Bletchley Park and the Development of the Rockex Cipher Systems: Building a Technocratic Culture, 1941–1945

Smith, C

Original citation & hyperlink:
Smith, C 2017, 'Bletchley Park and the Development of the Rockex Cipher Systems: Building a Technocratic Culture, 1941–1945' *War in History*, vol 24, no. 2, pp. 176-194
https://dx.doi.org/10.1177/0968344515613539

DOI 10.1177/0968344515613539
ISSN 0968-3445
ESSN 1477-0385

Publisher: Sage

Bletchley Park and the Development of the Rockex Cipher Systems: Building a Technocratic Culture, 1941–1945

The Government Code and Cypher School (GC&CS), housed at Bletchley Park during the Second World War, has widely been acknowledged to have been a major hub of wartime technological research. Despite its reputation for technocracy, until relatively late in the war the design and construction of technology by the agency was conducted in an *ad hoc* and piecemeal fashion to address specific problems. More generally, the agency's initial approach to its mandate (the reading of communications traffic of foreign powers and the security of Britain own traffic) was notable for its collegiate amateurism. Yet, in 1943, it undertook a machine development project which was very different from the technology projects which had preceded it because it was characterised by professionalism and long-term planning. That project was the Rockex cipher system, and it marked the culmination of a wider cultural transformation in the wartime agency as it moved towards professionalism. That Bletchley Park underwent transformation has been well established and some of the important social and bureaucratic aspects of these changes have been considered in detail.[1] However, the actual processes of cultural change within the agency, resulting in professionalisation and mechanisation, still remain poorly understood. This article, utilising the Rockex project as a case study will outline those processes, moreover it will demonstrate that the project itself played a hitherto unrecognised key role as a catalyst in that process.

At the beginning of the Second World War, GC&CS was woefully unprepared for the contest that would come over following six years. The agency had been crippled by retrenchment following the

[1] Christopher Grey, *Decoding Organization: Bletchley Park, Codebreaking and Organization Studies* (Cambridge, Cambridge University Press, 2012); Christopher Smith, A Social History of Bletchley Park, 1939-1945 (Unpublished PhD Thesis, Aberystwyth University, 2012).

First World War, and had only gradually rebuilt its resources over the interwar period.[2] In 1939 it had only around 200 staff members, and had little in the way of (or regard for) cutting edge technology.[3] It was largely staffed by a contingent of Oxbridge graduates educated in the Arts and Classics, and a modest clerical and administrative team.[4] Yet, by the end of the war it employed over 10,000 staff members, was a world leader in technology, and had expanded its ranks to incorporate increasing numbers of mathematicians, scientists, engineers, and professionals from the business world. As Jon Agar notes, by 1944 it had transformed from a collegiate organisation modelled on the university common-room into a highly sophisticated information processing factory, and that mechanisation was key to that evolutionary process.[5] The challenges of the Second World War had forced the agency constantly to adapt to changing circumstances to stay ahead of its rivals in the information war. Gradual professionalisation and mechanisation were the products of that process. The organization theorist Christopher Grey has outlined how the agency was able to introduced mechanised factory-like, sections while also retain considerable elements of its pre-war character. At least some of the collegiate quality of several core sections of the agency remained intact, and both types of section were utilised in conjunction over the course of the war. The result was that the culture of the agency was a composite or, as Grey describes it, a 'matrix', that brought together numerous different groups determined by differing social classes, backgrounds, educations, ages, and professions.[6] Meanwhile, for Agar, Bletchley Park serves as an example of wider transformation across government as a whole, a result of the growth of an increasingly powerful scientific specialist middle rank of the civil service, with a technocratic ideology, who were able to

---

[2] Ralph Bennett, *Behind the Battle: Intelligence in the war with Germany, 1939-1945* (London, Pimlico, 1994, 1999), p. 32. For further details regarding the position of British intelligence prior to the outbreak of war, see: Wesley K. Wark, *The Ultimate Enemy: British Intelligence and Nazi Germany, 1933-1939* (Ithaca, NY, Cornell University Press, 1985); Richard Overy, 'Strategic Intelligence and the Outbreak of the Second World War', *War in History*, V (1998), 451-480.

[3] Christopher Smith, 'How I Learned to Stop Worrying and Love the Bombe: Machine Research and Development and Bletchley Park', *History of Science*, LII (2014), p. 208.

[4] Alistair Denniston, 'The Government Code and Cypher School between the wars', *Intelligence and National Security*, I (1986), pp. 48-70.

[5] Jon Agar, *The Government Machine: A Revolutionary History of the Computer* (Cambridge, MA, MIT Press, 2003), p. 209.

[6] Grey, *Decoding Organization*, p.166.

mechanise processes of the state.[7]

Profound though the introduction of machines to the agency was, it is necessary to recognise that these devices were only tenuous solutions to the problems the agency faced; minor alterations in the cryptographic techniques of the Axis powers would render the agency's machines obsolete. The result was that, in spite of their successes with machines, by 1943 important technocratically-minded individuals within the agency's management, such as the mathematician Gordon Welchman, viewed the agency's history of building and incorporating machines with growing dissatisfaction. The technocrats within the agency represented a new breed of cryptanalyst and manager. Where the agency's traditional hunting grounds for recruits had been the humanities departments of Britain's ancient universities, in wartime the agency instead increasingly turned to mathematicians. The result was that some of these individuals had technical and mechanical skills that led to the agency's early mechanisation programme. The process of mechanisation they initiated was transformative but gradual, and by the end of the war the agency was instead characterised by professionalism, and by its strong emphasis on planning and mechanised industrialism. So considerable was this transformation that Britain was to emerge in 1945 as a world leader in communications security and cryptanalysis, complete with cutting edge technologies.[8] The project to build Rockex family of cipher machines marked a hitherto unrecognised turning point that process of transformation. When the agency adopted the project in 1943, the cultural changes that had been underway since 1939 were catalysed, and the project was identified by men like Welchman as a new beginning for the agency.

---

[7] Agar, *The Government Machine*, p. 414.

[8] John Ferris, *Intelligence and Strategy: Selected Essays* (Abingdon, Routledge, 2005), p. 180. The intelligence gathered by the agency was also of considerable significance to the Allied war effort, so much so that the intelligence historian Christopher Andrew has felt able to contend that it shortened the war and 'saved millions of lives'. Christopher Andrew, *Secret Service: the Making of the British Intelligence Community* (Sevenoaks, Sceptre, 1986), p. 679.

On a technical level, the Rockex project itself marked the next step in the evolution of machine cryptography.[9] Where the previous generation of cipher machines typically utilised rotors as the primary means to scramble messages, Rockex utilised teleprinter technology to jumble two streams of data together. Significantly, the project also marked the next step in how the agency went about designing and introducing new machines. The project incorporated the lessons of machine design and implementation learned earlier in the war, but more importantly was seen as an opportunity to serve as a test case for future projects. Moreover, unlike previous wartime machine development projects, the Rockex was designed with long-term objectives in mind; the security of British communications well into the post-war period.

By 1943 GC&CS was in a position to approach the process of mechanisation in the manner suggested by its technocrats; with a clear emphasis on planning and testing. Its successes had won the agency the respect of Whitehall and the armed services, but more importantly the gradual cultural transformation towards professionalisation had progressed sufficiently to allow the Rockex project to serve as a trial for extending that professionalism to the key area of mechanisation, and the project itself served to further catalyse that process. Machine research and development had at last taken centre stage in the agency's vision for its long-term future.

Mechanising the Government Code and Cypher School

GC&CS had come a long way by 1943. The agency, born in 1919, was an amalgamation of the Admiralty's First World War cryptanalytic bureau, Room 40, and its War Office counterpart, Military Intelligence 1B. The two bureaus had been relatively modest institutions during the First

[9] Ferris, *Intelligence and Strategy*, p. 176.

World War; Room 40, for example, had some 100 staff members on its books at its height.[10] However, the newly formed GC&CS suffered under post-war retrenchment and began life with just 56 staff members.[11] Over the twenty years from its inception to the outbreak of the Second World War, the agency had profited only little from Britain's rearmament policy, and, as noted above, when GC&CS relocated to Bletchley Park in 1939 it still employed only 200 staff.[12] Moreover, most of these were relatively new to the agency, having been recruited in the late 1930s as the international situation became increasingly tense.[13] The result was that GC&CS was unprepared for the challenges posed by a new global conflict. A significant problem was that over the course of the inter-war period communications security had undergone a major transformation. During the First World War ciphers had been non-mechanical, but during the inter-war period the Axis powers had introduced highly sophisticated mechanical cipher systems, the most famous of these being Enigma.

Enigma posed an unprecedented problem for cryptanalysts. The system revolutionised cipher security by offering portability, relatively swift operation, and an extremely high degree of security. Indeed, the system was so secure that British cryptanalysts swiftly arrived at the conclusion that it unbreakable and invested their energies in other less secure communications networks, in particular Soviet traffic.[14] In the late 1930s, the only potential means that the agency could see to make major headway with Enigma was to place faith in technology: the problem posed by a mechanical cipher machine required a mechanical solution.[15] However, at that time, GC&CS had no such technology,

---

[10] Brian Oakley, *The Bletchley Park War: Some Outstanding Individuals* (Bletchley, The Bletchley Park Trust, 2006), p. 2.
[11] Denniston, 'Government Code and Cypher School', p. 50.
12 Kerry Johnson and John Gallehawk, eds., *Figuring It Out at Bletchley Park 1939-1945* (Milton Keynes, Booktower, 2007), pp. 3-14.
[13] Denniston, 'Government Code and Cypher School', pp. 50-53.
[14] Michael Smith, 'The Government Code and Cypher School and the First Cold War', in Michael Smith and Ralph Erskine, eds., *Action This Day:Bletchley Park from the breaking of the Enigma Code to the birth of the modern computer* (London, Bantam Press, 2001), pp. 15-40.
[15] Frank Birch, *The Official History of Sigint*, vol. 1 (part 1), John Jackson, ed. (Military Press, Milton Keynes, 2004),

and neither did it have the technically proficient staff to design one, nor the inclination let alone resources to put any such design into production. The looming hostilities in the final months of the inter-war period demanded a reconsideration of this position.[16]

A shift towards mechanising cryptanalysis was generate shortly before the German invasion of Poland, when a conference between British, Polish and French cryptanalysts was organised. Unbeknownst to GC&CS, Polish cryptanalysts, of course worried by a resurgent and increasingly militaristic and expansionist Germany, had been investigating Enigma to.[17] Unlike the British, however, the Poles had heavily invested in the problem and applied their most proficient young cryptanalysts to addressing it. Like their British counterparts in GC&CS, the Poles concluded that the development of new mechanical cryptanalytic technology was essential not merely to break the variants of Enigma being used at that time by the German military services, but to break it regularly and in a sufficiently timely fashion to allow the Polish intelligence service to make use of the information gained. However, unlike the British, the Polish cryptanalysts had set about designing and developing just such a machine, namely the Bomba.[18]

The fact that the Poles had designed, built and begun successfully to utilise a custom-made cryptanalytic machine to address the new problems posed by mechanised ciphers, while GC&CS

---

p. 20. This volume, in addition to its counterpart, vol. 1 (part 2) & vol. 2, John Jackson, ed. (Military Press, Milton Keynes, 2007), is a published reproduction of an internal history of the GC&CS held at the National Archives, Kew (TNA). Frank Birch, History of British Sigint, 1914-1945, TNA, HW 43/1–2.

[16] Hugh Foss, 'Reminiscences on Enigma', in Michael Smith and Ralph Erskine, eds., *Action This Day:Bletchley Park from the breaking of the Enigma Code to the birth of the modern computer* (London, Bantam Press, 2001), pp. 41-46.
[17] R. A. Ratcliff, *Delusions of Intelligence: Enigma, Ultra, and the End of Secure Ciphers* (Cambridge, Cambridge University Press, 2006), p. 2.
[18] Gordon Welchman, 'From Polish Bomba to British Bombe: The Birth of Ultra', in Christopher Andrew, ed., *Codebreaking and Signals Intelligence* (London, Frank Cass, 1986), p. 73.

had identified the same problem and solution but had progressed no further, reflected the difference in the respective nations' intelligence cultures. After the First World War, the newly-formed GC&CS had modelled itself on its predecessor organisations, primarily Room 40, and retained the same modes and methods of recruitment. Emphasis was placed on the recruitment of like-minded individuals to those already in post: primarily linguists and classicists from Britain's ancient universities.[19] The problem of mechanical cipher systems was to change this policy. In the late 1930s it became increasingly obvious that a new breed of cryptanalyst, individuals with mathematical expertise, were required. While some mathematicians had been recruited to work as cryptanalysts since the late 1920s, in the run up to the Second World War the agency's recruiters increasingly turned to the mathematics departments of Britain's universities.[20] The Poles, on the other hand, placed a primacy on the recruitment of mathematicians from the moment that their serious investment in cryptanalysis began. The recruitment of highly accomplished mathematicians brought to the Polish camp a range of skills and approaches to the Enigma problem that Britain's cryptanalysts, even with their experience from the First World War, could not bring to bear. In particular, the Polish mathematicians possessed a technical understanding of mechanics and engineering which would allow the development of cryptanalytic technology like the Bomba.

The revelation that cryptanalytic machinery could be developed, and the influx of scientists and mathematicians into the agency in the late 1930s, chief among them the young Cambridge University mathematicians Alan Turing and Gordon Welchman, provided GC&CS the opportunity to emulate the Polish example.[21] Nevertheless, despite the clear necessity of developing machine

---

[19] Christopher Andrew, 'F. H. Hinsley and the Cambridge Moles: two patterns of intelligence recruitment' in Richard Langhorne, ed., *Diplomacy and Intelligence During the Second World War, Essays in Honour of F. H. Hinsley* (Cambridge, Cambridge University Press, 1985), p. 35.

[20] Smith, A Social History of Bletchley Park, pp. 97-101. See also, Christopher Andrew, *Secret Service: The Making of the British Intelligence Community* (Sevenoaks, Sceptre, 1986), p. 634.

[21] Andrew Hodges, *Alan Turing: The Enigma* (London, Vintage, 1983, 2012), pp. 175-176.

technology to counter the Enigma problem, there remained little enthusiasm to break with tradition and develop a British machine to attack Enigma. It was only the perseverance of Turing, Welchman, and a very few members of GC&CS's 'Old Guard' who saw the potential in mechanised solutions to the Enigma problem, that led the development of the British Bombe (named in honour of the Polish Bomba, its spiritual, though not technical, predecessor).[22]

The genesis of the Bombe machine, designed by Turing and further upgraded by Welchman, proved a major technical breakthrough for GC&CS and transformed its ability to rapidly break and read Enigma traffic. However, before mass production of the machine could be undertaken, three major structural changes to the agency were necessary. First, the agency had to forge important links with external institutions capable of turning the ideas behind the machine into a mechanical reality. The agency had neither the engineering expertise nor the factory facilities to build Bombe machines, still less to produce them in substantial numbers on a regular basis. To facilitate a building programme, the agency turned to the British Tabulating Machine Company and its workshops housed in Letchworth.[23] Second, the agency also required a substantial staff contingent to operate the machines. This was absolutely imperative: for each machine that arrived from BTM's production line, at least ten staff were required to operate it on a 24-hour basis.[24] Furthermore, once the Bombe machines began rapidly to accelerate the rate at which GC&CS could produce viable intelligence, greater bureaucratisation of the agency was necessary. Further staff were required to perform the substantial additional administrative and clerical work arising, and to establish a major communications machine section to distribute a large amount of information to Whitehall and commands in the field. Fortunately, GC&CS was able to draw upon the sizable pools of labour at the disposal of its client ministries. In the case of Bombe operation, the agency requested that the

[22] Welchman, 'Polish Bomba to British Bombe', p. 72.
[23] For a full discussion of the role of BTM in the production of Bombe machines see: John Keen, *Harold 'Doc' Keen and the Bletchley Park Bombe* (Kidderminster: B & B Baldwin, 2012).
[24] Diana Payne, 'The Bombes', in F. H. Hinsley and Alan Stripp, eds., *Codebreakers: The Inside Story of Bletchley Park* (Oxford, Oxford University Press, 1993), p. 133.

Admiralty to provide operators in the form of young women from the Women's Royal Naval Service, while communications staff and clerical workers were drawn from the Women's Auxiliary Air Force and Foreign Office respectively.[25] Third, the amount of Axis traffic intercepted by the British increased rapidly, and beyond the capacity of the new Bombe machines to easily process. In turn, this required the creation of a bureaucratic process to allocate machine time, which would distribute Bombe usage so to prevent GC&CS's machine resources being monopolised by just one of the agency's actual or potential client ministries.[26] Ultimately, GC&CS, in order to successfully utilise its new technology, was slowly to develop an information production line operated on professional factory principles.

This process of professionalisation was, however, by no means smooth. As in the case of developing the Bombe machine, in the first instance there was both resistance and lethargy within the agency when it came to the creation of a bureaucratic body to allocate Bombe time. Indeed, despite the first Bombe machine being delivered to Bletchley Park in 1940, it was not until 1942 that a committee to oversee the allocation of Bombe time was introduced.[27] Also problematically, the machines developed by GC&CS, though ultimately successful, were only barely sufficient to address the volume of traffic that arrived at Bletchley's gates and the complexity of the ciphers which protected that traffic.[28] Minor alterations to Axis cipher procedure, or to technical specifications of the cipher machines, could swiftly render the Bombe machines, and those designed to tackle other cipher systems, ineffective. Moreover, the actual building of machines and development of improvements were processes fraught with difficulty. First, the agency suffered

[25] TNA, HW 50/50, Nigel De Grey, Memorandum, 17 August 1949.
[26] TNA, HW 25/1, C.H.O'D. Alexander, *Cryptographic history of the work on the German Naval Enigma* (no date, c. 1945), p. 37. This document was accessed online courtesy of Graham Ellsbury, http://www.ellsbury.com/gne/gne-000.htm (accessed: 25 June 2013)
[27] TNA, HW 25/1, C.H.O'D. Alexander, *Cryptographic history of the work on the German Naval Enigma* (no date, c. 1945), p. 37.
[28] TNA, HW 62/6, A.D.(Mech) [Gordon Welchman] to Director [Edward Travis], 10 July 1944.

production and supply problems, and machines arrived from Letchworth in only limited numbers until 1943. [29] Though this was not the fault of GC&CS, the lethargy in the implementation of a system to allocate Bombe time served only to aggravate the problem. Second, the agency arranged for two different teams of contractors to work on the development of upgrades for the system and the competition between the rival groups, as well as their champions within the agency, resulted in months of bitter acrimony and delay.[30]

There was also a failure to adequately address the personnel problems derived from mechanisation. First, GC&CS did not receive enough operators, an issue which came to a head in October 1941 when four of the agency's most senior cryptanalysts wrote directly to the Prime Minister, going over the heads of the agency's commanding officer, Alistair Denniston, as well as its Director and head of the Secret Intelligence Service, Sir Stewart Menzies, to request more personnel and resources.[31] However, with increasing personnel came other problems, not least accommodating and feeding workers. In these arenas GC&CS lurched from one administrative crisis to the next as the number of employees increased beyond the capacity of the existing facilities to cope. In each instance, the agency was forced repeatedly and rapidly to develop new solutions to both accommodation and catering as the existing services were pushed to breaking point.[32]

---

[29] John Keen, *Harold 'Doc' Keen and the Bletchley Park Bombe* (Kidderminster, M & M Baldwin, 2012), p. 42

[30] TNA, HW 62/5, Gordon Welchman to A.D.(S) [Nigel De Grey], 4 June 1943.

[31] A. M. Turing, W. G. Welchman, C. H. O'. D. Alexander, P. S. Milner-Barry to Winston Churchill, 21 October 1941, reproduced in Michael Smith and Ralph Erskine, eds., *Action This Day: Bletchley Park from the breaking of the Enigma Code to the birth of the modern computer* (London, Bantam Press, 2001), pp. ix-xii.

[32] For examples see: TNA, HW 64/56, Alistair Denniston, Catering, 21 September 1941; TNA, HW 64/56, A. D. Bradshaw, Sandwich Lunches, 12 March 1942; TNA, HW 64/65, A.D. Bradshaw, Cafeteria, 18 April 1944. Regarding accommodation, many war workers were billeted in the homes of local residents and by 1943 rooms had become sufficiently scarce that the Bletchley Urban District Council had begun considering taking legal action against residents who refused to co-operate. Centre for Buckinghamshire Studies, Aylesbury (hereafter CBS), DC 14/1/20, *Minute Book of the Bletchley Urban District Council: 1942-43*, 6 July 1943, p. 43. The solution to this problem was to place war workers in custom built hostels constructed near Bletchley Park. CBS, DC 14/1/20, *Minute Book of the Bletchley Urban District Council: 1943-44*, 8 June 1943, p. 21.

The perennial problem GC&CS faced in the opening years of the war was that its primary mandate, the rapid breaking and subsequent reading of Axis traffic, and required increasingly vast resources and bureaucratic structures. The retrenchment of the inter-war period, and the institutional culture of that period, had left the agency unprepared for the challenges posed by the Second World War. The introduction of mechanised cryptanalytic processes required an exponential increase in both staffing and materiel which agency officials had no experience in either managing or developing. Importantly, the escalation of the war, and with it the rapid increase in the amount of traffic the agency was required to read, meant that systematic envisioning of future requirements was all but impossible, and therefore planning was hindered. The agency was forced to develop *ad hoc* remedies to the problems it faced and the resulting solutions, bureaucratic and technological, were fragile and in need of constant adaptation.

The result was that the agency of 1943 was remarkably different to the agency of 1939. First, it was substantially larger, having accumulated grown from around 200 in 1939 staff to 5,053 by June 1943.[33] Second, the once green lawns and gardens of the Bletchley Park estate had been transformed into a hive of prefabricated huts and concrete blocks. Third, the personnel inhabiting the estate's buildings, once dominated by staff drawn from the universities, primarily comprised young women performing any one of a number of essential low grade functions, from machine operation to administration of the agency's sprawling bureaucracy.[34] Further up the agency's food-chain, the ranks of the cryptanalysts, once dominated by classicists and arts graduates, were now increasingly populated by mathematicians and other scientists. In short, the agency had, in a manner that was almost entirely unplanned, evolved into a vast and unique bureaucracy, centred on effective

[33] Johnson and Gallehawk, eds., *Figuring It Out*, pp. 3-14.
[34] Grey, *Decoding Organization*, pp.173-175.

utilisation of technology. With the lessons of the recent past in mind, the agency would approach the Rockex project with a hitherto unprecedented degree of technocracy and professionalism.

The Rockex System

The Rockex was a machine which utilised teleprinter technology to produce ciphers capable of concealing the content of messages transmitted both by cable and wireless.[35] While this machine still remains has failed to attract the public and scholarly interest of some of GC&CS's other machines, most notably the Bombe machine, it has been some historical study. For instance, the intelligence historian John Ferris, as well as the published internal history of the British Security Coordination, have already summarised the technical specifications and operation of the machine.[36] In addition, Ferris considered the influence of geopolitical and diplomatic environment on the development of Rockex. It is, therefore, beyond the provision of a brief, unnecessary to comment on the machine's technical specifications or origins here. However, missing from Ferris' account is a commentary on the internal cultural forces within the agency, which drove GC&CS towards professionalisation and mechanisation, and had a profound influence on the machine's development. Similarly, also missing is consideration of the role of the Rockex project itself in further catalysing change within the agency's internal culture. In particular, they include Gordon Welchman's dissatisfaction with the agency's previous wartime machine development programme and his efforts to professionalise technological development within the agency.

Specifically, the significance of the Rockex project is that it demonstrates the increasing importance

[35] TNA, HW 62/5, Rockex II, 9 June 1944.

[36] William S. Stephenson, *British Security Coordination: The Secret History of British Intelligence in the Americas 1940-45*, Nigel West, ed. (New York, NY, Fomm International Publishing, 1998). Ferris, *Intelligence and Strategy*, pp. 168-178.

of technology to the wartime agency, the role envisioned for technology in the agency's post-war future, and the machine's position as a major test case for future technological research and development. The system's development highlighted, the perceived problems with the past *ad hoc* approach, demonstrated a clear desire to cut a new path for the future, and showcased a profound shift in the development of the agency's own culture, with technology taking centre-stage.

The Rockex system came into being at a fortuitous moment. By 1942, those branches of the British state with a direct vested interest in the security of British communications traffic – particularly the intelligence agencies, the Foreign Office, Cabinet Office, and Service Ministries – were becoming increasingly concerned about the potential weakness of existing cipher systems. Since the 1930s, the British state's high-grade material was enciphered by the machine cipher system Type-x. Type-x was modelled, albeit with significant security improvements, on the German Enigma system. While the system offered an extremely high degree of security, Britain's own successes against Enigma, which the Axis powers believed was unbreakable, highlighted the dangers of taking security for granted. Some worrying, though unconfirmed, signs were beginning to emerge that Type-x might be vulnerable. Meanwhile, some of Britain's traffic, enciphered using lower graded systems, had certainly been read.[37] Of course, Britain did not need to worry only about enemy powers. There was always the threat that cryptanalysts in the employ of friendly powers might also attempt to read British traffic. Chiefly, despite being Britain's closest ally, of creasing concern was the United States of America.[38] Though coming to the realm of signals intelligence somewhat late, by 1943 the US had developed significant cryptanalytic capabilities – and British security specialists had become

[37] Bradley F. Smith, *The Ultra-Magic Deals: And the Most Secret Special Relationship, 1940-1946* (Novato, CA, Presidio Press, 1992), pp. 173-175; Richard J. Aldrich, *GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency* (London, Harper Press, 2010), pp. 54-57.
[38] TNA, CAB 122/561, Commander Dawnay, Memorandum for Brigadier Redman, 24 April 1943.

convinced that if a US effort were made to read British traffic, it could very well succeed.[39]

Clearly then, Britain needed a new system to alleviate the growing sense of unease. The system elected for development was Rockex. Rockex had its origins in an American commercial Teleprinter cipher system, developed by the Western Union Telegraph Company, called Telekrypton. In the most simplistic of terms, Telekrypton enciphered teleprinter traffic. Teleprinters employed a reel of tape to encode a message into teleprinter code, which could then be transmitted by cable. Telekrypton added a second reel of tape, but rather than containing a message, this tape was composed of random data. Combining the data from the two tapes, the resulting information was seemingly meaningless. A receiving machine armed with a duplicate reel of the same random tape could subtract the random data, leaving behind only the original message. Without a Telekrypton machine primed with an identical reel of random data, nobody could conceivably read the message. However, Telekrypton had two major problems. First, the machine was technically overly complex and prone to mechanical failure. Second, the tape containing random data was fed into the machine in a loop. In order to maximise security, and in doing so generate a 'one-time pad' (so named because the cipher's key, generated at random, is used once and only once), the tape needed to be potentially infinite in length.[40]

Despite Telekrypton's clear flaws (which had made it a commercial failure), Benjamin De Forest

---

[39] TNA, HW 25/2 A.P. Mahon, *The History of Hut Eight 1939-1945*, HW 25/2, p. 89. This document was accessed online courtesy of Graham Ellsbury, http://www.ellsbury.com/gne/gne-000.htm (accessed, 25 June 2013). Also see, Ferris, *Intelligence and Strategy*, pp. 168-169. Mistrust between the two allies remained throughout the war. In February 1945, when US officials asked the War Office for information regarding the Secratype cipher system, a project under development for use by army units in the field, the Cypher Policy Board recommended that all such requests regarding research on British cipher systems be rebuffed and pointed out that the US had not supplied any similar information regarding their own systems. Clearly, the Cypher Policy Board was sufficiently satisfied with the security of their new systems (and equally optimistic regarding future projects) and did not wish to jeopardize that by sharing technical details even with the US. TNA, CAB 21/2522, Minutes of Fourth Meeting of Cypher Policy Board, [no day] February 1945.

[40] Such is the strength of a one-time pad that it is mathematically impossible for a cryptanalyst to break such a cipher. Therefore, a randomly generated stream of data of infinite length constitutes just such a key.

'Pat' Bayly, a Canadian professor of Electrical Engineering, still saw some potential in the system. Bayly had been recruited in 1941 by British Security Coordination (BSC), the Secret Intelligence Service's (SIS) arm in the US, to run its communications network, transmitting messages between London and New York via Ottawa. The volume of this traffic, and bottle-necks in the existing network, were causing delays. Bayly determined that a new mechanical apparatus, which would increase the speed at which messages were enciphered and forwarded from Ottawa, was necessary. He concluded that, by remodelling Telekrypton, and eliminating its flaws, he could make the system serve as an elegant solution to his problem. Consequently, Bayly set about stripping the machine of unnecessary parts and redesigning it to operate as a one-time pad system. However, before the system could be effectively used to transmit transatlantic traffic, Bayly needed to devise a method of converting teleprinter data into a form of data capable of being transmitted via wireless and in the medium of Morse Code. Teleprinter code employed 32 characters, but Morse only 26, and the additional six characters would, if not removed, corrupt the transmitted text. Bayly was able to solve this problem, and in doing so he created a new cipher system which was relatively rapid and enjoyed the unrivalled security offered by a one-time pad system.[41] The new system was code-named Rockex, though still called Telekrypton in some quarters. Its potential to provide 'complete security' (including against American attack) was advertised across Whitehall.[42]

In addition to his work for BSC, Bayly's expertise in communications technology had led him into contact, in a consultancy role, with GC&CS. Bayly regularly advised the agency on cryptanalytic machinery, and communications systems, and liaised on behalf of the agency with its US counterparts.[43] Unsurprisingly given both GC&CS's own direct interest in the field of

[41] TNA, HW 62/6, CSC, 'Rockex-II', 11 May 1944.

[42] TNA, CAB 122/561, Joint Staff Mission to War Cabinet Offices, 'LETOD 992', 24 April 1943.

[43] For instance, see: TNA, HW 62/5, Gordon Welchman to DD(S) [Commander Edward Travis, director of GC&CS],

communications security, GC&CS took a great deal of interest in Rockex. GC&CS would go on to play a major role in advocating further research and development in the system. The fruit of this additional research and development was Rockex II.[44]

Building Rockex II

Bayly's work on a new cipher system was welcomed by GC&CS from the start because the agency required a secure means of transmitting its own secret wares across the Atlantic. Ferris notes that Commander Edward Travis, Bletchley Park's commanding officer from 1942, visited BSC in New York in January 1943 and was treated to a viewing of Bayly's new machine at the Rockefeller Centre, and that the first prototype of Rockex was shipped to England in the same month.[45] However, some evidence suggests that work on the first prototype did not begin until January 1943 and that it was not until April that a machine was ready for shipping.[46] Regardless, it is clear that GC&CS, in its capacity as Britain's chief cryptographic bureau and (along with SIS) one of the first employers of the system, was involved in monitoring the development of Bayly's machine from the earliest stages of the project.

Rockex allowed almost instantaneous transmission of messages on a one-to-one basis. This meant that important messages could be transmitted very quickly and securely and GC&CS recognised the significance of Bayly's system from the first. Nevertheless, it was clear that the system would require further improvement if it were to take on a greater role in the British communications network. [47] Following Travis's initial viewing of the machine, Bayly set about producing further

16 October 1943; TNA, HW 62/6, DD(S) [Edward Travis] to DNI [Director of Naval Intelligence], 11 January 1944.
[44] TNA, HW 62/6, CSC, 'Rockex-II', 11 May 1944.
[45] Ferris, *Intelligence and Strategy,* p. 172.
[46] TNA, HW 62/5, Appendix: History, present position and future development, 7 December 1943.
[47] Ferris, *Intelligence and Strategy,* p. 173.

prototype machines. Soon after the production of the first prototype, a second was constructed and transatlantic tests began. By May 1943 Rockex began carrying SIS and Ultra messages across the Atlantic.[48]

Of course, because the original Rockex system was designed in order to secure the passage of potentially highly sensitive transatlantic traffic, GC&CS and SIS were not alone in having a vested interest in the utility of Bayly's work. The Cabinet Office, the Admiralty and the Foreign Office in particular also wished to make use of any new system and, like GC&CS, and closely followed the project's progress. The Cabinet Office and the Admiralty both had Rockex machines installed in September 1943.[49] This was not, however, an inevitability. From the perspective of the Cabinet Office, the adoption of the Rockex system was a difficult decision. Other systems emerging in the same period, particularly the American voice-scrambling system 'X-Ray', provided stiff competition to Rockex. Rockex and X-Ray each had their own distinct advantages. X-Ray, on first examination, like Rockex was deemed to provide excellent security. Importantly, it offered the further advantage of allowing officials and ministers to correspond by voice. However, further investigation into X-Ray revealed a number of potential problems from both technical and security perspectives. From the technical point of view, X-Ray muffled voices, creating the potential for a loss of clarity. Meanwhile, from a security perspective, because the system was of American origin, there was the potential that American cryptanalysts might prove able to eavesdrop on the conversations of British officials.[50] The latter proved to be an intolerable risk, and Bayly's system gained the upper hand because it offered security from those who might intercept British traffic − be they enemies or

[48] Ferris, *Intelligence and Strategy,* p. 173.
[49] TNA, CAB 122/561, War Cabinet Office to Joint Staff Mission, 20 September 1943.
[50] TNA, CAB 122/561, Joint Staff Mission to War Cabinet Offices, 17 September 1943.

allies.[51] Clearly, the existence of major rival systems highlighted the importance of both planning and experimentation.

Despite the existence of a potential competitor system, Rockex continued to generate significant interest from across Whitehall. As early as August 1943, Edward Travis, then commanding officer of GC&CS, was providing reports of the system's capability that intrigued Foreign Office officials. They were impressed by the claim that the machine's speed was only 'limited by that obtainable from a good touch-typist, say 50 words a minute.' They also saw considerable utility in the fact that Bayly's modifications to the system allowed it to be used not only to transmit messages directly by telegraph (a feature the Foreign Office had little use for) but also as a standard cipher machine producing a stream of cipher text which could be transmitted via wireless. Additionally, the promise of more improvements to come made Bayly's machine increasingly attractive. As a result of Travis' outline of the system's specifications, the Foreign Office suggested that the system undergo immediate and thorough testing to ensure that it could indeed perform as described.[52] The Foreign Office's request for swift action was the product of two issues. First, the system's promised specifications suggested a very formidable machine. Second, it was projected that the establishment of missions in re-occupied countries would place a great strain on the Ministry's communications infrastructure and staff that could create the 'danger of complete breakdown of cypher communications.'[53]

Bayly's earlier work as a consultant for GC&CS resulted in a growing personal and professional

[51] TNA, CAB 122/561, Joint Staff Mission to War Cabinet Offices, 17 September 1943.
[52] TNA, FO 850/47b, Minutes, Y5031, 31 August 1943.
[53] TNA, FO 850/47b, W.M. Cadrington to 'C' [Sir Stewart Menzies, Director of SIS], 6 September 1943.

friendship between himself and Gordon Welchman, the technocratic, managerially-minded and senior ranking cryptanalyst.[54] In addition to considering mechanical cryptographic problems, one of the key discussions between Welchman and Bayly was on the future of machine cryptography. During a visit by Bayly to GC&CS, he and Welchman forged ahead with the problems inherent in turning Rockex into a viable machine for widespread use by GC&CS and other branches of the British state. The key problem remained the issue of converting Rockex into a system that could produce a cipher transmittable by wireless without corruptions. In a report to Commander Travis, Welchman warned that considerable theoretical work followed by a significant period of testing and experimentation were required before any viable system could be introduced.[55]

When Bayly returned to his post in Canada, he and Welchman kept in touch, and Welchman remained intrigued by the Rockex system and how it could be improved.[56] Work on producing a more robust system of greater flexibility soon developed into the Rockex II project. Bayly continued to liaise with GC&CS, including discussions with Alan Turing as well as Welchman during various trans-Atlantic visits.[57] Work on Rockex II generated swift results, and in December 1943 GC&CS reported on the progress of the project. It commented that 'The fact that it has been possible to design and build machines so quickly and the small amount of trouble that has been encountered in preliminary tests are encouraging indications of the simplicity of probable reliability of the apparatus.' However, this optimistic appraisal of the situation was qualified with the caveat that nevertheless 'there is no doubt that the development has been done in a hurry and that these first machines must be regarded as ~~pre~~-prototypes, and more extensive trials are likely to suggest modification.' It was recommended that, prior to engaging in mass production of the machine,

---

[54] W. G. Welchman, *The Hut Six Story: Breaking the Enigma Codes* (New York, McGraw-Hill, 1982), p. 171.
[55] TNA, HW 62/5, Gordon Welchman to DD(S) [Commander Edward Travis, director of GC&CS], 16 October 1943.
[56] TNA, HW 62/5, Welchman to Bayly, 26 November 1943.
[57] Ferris, *Intelligence and Strategy,* p. 172.

further prototype models be constructed and the experiences gained with these machines be utilised in plans for future Rockex production.[58] Over the next few months of testing, GC&CS's machine development specialists continued to be impressed by the progress made on Rockex II.[59] The initial prototype work on Rockex II continued to be conducted in New York. However, by the summer of 1944 the work had progressed still further and the first prototype machine arrived in England for experimentation in June.[60] The emphasis on experimentation stood in contrast to the earlier processes of technological development utilised by GC&CS. For instance, following the development of the Bombe machine, while also subject to periods of testing and experimentation, early models went into service extremely rapidly with orders placed for more machines, and much of the necessary refining of the apparatus for future models was the result of trial and error on live machines.[61] Rockex II, on the other hand, as shown above, was subjected to a far more rigorous process of refinement before mass-production was to be contemplated.

Once production was underway the task of making one time tape was assigned to the War Office and monitored by GC&CS. Meanwhile, the task of building Rockex-II units was handled by the Radio Security Service at Hanslope Park, under the direction of Brigadier Richard Gambier-Parry, and machines were built there until 31 December 1946.[62] Such were the expectations of the machine that even before the parts for the first model of Rockex II had been assembled, orders for large numbers of machines began flooding in, most notably from the War Office and the Foreign Office. This was likely to prove problematic because the supply of some of the system's key

[58] Strikethrough as per the original document. TNA, HW 62/5, Appendix: History, present position and future development, 7 December 1943.
[59] TNA, HW 62/5, W. G. Welchman to DD(S) [Commander Edward Travis], 15 January 1944.
[60] TNA, CAB 21/2522, Unknown [illegible signature, probably Stewart Menzies] to Sir Edward Bridges, 2 June 1944.
[61] For a full discussion of Bombe development and implementation see: Smith, 'How I learned to stop worrying'.
[62] TNA, AVIA 22/1483, Minutes of the Third "War Office Sub-committee" of the Cypher Machine Development Committee, 30 January 1945; TNA, T 220/1444, Minutes Held at the Offices of the Cypher Policy Board, 22 March 1946,

components was limited.[63] Mass production of Rockex II was also projected to be an expensive undertaking. In June 1944, the Treasury, while amenable to arguments stressing the need for the development of secret machinery, foresaw problems with the substantial cost of building just 50 'experimental' machines. That cost was estimated at £70,000, only £10,000 of which was non-recurring. The Cabinet Secretary, Sir Edward Bridges, wrote that he had 'had an unofficial word on the subject with [Sir Herbert] Brittain of the Treasury, who looks after the non-audit vote, and although he was only too ready to help, it was clear he did not much relish the idea of this expenditure being tabulated under S.S. monies.' Bridges' solution was to suggest that, rather than the costs be charged to the books of the 'S.S.' (presumably the Security Service), they be individually charged to recipient departments and that they be described as 'experimental'. This, as Bridges pointed out, was, in fact slightly misleading. Prototype machines had already undergone significant development and testing.[64] However, it was certainly the case that 50 was a comparatively low number of machines given the growing demand for them from Whitehall departments.

The ‘experimental’ system of financing the construction of machines continued until 1951, when the scale of expenses, approximately £1 million per annum without any formal auditing, made Gambier-Parry ‘uncomfortable’ and he turned to the Treasury for assistance. By 1949, Gambier-Parry had acquired a factory at Borehamwood, Hertfordshire, and had created a highly unorthodox system for hiding the cost of this secret enterprise. By then, money was flowing in from four sources: SIS, the Ministry of Supply, the Diplomatic Wireless Service, and the Commonwealth Relations Office. Of the £1,000,000, £600,000 came from the latter two and went into public bank accounts while the monies from the former two, approximately £400,000, went into two private

[63] TNA, HW 62/6, Brigadier E. I. C. Jacob [Offices of the War Cabinet] to Commander Travis, 30 April 1944.
[64] TNA, HW 62/6, Sir Edward Bridges to Cdr. Travis cc. Capt. Wilson, 2 June 1944.

accounts in Gambier-Parry's own name. The purpose of this 'auditor's nightmare', as a Treasury official described it, was to keep the factory secret. The Treasury's solution was to create a single suspense account operated by the Foreign Office.[65] Of course, during the war and before it began to mount again, this expenditure was (despite the Treasury's initial concerns) comparatively modest, even in relation only to wider spending on cryptanalytic machinery – which Welchman estimated already to have reached £3 million by July 1944.[66]

Of course, the auditing crisis lay in the future and was out of GC&CS's hands; in 1944, the agency did, however, have concerns of its own. Well aware of the fragile nature of the structures the agency had developed, Welchman, by then an Assistant Director at GC&CS and charged with the agency's programme of mechanisation,[67] was determined that the agency learn from the problems it had encountered. Specifically, Welchman wanted a transformation in how the agency went about the design, development and utilisation of new technology. In July 1944, he outlined his vision of GC&CS's future role in Britain's communications security. He acknowledged that the agency's cryptanalytic machinery had only barely been up to the tasks for which they had been designed, that the machine building process had been amateurish, and that the agency had failed to envision the production and logistical problems involved in mass-production of machine technology.[68] His most discerning observation was that cryptanalysis and cryptography were 'far more deeply interrelated than is superficially obvious', and that all future endeavours in the field of cryptography must contain clear input by seasoned, professional cryptanalysts. His suggested remedy was that a small team of carefully chosen individuals, provided with advice from expert technicians, be tasked with

---

65 TNA, T 220/1444, Unknown [illegible signature] to Sir Edward Bridges, 17 July 1951.
66 TNA, HW 62/6, A.D.(Mech) [Gordon Welchman] to Director [Edward Travis], 10 July 1944.
67 TNA, HW 62/6, DD(S) [Commander Edward Travis], Machine Co-ordination and Development Section, 10 September 1943.
68 TNA, HW 62/6, A.D.(Mech) [Gordon Welchman] to Director [Edward Travis], 10 July 1944.

the planning of new cipher machines within the wider context of communications planning. His justification for this decision was:

> partly because of the enormous growth of wireless communications and partly because of the increasing part played by machinery. Cryptography must now merge into the wider problem of providing secure and efficient communications, which must involve coordination between the development of cipher apparatus and the development of communications both on the technical side and the organisational side.

This hard earned awareness, that new technology could not simply be introduced and operate smoothly without sufficient logistical, administrative and bureaucratic systems in place to support its implementation, meant he was keen to ensure that the design, construction programme and utilisation of Rockex II would be a different story. Welchman recognised that the Rockex II, to ensure that Britain had a long-term and robust security system, needed to be the subject of considerable planning, meticulous design, and developed with suitable factory facilities capable of swift mass-production.[69] Welchman clearly won success in his effort to turn the development of Rockex II into a watershed project, in which a new approach to machine research and development was to be undertaken. When he and Bayly sought to begin work on another new cipher machine, a portable field unit, called RM(26), the work was to be conducted along the same lines that Welchman had stipulated for Rockex II. A team of GC&CS's best cryptographers were seconded for six months to work on the project and the aim was, as with Rockex II, to 'embody all the lessons learned during this war' and meet Britain's 'security requirements for many years to come.'[70]

---

[69] TNA, HW 62/6, A.D.(Mech) [Gordon Welchman] to Director [Edward Travis], 10 July 1944.
[70] TNA, CAB 21/2522, Future Machine Development, Unknown [illegible signature] to Sir Edward Bridges, 27 June 1945.

RM(26), despite early promise, was eventually jettisoned before it left the prototype stage because it proved incompatible with US cipher systems.[71] Nevertheless, the approach to work on the system demonstrates the significance of the agency's new professionalised approach to the development of technology, which if well designed and implemented had the potential for years of service before obsolescence, which had been first adopted with the Rockex II project.

It is clear that other senior officials, with a stake in secure communication, had also reached similar conclusions. Six months earlier, in response to successful Axis penetration of some of Britain's less secure cipher systems, the Cypher Policy Board had been established to oversee research, design, production and implementation of communications security systems and protocols.[72] In addition to Sir Stuart Menzies, the head of SIS who acted as chairman, the Board also included GC&CS's director Edward Travis, and from 1945 Welchman was its chief technical adviser.[73] By October 1945, Welchman's prescription, that a dedicated group should manage cipher machine development, was becoming still closer to a reality with the formation of the Cypher Machine Development Committee (CMDC). The CMDC was comprised of numerous senior officials, tasked with communications matters, from across the Service Ministries, the Cypher Policy Board and GC&CS – including Welchman.[74]

As noted, security had become an increasingly important concern throughout the war. Looking back at the issue retrospectively in September 1945, Menzies, in his capacity as chair of the Cypher

[71] Joel Greenberg, *Gordon Welchman: Bletchley Park's Architect of Ultra Intelligence* (London, Frontline, 2014), p. 98.
[72] Aldrich, *GCHQ*, pp. 56-57.
[73] Aldrich, *GCHQ*, p. 57.
[74] For examples of attendees, see: TNA, CAB 21/2522, Minutes of the Fourth Meeting of the Cypher Development Committee, 14 September 1945.

Policy Board, reminded his colleagues of the difficulties Britain's security experts had endured until 1944.

> Members are well aware that we have only maintained the security of British Communications throughout the war with considerable difficulty and that in certain fields, our security has been nothing like as good as it should have been
>
> Although a great deal has been done to improve the situation over the 18 months and the existence of the Cypher Policy Board and its supporting organisation should ensure that British Communications Security is given adequate consideration in future, the position cannot yet be regarded as satisfactory.

Menzies also complained that while GC&CS had considerable expertise in the field of cryptography, throughout the war there had been 'no planned means' to apply that expertise and experience to the 'security of British communications as a whole'. This was a gap that required filling, so that GC&CS could not only provide advice to its client ministries but also to ensure that, in future, the agency's store of knowledge and experience was available to 'planners and operators of Britain's Communications.'[75]

Much like in the case of GC&CS, the wider difficulties faced by British wartime security officials resulted in the measures and organisational apparatus put into place to deal with communications security being less the product of directed guidance and more the product of circumstance. The

[75] TNA, CAB 21/2522, Minutes of 2nd Meeting of Cypher Policy Board - Annex B, 19 September 1945.

failure to establish a central committee, in the form of the Cypher Policy Board, to address the question of communications security, until the final months of the war, is indicative of the wider failure to appreciate the benefits of centralised professional communications security planning across Whitehall until remarkably late in the day.

Conclusions

The development of the Rockex system, and its much improved successor Rockex II, was a lengthy process that saw inter-Service and department cooperation to develop a complex and revolutionary cypher system. The design and manufacture of the machine saw an unprecedented planning process by GC&CS which used the development of the machine as an opportunity to create a benchmark for future machine research and development. Such was the success of these efforts that variants of the Rockex family were still being utilised in some British embassies until at least the 1970s.[76] As Ferris notes, in developing and adopting the machine in the final stages of the Second World War, the British state placed Britain as a world leader in cipher security at the outset of the Cold War.[77]

Prior to the development of Rockex, machine design and research had been a fraught process instigated as a last resort to resolve pressing problems instigated by mounting wartime pressures. Frank Birch, a senior figure within the agency and the author of its internal history written in the early 1950s, complained in that history that the agency's general administration and organisation in 1940 had been like 'a rudderless vessel'. This, he explained, was because when faced with 'a succession of emergencies, only hand-to-mouth empirical improvisations are possible.'[78] This was also very much true of machine development. By 1944, the agency had come to realize and accept

[76] TNA, FO 850/134, Note from Foreign Office Archivist, 16 April 1973.
[77] Ferris, *Intelligence and Strategy*, p. 176.
[78] Frank Birch, *The Official History of Sigint*, vol. 1 (part 1), John Jackson (ed.) (Milton Keynes: The Military Press, 2004), p. 90.

that this relatively last-minute and *ad hoc* approach (though necessary at the time) to developing its machine sections, could not continue. The machines developed under this approach, while enormously successful, were fragile solutions that could be easily undone by minor alterations to Axis cipher security systems or protocols. The experience of machine development had shown that both cryptanalysis and cryptography had entered a new age, and that future success would be predicated not only on the labours of technical experts with bright ideas, but on long term planning, bureaucratic oversight, and the building of logistical structures.

These were lessons that were learned through trial and error and under conditions of enormous pressure to generate results. But, by the final years of the war, the pressures on the agency had been eased by the arrival of American resources and expertise. Furthermore, GC&CS had evolved into a large, professional and mechanised bureau, complete with teams of expert machine designers and builders and contacts with experts in high-end technology industries. The British state as a whole had also radically realigned itself to deal with the problem of developing communications security, with the formation of inter-service and ministry committees dedicated to overseeing and directing the development of cipher security. Without this combined shift in alignment, across the services and the agency, it is impossible to see how a system such as Rockex II could have been developed in the manner that it was. It is clear that GC&CS had transformed from a collegiate agency that had rapidly, and sometimes unwillingly, adopted mechanised solutions to address machine generated problems into an agency which placed massive emphasis on technology complete with an ingrained technocratic culture. The development of the Rockex family of cipher system was the first major product of that transformation.

For the historian looking to understand how and why GC&CS transformed itself from an archaic and beleaguered organisation, into a highly successful, professional and technologically first-rate intelligence agency, the development of the Rockex family of cipher machines is highly revealing. First, by juxtaposing the project with earlier machine development initiatives, Rockex clearly demonstrates the point at which the agency ceased to invest in technology as a last resort to address what had, hitherto, been unassailable problems. Instead, the agency had begun to see its newly forged technological prowess as a fundamental strength, which required careful nurturing and full integration into the agency's plans for the future. Second, the development of Rockex highlights the importance of the somewhat under-recognised connections made by the agency with bodies such as BSC. The agency's ability to recognise invaluable expertise in other quarters, and to cultivate connections with key specialists, such as Bayly, was central to its success.[79] Third, the development of the system show-cases what was, perhaps, the greatest asset the agency possessed: the capacity for honest introspection. Only by careful critical examination of the agency's performance, could GC&CS's senior figures identify key grounds for improvement. The Rockex project, and the emphasis on learning from both successes and failures of the agency's war to that point, was symptomatic of wider professionalising cultural changes within GC&CS that historians are only beginning to unravel.

[79] Despite his clear importance, Bayly's role as a consultant at Bletchley Park remains largely unexplored. Furthermore, even the well-known relationship between GC&CS and The British Tabulating Machine Company, which built the agency's Bombe machines, is the subject of only one book. Keen, *Harold 'Doc' Keen.*