ski. He married Margaret Leadeham in 1952 at Blandford, Dorset and they had two children Paul and Elizabeth. He retired from the Army in 1982 and took up an appointment with International Military Services, the commercial arm of the Ministry of Defence for which he spent much time in Jordan and Oman. His home was at West Hatch, near Taunton, Somerset. He died on 31 October much mourned by his many friends in the Corps.

COLONEL GJC MOSS MBE

Gordon John Collison Moss was born on 20 March 1921, and joined the Army on 1 September 1939. He was commissioned into the Royal Corps of Signals on 25 May 1940. Little detail of his wartime service is recorded, but he did serve for a time with 33 Corps Signals. In 1945 he was awarded the MBE for his wartime service, and had attained the rank of temporary Major, which he held until 1948 when he was sent to RMCS Shrivenham.

In 1951 he was posted to HQ BAOR Signal Regiment, and regained the rank of Major before going on to the Army Staff College, Camberley in 1953. On completion, he was posted to the War Office Signals 5 in 1955, moving to the Supply Branch in 1958. He continued to serve at the War Office until 1961, when he was posted to FARELF on promotion in November of that year. Three years later, he was once more back on the staff in the renamed Ministry of Defence until 1966, when he took up post as a Staff Officer at the School of Signals.

In 1969, he was promoted and took up his final posting as a Colonel GS back in the Ministry of Defence, from where he retired in October 1970. In retirement, he settled in Purley, and maintained a keen interest in all Corps affairs. He died on 15 February this year.

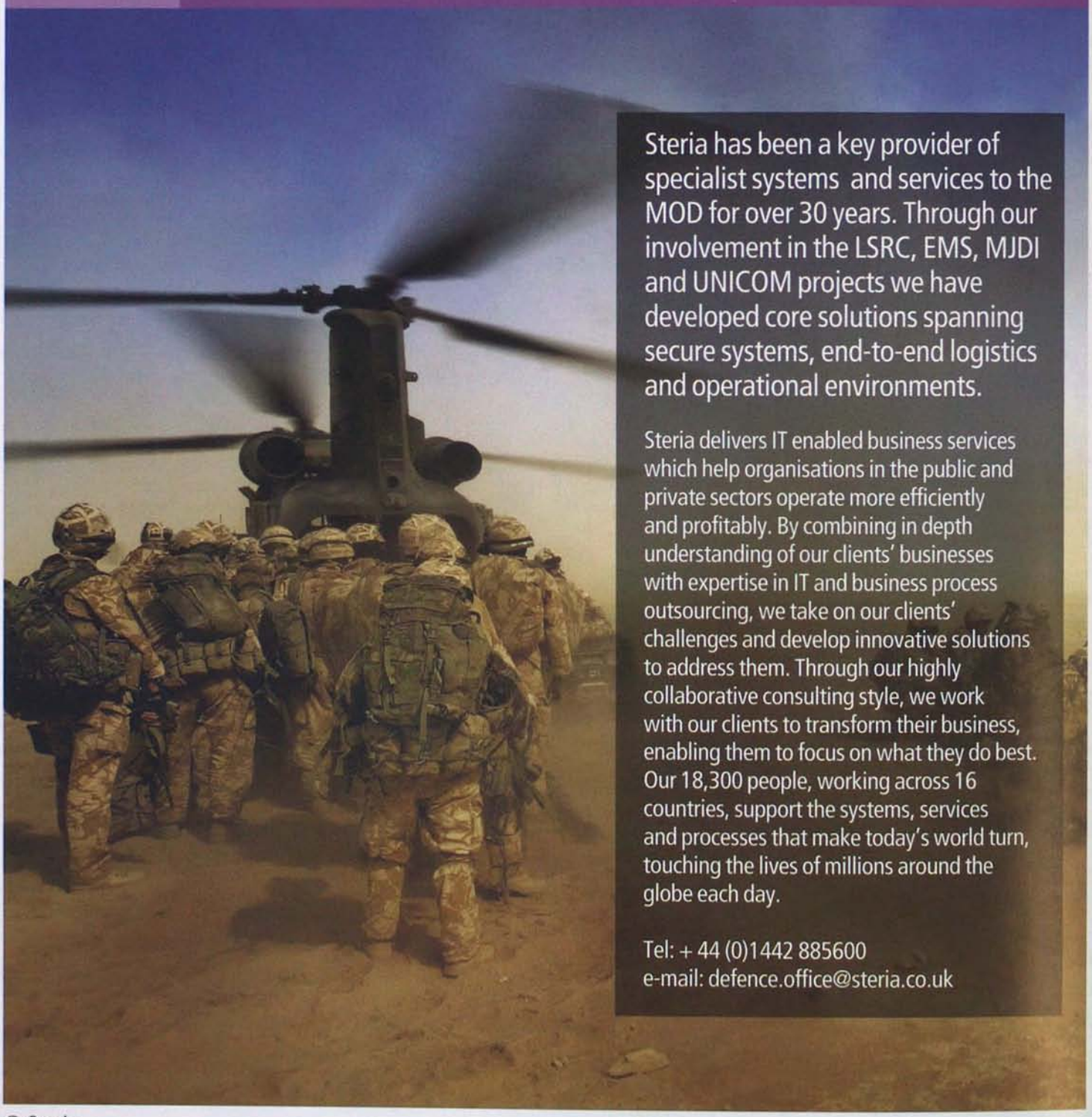

tried,
tested,
true
When the heat is on, you can depend on Paradigm.
Via the Skynet 5 satellite constellation, we provide the world's most advanced, resilient, secure and flexible military satellite communications service.
We are Paradigm:
with us, everything connects.
Learn more at:
paradigmservices.com/connect/signals1
paradigm
An EADS Astrium Services Company

steria

www.steria.co.uk

Committed to Defence

Through our involvement in projects across Europe, Steria has developed core solutions spanning Defence and Homeland Security.



Steria has been a key provider of specialist systems and services to the MOD for over 30 years. Through our involvement in the LSRC, EMS, MJDI and UNICOM projects we have developed core solutions spanning secure systems, end-to-end logistics and operational environments.

Steria delivers IT enabled business services which help organisations in the public and private sectors operate more efficiently and profitably. By combining in depth understanding of our clients' businesses with expertise in IT and business process outsourcing, we take on our clients' challenges and develop innovative solutions to address them. Through our highly collaborative consulting style, we work with our clients to transform their business, enabling them to focus on what they do best. Our 18,300 people, working across 16 countries, support the systems, services and processes that make today's world turn, touching the lives of millions around the globe each day.

Tel: + 44 (0)1442 885600
e-mail: defence.office@steria.co.uk