Putting the spooks back in? The UK secret state and the history of computing

email: jonathan.agar@ucl.ac.uk

Jon Agar is Professor of Science and Technology Studies at University College London. He is the author of *The Government Machine* (2003), *Constant Touch: a Global History of the Mobile Phone* (2003) and *Science in the Twentieth Century and Beyond* (2012). Mailing address: STS, UCL, Gower Street, London, WC1E 6BT

Writing of Cold War historiography, Richard Aldrich, the historian of GCHQ, agrees with Christopher Andrew, the historian of MI5:

> shortly after VJ-Day, something rather odd happens. In the words of [Andrew], the world's leading intelligence historian, we are confronted with the sudden disappearance of signals intelligence from the historical landscape. This is an extraordinary omission which, according to Andrew, has "seriously distorted the study of the Cold War"[1]

The same can be said for the way that the near absence of branches of the secret state has distorted the historiography of post-war computing. This lacuna has been pointed out recently for the American case by Paul Ceruzzi. Historians, he felt, have 'done a terrible job, because they have failed to chronicle the critical work done by the NSA [National Signals Agency] and other related agencies in computing.[2] While he identified a few notable exceptions, I think the point stands: the work that has been done is patchy, and the overall significance of the secret state has not yet been assessed. In this paper I survey the UK case, piecing together what we might reliably know.

For the British secret state, signals intelligence, primarily the successor to Bletchley Park, the Government Communications Headquarters (GCHQ) was most likely the most important agency in the story of computing. Other organisations also have had strong interests in information management, data processing and associated technologies. These other bodies would include the Security Service (aka MI5, the counter-intelligence agency), the Secret Intelligence Service (SIS, aka MI6, which ran spies abroad), the central bureaucratic apparatus (parts of the Ministry of Defence, including the Defence Intelligence Staff, and Cabinet Office, such as the Joint Intelligence Committee or JIC), and indeed the security-related wings of the police force. All of these are largely invisible in the historiography of computing. The primary cause for the disappearance, of course, is not a mystery: UK authorities believed that the intelligence services could only operate in conditions of extreme secrecy.

But the effect of such secrecy has been two-fold. We don't have the sources, the evidence, in the form of access to reliable, official documents, to make the extensive and sound historical inquiries we wish. Furthermore, we have not asked the counterfactual question: even if we don't know, at the level of complete sources, what happened, what can we say about the possible influence of the secret state anyway? In the following I will review the available sources, offer a series of hypotheses, and discuss the evidence for them.

What sources do we have?

First, we have some substantial, recently published secondary sources on the main branches of the secret state. Some of these are official and some unofficial. Christopher Andrew's *The Defence of the Realm*, is, as the subtitle tells us, an authorized history of MI5. His book was essentially commissioned to mark the centenary of the organisation, which fell in 2009. Andrew was given access to a portion at least of MI5's 400,000 file archive, and his role was as an 'independent historian', although inevitably he had to strike a 'balance in the text between openness and the protection of national security', a necessity which entailed 'a complex and demanding exercise requiring many hours of detailed discussion'[3]. An official history of MI6 was also published around the centenary, but only covers the first fifty years of the organisation.[4] GCHQ is the subject of Richard Aldrich's unauthorised study, a remarkable and detailed account of the key site of UK code-

breaking and signals intelligence.[5] Aldrich's study was 'compiled from open sources, and no classified material was used', and benefitted from a period in the mid- to late-1990s when more documents were released at Kew in the spirit of making government more accountable through greater openness.[6] Aldrich chose not to interview 'former British officials' for 'legal reasons'. In addition to these monographs, there is further secondary literature that examines aspects of how the secret state has operated and intersected with other foci of historical interest, such as foreign policy.[7]

Second, we can look to see what historians have been able to find out about the situation in other countries. These countries have significantly different regimes of secrecy and rules over the release of documents. The most important other country is the United States. Not only was the United States the UK's senior partner in the Cold War, and the leader in information technologies, but also more information has been released that enables us to have a better picture of American secret computing compared to the British case. There exists, for example, an only partly-redacted history of pre-NSA and NSA computing, covering the years 1930 to 1960, written by an academic historian who was temporarily admitted behind the fence.[8] From this book alone we find out that, while the relationship had ups and downs, there is substantial evidence behind the claim that the NSA emerged to 'become one of world's largest data processors', 'a computer leader', and a 'the largest single user of advanced computing machines in the world'.[9]

Third, historians of computing have examined the post-war UK secret state where sources have been available, but these are few and far between. Martin Campbell-Kelly in his history of ICL, published in the 1989, unsurprisingly makes no mention of GCHQ.[10] Simon Lavington, who was granted special access, has been able to describe the digital cryptanalytical GCHQ projects of the first post-war decade.[11]

Fourth, a trickle of primary sources relating to post-war secret computing has begun to be released at the National Archives, and can be studied at Kew. These primary sources, perhaps unsurprisingly, relate to the least sensitive, most mundane aspects. Even when they are available they are often missing technical detail, or are incomplete, still having parts retained under the Official Secrets Act. Nevertheless, these sources are invaluable. The pre-1945 records are much more substantial, and, through reconstruction of trajectories, might help us speculate about developments and concerns, particularly in the immediate post-war years.

The shroud of secrecy is thickest over the primary sources relating to the core institutions of the secret state – GCHQ, MI5, MI6, the Joint Intelligence Committee of the Cabinet Office. But the influence of secret computing may be found around the edges, as the demands of secret computing affect, enrol and shape the civilian world. I have therefore been on the watch for evidence of such influence in the records of civil bodies, such as those relating to the police, universities, and government research establishments.

Finally, there is information in the public realm which addresses the secret state, secret computing included, which goes further than the above sources, but is harder to judge in terms of reliability, since their claims are not necessarily secured by citations to traceable documents. These sources are various: the results of investigative journalism, the claims of whistle-blowers, anonymous contributions to Wikipedia, and the historical writing by authors whose aim is not history of an academic standard. Such material is not used here.

There is no easy way to estimate the volume of documents and other sources that would be valuable to the historian that are at present inaccessible. Certainly the core institutions have retained documents that reach back to the beginnings – and beyond - of the period under study here. Furthermore, GCHQ, for example, has its own museum, containing artefacts - a few of which have occasionally been shown in public (for example in the Science Museum's temporary *Codebreaker* exhibition, which closed in 2013). None of these inaccessible documents or sources is used here.

What hypotheses can we make?

I will propose seven hypotheses, and then turn to see what evidence from primary and secondary sources might address them. First, the UK secret state was a major user of computing technologies, and within the secret state, signals intelligence (and codebreaking) was the heaviest user. Second, signals intelligence generates computing tasks characterised by large quantities of data subjected to speedy, repetitive, relatively simple analysis. We would therefore expect the demands to be on size of memories, peripheral technologies (storage of data), and fast computing. Third, the demands of the secret state in computing shaped the development of the computer industry. Fourth, in this interaction with industry there were opportunity costs, for example that the absorption of trained staff drew skills and knowledge away from civil sectors and from military non-secret state sectors. Fifth, in common with the rest of Whitehall, which I have made the subject of a separate substantial study, mechanisation and computerisation of clerical tasks was widespread and significantly shaped capacity for administration.[12] Sixth, technological innovations that originated in response to problems raised by the secret state sometimes spread out to civil applications. Finally, my seventh hypothesis is that security was a constraint, raising its own problems which in turn invited socio-technical solutions.

What do we know?

(1) The Secret State as a Major User of Computing Technologies

Of course, the secret state is part of the canonical history of computing. But these appearances are rare and selective. Most well-known is the work of the Government Code and Cypher School, also known as Bletchley Park. It was there that Turing, and many others, gathered to attack German coded messages.

The immense, current cultural interest in Bletchley Park has several motivations. There is fascination in, and uses of, the tragic story of Turing himself. Most powerfully Turing's life and work has become an icon and rallying point in LGBT politics. This interest has motivated the best historical work on Turing in the form of Hodges' biography.[13] Second, there is the attraction of the secret, compounded by the fact that a silence, partly officially but also partly self-imposed, around Bletchley Park activities lasted until the 1970s. The subsequent rush of information, all the more emotionally-charged for having been pent up so long, has given Bletchley Park extraordinary prominence. Third, there is a narrative, inflected with nationalism, that celebrates Bletchley Park as a distinctively British contribution to the defeat of Nazism: it was by brain-power not brute production (undercutting

claims that it was Russian and American contributions that were decisive), it is presented as amateur (it was anything but), and it is nostalgic.

At Bletchley Park, the signals intelligence (sigint), collected by outlying stations, was channelled and made subject to cryptanalytical attack. The messages coded using the Enigma machines were subject to human and machine ('bombe') analysis. The messages encrypted using a cipher machine codenamed 'Tunny' were processed by Colossus, the extraordinary electronic valve-based, symbol-manipulating machine designed and built by the General Post Office team under Thomas H. Flowers. The first Colossus was built in 1943. Ten Colossi were in operation by 1945.

We should remember that Bletchley Park was an industrial operation: large-scale, focused on speed and flow, with innovation and mechanisation at reverse salients (in the sense used by historian of technology Thomas P. Hughes). I made this observation in *The Government Machine* (2003). Other historians agree. Aldrich writes of the wartime sigint sites: 'All of them were symptomatic of an industrial revolution in secret intelligence: both Bletchley Park and the outstations operated like factories, with three gruelling shifts each day'.[14] Copeland describes the 'two vast steel-framed buildings' that housed the Colossi as 'a factory dedicated to breaking Tunny'.[15]

It is precisely the scale of such operations that suggests that the secret state is probably an important and under-estimated factor in shaping the history of post-war computing. In April 1946, British codebreaking moved from Bletchley Park to Eastcote in London. The centre also had a new name, the Government Communications Headquarters (GCHQ). Of the ten Colossi, two moved to Eastcote. (Lavington has the two Colossus II machines being assembled at Eastcote.[16])The rest were supposedly destroyed. Aldrich writes, almost certainly erroneously:

> Much of the machinery was broken up, including examples of the mighty 'Colossus' computational machine. However, Professor Max Newman, who had been central to its development, managed to secure two 'Colossus' machines for his new computing department at Manchester University. These were transported by the Ministry of War Transport at the price of thirty-four shillings a ton. Newman offered to send a junior university lecturer down 'to sit on the van' to make sure that the precious machines were not damaged in transit.[17]

One possibility is that Newman was in fact involved in the move of the two Colossi to Eastcote. Historian J.V. Field, in partial support of this interpretation, says that Manchester received components of old Colossi.[18]

Copeland writes:

> Some machines did survive the dissolution of Newmanry [the Bletchley Park section]. Two Colossi made the move from Bletchley Park to Eastcote, and then eventually on to Cheltenham. They were accompanied by two of the replica Tunny machines manufactured at [GPO research station] Dollis Hill. One of the Colossi, known as "Colossus Blue" at GCHQ, was dismantled in 1959 after 14 years of post-war service. The remaining Colossus is believed to have stopped running in 1960.[19]

The two post-war Colossi had several uses. They almost certainly continued to be used for cryptanalysis; they were 'used extensively for training', at least towards the end of their lives, 'ex-

Newmanry engineers developed a random noise generator', employing 'some of Flower's circuitry from Colossus' to generate one-time pads, random secret keys used in encryption.

In 1952, GCHQ began its move, completed in 1954, from Eastcote to a new, spacious site at Cheltenham. The expansion came with a generous boost in new funding, agreed to at a meeting on 22 January 1952 between the British Chiefs of Staff and the Permanent Under-Secretary of the Foreign Office; the resulting five-year plan, designated "Methods to Improve", paid for what Aldrich describes as 'larger computers and "high speed analytical equipment" for renewed attacks on high-grade Soviet communications'.[20] At Eastcote and Cheltenham, GCHQ undertook several projects drawing on contemporary experiments in computing and electronic memory storage. In the 2000s, historian of computing Simon Lavington has been able to trace this early history based on declassified information.[21] First, the Colossus Red was "rebuilt in a more generalised form" between 1948 and 1951; second, four "Robinsons [war-time cryptanalytic machines, smaller than Colossus] were installed at Eastcote using Colossus type circuits, tape readers and output printers", an upgraded Robinson project was called 'Johnson'; third, technical staff from GCHQ spent time at Manchester University, and transferred the magnetic drum technology back, resulting in a machine called Colorob, which was designed to "combine the functionality of Colossus and Robinson" but although begun by 1952 not operational until 1960.[22] Fourth, GCHQ purchased a Ferranti Mark I Star general-purpose electronic computer, which was in operation at Cheltenham in mid-1954.[23]

Finally, drawing on the Ferranti Mark I Star's drum design, Tony Ridlington designed GCHQ's own special-purpose machine, Oedipus, running by May 1954.[24] Oedipus, 'a rapid pattern-matching machine', writes Lavington, 'was in fact the first GCHQ machine to fully exploit the potential of high-speed digital storage'. Specifically, Oedipus compared plausible transforms of around 10,000 15-character phrases with incoming text, and ranked the results by a measure of importance. As Lavington says, such a machine had to be extremely fast and required a 'huge amount of internal direct-access memory'.[25] Indeed, these demands were 'well beyond the capability of early 1950s general-purpose stored-program computers', which is why Oedipus was a special-purpose electronic machine. Technologies used were magnetic drum storage (holding 768,000 digits, from Ferranti and Manchester), read-only memory made of semiconductor diodes (designed by GCHQ and built by Elliott Brothers), and Williams tubes (also from Manchester). Input was by 200-character per second optical tape reader (from Ferranti) and output by Hollerith punched cards. Lavington shows that Oedipus could implement more instructions per second and had larger online storage than any mid-1950s computer.[26] 'The significance of Oedipus was that it was a powerful rapid-character-comparison machine with a capability greatly exceeding that of any general stored programme machine available commercially in the 1950s and 1960s', writes Aldrich, who goes further than Lavington by stating what the target of the machine was: much of 'this elaborate technology was devoted to unsuccessful attacks on high-grade Soviet diplomatic cyphers'.[27]

In 1958 a second 'Methods to Improve' five year plan started, channelling funds into signals intelligence. IBM computers were purchased. 'GCHQ bought IBM computers not only because of NSA compatibility, but because its machines were cutting edge', says Aldrich.[28] Burke, in his history of NSA computing, notes that this moment was 'sad':

> the crypto-technology tables had been turned. No longer was the United States a dependent waiting for the secrets of the British Bombe to be sent from GC&CS. Millions were to be

> spent to provide Britain with a new computer so that it could continue its anti-[redacted] research.[29]

However, by 1962, with costs rising and no success with breaking Soviet codes, a 'comprehensive review' of GCHQ, with the initial aim of cutting costs, was launched, chaired by an Oxford don Sir Stuart Hampshire.[30] 'Remarkably, after much debate GCHQ got its money', notes Aldrich, after 1962 'the budgets of most of Britain's overseas departments went down by 10 per cent, but the sigint budget went up by the same amount'. The trump card was the unwillingness to disturb the close UKUSA relationship ('UKUSA' was the official label for UK-USA signals intelligence agreements). [31]

Between the 1960s and 1970s, two very significant trends intersected. The first was the drive to computerise the vast paper and card databases (registries that were among the largest in Britain[32], card indexes, etc) and make them searchable by keyword. Computing was no longer just for cryptanalysis but enabled other tasks too. The second was the use of information technologies to share such data, as well as sigint, with allies across government and with national partners. Furthermore, with the opening of satellite communications systems the quantity of available signals was multiplying rapidly. The establishment in the 1960s of GCHQ Bude in Cornwall, near enough to the satellite earth station at Goonhilly Downs and next to the beachhead of the undersea Atlantic telephone cables, made prodigious amounts of data available to the UKUSA intelligence community.

The NSA and GCHQ developed 'revolutionary new systems for analysing and distributing the huge volume of intelligence intercepts, with computers being used to search for keywords that indicated subjects of interest'.[33] The system that 'combed the traffic for keywords and predesignated phrases' and shared the data according to access clearances was called 'Dictionary', available from 1969.

The development of methods to share intelligence electronically had its immediate origins in a US project begun in 1965 called COINS (Community On-line Intelligence System), which would allow the NSA to share files and give the Pentagon and State Department "read only" access.[34] COINS in the US was failing, but in 1969 the UK, in the form of Dick White, the Cabinet Office intelligence coordinator and Joe Hooper, the director of GCHQ, took inspiration from it, although they also noted considerable problems, including duplication of files, non-standardisation of file formats, faults in the system itself, and, in an early hint of catastrophic problems – think of Chelsea Manning – that would lie ahead, the 'problem of restricting access to any given information so that is available only to those with a need to know and authorised to receive it'.[35]

Further moves to coordinate automatic data processing were in place by the early 1970s, and some of the preliminary developments are discussed below.

We also know that

> In 1967, Ken Sly, who had commanded the sigint unit at Hong Kong, took over from Nicodemus Doniach as head of a GCHQ branch called the Joint Technical Language Service, a group of thirty highly qualified linguists who not only undertook translations, but also compiled material ranging from dictionaries of Soviet military terms to handbooks of Arab names. When Sly took over they were working from a vast wall of index cards thirty yards long. He began a determined programme of computerisation, so this vast body of knowledge gradually became available to everyone in GCHQ. This change was of the first

> importance. GCHQ could see that computers were the shape of the future, and wanted to use them to improve every stage of the intelligence process.[36]

In the 1970s 'the old "blue jacket" files full of sigint intercepts started to disappear, and online access for policy-makers slowly began to take over'.[37] Computers were used to cut staff numbers in the mid-1970s as part of a search for cuts.[38]

In 1976, GCHQ placed an order for one of Seymour Cray's first supercomputers. The machine, delivered the following year, required a new building (Benhall) and organisation (X Division), but the increased speed and power paid dividends: the NSA's Crays recovered the 'long-lost ability' to break high-level Soviet communications between embassies in 1976.[39] Likewise, on the front-line of eavesdropping, small computers – in the form of Honeywell terminals, on advice of the NSA, which used the same – became part of the measures needed to process the increasing quantities of sigint. 'Keepnet' improved recording, while 'Livebait' improved comparison of data, not least through the distinctive secret state technology of wordsearch.[40] MI5 was demanding a small computer in 1975.[41]

If terminals and small computers was one technical trend familiar to historians of computing that was adopted within the secret state, the other big trend, towards networks, will certainly be the primary focus of future historians. With the revelations of Edward Snowden in 2013 the fact and extent of global surveillance of computer networks by the NSA and GCHQ, among other agencies, has been headline news. It will be many years, however, before historians, working directly with primary documents, will be able to separate claims from counterclaims. One interesting preliminary finding, however, is that GCHQ was relatively late to the surveillance of internet networks. Aldrich suggests that a mind-set that still defined the main enemy as the monolithic Soviet Union, hampered designs for new systems based around networked computers.[42] But once the transition began, internet sources became major targets of surveillance.

(2) The characteristic technical demands of the secret state, and (3) consequences for the computer industry

My second hypothesis – that signals intelligence generated computing tasks characterised by large quantities of data subjected to speedy, repetitive, relatively simple analysis, leading to technical demands on the size of memories, peripheral technologies (storage of data), and fast computing – and my third hypothesis – that the demands of the secret state in computing shaped the development of the computer industry – are best considered together.

We have already seen that GCHQ requested and received supercomputers, evidence that speed of operation was a desirable priority. We have also already discussed how early post-war GCHQ computing projects featured special-purpose bespoke machines that were unusual in their capacity to store and make fast comparisons between data. Other secret state projects raised particular technical demands.

For example, one method of electronic signals intelligence (electronic sigint also called "elint") gathering was to place eavesdropping equipment in aircraft that could fly near the borders of the Eastern Bloc. In 1954, a substantial, expensive project was approved by the Treasury to build three dedicated sigint platforms using the new de Havilland Comet C2 aircraft.[43] The Comet sigint project

was nearly derailed when a fire in a hangar in 1959 destroyed one aircraft. In a way that is comparable to the Admiralty's need to squeeze more capacity out of the limited space offered by available ship space, the 'task to cram a whole mini-sigint ground station into the cramped interior of an airliner' created demands for miniaturisation in components and in design, and for automation to replace bulky human operators with machines.[44]. Later in the 1970s, next generation Nimrod R1 sigint aircraft came into service, 'state-of-the-art' spy planes that complemented American satellite capabilities and 'offered something no other European country had … something that marked Britain out as special'.[45] Plessey provided the sideways-looking elint system. Aldrich remarks on the transition from Comet to Nimrod that further automation of the human operator was by design:

> The existing Comet aircraft depended on teams of human operators wearing headphones who undertook the reception and analysis manually, using narrow-band receivers. However, the growing density and complexity of electronic signals meant that they were simply being overwhelmed. It was 'impossible for the operator to sort out and examine all the active transmissions' in the limited time that an aircraft spent over the search area. This meant that the most interesting material, the unusual signals that might mean new enemy equipment, was being lost. Plessey's new system was designed to do much of the work of the operator, and store what it detected for leisurely analysis after the aircraft had returned from its mission.[46]

In other areas, too, a distinctive feature of sigint was the sheer volume of data that needed to be stored and analysed. One of the greatest intelligence coups of the period was the tapping of Soviet messages from a tunnel under Berlin in the 1950s by a joint operation of the CIA and the Secret Intelligence Service (MI6). It lasted until 1956. Aldrich notes the scale of the eavesdropping, but also the combination of basic magnetic tape technology and manual processing:

> Some twenty-eight telegraphic circuits and 121 voice circuits were being monitored at any one time. Voice traffic was recorded on fifty thousand reels of magnetic tape, amounting to twenty-five tons of material. At the peak of operation the voice processing centre at Chester Terrace, overlooking Regent's Park in London, employed 317 people, and eventually 368,000 conversations were transcribed. The teletype processing centre employed a further 350 people. For each day of the tunnel's operation the output was four thousand feet of teletype messages.[47]

Likewise when in the 1960s and 1970s telephone calls were increasingly sent by microwave radio link and, even more so, by satellite uplink and downlink, a 'veritable fountain of intelligence', 'inconceivable volumes of material … too large for any human to read', the secret state was presented with dramatic spikes in quantities of data.[48] And again, as the turn towards internet surveillance was made in the 1990s, NSA and GCHQ were initially 'simply overwhelmed by a tidal wave of data'.[49] The response, however, was data storage projects, at Cheltenham and in Utah, that are certainly amongst the biggest and most expensive in history. All of this gear had to be made by industry, and therefore we must expect to find significant pressures on technical development and the directions of industrial sector growth.

My suspicion is that we are not yet seeing this industrial influence because only the earlier records are available for direct study. Plessey, which built the key electronic systems for Nimrod R1, was predominantly a defence contractor, and so this contract was one of other similar demands, and so

did not disturb that company's relationship with its main patron, the UK government. Other companies, however, had more diverse portfolios. Even though Ferranti and Elliott Brothers were sub-contractors, Lavington argues that 'Security considerations ensured that [Oedipus's] design had no discernible impact on the history of general-purpose computer development'.[50] There may have been an 'indirect' effect on Ferranti by 'helping to refine the company's drum technology', but for Elliott Brothers, this special-one-off machine was a distraction, and the 'technological spin-off was minimal'.[51]

'GCHQ's impact on computer development', writes Aldrich, 'was not as great as that of NSA'.[52] Aldrich notes that the National Security Agency (NSA), GCHQ's US equivalent, has been 'able to claim a string of very considerable computer firsts', including the 'first parallel electronic computer with a drum memory' (Atlas 1, 1950), 'the first core memory computer' (Atlas 2, 1953), the 'first computer that relied wholly on transistors' (Solo, 1958), and 'the first large computer with a completely automated tape library' (Harvest, 1962). These American achievements were not only firsts, but fed back to drive civil computer development. Solo was the model for Philco's commercial computers, for example, while Harvest 'influenced the design of the IBM System 360'.

Burke tells us that 'On top of the special computing needs of cryptanalysis, NSA's insatiable need for what many times was unique data processing equipment' was what made it a 'computer leader', in the sense of shaping the development of the computer industry. Furthermore this 'influence' was

> not … because of its mathematical wizardry or because it has a mandate to transfer technology to the private sector. The Agency's contributions have become because of the unique nature of cryptanalysis and SIGINT and the increasing difficulty of fulfilling a central responsibility: the production of signals intelligence.[53]

The influence in the United States then was due to specific needs, which generated specific contracts for specific kinds of computing technology (big data, fast, later parallel, processing) that encouraged industry in certain directions. The contract for Nomad – in the end a failure – which went to IBM was, says, Burke, nevertheless 'a great prize, and in some ways more important to the computer industry than the massive Sage early-warning computer project that IBM was taking on'.[54] This statement alone should make historians of computing sit up, given the importance accredited to Sage by, for example, Paul Edwards.[55] Furthermore, by the late 1950s, NSA was not merely handing out very large contracts, but was, as part of moves explicitly drawn as a parallel to the Manhattan Project, but also became 'a sponsor of basic research within industry', a second route of influence.[56]

So, in the eyes of the two historians who have mostly closely studied this question, the NSA had a major influence on post-war computing, less so GCHQ. Why this difference? First, it might be an artefact – a result of the contrast between total silence in public about GCHQ and the severely limited but nevertheless present public knowledge, often circulated for political alliance-maintenance, of the NSA's activities. Second, perhaps the demand for computing power was quantitatively greater from NSA compared to GCHQ. The NSA's director boasted of 'over a hundred computers occupying almost five acres of floor space' by 1968.[57] Third, GCHQ began purchasing American machines: IBM 360s, IBM 700s and Crays. In this way, GCHQ added to the strength of American computing industry.

Nevertheless, there is some counter evidence that suggests that the choices of the UK security state might have been indirectly significant for the development of the UK computer industry. Even before GCHQ was choosing Cray supercomputers and Honeywell terminals, in 1972 the JIC sub-committee on data processing considered what was called 'commercial-in-confidence' information about an IBM emulator of the ICL1900 series of large mainframe computers. This was significant because IBM vs ICL was a decision of national interest, and ICL1900 machines were being purchased elsewhere, for example for the Defence Intelligence Service, while GCHQ could justify IBM machines.[58]

But there were also other countervailing effects. There was much debate about the security problems of using software firms, for example in the early 1970s.[59] This meant there was pressure to write software in house, which must, first, have been increasingly difficult as the scale of software increased, and, second, meant that the shaping influence must have been blunted. I return to this point below.

(4) Opportunity costs

My fourth hypothesis was that there were opportunity costs – the absorption of trained staff drew skills and knowledge away from civil sectors. For Oedipus, Elliott Brothers were at first in the frame to be the sole contractor. But, Lavington says, the company wanted to complete its other projects, including a nickel delay line memory for its 401 series of commercial computers. Lavington quotes Ridlington, the GCHQ engineer, that Oedipus "was too much for Borehamwood [Elliott's factory, neat Eastcote], so it was decided that GCHQ would do the project in-house with Elliott and Ferranti as major sub-contractors".[60] Aldrich tells us that GCHQ's "Methods to Improve" programme was given very high priority, with suppliers informed of this fact.[61] Combining these two points it is plausible that Oedipus pulled resources away from other, more economically productive, post-war computing projects. Nevertheless, the fact that Ferranti and Elliot staff were working on such specialist tasks meant that the firms were developing knowledge within the company. While there might have been temporary delays to progress on civil projects, this knowledge could plausibly have been drawn upon for innovation in the longer term.

(5) Continuities with Whitehall computerisation

My fifth hypothesis was that, in common with the rest of Whitehall, mechanisation and computerisation of clerical tasks was widespread and significantly shaped capacity for administration. Since the mechanisation of clerical tasks was regarded as relatively non-sensitive, documents relating to clerical 'automation' have been released at the National Archives and provide a more detailed glimpse into this aspect of secret computing.

MI5 adopted Hollerith punched card methods, a move away from pure filing, during the Second World War.[62] However, we need more research, and more detailed sources, to discuss the extent to which mechanisation presaged computerisation.

In 1961, the Joint Intelligence Board (JIB) produced a document on 'automation'.[63] It considered two types: 'storage and recovery of reports and facts' and 'data processing'. On the first, it noted that the CIA ('and possibly other intelligence agencies') in the United States were considering moving from a 'complex of index sub-systems, most of which rely on commercially available punched card systems' to 'a new structure of document holding', with micro-photographic and magnetic tape

storage both options. The JIB considered that it would be necessary to 'keep in touch', and 'if we do follow their example, and store information mechanically, we should probably use the same type of equipment'. On data processing, the JIB thought that progress in the United States was slow, oddly 'because of the opposition of scholarship to the idea that a machine can simulate mental processes'. Nevertheless, a 'good deal of work' was being done on 'mechanised translation', adding:

> Those in favour of more automatic data processing in intelligence work point out that a very large part of an analyst's work is collative rather than decision making. Comparisons are made with predetermined criteria, and this a mechanical system can do.

By 1967 a more serious look at electronic data processing was underway. For example a paper on 'The use of computers in the diplomatic service' was circulating. It was suggested that Treasury O&M, the experts, should be tapped. Others were more generally sceptical:

> Probably most people first considering the uses of computers in a new field are, as a result of years of shameless commercial propaganda about computer potential, left with a guilty feeling that all one's problems could be solved in one incredibly efficient system – if only one were clever enough to devise one.
>
> If we could collect the inputs and model the Russian computer system with a clear knowledge of what aims had been set, we should know what automatic decisions ("machine judgements") were being made and would also have available the facts in the form presented to human decision makers. But we cannot assume that their decisions will be logical, and it would require human intellect to judge what these decisions might be. One can weigh facts and derive probabilities, but not quantify illogical functions like Russian patriotic pride in Space achievements, or, in China, the fear of producing a scientific elite class, or, in Greece, King Constantine's sense of dynastic duty.[64]

The Automation working party pulled together interests in mechanisation and computerisation from across the secret state. Some interesting facts were aired:

> Mr Christie, of GCHQ, told the meeting that GCHQ had had data banks in operation for some years. These are now being enlarged and the new systems will have a disc store with a capacity of some 200 million characters. Remote access stations should be in operation in a year or 18 months, and in 1970/71 there should be the possibility of providing departments in London with remote access equipment, at a cost of about £11,000 per terminal including crypto equipment. [65]

In comparison, Treasury O&M stated that the 'largest disc file' available was about 400 million characters, while the Home Office was already bringing in a system with multiple access of 600 terminals.[66]

A new sub-committee on automatic data processing of the JIC was set up in 1969, with representatives from GCHQ, MI5, MI6 and the DIS section of the Ministry of Defence.[67] Its brief was to investigate requirements for ADP among the UK intelligence community, study applications, make recommendations, and offer advice, all while keeping an eye on the needs of international collaboration.[68]

After this date, direct sight of primary documents begins to dry up. MI6 and GCHQ were in discussion about automatic data processing (ADP) for payroll in 1976.[69] We know that some of the computerisation of the secret state ran into the budget overruns and occasional failure that marked the civil projects. Infamous examples are the overrun of the Project Pindar Whitehall defence bunker and the abandonment of the Defence Intelligence Staff system called 'Trawlerman' (1988-1996) and the MI5 system called 'Grant'.[70]

(6) Technological innovations that originated in response to problems raised by the secret state sometimes spread out to civil applications

Neither secret state organisations nor their contractors and collaborating research organisations were likely to shout about spin offs to civil applications. This discretion makes tracking such effects difficult. However, especially around the penumbra of the secret state, some fascinating connections can be found.

We've already seen that it was thought that the US was making progress on mechanised translation for intelligence in 1960. What GCHQ really 'thirsted for', notes Aldrich, was 'progress on machine translation that would do some of the jobs currently undertaken by linguists, but so far this had failed on grounds of high costs and complexity'.[71] The demand was widespread across the Western secret states, and prompted visits to the UK by US experts in 1966[72], and discussion of a French proposal for a NATO project in 1968.[73] From 1959, a team at the Autonomics Division of the National Physical Laboratory, a body most familiar to historians of computing as one of the locations of innovations in packet-switching techniques[74], was working on computerised translation of Russian scientific texts into English. In 1967 it issued a report, a 'comprehensive account', summarising evaluations of the usefulness of different procedures, concluding that the 'results give clear evidence that the basis of a genuinely useful automatic translation service has been achieved'.[75] The probable principle customer for such research can be inferred from the following:

> It would not be the role of the NPL to provide a production translation service based on our system, so we look to some other agency to enquire further into this problem. However, it will be our *continuing* concern to seek to interest and advise the several agencies who may wish to assess the viability of a production service, based on the techniques we have now proven.[76]

On the way, the NPL team had built components of 'considerable independent importance', including am 'automatic Russian-English dictionary, covering all forms of some 17,000 Russian words, and available on punched cards', a 'scheme of comprehensive morphological representation', and 'detailed methods of Russian syntactic analysis and computer model of linguistic structure, capable of wide application'; all of these, along with advice, were available to 'bona-fide researchers'.[77]

We might assume (but cannot yet prove) that NPL were not working for eight years merely on the hope that it might interest agencies in the secret state, but that contact was both more substantial and communications flowed two-way. There is a further twist. The machine translation work at NPL found an output in civil policing.[78] It fed into plans for a C11 branch criminal intelligence computer

project – the “supertec” (a nickname the media gave, disliked by the civil servants). The connection back to the NPL, and perhaps therefore back to the secret state is referred to only briefly:

> The computer will speak English. You will type (in plain English) questions to it, and it will answer. It will even look up words it does not know, and learn as it goes… The programming is done at the National Physical Laboratory … they learnt a great deal from their earlier work in translating English and Chinese and Russian into each other.[79]

Universities, too, also sought to interest secret state patrons. For example, in the same period the Cambridge Language Research Unit proposed an ‘automated reactive dictionary’ and requested support from the Defence Intelligence Staff. While this specific request was refused because an alternative partially-automate ‘simple and fully adequate solution’ seemed available, the discussion also recorded the interested parties:

(a) The Security Service were chiefly interested in general translations from languages in the Communist bloc.
(b) MI6 were interested
(c) GCHQ (and NSA) were already involved in this general area of work and would probably have a requirement for any system proposed.
(d) The Foreign Office should be consulted at some stage.[80]

Furthermore, machine translation was not simply a response to the overwhelming flood of potentially important intelligence from the Eastern Bloc, the requirement for Western countries to cooperate, such as through NATO, also increased demand for translation services, as one official noted: ‘the requirement was now much greater than before and much of it arose from our participation in NATO and other international organisations which sponsored joint projects’.[81]

The whole area of the transfer of innovations between the secret state and the non-secret state, as well as between policing and civil researchers deserves much more scrutiny from historians of science and technology. Another interesting example of where policing technology was sourced, for example, was the translation of technology developed at University College London in the 1970s to analyse bubble chamber tracks automatically subsequently applied to automatic vehicle number plate readers for the Home Office and police.[82]

(7) Security was a constraint, raising its own problems and socio-technical solutions.

The agencies of the secret state have a particular, shared concern with security. In particular, they not only wanted their own communications to be secure, and wanted to subvert the communications security of their targets. Much of Bletchley Park’s ingenuity was, of course, devoted to solutions of the latter. In the post-war period this focus remained, throwing up problems and demanding socio-technical solutions. Another problem was that as electrical equipment, including computer terminals, electric typewriters and other peripherals, were introduced in the name of office efficiency, so there was an increased danger that such equipment might, through detectable signals generated in operation, become a serious security risk.[83] The discovery that cypher machines radiated detectable signals over a hundred yards (a problem called “Tempest”) was made in the 1950s.[84] In the mid-1960s, the Joint Intelligence Committee’s Automation Working Party (on which

all agencies were represented) expressed interest in electrical 'tape-controlled typewriters', but these had 'radiation' problems, and therefore required 'purpose-built intelligence centres with adequate physical and electronic security'.[85] Later, GCHQ investigated the security weaknesses of IBM 2260 visual displays, an episode that shows there were exchanges back and forth between security agency and computer manufacturer.[86]

As programming, rather than hardware, became the most costly component in developing computer projects in the 1960s (leading to the so-called "software crisis"), so writing software securely in house became untenable, another major security issue for the secret state. Moreover there was political pressure to encourage the sector, and this too ran against security interests. As the chair of the Joint Intelligence Committee working party reflected in 1972:

> It was national policy to make use of software firms where appropriate. It was his view that software contracts, like any other contracts be placed with selected firms where profitable, and where practicable within the necessarily stringent security constraints applicable in the intelligence field. In the case of GCHQ this was likely to exclude general purpose computer work but could include certain total special purpose computer-based systems.[87]

In discussion, the 'general view emerged that from the security angle, there were considerable difficulties involved in dealing with software firms, stemming from the need to involve manufacturers at a very early stage, … [but an] apparently unclassified project could unexpectedly turn out to involve highly classified problems relating to operational files. One general point to notice is that these restrictions might have constrained the secret state's influence on the developing computing industry in ways that meant it did not have the impact its sheer size might lead us to expect.

Finally, there were similar problems raised by tension between the benefits from sharing information within the secret state and the dangers of unauthorised access. GCHQ advised on remote access computer terminals in 1969. It noted that commercial remote access facilities, for example IBM's, could be adapted with 'special interface units' so that they could be combined with 'modern cryptographic equipment'.[88] Cryptographic protection was essential of course. At this time, in 1969, GCHQ's 'conventional teleprinter' operating at 100 words per minute (75 bits/second), costing £500, was made secure using the UK on-line cypher equipment called Alvis, which added a cost of £1500. When higher-speeds were available then new crypto equipment would be needed. This was likely 'before the mid-seventies' – by which point, presumably, Alvis had left the building.

Conclusion

The reliable historical sources on the computing projects, interests and influence of the secret state of the United Kingdom are few in number and most primary sources are still retained under the Official Secrets Act. Nevertheless, in this paper I have proposed seven hypotheses, and discussed what evidence might address them. My assessment of each hypothesis would be as follows. First, the UK secret state was indeed a major user of computing technologies, and within the secret state, signals intelligence was the heaviest user. Second, signals intelligence generated computing tasks characterised by large quantities of data subjected to speedy, repetitive, relatively simple analysis.,

which in turn put particular emphasis on seeing developed, with select industrial partners, larger memories, other peripheral technologies, and techniques of fast computing. Nevertheless, third, the dimensions of influence of these demands of the secret state on the computing industry, especially UK industry, are still unclear. Fourth, in this interaction with industry there were probable opportunity costs. Fifth, in common with the rest of Whitehall there was widespread interest in the application of automatic data processing to office work, including the specific information and document handling peculiar to the intelligence world. One reason that picture is clearer on this point is that the subject of automatic data processing was regarded as relatively mundane and therefore less sensitive. Sixth, while it is not proven that technological innovations spread from the secret state to civilian applications, it was shown that there were shared interests and probable patronage, as well as presumably less documented conversations. Finally, security was indeed a constraint, raising problems and calling for solutions. This understandable restriction might provide part of the answer of why the secret state, despite being a major customer for information technologies, can only be shown – so far – to have had an ambiguous, even limited, effect on the computing industry. In general, however, the overall question – what is the place of the secret state in the history of computing – deserves more scrutiny from historians, especially as new sources are revealed.

Acknowledgements: I would like to thank the organisers and the audience of the conference 'Interpreting the Information Age: new avenues for research and display', 3-5 November 2014, Science Museum, London, for their comments. I would also like to thank Paul Ceruzzi for sharing his draft papers.

[1] Richard J. Aldrich, *GCHQ: the Uncensored Story of Britain's Most Secret Intelligence Agency*, London: Harper Collins, 2010, 2.

[2] Paul Ceruzzi, 'Are historians failing to tell the real story about the history of computing', *IEEE Annals of the History of Computing* (2014) 36(3), 94-95, 94.

[3] Christopher Andrew, *The Defence of the Realm: an Authorized History of MI5*, London: Allen Lane, 2009, quotes from foreword by the Director General of the Security Service, Jonathan Evans, xv-xvi.

[4] Keith Jeffery, *MI6: The History of the Secret Intelligence Service 1909-1949*, London, Bloomsbury Publishing, 2010.

[5] Aldrich, *GCHQ*.

[6] Aldrich, *GCHQ*, preface.

[7] Philip H.J. Davies, *MI6 and the machinery of spying*, London: Frank Cass, 2004.

[8] Colin Burke, *It Wasn't All Magic: the Early Struggle to Automate Cryptanalysis, 1930s-1960s*, United States Cryptologic History, Special Series: Volume 6, National Security Agency, 2002. See also: Samuel L Snyder, 'Computer advances pioneered by cryptologic organizations', *IEEE Annals of the History of Computing* (1980) 2(1), 60–70.

[9] Burke, *Magic*, 5.

[10] Martin Campbell-Kelly, *ICL: a Business and Technical History*, Oxford: Clarendon Press, 1989.

[11] Simon Lavington, 'In the footsteps of Colossus: a description of Oedipus', *IEEE Annals of the History of Computing* (April-June 2006) 28, 44-55
[12] Jon Agar, *The Government Machine*, Cambridge, MA: MIT Press, 2003.
[13] Andrew Hodges, *Alan Turing: the Enigma*, London: Burnett Books, 1983.
[14] Aldrich, *GCHQ*, p. 63.
[15] B. Jack Copeland, *Colossus: the Secrets of Bletchley Park's Codebreaking Computers*, Oxford: Oxford University Press, 2006, 2.
[16] Lavington, 'Oedipus', 45.
[17] Aldrich, *GCHQ*, 70. Aldrich cites a reference in a UK National Archives (hereafter 'TNA') file: HW 64/59. Newman (Manchester University) to DDA (GCHQ), 12 November 1945.
[18] J.V. Field, private communication.
[19] Copeland, *Colossus*, 173.
[20] Aldrich, *GCHQ*, 120.
[21] In his Oedipus paper, Lavington notes 'The technical details presented in this article are based on information recently provided by the principal Oedipus designers, Tony Ridlington of GCHQ and Harry Carpenter of Elliott Brothers' Borehamwood Laboratory, together with comments from GCHQ historian Peter Freeman'. Lavington also has other informants.
[22] H.J. (John) Crane, a GCHQ engineer, quoted in Lavington, 'Oedipus', 46. Peter Freeman (on "functionality") quoted in Lavington, 'Oedipus', 46.
[23] Lavington, 'Oedipus', 46.
[24] Lavington, 'Oedipus', 46.
[25] Lavington, 'Oedipus', 47.
[26] His data compares KIPS and storage (in kBytes) of Oedipus with those of the Ferranti Mark I Star, IBM 704, the English Electric DEUCE, the Ferranti Pegasus and Ferranti Mercury.
[27] Aldrich, *GCHQ*, 348.
[28] Aldrich, *GCHQ*, 348.
[29] Burke, *Magic*, 303.
[30] Aldrich, *GCHQ*, 219.
[31] It was also helped by personal connections. Hampshire had worked for SIS during the Second World War, while 'Clive Loehnis and his deputy Joe Hooper … were greatly helped by the fact that Burke Trend, a fan of secret service, moved from the Treasury to replace Norman Brook as Cabinet Secretary in 1963'. Aldrich, *GCHQ*, 219.
[32] In the 1970s, GCHQ's 'Registry held a massive twenty-three thousand shelf feet of records generated by GCHQ's twenty different divisions, and was adding four thousand files every year. The Registry predicted that it would hit a quarter of a million files by the year 2000. Matters were made worse by the determination of each division to keep its own over-stuffed registry'
[33] Aldrich, *GCHQ*, 343.
[34] Aldrich, *GCHQ*, 353.
[35] TNA CAB 163/119. Joe Hooper to Dick White, 3 March 1969.
[36] Aldrich, *GCHQ*, 351.
[37] Aldrich, *GCHQ*, 351.
[38] 'By 1974, Dick White's successors as Intelligence Coordinator would be looking to computers in a desperate effort to cut staff numbers in the face of swingeing cuts to the intelligence and defence budgets'. Aldrich, GCHQ, 354.
[39] Aldrich, *GCHQ*, 351.
[40] Aldrich, *GCHQ*, 458. Ceruzzi, 'Historians failing', notes the importance of text-processing for the secret state.
[41] TNA CAB 182/95. Minutes, JIC(ADP) 4 February 1976.
[42] Aldrich, *GCHQ*, 526. The mind-set influenced the initial design of the Benhall building.
[43] Aldrich, *GCHQ*, 122.
[44] The quotation is from Aldrich, GCHQ, 122. The naval parallel is discussed in Eric Grove, 'Naval command and control equipment: the birth of the late twentieth-century "Revolution in Military Affairs", in Robert Bud and Philip Gummett, *Cold War Hot Science*, Amsterdam: Harwood Academic Press, 1999, 251-262. For relations between the Admiralty and Elliott Brothers (London) Ltd, see: Simon Lavington, 'Swords and ploughshares: connections between computer projects for war and peace, 1945-55', *Dependable and Historic Computing* (2011) 6875, 313-322.
[45] Aldrich, *GCHQ*, 267.

[46] Aldrich, *GCHQ*, 267.
[47] Aldrich, *GCHQ*, 172.
[48] Aldrich, *GCHQ*, 340.
[49] Aldrich, *GCHQ*, 507.
[50] Lavington, 'Oedipus', 54.
[51] Lavington, 'Oedipus', 54. See also: Simon Lavington, *Moving Targets: Elliott-Automation and the Dawn of the Computer Age in Britain, 1947-67*, Springer, 2011.
[52] Aldrich, *GCHQ*, 349.
[53] Burke, *Magic*, 5.
[54] Burke, *Magic*, 278
[55] Paul Edwards, *The Closed World: Computers and the Politics of Discourse in Cold War America*, Cambridge. MA: MIT Press, 1996.
[56] Burke, *Magic*, 305.
[57] Marshall Carter quoted in Aldrich, *GCHQ*, 350.
[58] TNA CAB 182/81. Minutes, JIC(A)(ADP)(72) meeting, 19 June 1972.
[59] TNA CAB 182/81. Minutes, JIC(A)(ADP)(72) meeting, 23 October 1972.
[60] Lavington, 'Oedipus', p. 53.
[61] Aldrich, *GCHQ*, 220, 348.
[62] Andrews, *Defence*, 228.
[63] TNA CAB 163/119. JIB, 'Automation', 1961.
[64] TNA CAB 163/119. David Evans (MoD) to F.B. Richards (Cabinet Office), 19 January 1968.
[65] TNA CAB 163/119. Minutes, 'Working party on computers', 3rd meeting, 14 December 1967.
[66] TNA CAB 163/119. Minutes, 'Working party on computers', 2nd meeting, 22 November 1967.
[67] TNA CAB 163/119. Allinson to Bristow, 25 February 1969.
[68] Dick White in the early 1970s 'had persuaded the Joint Intelligence Committee to get busy in the area of new technology. Brian Stewart, Secretary of the JIC, created a joint team on Automatic Data Processing which also comprised MI5, SIS, the Defence Intelligence Staff and the Foreign Office. Teddy Poulden from GCHQ was given the job of chairing it'. Aldrich, *GCHQ*, 353.
[69] TNA CAB 182/95. Minutes, JIC(ADP) 4 February 1976.
[70] Aldrich, *GCHQ*, 527, 528.
[71] Aldrich, *GCHQ*, 353.
[72] TNA CAB 182/58. Notice of talk on machine translation by unnamed CIA visitor, 22 June 1966.
[73] TNA CAB 182/58. 'NATO machine translation automation project', 12 November 1968.
[74] Janet Abbate, *Inventing the Internet*, Cambridge, MA: MIT Press, 2000.
[75] TNA DSIR 30/141. J. McDaniel, A.M. Day, W.L. Price, A.J.M. Szanser, S. Whelan and D.M. Yates, 'Translation of Russian scientific texts into English by computer', Auto 35, July 1967.
[76] McDaniel et al, 'Translation', 1, my emphasis.
[77] McDaniel et al, 'Translation', 63-64.
[78] After the JIC sub-committee on ADP had been set up in 1969, with core members GCHQ, MI5, MI6 and MoD, there was immediate interest from the Home Office. It was agreed that 'In view of the growing interest of the Home Office in the application of computer techniques in police work and their desire to draw on the experience of the intelligence community in analogous areas, the Home Office should be informed of the existence of the new JIC(A) sub-committee on Automatic Data Processing and be invited to consult it when necessary'. TNA CAB 163/119. JIC(A), Sub-Committee on Automatic Data Processing. Note by Fewtrell, undated (1969).
[79] TNA HO 303/76. Hudson to McCaffrey, 10 February 1969. For the history of police computing, see: Chris A. Williams, *Police Control Systems in Britain, 1775-1975: From Parish Constable to National Computer*, Manchester: Manchester University Press, 2014.
[80] TNA CAB 182/58. Minutes, JIC(A)(WP)(68)1st, 8 April 1968.
[81] TNA CAB 182/58. Minutes, JIC(A)(WP)(68)1st, 8 April 1968.
[82] TNA HO 377/238. R. Stevens, 'A proposal for the development of an automatic vehicle number plate reader', 1976.
[83] The 'security problems were twofold. Firstly there was the question of radiation security and in this field M.37 of GCHQ were in touch with the Security Service. There was also the problem of encryption' TNA CAB 182/58. Minutes, JIC(A)(WP)(68)1st, 8 April 1968.

[84] Aldrich, *GCHQ*, 209. One consequence was that the United States undertook to supply allies with improved, but expensive cypher machines. This was also done partly to stop Western countries developing their own machines.
[85] TNA CAB 182/58. Minutes, JIC(A)(WP)(66)1st, 2 May 1966.
[86] TNA CAB 182.81. Minutes, JIC(A)(ADP)(72)2nd, 19 June 1972.
[87] TNA CAB 182/81. JIC(A)(ADP)(72)3rd, 23 October 1972.
[88] TNA CAB 182/58. 'Secure remote access terminals. Progress report by GCHQ', 15 January 1969.