Whitehall wiring: The Communications-Electronics Security Group and the struggle for secure speech

Richard J Aldrich

Public Policy and Administration 2013 28: 178 originally published online 20 November 2012

DOI: 10.1177/0952076712458111

Article

Public Policy and Administration
28(2) 178–195

DOI: 10.1177/0952076712458111
ppa.sagepub.com
SAGE

Whitehall wiring: The Communications-Electronics Security Group and the struggle for secure speech

Richard J Aldrich
University of Warwick, UK

Abstract
Britain's Government Communications Headquarters (GCHQ) enjoys two main roles, signals intelligence and communications security. We know a great deal about signals intelligence but far less about the defensive security side of its activities. This article traces the development and growth of Britain's communications security establishment as an unknown fourth British secret service during the 1950s and 1960s. This body was the antecedent of the Communications-Electronics Security Group (CESG), the UK's current National Technical Authority. This article focuses on one of the key communications security challenges faced by Whitehall over the last half century, the struggle to achieve secure speech. The lessons to be drawn are that ambitious "big bang" technical projects with requirements specified years ahead are a recipe for failure. Incremental enhancements that draw on commercial solutions are more sustainable and permit adaptation.

Keywords
administrative organisation and structures, budgeting, central administration, civil service, GCHQ, ICT, planning, policy making, public administration, secrecy

Corresponding author:
Richard J Aldrich, Institute of Advanced Study, Milburn House, University of Warwick Science Park, Coventry CV4 7AL, UK.
Email: r.j.aldrich@warwick.ac.uk

> This is a very advanced equipment, as few people as possible should know what it does, or even of its existence.
>
> Major General Thuillier, Cabinet Office, 14 January 1960 (Cabinet Office, 1960a)

In May 1960, the Prime Minister of Ghana, Kwame Nkrumah, came to London to discuss final arrangements for independence. While visiting Harold Macmillan at 10 Downing Street, Nkrumah spotted something unusual sitting on the Prime Minister's desk. Alongside the normal black telephone and the green scrambler phone – items that were both familiar furniture in Whitehall – was an ostentatious red telephone. Nkrumah correctly concluded that the British had developed something rather better than the routine scrambler phone. What Nkrumah had spotted was a pro-type model of "Pickwick", a system which delivered highly secure enciphered speech. There was no question of making this new equipment available to the Commonwealth and officials encountered some difficulty deflecting his probing questions. Pickwick had been ten years in the making and a Pickwick terminal was about to be installed in the White House, permitting secure transatlantic conversations between premiers. The following month, Philip Zuleta, Macmillan's private secretary, reported that other visitors had noticed the red phone and feared that it was becoming an unwelcome conversation piece. Eventually, the Pickwick handset was moved to a more discreet position in the Prime Minister's study (Cabinet Office, 1960d).

Britain has long enjoyed a historical reputation for success with secrets and ciphers, symbolised by Bletchley Park. At this celebrated wartime location, a cluster of wooden huts in the Buckinghamshire countryside, intelligence was derived from the interception and deciphering of enemy communications. The triumphs of Britain's code-breakers over the German Enigma machine have become the stuff of legend. Few narratives are more heartwarming than bumbling professors dressed in their hand-knitted woollies helping to thwart Hitler's legions (McKay, 2010). Yet while we have widely celebrated the activity known as signals intelligence, we have neglected its obverse, the practice of communications security. This is a defensive activity that consists of code-making and communications protection rather than code-breaking. John Ferris and Rebecca Ratcliff have written eloquently on British communications security in the period up to 1945, but beyond this date the subject is curiously neglected (Ferris, 1987; Ratcliff, 2006). The reasons for this are not clear but it may reflect the fact that the available records for this subject are highly disaggregated.

Modern British communications security evolved in response to two security panics. First, the invasion of Europe in 1944 revealed the alarming extent of Axis success in penetrating Allied operational ciphers and prompted Churchill to revamp the structure of Britain's communications security, which had been remarkably weak during the Second World War. Second, during the early 1950s, the discovery – or more correctly the rediscovery – of a phenomenon called "Tempest", the tendency of cipher machines and ancillary equipment to radiate out a plain-text version of their activities at a distances up to two hundred yards, prompted Britain to create a new body tasked solely with communications security. Initially called the London Communications Security

Agency (LCSA), this obscure body eventually became what is now the defensive component of Government Communications Headquarters (GCHQ), known as the Communications-Electronics Security Group (CESG). This organisation existed as a separate entity for almost two decades, and despite constituting a fourth British secret service it remains relatively unknown (Aldrich, 2010: 191–217).

The central task of the LCSA was to protect Britain's codes, ciphers and communications. The history of Britain's codes and ciphers is a complex story and cannot be examined here. However, a parallel communications challenge for LCSA was the generation of secure speech for use with official telephones. Academics have frequently remarked on the rise of international summitry – the tendency of premiers to short-circuit their ambassadors and to conduct business face to face (Berridge, 2002; Dunn, 1996; Reynolds, 2009). This was accompanied by a wish for direct conversations by telephone. Indeed, the growing desire of premiers to speak to each other directly is a central component of the history of international diplomacy. From the mid-twentieth century, technology allowed the leaders of Allied nations – beginning with Roosevelt and Churchill – to converse with increasing freedom and security. When this facility was not available they were inclined to express their discontent volubly.

Beyond 1945, the threat of nuclear Armageddon created an additional need for secure speech. This included "hotlines" to the enemy, together with a desire for direct voice control over strategic weaponry in crisis situations as timelines for national decision making shrunk alarmingly. In the worst case, premiers needed real-time voice communications with key officials to prepare for the unthinkable – the launch of nuclear weapons. By the 1960s, the secure speech network for Whitehall and Westminster represented nothing less than a map of the secret state, connecting Downing Street, the Cabinet Office, intelligence agencies that were involved in war warning and the machinery of deterrence. Peter Hennessy has noted the arcane challenge presented by the need to extend secret speech for crisis consultation to Harold Wilson's holiday bungalow in the Scilly Isles (Hennessy, 2011).

Secure speech was a huge technical and administrative challenge, representing orders of difficulty much greater than protecting documents or telegrams. Systems had been designed to provide precise levels of classification for secret documents and telegrams, together with ways of tracking their movement. However, a telephone conversation was ephemeral. Telegrams were easy to encrypt, but telephone signals were more challenging because of the need to encipher and decipher voice in real time, together with the need for considerable bandwidth to transmit the data backwards and forwards. The option of secure speech over ordinary telephone lines only became possible in the late 1970s and even then the costs were high because of the need for vocoders to turn speech into a stream of digits and the associated encryption equipment. Technology finally conquered these problems in the 1980s.

This article explores the valiant efforts of a rather obscure group of British officials, scientists and technicians to extend secure speech across Whitehall and beyond. A red phone on the desk became a status symbol amongst ministers and senior civil servants. However, in common with so many secret government-led

technical projects, including multi-level secure databases for intelligence, government research moved slower than parallel efforts in the private sector. The height of the struggle for secure speech was the vast and baroque Government Secure Speech Network initiated in 1965 and which – with some 5000 planned terminals – eventually collapsed under its own weight. Commercial solutions overtook government programmes. The eventual result was the ''Brent Phone'', the ubiquitous furniture of the British security state of the last two decades.

Britain's communications security organisations

In the autumn of 1943, British authorities suffered a shock. The Italians had now capitulated and captured code-breakers in Rome revealed their successes against British communications. Although the Italians has not attacked Britain's top grade cipher machine, the Typex (not dissimilar to Enigma), they had broken many other systems. Captain Edmund Wilson, who helped to look after cipher security at Bletchley Park, held prolonged ''conversations'' with Commander Cianchi, head of the Italian Cryptographic Bureau in Rome, and his staff. Cianchi enthusiastically set out the triumphs of the Italians, especially against British Admiralty communications. The subsequent Allied invasion of Germany and the rounding up of Nazi code-breakers confirmed that British naval cipher security had been especially weak. B-Dienst, the German naval signals intelligence service, had been reading British naval codes and ciphers easily at the start of the war. In 1942, the Dieppe raid had been given away to the enemy before it took place and poor cipher security had placed the Atlantic convoys in jeopardy (Aldrich, 2010: 55–56).

Churchill was disturbed by these revelations and demanded immediate action. Accordingly, the autumn of 1943 saw a long-overdue inquiry into the security of British ciphers, carried out by Brigadier Chitty, who began by visiting Bletchley Park. His findings did not make for comfortable reading. 'It is true', he reported, 'that of the fourteen sections working at B.P. [Bletchley Park] one is named Security of Allied Communications. From a total staff of some six thousand, however, the part-time services of only one man (Dudley-Smith) plus two or three girls, are spared to equip this section' (Aldrich, 2010: 55). At a higher level there was a supervising body called the Cypher Security Committee, supposedly chaired by Sir Stewart Menzies, who controlled both MI6 and the Government Code and Cypher School. However, this subject had not been given much attention by Menzies; moreover, the committee lacked the power to compel Whitehall departments to give cipher security a high priority.

Churchill insisted on the creation of a new body, the Cypher Security Board, to underline the importance he attached to this subject. Captain Edmund Wilson was promoted to a new post of Deputy Director of the Government Code and Cypher School with the title of Communications Security Adviser. After the war, Wilson was replaced by Commander T.R.W. Burton-Miller, who initially operated from a new headquarters at 10 Chesterfield Street in central London, conveniently close to both MI5 and SIS (Secret Intelligence Service). Soon they had extended their

authority over the design, production and operation of all British cipher machines, most of which were made at Hanslope Park or at a secret Foreign Office factory at Chester Road in Borehamwood (Davies, 2000: 187, 238).

After the Second World War, the Government Code and Cypher School changed its name to the Government Communications Headquarters or GCHQ. In April 1946 its military component vacated Bletchley Park and moved to Eastcote near Uxbridge. Here they occupied a range of unattractive single story huts that had hitherto accommodated wartime auxiliary units supporting the attack on Enigma. In the early 1950s GCHQ moved again, this time to Cheltenham, but at this point the communications security element was separated from GCHQ and remained behind in London.[1] Fearsome rows had developed between GCHQ and the armed services, who complained about delays in the production of cipher equipment and scrambler phones, as well as their poor quality. T.R.W. Burton-Miller, who was in charge of communications security, had done his best to achieve good relations with the military. However, in 1953 many felt it was better to make a fresh start by creating a completely new service, the London Communications Security Agency (LCSA). This decision to separate communications security and signals intelligence was controversial, but it was backed by the new GCHQ Director, Eric Jones, and one of his key subordinates, Joe Hooper (Penney, 1957b).

The creation of LCSA was also underpinned by new resources. The UK security authorities were in a panic as a result of the discovery of a phenomenon called "Tempest". This was the tendency of electromechanical devices such as cipher machines and teleprinters to radiate out a clear signal of their activities, something that could be exacerbated by the proximity of conductors such as copper piping and central heating pipes. Tempest conjured up a range of technical nightmares and required serious investment in both better equipment and also improved physical security in buildings. Government reconciled itself to spending more money in this domain, since Tempest had rendered many of Britain's existing cipher machines – including the much admired Rockex II – potentially vulnerable. Britain's response to this challenge was the creation of LCSA to thwart listening attacks by the enemy. LCSA was, in effect, a fourth secret service – the technical security equivalent of MI5.

LCSA's first chief was Major General William Penney, who had been Mountbatten's Director of Intelligence in South-East Asia. The move by GCHQ to Cheltenham in the early 1950s permitted increased space for Britain's expanded communications security effort, which remained at Eastcote. The location was ideal because they co-operated closely with the Research and Development branch of the Post Office, located at nearby Dollis Hill. Post Office engineers played an important role in both intelligence and security. They had helped to build the Colossus computer that had attacked the most secure German communications during the war (Copeland, 2006). They had also been involved in the combined MI6/CIA operation to tap into Soviet Bloc telephone cables by tunnelling under East Berlin in the 1950s (Stafford, 2003). While LCSA's technical staff for communications security remained at Eastcote and nearby Northwood Hills, Penney and his senior officers

enjoyed additional executive premises at 8 Palmer Street, which doubled as GCHQ's London office. Palmer Street was adjacent to one of the oldest underground stations in London, St James's Park, and close to many of the embassies. GCHQ's L Division also worked closely with LCSA and helped to produce cipher material for user departments (Aldrich, 2010: 134).

The protection of Britain's ciphers for written communication enjoyed a long history stretching back over centuries. This had now been joined by a new field, initiated by the arrival of the telephone, known as secure speech. The use of the telephone for government business had almost immediately created the desire for better security to prevent eavesdropping. Over a period of half a century the main challenge for scientists and technicians was to discover methods of reducing the bandwidth required for transmitting encrypted voice messages over telephone lines. Voice encryption was complex and generated vast amounts of data, usually too great for normal telephone networks to handle. In the spy films of this period, protagonists had seemingly easy access to ''scrambler phones''. However, in reality scrambler phones that used the normal telephone network only offered security against the casual eavesdropper and could easily be defeated. Anything better required vast technological support and considerable resource. In short, the challenge of delivering reliable and affordable secure speech was immense.

By 1945, there were as many as half a dozen different bodies working on scrambler phones and voice coders (known as vocoders). These were brought together in 1953 as the Joint Speech Research Unit (JSRU), which looked after both civil and defence applications. Located alongside the LCSA technical staff at Eastcote, JSRU was mostly staffed by Post Office engineers and scientists from London University. The head of the unit was John Swaffield, who had been involved in the design of vocoders since the 1940s (Smithsonian, 1986). Although JSRU was considered a Post Office unit, John Swaffield appeared in government documents as a GCHQ official (War Office, 1955). These personnel arrangements were awkward, since the Post Office was effectively lending the security agencies numbers of specialist high-grade staff, one of many indirect subsidies to the secret agencies. The Post Office only tolerated this eccentric arrangement for a decade. In August 1963, the Post Office asked to be relieved of the responsibility for both JSRU and the Services Cypher Development Unit (located at Dollis Hill and Eastcote), which it also staffed. On 1 April 1965, LCSA formally absorbed both these bodies. LCSA denoted this aggrandisement by changing its name to the Communications-Electronics Security Department (CESD) (Cabinet Office, 1968).

During the mid-1960s, JSRU numbered over forty and was the focal point for the development of secure speech communication equipment for military and other government applications. Their main challenge continued to be achieving high-quality digitalised speech that could be sent over traditional telephone lines, since this would open the door to the widespread use of encrypted terminals. However, public networks could only accommodate a narrow bandwidth, perhaps less than 2 kilobytes per second. Meanwhile, both JSRU and its parent organisation LCSA struggled to recruit the best-quality scientists within the confines of

government pay scales. Continual changes were implemented to try and address this. In 1967, JSRU was split into two roughly equal parts, separating out the operational and research functions. Operations were increasingly undertaken by military elements, while JSRU then focused more narrowly on research with some twenty staff (Smithsonian, 1986).

Despite these changes, the core problem of maintaining a critical mass of scientific and technical expertise became ever more difficult. The electronics industry was now accelerating on the western side of London, drawing away expertise to jobs in the private sector with attractive salaries (Cabinet Office, 1968). In 1968, during a period of wide-ranging reform and re-organisation for the British intelligence and security community, it was decided to merge CESD with GCHQ in the hope of achieving a more sustainable base for scientific research (Aldrich, 2010; Young, 2001). Between 1969 and 1978 the LCSA communications security (comsec) elements, including JSRU that had abided at Eastcote for some two decades, were gradually moved to Cheltenham and integrated into GCHQ.

Rationalisation and consolidation continued during the 1970s and 1980s. Alongside the work of the intelligence and security agencies, the military had sustained their own secure voice capability focused on tactical and battlefield systems. This had been located at the Signals Research and Development Establishment at Christchurch and was funded by the Ministry of Supply (War Office, 1955). In 1976, this was rationalised and became part of Royal Signals and Radar Establishment (RSRE) at Malvern, which hosted its own speech research group. Thereafter, two speech security units laboured alongside each other at RSRE Malvern and GCHQ Cheltenham, only thirty-one miles apart. Although their tasks were different, there was nevertheless some duplication. This situation continued until 1 November 1985, when the JSRU at Cheltenham was amalgamated with the speech research group at RSRE to form a newly named Speech Research Unit, with all personnel based at Malvern. GCHQ had effectively abandoned the business of secure speech research, although it maintained a strong interest in automatic voice recognition (House of Commons, 1985).

In 1999, the Speech Research Unit at Malvern formed part of the privatisation of the UK defence research capabilities. The Speech Research Unit was transformed into a company called 20/20 Speech Ltd in November 1999, a joint venture between DERA (later QinetiQ) and NXT plc. In March 2005, 20/20 Speech Ltd changed its name to Aurix. Both these companies retained much of their Malvern heritage. Professor Roger K. Moore, initially from the Phonetics Department at University College London, had led the speech recognition research team at the RSRE in Malvern since 1980. From 1985, he led the newly merged Speech Research Unit, incorporating the elements from Cheltenham. After the privatisation of the Speech Research Unit in 1999, Moore continued to provide the technical lead as Chief Scientific Officer at 20/20 Speech Ltd before departing to take up the Chair of Spoken Language Processing at the University of Sheffield in 2005. Aurix was acquired by Avaya in October 2011 and its core business is now speech analytics and audio data mining (Aurix, n.d., and private information).

The JSRU, with its Post Office heritage, is probably one of Britain's most obscure security units. Yet it can claim a distinguished history and has achieved some remarkable "firsts". In the 1960s it produced the first demonstration of human-quality synthetic speech and developed one of the world's first text-to-speech synthesizers. In the 1970s it launched the prize-winning LOGOS continuous automatic speech recognition system. Many of these developments had signals intelligence as well as communications security applications because of the shift by NSA and GCHQ to collecting international telecom data during the 1970s and 1980s. This was typified by the interception of traffic from commercial telecom satellites and later by development of Project Runway, which saw GCHQ analysing a great deal of telecom traffic collected by NSA satellites (Aldrich, 2010; Richelson, 2008).

Pickwick and Twighlight

At the beginning of the Second World War, the only available secure voice system was a device known as the A-3 Scrambler, developed by AT&T in New York. Although impressive at first glance, it drew on 1920s technology and was not, in fact, very secure. Quite simply, it added additional sound at one end and subtracted it at the other. In other words, it did not offer encipherment and instead merely masked the sound of the speakers. Unbeknownst to the Allies, the Germans had already developed the ability to eavesdrop on A-3 using a site on the Dutch coast, and by 1940 had begun to intercept calls between Roosevelt and Churchill that used this system.

Simultaneously, a team at Bell Telephone Laboratories led by A.C. Clark were working on a new generation of secure speech machines and vocoders. Assisted by the brilliant British mathematician Alan Turing, their most carefully guarded enterprise was a high-level speech security system which they nick-named "the Green Hornet". This name arose because eavesdroppers trying to listen in heard only a buzzing sound. The production units were later given the name "Sigsaly" and became available in early 1943. Turing was the only British citizen allowed to inspect the inner workings of Sigsaly and he suggested a number of last minute refinements (Hodges, 1983: 248–249). Sigsaly achieved a number of firsts, including the first transformation of speech into a stream of digital data that could then be enciphered, affording the same high-level protection given to top secret telegrams. This was the forerunner of present day digital voice, data and video transmission. However, the downside was that the equipment looked like the contents of small factory and weighed some fifty tons. General Douglas McArthur used one in the Pacific to hold telephone conferences with senior figures in Washington, but the equipment had to be installed in a small ship. Winston Churchill's Sigsaly unit was too large to be accommodated in Whitehall and had to be hidden in the basement of Selfridges department store in Oxford Street. Some two dozen Sigsaly units were in operation by the end of the war (Weadon, 2000).

However, such vast resource could not be extended to protect the telephone calls of ordinary mortals. During the war, even high-level commanders routinely made use of basic scrambler phones known as the ''Secrephone'' for the discussion of sensitive business (Murphy, 1948: 195, 204). In 1946, some twenty-two Secrephones were available in Headquarters Control Commission Germany (Berlin Element) 'for the use of VIPs'; however, they were known to offer doubtful security against the Russians (Foreign Office, 1946). The main antidote was to continually exhort those in possession of secrets not to discuss them on the phone, but under pressure of urgent business this instruction was frequently ignored (Foreign Office, 1946). Similar equipment, known as ''the green phone'', was widely available to Whitehall officials in the 1950s.

In 1957, LCSA's Director William Penney retired due to ill health and was replaced by Fred Stannard (Penney, 1957a). By this time, LCSA had developed plans for a new high-level encrypted telephone system codenamed ''Pickwick'' that delivered effective speech security. Although this did not require the factory-sized facilities demanded by SIGSALY, the support mechanisms were still elaborate and phone calls required teams of people to operate the equipment. While LCSA were adamant that green scrambler phones provided 'no security whatsoever' they also recognised that the new Pickwick system was so expensive that it could only be rolled out to high-level users, providing only a partial solution to what they called 'the green phone problem' (Treasury, 1960a, 1960b).

An important driver for LCSA's new Pickwick system was the desire for secure voice communications between 10 Downing Street and the White House. The transatlantic version of Pickwick – called Project Twighlight – was proposed by LCSA in late 1958 and agreed at a meeting at the headquarters of the National Security Agency (NSA) in February 1959 (Cabinet Office, 1960f). Stannard worked closely with his friend Dick Chiles, Head of the Office of Comsec Doctrine at NSA, to ensure the installation of the Twighlight project, overcoming obstinacy on the part of American telephone companies and indecision on the part of the White House.[2] Predictably, LCSA was also keen to pass off some of the costs of Twighlight to the Americans (Cabinet Office, 1960e). Seven type-B models were in existence by October 1960, one at 10 Downing Street, one at Chequers and one at Birch Grove (Macmillan's private residence). Two more were located at GCHQ, one at the Foreign Office and one at the Ministry of Defence. The control unit for this embryonic Pickwick network, known as the Copperfield exchange, was located in King Charles Street in Westminster. Two further type-B models were created for the Twighlight link to the United States. Production models were due to arrive for the rest of the network in 1962 (Cabinet Office, 1960c). Pickwick was gradually rolled out across Whitehall to some 250 users during the early 1960s (Cabinet Office, 1960b).

The Cuban Missile Crisis of October 1962 focused the minds of ministers on transatlantic conversations. Rab Butler, Macmillan's Foreign Secretary, asked his officials how he would talk to his opposite number in Washington, Dean Rusk, in an emergency. The answer was the newly installed Pickwick system in its

transatlantic mode. This performed well but took more than two hours to set up, making it 'virtually useless' in a crisis (Foreign Office, 1963a). If time was short, Butler would have had to go to No.10 Downing Street and use the American KY-9 phone that only took half an hour to set up. But officials confessed that the quality of speech was poor – little better than a 'talking teleprinter' (Foreign Office, 1963b). Americans referred to it as the Donald Duck system. John F. Kennedy had recently refused to use it when a Pickwick call to Macmillan broke down (Foreign Office, 1963a, 1963b; Johnson, 1995: 380). Because the Pickwick was an elaborate broadband secure speech system, it also needed a number of transatlantic cables to be booked in advance, since it required some 15 kilobytes per second of bandwidth. The two-hour preparation time was deemed 'unacceptable' to both 10 Downing Street and the White House (Foreign and Commonwealth Office, 1967e). During 1964, efforts focused on providing better protection against eavesdropping through Tempest attack. All of this equipment in Downing Street and the Cabinet Offices was inspected, with Admiralty House being regarded as especially vulnerable. New low-power teleprinters were installed and a team of engineers from LCSA carried out 'radiation test measurements' using eavesdropping equipment in a dedicated Commer truck (Cabinet Office, 1963).

In the mid-1960s, Stannard did his best to converge British efforts with America's NSA to try to save on costs. In June 1964 Stannard had sent his deputy, Brigadier Jes Gardiner, across to NSA at Meade to try to achieve a common approach to a whole range of systems including VHF combat radio equipment (War Office, 1964). However, no-one expected any operational hardware to be generated by this collaboration in the short term (Ministry of Defence, 1968). Instead, efforts to improve on Pickwick were home grown. In late 1965, John Swaffield of JSRU succeeded in producing a highly efficient vocoder codenamed ''Belgard'', which allowed the production of digitised speech at much lower levels of bandwidth but without serious speech distortion. This breakthrough offered the possibility of cheaper and more widely available units, though they would still require their own dedicated cable network (Holmes, 1980: 53–55). Accordingly, in December 1965 the Defence Signal Board created a working party to forecast UK secure speech requirements for the 1970s. Although the Defence Signal Board operated under the authority of the Chiefs of Staff it also enjoyed representation from the Cabinet Office, the Foreign Office and GCHQ. This recommended a network of no less than 2,000 terminals and predicted a cost of £2.6 million, working in co-operation with Standard Telephone Laboratories as the main supplier. Standard Telephone Laboratories worked closely with government and was taken over by GPO in 1970. The Cabinet's Communications-Electronics and Space Committee were delighted by Belgard and approved the project (Treasury, 1971).

The top priority was to replace the cumbersome transatlantic variant of Pickwick known as Twighlight. The new Belgard system was first used in an experimental form between the Foreign Office and the British delegation at the United Nations in New York in 1967.[3] The success of the pilot link to New York was a major feather in Stannard's cap as head of what was now called the

Communications-Electronic Security Department (CESD). 'All concerned, both here and in New York, are delighted with this new facility' the diplomats exclaimed. 'It is in use almost every day and I am happy to say that in both quality and reliability the system has so far more than lived up to our expectations' (Foreign and Commonwealth Office, 1967b). The Belgard models in use between the Foreign Office and its United Nations delegation in New York were only 'CESD laboratory models' (Commonwealth Office, 1967d). However, production models of the new system were soon installed in Washington with the help of the White House Communications Agency, while KY-9 was retained as a back-up system (Foreign and Commonwealth Office, 1967c). The British Embassy in Washington confessed 'we shall not be sorry to lose ''Twighlight'' which is so expensive and complicated to set up that we have never made any use of it' (Foreign and Commonwealth Office, 1967f). The same system was installed for the 'special link to Evere' that served a new GCHQ cell that had been established to supply intelligence to NATO's headquarters outside Brussels (Foreign and Commonwealth Office, 1967d). The other top priorities for the installation of Belgard were the ''Scillies circuit'', providing secure voice for Harold Wilson's holiday home, and similar secure facilities to allow the Prime Minister to stay in touch with Whitehall during the Labour Party Conference (Foreign and Commonwealth Office, 1967a).

The Government Secure Speech Network (GSSN)

The development of Belgard prompted an ambitious programme to deliver secure speech across Whitehall, together with key locations overseas, called the Government Secure Speech Network (GSSN) (Holmes, 1980). GSSN aimed to provide secure speech for 2000 government subscribers. However, although the breakthrough Belgard terminals were relatively cheap, the continued need for special dedicated telephone lines pushed costs up and so by 1967 the estimates had already risen from £2 million to £15 million. These escalating costs were initially accepted because of increased fears of hostile telephone tapping. Officials now believed that that 'foreign intelligence services would seize any reasonable chance to carry out intercept operations if these promised to produce worthwhile intelligence' (Treasury, 1971). This problem had become greater because telephone calls increasingly passed over long-distance radio relay circuits. GCHQ warned that 'radio links radiating from London (and, to a lesser extent, from Northern Ireland) are targets for sustained interception operations' (Treasury, 1971). Calls that were dialled to identifiable numbers of intelligence agencies or that used scramblers were the particular subjects of attack (Treasury, 1971).

By May 1972, GSSN requirements had mushroomed to over 5000 terminals. The plans for this secure speech network now constituted a veritable map of the secret state. Predictably perhaps, GCHQ at Cheltenham had a requirement for 858 terminals, more than any other single location. Of the 353 terminals in the London area, GCHQ was allocated 87 at its Empress State Building facility in

Earls Court, 52 at Palmer Street and another 8 for its Russian translators known as the London Processing Group at St Dunstan's near Tower Bridge. MI6 was scheduled for 91 terminals at Century House and a further 29 at Windsor House in Victoria Street in SW1. MI5 warranted a paltry 72 terminals across two sites at Leconfield House and Marlborough Street (Ministry of Defence, 1972).

However, by 1974 delays and cost overruns meant that, almost a decade after its inception, GSSN had not been fully installed. The problems were brutally exposed by the Cyprus crisis of July 1974. Because GSSN had still not been widely deployed many were still using the elderly Pickwick system, which had been overwhelmed by the speed of the crisis and the volume of traffic. The Defence Intelligence Staff had encountered real trouble speaking to NATO, SHAPE, Strike Command and UK Land Forces. Louis Le Bailly, the Director General of Intelligence at the Ministry of Defence, complained that he could not speak directly with GCHQ (Ministry of Defence, 1974). On Saturday 20 July, the first day of the invasion, Roy Mason, the Secretary for Defence, had been unable to access 'his intelligence telephone' because the private secretary who had the master key 'does not like coming to work on Saturdays' (Donoughue, 2005: 167). The Whitehall communications situation was a shambles.

Moreover, by 1974, telephone technology had moved on. When GSSN was first envisaged, neither the UK public telephone system nor any of the existing switched private wire networks were sufficiently advanced to support narrow band secure speech. However, the UK public telephone network had improved rapidly while the GSSN project proceeded slowly (Cabinet Office, 1974a). Like so many government technology projects, GSSN was now vast, expensive and horribly behind schedule. Meanwhile the standard Post Office network had been rapidly upgraded to the point where it could support secure speech. Moreover, the new British Skynet satellite communication system began to extend secure communications to the military, since it offered vast bandwidth and freed them from the constraints of terrestrial landline networks wherever a Skynet terminal existed (Skilton, 1988).

In July 1974, the GSSN project was reviewed against the background of savage cuts in government spending. Officials noted that even in late 1973, with the project half-completed, there were forecasts of up to £24 million to finish the programme with a timescale of about seven years. In a tough economic climate there was little support for Phase II of GSSN. Procurement lessons were there to be learned and it was concluded that GSSN had embodied a monolithic 'once and for all project' that required users to specify fixed levels of participation years in advance of the installation date. The 'extreme inflexibility' of this approach combined with high costs meant that most sponsors were now backing away. In February 1975, GSSN was formally terminated 'on grounds of high cost and long time scale'. It was now necessary to seek 'some other method of fulfilling the requirement' (Cabinet Office, 1975b). GCHQ and CESG were asked to work with the Post Office to find a new solution (Cabinet Office, 1974b). In the short term, the death of GSSN created a severe gap in secure communications, since some 250 users were still on the elderly Pickwick system (Treasury, 1975a, 1975b).

Government now turned to a cheaper and more flexible system called the Secure Telephone Scheme (STS) (Cabinet Office, 1974c). The objective was to generate encrypted speech that could now be sent over a standard GPO telephone network with a modem, offering huge savings and greater flexibility. The plan was to introduce STS gradually, making use of improvements in technology, since a dedicated network was no longer required. CESG, the comsec component of GCHQ, was named as the technical agent for the scheme, with operations delivered by the Post Office. CESG focused on an improved duplex vocoder codenamed ''Burganet'' that was compatible with Skynet and with public telephone systems, and that typically offered 2.4 kilobytes per second and the possibility of remote key distribution by GCHQ. STS used the Burganet vocoder in combination with the Franton crypto equipment, although Franton would eventually be replaced by a more modern system codenamed ''Hora'' (Cabinet Office, 1974d).

Joe Hooper, a former Director of GCHQ, was responsible for this sensible decision. By 1975, Hooper chaired the Official Committee on Government Communications and had also replaced Dick White as Cabinet Office Intelligence Co-coordinator. He enjoyed a strong team of advisers on the committee, including Teddy Poulden, a veteran GCHQ technology officer. Teddy Poulden was a long-serving GCHQ official with a naval background who had advised the Heath government on problematic subsidies to the newly created UK computer combine International Computers Limited (ICL).[4] After Poulden's retirement in the spring of 1975, Ken Perrin took over as technical adviser with assistance from John Swaffield, GCHQ's long-serving speech security expert. Hooper expected that by 1979 STS would use purely electronic equipment, eliminating old fashioned tapes for the cryptological keys in each handset and perhaps even allowing direct electronic key distribution from GCHQ (Cabinet Office, 1975a). In January 1978 Brian Tovey, Director of CESG, reported that STS was ready for manufacture. Interestingly the majority of the work was still being carried out at CESG Eastcote, ten years after the merger with GCHQ (Cabinet Office, 1978a). GCHQ were allocated 100 of the 370 units planned for the first phase, suggesting that real-time telephone discussion of signals intelligence was a high priority (Cabinet Office, 1978b).

In the 1970s, terrorism increased the need for secure communications. Pressure was coming from the Home Office who wanted a secure means for MI5 to talk to the Special Branch units in the regions. MI5 was also 'pushing' for a wider network on the grounds that too much sensitive business was currently conducted on open lines (Treasury, 1975b). GCHQ was concerned that the IRA might use intercept receivers to eavesdrop on army and police patrols and this resulted in a crash programme to develop a cheap low-grade speech security device for use with car radios and walkie-talkies (Benjamin, 1996: 156). Terrorist incidents had also revealed the problem of eavesdropping by journalists (Treasury, 1973). This was dramatically illustrated during a hi-jacking crisis at Heathrow in early January 1975. The hi-jacking itself was not especially serious, being carried out by an amateur who was 'possibly deranged' (Home Office, 1975b). What really disturbed the

Home Office was the fact that ITN reporters managed to intercept the radio communications carrying the conversations between the control tower and the pilot. ITN then broadcast them to dramatic effect on News at Ten (Home Office, 1975b). The Home Office noted that 'the BBC too had transgressed'. This tactic has encouraged others and now 'various police radio channels were busily being monitored by all the [news] agencies' (Home Office, 1975a). The authorities worried that in a future hostage crisis, all the terrorists would have to do was tune into news broadcasts 'to hear of our detailed plans to deal with them' (Home Office, 1975b).

By 1981, STS had blossomed into a family of secure phones called ''Melody'', all of which used the same cryptosystem and were capable of using the public phone network. ''Brahms'' was a light-weight version of STS for 'contingency operations' carried in an attaché case (Cabinet Office, 1981). Because of its reduced capability it was ''push to talk'' only, akin to a walkie-talkie. STS was the full version for permanent installation in an office and where there was a concentration of units these were accompanied by a rack-installed Shared Equipment Package that looked like a bank of modern computer servers. In 1981, STS was still ''push to talk'' only, but a two-way (duplex) version was imminent. ''Carotene'' was an improved version of the Shared Equipment Package, with a higher number of cryptovariables offering increased security. At £20,000 each, STS units were still a significant investment for government departments (Cabinet Office, 1981). The Americans were moving down a similar path that allowed an incremental approach that adapted continuously to the new technology and that saw the introduction of their STU-III unit in 1983 (Johnson, 1998: 149–150). By the 1990s, STS had evolved into the Brent Phone, which the British Foreign Secretary praised as 'highly effective' and 'the cheapest totally secure telephone system ever produced' (House of Commons, 1998).

Over this period, the main focus of Britain's comsec organisation gradually moved from its multiple London sites down to Cheltenham. Renamed the Communications-Electronics Security Group, they were now a more integrated part of GCHQ. This move had gone some way to resolving their problems with the recruitment of scientists that had plagued them for decades. Yet the research and development capability of both GCHQ and CESG in the realm of telecommunications research remained remarkably small given the scale of challenges it confronted. Its Research and Development Division possessed only 142 staff, yet CESG was tasked to take the lead on cryptographic equipment, ''Tempest'' research and secure speech. This empire was presided over by the GCHQ Chief Scientist Ralph Benjamin and in 1975/6 it was spending about £2 million a year. However, GCHQ was always conscious of its defence rival just up the road from Cheltenham. This was the Royal Signals and Radar Establishment at Malvern which, together with the Services Electronics Research Laboratory at Baldock, boasted four times the staff and ten times the budget. It was almost inevitable that Cheltenham's speech research centre – the JSRU – would be assimilated in Malvern in 1985 (Cabinet Office, 1975c).

Surprisingly, the real giant in communications security remained the Post Office Research Department. They traced their lineage back to the figures who had built the Colosssus computer in the 1940s and their research capacity remained enormous. With no less than 3197 staff and a budget of over £27 million, the Post Office Research Department was in the process of moving from Dollis Hill in North London to a vast space-age site that had been purpose built at Martlesham Heath in Suffolk. This unit had more telecommunications research and development capacity than all government departments combined. Officials lamented that it was only the Post Office that had the budget and indeed the ambition to do 'longer-term and more speculative work' (Cabinet Office, 1975c). Precisely because they were undertaking exploratory research, they attracted some of the best scientists. It was for this reason that Martlesham would be behind revolutionary new developments in telecommunications (Cabinet Office, 1975c). This included the use of fibre-optic cables, developed at Martlesham in the late 1970s. The arrival of low cost fibre-optic cables – which were notoriously hard to tap – presented a major headache for NSA and GCHQ in the 1980s (Newns et al., 1977).

Acknowledgements

I am indebted to a number of speech security specialists for comments on this article. The research for this article was supported by the award of a British Academy Large Grant.

Notes

1. GCHQ/CESD clearly had additional premises just the north of Eastcote at Northwood Hills as late as 1975. This consisted of no less than 35,000 square feet of space within a general government office facility constructed on the ''spur'' principle akin to Stanmore, located at Chamberlain Way and Tolcarne Drive, close to the Northwood Hills underground station. The site is now a housing development. Some staff were transferred from Northwood Hills to the Empress State Building at Earls Court in 1961 (Ministry of Works, n.d.).
2. J.R ''Dick'' Chiles had negotiated many of the key comsec co-operation agreements with the British in the 1950s. His deputy on the Twighlight project was F.C. Buck.
3. The vocoder was called ''Belgard'', while the cipher key generator was called the KG-13 ''Franton'', which loaded by pulling a 7-inch strip of punched 8-hole tape through a reader. It also required a SEBIT-24 modulator–demodulator.
4. After his retirement from GCHQ in 1976, Teddy Poulden became the first computer officer at MI6.

References

Aldrich RJ (2010) *GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency*. London: HarperCollins.

Aurix Ltd (n.d.) A proud heritage. Retrieved 23 December 2011 from http://www.aurix.com/pages/3376/History.htm.

Benjamin R (1996) *Five Lives in One: An Insider's View of the Defence and Intelligence World*. Tunbridge Wells, UK: Parapress.

Berridge GR (2002) *Diplomacy: Theory and Practice*. London: Palgrave.

Cabinet Office (1960a) CAB21/4397, Thuillier (CAB) to Harris (GPO Engineer in Chief), 'Pickwick Speech Secrecy Equipment', 14 Jan. 1960.
Cabinet Office (1960b) CAB21/4397, Cabinet Office, 'Record of an informal meeting in held in the Cabinet Office on 25 January 1960 to discuss Pickwick speech security equipment', 26 Jan. 1960.
Cabinet Office (1960c) CAB21/4397, Summary of an informal mtg. held in the Cabinet Office between LCSA, NSA, GPO and Cabinet Office, 11 May 1960.
Cabinet Office (1960d) CAB21/4397, Thuillier to Rogers (LCSA), 14 Apr.1960.
Cabinet Office (1960e) CAB21/4397, Stannard (LCSA) to Thullier (CAB), 16 May 1960.
Cabinet Office (1960f) CAB21/4397, Notes and conclusions of a meeting held in Washington, 28 October 1960.
Cabinet Office (1963) CAB21/5429, Reed (Joint Communications-Electronics Staff) to Cabinet Office, 'Defence Inter-Departmental Teleprinter network', 1 Jul. 1963.
Cabinet Office (1968) CAB164/312, Gardiner (CESD) to Rose (Deputy Secretary Cabinet Office), 24 Jan. 1968, ER02C/5618, enclosing Annexure A: 'Note on the Transfer of Post Office Staff to CESD and Attendant Problems'.
Cabinet Office (1974a) CAB134/3848, T(74) 9, 'Provision of Secure Telephone Facilities for Government Use', 17 Jul. 1974.
Cabinet Office (1974b) CAB134/3848, T(74) 1st mtg. (1) 24 Jul. 1974.
Cabinet Office (1974c) CAB134/3848, T(74) 18, 'Secure Telephone Scheme – Organisation and Management Arrangements', 19 Dec. 1974.
Cabinet Office (1974d) CAB134/3848, T(74) 20, Note by CESG, 'Secure Telephone Facilities for Government', 23 Dec. 1974.
Cabinet Office (1975a) CAB134/3967, Comments of Hooper and Foden at T(75) 1st mtg., 14 Jan. 1975.
Cabinet Office (1975b) CAB134/3967, T(75) 1, 'The Responsibility For Approving the Overall Security of Secure Telephone Schemes', note by the Security Service, 4 Feb. 1975.
Cabinet Office (1975c) CAB134/3967, T(75) 13, 'Research and Development in Support of Government Communications', 7 Aug. 1975.
Cabinet Office (1978a) CAB134/4279, Tovey (D/CESG) to Cab, 'Secure Telephone Scheme: Design Acceptance Certifcate.', D/6847/1604/3130, 30 Jan. 1978.
Cabinet Office (1978b) CAB134/4279, T(79) 10, Note By the Cabinet Office', The Secure Telephone Scheme Future Expansions', 24 Aug. 1979.
Cabinet Office (1981) CAB134/4572, CESG, 'Secure Telephone Equipments (An Introduction to Melody)', April 1981.
Copeland J (2006) *Colossus: The Secrets of Bletchley Park's Code-Breaking Computers*. Oxford: Oxford University Press.
Davies P (2000) *MI6 and the Machinery of Spying*. London: Routledge.
Donoughue B (2005) *Downing Street Diary: With Harold Wilson in No. 10 (entry for 17 July 1974, p. 167)*. London: Jonathan Cape.
Dunn DH (ed.) (1996) *Diplomacy at the Highest Level: The Evolution of International Summitry*. London: Macmillan.
Ferris J (1987) The British ''Enigma'': Britain, signals security and cipher machines, 1906–1946. *Defense Analysis* 3(2): 153–163.
Foreign and Commonwealth Office (1967a) FCO19/30, Minutes of Belgard mtg. at Palmer St, chaired by S.F. Nichols, 15 Aug. 1967.

Foreign and Commonwealth Office (1967b) FCO19/30, Bates (FCO) to Stannard (D/CESD), 7 Dec. 1967.
Foreign and Commonwealth Office (1967c) FCO19/30, Stannard (D/CESD) to Bates (FCO). 14 Dec. 1967.
Foreign and Commonwealth Office (1967d) FCO19/30, Stannard (D/CESD) to Burrough (C/GSPS), AG11B3/6116, 22 Feb. 1968.
Foreign and Commonwealth Office (1967e) FCO19/30. Burrough (C/GSPS) to Morgan (FCO) 28 Feb. 1968.
Foreign and Commonwealth Office (1967f) FCO19/30, Killick (Washington) to Ashe (FCO), 27 Mar. 1968.
Foreign Office (1946) FO371/54986, Brigadier (Chief Secretary) HQ CCG (BE) to British Signals Communications Board, 'Scrambler facilities for CCG (BE)', 7 Oct. 1946.
Foreign Office (1963a) FO850/321, Memo to SoS, 'Emergency Communication with HM Ambassador, Washington, and with US Secretary of State', 14 Nov. 1963, YP4/19.
Foreign Office (1963b) FO850/321, Rab Butler min. 14 Nov. 1963, ibid. See also Johnson, 1995, p.380.
Hennessy P (2011) *The Secret State: Preparing for the Worst 1945–2010*. London: Penguin.
Home Foreign Office (1975a) HO256/897, Memo to James (HO), 'Secure Speech Communications', 8 Jan. 1975.
Home Office (1975b) HO256/897, Memo to Sir James Wadell (HO), 'Hi-Jacking', 13 Jan. 1975.
Hodges A (1983) *Alan Turing: The Enigma of Intelligence*. London: Hutchinson.
Holmes JN (1980) The JSRU channel vocoder. *Communications, Radar and Signal Processing*, IEE Proceedings 127(1): 53–60.
House of Commons (1985) HC Deb 1985, 'GCHQ Cheltenham', 11 Nov. 1985, vol.86, c84W 84W.
House of Commons (1998) HC Deb 1998, 'Intelligence and Security Services', 2 Nov. 1998, c581W 12W.
Johnson TR (1995) *American Cryptology, Book II: Centralization Wins, 1960–1972*. Fort Meade, MD: NSA.
Johnson TR (1998) *American Cryptology, Book III: Retrenchment and Reform, 1972–1980*. Fort Meade, MD: NSA.
McKay S (2010) *The Secret Life of Bletchley Park: The History of the Wartime Codebreaking Centre by the Men and Women Who Were There*. London: Aurum.
Ministry of Defence (1968) DEFE59/25, DSB 31/69, memo by CESD, 'Tactical Secure Speech', 21 Oct. 1968.
Ministry of Defence (1972) DEFE26/16, Smith (CAB) to Stocker (MoD), 'GSSN: Operational Priorities for Phased Introduction of the GSSN Recommended by the User Requirement Working Party', 4 May 1972.
Ministry of Defence (1974) DEFE25/345, Le Bailly (DGI) to CDS, 'Promulgation of Intelligence in the Cyprus Situation to UKMILREP', 24 Jul. 1974.
Ministry of Works (n.d.) WORK12/679, Undated plan and accommodation scale for government offices at Northwood Hills.
Murphy RL (1948) *Last Viceroy: The Life and Times of Rear-Admiral the Earl Mountbatten of Burma*. London: Jarrolds.

Newns GR, Beales KJ, Day CR (1977) Development of Low-Cost Optical Fibers. 1977 International Conference on Integrated Optics and Optical Fiber Communications (IOOC), Tokyo. *Technical Digest* (July 1977): 609.
Penney (1957a) Samford (NSA) to Penney (LCSA), 5 August 1957. Penney Papers 2/24, Liddell Hart Centre for Military Archives.
Penney (1957b) 2/29, Hooper (GCHQ) to Penney (LCSA), 4 October 1957. Penney Papers, 2/29, Liddell Hart Centre for Military Archives.
Ratcliff RA (2006) *Delusions of Intelligence: Enigma, Ultra, and the End of Secure Ciphers*. Cambridge: Cambridge University Press.
Reynolds D (2009) Summitry and inter-cultural communication. *International Affairs* 85(1): 115–127.
Richelson J (2008) *The U.S. Intelligence Community*. Boulder, CO: Westview Press.
Skilton PJ (1988) Tactical or Military Satellite Ground Terminals – A Research and Development Review. RSRE Malvern Memo No.4262. London: HMSO.
Smithsonian (1986) Joint Speech Research Unit. Smithsonian Speech Synthesis History Project (SSSHP) 1986–2002.Available at http://americanhistory.si.edu/archives/speech synthesis/ss_jsru.htm.
Stafford D (2003) *Spies beneath Berlin*. London: John Murray.
Treasury (1960a) T219/1064, LCSA to Wyatt (Treasury) 24 April 1960.
Treasury (1960b) T219/1064, LCSB (57) 1 Final, 'Regulations concerning the installation and use of the Green Phone', 17 June 1957.
Treasury (1971) T227/3475, Dyer (T), 'Government Secure Speech Network' discussing CSC (71) 42, produced by the Communications-Electronics and Space Committee, 30 Nov. 1971.
Treasury (1973) T353/76, Trodden (HO) to Skinner (T), 'Cryptophon 1100 Speech Security Equipment', 31 Aug. 1973.
Treasury (1975a) T225/3474, Larkin (CAB), 'Government Secure Speech Network', 6 Nov. 1975.
Treasury (1975b) T353/122, Jackson to Skinder, 'Secure Telephone Service', 14 Jun. 1975.
Weadon PD (2000) *The Sigsaly Story Fort George G*. Meade, MD: NSA Center for Cryptologic History.
War Office (1955) WO195/13693 Attendance list attached to SRDE Report No.1100, 'Methods and Purposes of Speech Synthesis: Report of Colloquium held at SRDE on 8–9 Sept. 1955'.
War Office (1964) WO32/19631, Stannard (LCESA) to Robinson (MoD), 18 Nov. 1964.
Young J (2001) The Wilson Government's reform of Intelligence co-ordination, 1967–68. Intelligence and National Security 16(2): 133–151.