Article

WAR IN HISTORY

War in History
2017, Vol. 24(2) 176–194
© The Author(s) 2017
Reprints and permissions:
sagepub.co.uk/journalsPermissions.nav
DOI: 10.1177/0968344515613539
journals.sagepub.com/home/wih
SAGE

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

Christopher Smith
University of Kent, UK

Abstract

In 1943 Britain's security experts began to investigate the development of new cipher machine technologies. This resulted in the creation of the initial projects to construct the Rockex family of cipher systems. The development of the systems marked a major step in the building of a technocratic culture within Britain's primary wartime cryptanalysis agency, the Government Code and Cypher School housed at Bletchley Park. This article explores the evolution of Bletchley Park's wartime technocratic culture and utilizes the Rockex project as a case study; moreover it establishes the importance of the project as a catalyst of further institutional cultural change.

Keywords

Rockex, Bletchley Park, technocratic culture, signals intelligence, Second World War, Government Code and Cypher School

Since the revelation of the Ultra secret in 1974, the Government Code and Cypher School (GC&CS) housed at Bletchley Park has enjoyed a considerable reputation for technocracy.[1] Yet until relatively late in the Second World War the design and construction of

[1] 'Ultra' was the code name given to intelligence derived from the reading of high-grade Axis communications in the Second World War. The existence of Ultra intelligence

Corresponding author:
Christopher Smith, School of History, Rutherford College, University of Kent, Canterbury, Kent, CT2 7NX, UK.
Email: C.D.Smith@kent.ac.uk

technology by GC&CS was conducted in an ad hoc and piecemeal fashion, addressing specific problems as they arose. The agency's initial approach to its mandate (the reading of communications traffic of foreign powers and the security of Britain's 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 characterized 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 the agency, housed at Bletchley Park during the war, underwent a transformation has been well established, and some of the important social and bureaucratic aspects of these changes have been considered in detail.[2] However, the actual processes of cultural change within the agency which resulted in professionalization and mechanization remain poorly understood. This article, utilizing the Rockex project as a case study, will outline those processes, and will argue that the Rockex project itself served as a major and a hitherto unrecognized catalyst in that transformation.

At the beginning of the Second World War, GC&CS was woefully unprepared for the contest that would come over the following six years. The agency had been crippled by retrenchment following the First World War, and had only gradually rebuilt its resources over the interwar period.[3] In 1939 it had only around 200 staff members, and little in the way of (or regard for) cutting-edge technology.[4] It was largely staffed by a contingent of Oxbridge graduates educated in the arts and classics, and by a modest clerical and administrative team.[5] Yet, by the end of the war it employed over 10,000 staff members,

remained a state secret in Britain until 1974. Ultra was officially acknowledged when the British government approved the publication of the memoir by wartime intelligence officer Group Captain F.W. Winterbotham (*The Ultra Secret*, London, 1974). Since 1974 GC&CS's technical accomplishments have been highlighted in large numbers of books dedicated to the agency. Some of these include: Ronald Lewin, *Ultra Goes to War: The Secret Story* (London, 1978, 1980), p. 58; Brian Johnson, *The Secret War* (London, 1978), p. 327. In the twenty-first century the interest in the agency's technology shows little sign of abating. For example, see: B. Jack Copeland, ed., *Colossus: The Secrets of Bletchley Park's Codebreaking Computers* (Oxford, 2006); Paul Gannon, *Colossus: Bletchley Park's Greatest Secret* (London, 2006).

[2] Christopher Grey, *Decoding Organization: Bletchley Park, Codebreaking and Organization Studies* (Cambridge, 2012); Christopher Smith, *The Hidden History of Bletchley Park: A Social and Organisational History* (London, 2015).

[3] Ralph Bennett, *Behind the Battle: Intelligence in the War with Germany, 1939–1945* (London, 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, 1985); Richard Overy, 'Strategic Intelligence and the Outbreak of the Second World War', *War in History* V (1998), pp. 451–80.

[4] 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.

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

utilized state-of-the-art 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 undergone a transformation from a collegial organization modelled on the university common room into a highly sophisticated information-processing factory, and mechanization was key to that evolutionary process.[6] The challenges of the Second World War had forced the agency to constantly adapt to changing circumstances in order to stay ahead of its rivals in the information war. Gradual professionalization and mechanization were the results. The organization theorist Christopher Grey has outlined how the agency was able to introduce mechanized factory-like sections, while also retaining considerable elements of its pre-war character. At least some of the collegial quality of several core sections of the agency remained intact, and both types of section (collegial and factory-like) were utilized in conjunction with each other 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 characterized by differing social classes, backgrounds, educations, ages, and professions.[7] 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 who, equipped with a technocratic ideology, were able to mechanize processes of the state.[8]

Profound though the impact of the introduction of machines to the agency was, it is necessary to recognize that these devices represented 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 record of building and incorporating machines with growing dissatisfaction. These technocrats represented a new breed of cryptanalyst and manager within the agency. Where GC&CS's traditional hunting grounds for cryptanalysts had been the humanities departments of Britain's ancient universities, in wartime the agency turned increasingly to mathematicians instead. The result was that some of these individuals had technical and mechanical skills that facilitated the agency's early mechanization programme. The process of mechanization they helped initiate was transformative but gradual, and by the end of the war the agency was characterized by professionalism as well as a strong emphasis on planning and mechanized industrialism. So considerable was this change that Britain was to emerge in 1945 as a world leader in communications security and cryptanalysis, complete with cutting-edge technologies.[9] The project of

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

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

[8] Agar, *Government Machine*, p. 414.

[9] John Ferris, *Intelligence and Strategy: Selected Essays* (Abingdon, 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, 1986), p. 679.

building the Rockex family of cipher machines was a central turning-point in the agency's evolution. When the agency adopted the project in 1943, the cultural changes that had been building gradually since 1939 came fully together for the first time, and the project was identified by men such as Welchman as a new beginning for the agency.

On a technical level, Rockex itself marked the next step in the evolution of machine cryptography.[10] Where the previous generation of cipher machines had typically used rotors as the primary means of scrambling messages, Rockex utilized teleprinter technology to jumble two streams of data together. The Rockex project also marked the next step in how the agency went about designing and introducing new machines, incorporating the lessons of machine design and implementation learned earlier in the war. Still more importantly it was seen as a potential test case for future projects. Moreover, unlike previous wartime machine development projects, Rockex was designed with a long-term objective 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 mechanization in the manner suggested by its technocrats – that is, 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 to professionalism had progressed sufficiently to allow the Rockex project to serve as a trial for extending that professionalism to the key area of mechanization, and the project itself acted as a further catalyst in the wider processes of cultural change. Machine research and development had at last taken centre stage in the agency's vision for its long-term future.

I. Mechanizing 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 World War: Room 40, for example, had some 100 staff members on its books at its height.[11] However, the newly formed GC&CS suffered under post-war retrenchment and began life with just 56 staff members.[12] 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.[13] Moreover, most of these were relatively new to the agency, having been recruited in the late 1930s as the international situation became increasingly tense.[14] 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 interwar period communications security had undergone a major transformation.

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

[11] Brian Oakley, *The Bletchley Park War: Some Outstanding Individuals* (Bletchley, 2006), p. 2.

[12] Denniston, 'Government Code and Cypher School', p. 50.

[13] Kerry Johnson and John Gallehawk, eds, *Figuring It Out at Bletchley Park, 1939–1945* (Milton Keynes, 2007), pp. 3–14.

[14] Denniston, 'Government Code and Cypher School', pp. 50–3.

During the First World War, ciphers had been non-mechanical, but during the interwar 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 revolutionized cipher security by offering portability, relatively swift operation, and an extremely high degree of security. Indeed, the system was so secure that British cryptanalysts quickly arrived at the conclusion that it was unbreakable and invested their energies in other less secure communications networks, in particular Soviet traffic.[15] 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.[16] However, at that time, GC&CS had no such technology, 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 interwar period demanded a reconsideration of this position.[17]

A shift towards mechanizing cryptanalysis was generated shortly before the German invasion of Poland, when a conference between British, Polish, and French cryptanalysts was organized. Unbeknown to GC&CS, Polish cryptanalysts, of course worried by a resurgent and increasingly militaristic and expansionist Germany, had been investigating Enigma as well.[18] 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.[19]

The fact that the Poles had designed, built, and begun to successfully utilize a custom-made cryptanalytic machine to address the new problems posed by mechanized ciphers,

[15] 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, 2001), pp. 15–40.

[16] Frank Birch, *The Official History of Sigint*, vol. 1 (pt 1), ed. John Jackson (Milton Keynes, 2004), p. 20. This volume, in addition to its counterpart, vol. 1 (pt 2) & vol. 2, ed. John Jackson (Milton Keynes, 2007), is a published reproduction of an internal history of GC&CS held at the National Archives, Kew (TNA): Frank Birch, History of British Sigint, 1914–1945, TNA, HW 43/1–2.

[17] 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, 2001), pp. 41–6.

[18] R.A. Ratcliff, *Delusions of Intelligence: Enigma, Ultra, and the End of Secure Ciphers* (Cambridge, 2006), p. 2.

[19] Gordon Welchman, 'From Polish Bomba to British Bombe: The Birth of Ultra', in Christopher Andrew, ed., *Codebreaking and Signals Intelligence* (London, 1986), p. 73.

while GC&CS 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 organizations, 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.[20] 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, was 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.[21] The Poles, on the other hand, placed a primacy on the recruitment of mathematicians from the moment that their serious investment in cryptanalysis began. Taking on 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.[22] Nevertheless, despite the clear necessity of developing machine 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 mechanized solutions to the Enigma problem that led to the development of the British Bombe (named in honour of the Polish Bomba, its spiritual, though not technical, predecessor).[23]

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

[20] 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, 1985), p. 35.

[21] Christopher Smith, 'A Social History of Bletchley Park', unpublished PhD Thesis, Aberystwyth University, 2013, pp. 97–101. See also Christopher Andrew, *Secret Service: The Making of the British Intelligence Community* (Sevenoaks, 1986), p. 634.

[22] Andrew Hodges, *Alan Turing: The Enigma* (London, 2012, 1st publ. 1983), pp. 175–6.

[23] Welchman, 'From Polish Bomba to British Bombe', p. 72.

produce them in substantial numbers on a regular basis. To facilitate a building programme, the agency turned to the British Tabulating Machine Company (BTM) and its workshops housed in Letchworth.[24] 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.[25] Furthermore, once the Bombe machines began to rapidly accelerate the rate at which GC&CS could produce viable intelligence, greater bureaucratization 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 Admiralty 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.[26] Third, because the amount of Axis traffic intercepted by the British increased rapidly and beyond the capacity of the new Bombe machines to process easily, the creation of a bureaucratic process was required to allocate machine time which would distribute Bombe usage, in order to prevent GC&CS's machine resources being monopolized by just one of the agency's actual or potential client ministries.[27] Ultimately, GC&CS, in order to successfully utilize its new technology, was slowly to develop an information production line operated on professional factory principles.

This process of professionalization 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.[28] 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.[29] 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

[24] 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, 2012).

[25] Diana Payne, 'The Bombes', in F.H. Hinsley and Alan Stripp, eds, *Codebreakers: The Inside Story of Bletchley Park* (Oxford, 1993), p. 133.

[26] TNA, HW 50/50, Nigel De Grey, Memorandum, 17 August 1949.

[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. This document was accessed online courtesy of Graham Ellsbury: http://www.ellsbury.com/gne/gne-000.htm [accessed 25 June 2013].

[28] Ibid., p. 37.

[29] TNA, HW 62/6, A.D.(Mech) [Gordon Welchman] to Director [Edward Travis], 10 July 1944.

suffered production and supply problems, and machines arrived from Letchworth in only limited numbers until 1943.[30] 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.[31]

There was also a failure to adequately address the personnel problems derived from mechanization. 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 (SIS), Sir Stewart Menzies, to request more personnel and resources.[32] 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.[33]

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, required increasingly vast resources and bureaucratic structures. The retrenchment of the interwar 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 mechanized 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

[30] Keen, *Harold 'Doc' Keen*, p. 42

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

[32] 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, 2001), pp. ix–xii.

[33] 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 cooperate. 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.

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 from the agency of 1939. First, it was substantially larger, having grown from around 200 staff in 1939 to 5,053 by June 1943.[34] 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.[35] 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 utilization 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.

II. The Rockex System

The Rockex was a machine which utilized teleprinter technology to produce ciphers capable of concealing the content of messages transmitted by both cable and wireless.[36] While this machine has failed to attract the public and scholarly interest of some of GC&CS's other machines, most notably the Bombe machine, it has received some historical study. For instance, the intelligence historian John Ferris, as well as the published internal history of British Security Coordination (BSC), has already summarized the technical specifications and operation of the machine.[37] In addition, Ferris considered the influence of the geopolitical and diplomatic environment on the development of Rockex. However, missing from his account is a commentary on the internal cultural forces within the agency which drove GC&CS towards professionalization and mechanization, 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, Gordon Welchman was dissatisfied with the agency's previous wartime machine development programme, and was keen to use the Rockex project as a means to professionalize technological development within the agency.

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

[34] Johnson and Gallehawk, eds, *Figuring It Out*, pp. 3–14.

[35] Grey, *Decoding Organization*, pp. 173–5.

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

[37] William S. Stephenson, *British Security Coordination: The Secret History of British Intelligence in the Americas, 1940–45*, ed. Nigel West (New York, NY, 1998). Ferris, *Intelligence and Strategy*, pp. 168–78.

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.[38] 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 of increasing concern, despite being Britain's closest ally, was the United States of America.[39] Though it had come to the realm of signals intelligence somewhat late, by 1943 the US had developed significant cryptanalytic capabilities – and British security specialists had become convinced that if a US effort were made to read British traffic, it could very well succeed.[40]

Clearly, then, Britain needed a new system to alleviate the growing sense of unease. The system elected for development was Rockex, which 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,

[38] Bradley F. Smith, *The Ultra-Magic Deals: And the Most Secret Special Relationship, 1940–1946* (Novato, CA, 1992), pp. 173–5; Richard J. Aldrich, *GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency* (London, 2010), pp. 54–7.

[39] TNA, CAB 122/561, Commander Dawnay, Memorandum for Brigadier Redman, 24 April 1943.

[40] 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/hut8/hut8-000.htm [accessed 25 June 2013]. Also see Ferris, *Intelligence and Strategy*, pp. 168–9. 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 its own systems. Clearly, the Cypher Policy Board was sufficiently satisfied with the security of its 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.

but rather than containing a message, this tape was composed of random data. The information resulting from the combined data from the two tapes 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 maximize security, and in doing so generate a 'one-time pad' (so named because the cipher's key, generated at random, is used only once), the tape needed to be potentially infinite in length.[41]

Despite Telekrypton's clear flaws (which had made it a commercial failure), Benjamin De Forest 'Pat' Bayly, a Canadian professor of electrical engineering, still saw some potential in the systèm. Bayly had been recruited in 1941 by BSC, SIS's arm in the US, to run its communications network, transmitting messages between London and New York via Ottawa. The volume of this traffic, and bottlenecks in the existing network, was 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 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 6 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.[42] 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.[43]

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. He regularly advised the agency on cryptanalytic machinery and communications systems, and liaised on behalf of the agency with its US counterparts.[44] Unsurprisingly, given GC&CS's own direct interest in the field of communications security, GC&CS took a great deal of interest in

[41] 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.

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

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

[44] For instance, see: TNA, HW 62/5, Gordon Welchman to DD(S) [Commander Edward Travis, director of GC&CS], 16 October 1943; TNA, HW 62/6, DD(S) [Edward Travis] to DNI [Director of Naval Intelligence], 11 January 1944.

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.[45]

III. 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 product 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.[46] 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.[47] 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 recognized 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.[48] Following Travis's initial viewing of the machine, Bayly set about producing further prototype machines. Soon after the production of the first, a second was constructed and transatlantic tests began. By May 1943 Rockex began carrying SIS and Ultra messages across the Atlantic.[49]

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, closely followed the project's progress. The Cabinet Office and the Admiralty both had Rockex machines installed in September 1943.[50] 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 'X-Ray' voice-scrambling system, provided Rockex with stiff competition. 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

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

[46] Ferris, *Intelligence and Strategy*, p. 172.

[47] TNA, HW 62/5, Appendix: History, Present Position and Future Development, 7 December 1943.

[48] Ferris, *Intelligence and Strategy*, p. 173.

[49] Ibid., p. 173.

[50] TNA, CAB 122/561, War Cabinet Office to Joint Staff Mission, 20 September 1943.

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 angle, 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.[51] 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 allies.[52] 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's 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.[53] 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 reoccupied 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'.[54]

Bayly's earlier work as a consultant for GC&CS resulted in a growing personal and professional friendship between him and Gordon Welchman, the technocratic, managerially minded senior ranking cryptanalyst.[55] In addition to considering mechanical cryptanalytic 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 how to convert 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, was required before any viable system could be introduced.[56]

[51] TNA, CAB 122/561, Joint Staff Mission to War Cabinet Offices, 17 September 1943.

[52] Ibid.

[53] TNA, FO 850/47b, Minutes, Y5031, 31 August 1943.

[54] TNA, FO 850/47b, W.M. Cadrington to 'C' [Sir Stewart Menzies, Director of SIS], 6 September 1943.

[55] W. G. Welchman, *The Hut Six Story: Breaking the Enigma Codes* (New York, 1982), p. 171.

[56] TNA, HW 62/5, Gordon Welchman to DD(S) [Commander Edward Travis, director of GC&CS], 16 October 1943.

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.[57] 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 transatlantic visits.[58] 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 and 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, further prototype models be constructed and the experiences gained with these machines be utilized in plans for future Rockex production.[59] Over the next few months of testing, GC&CS's machine development specialists continued to be impressed by the progress made on Rockex II.[60] 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.[61] The emphasis on experimentation stood in contrast to the earlier processes of technological development utilized 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.[62] 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 under way, 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.[63] Such were the expectations of the machine that even before the parts for the first

[57] TNA, HW 62/5, Welchman to Bayly, 26 November 1943.

[58] Ferris, *Intelligence and Strategy*, p. 172.

[59] Strikethrough as per the original document. TNA, HW 62/5, Appendix: History, Present Position and Future Development, 7 December 1943.

[60] TNA, HW 62/5, W.G. Welchman to DD(S) [Commander Edward Travis], 15 January 1944.

[61] TNA, CAB 21/2522, Unknown [illegible signature, probably Stewart Menzies] to Sir Edward Bridges, 2 June 1944.

[62] For a full discussion of Bombe development and implementation, see: Smith, 'How I Learned to Stop Worrying'.

[63] 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.

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 components was limited.[64] 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 being 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 slightly misleading. Prototype machines had already undergone significant development and testing.[65] 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 million, £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 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.[66] 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.[67]

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 mechanization,[68] was determined

[64] TNA, HW 62/6, Brigadier E.I.C. Jacob, [Offices of the War Cabinet], to Commander Travis, 30 April 1944.

[65] TNA, HW 62/6, Sir Edward Bridges to Cdr. Travis cc. Capt. Wilson, 2 June 1944.

[66] TNA, T 220/1444, Unknown [illegible signature] to Sir Edward Bridges, 17 July 1951.

[67] TNA, HW 62/6, A.D.(Mech) [Gordon Welchman] to Director [Edward Travis], 10 July 1944.

[68] TNA, HW 62/6, DD(S) [Commander Edward Travis], Machine Co-ordination and Development Section, 10 September 1943.

that it learn from the problems it had encountered. Specifically, Welchman wanted a transformation in how the agency went about the design, development, and utilization 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.[69] 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 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.

It was this perception that singled Rockex II out as a watershed for GC&CS. This hard-earned awareness that new technology could not simply be introduced and operated smoothly without sufficient logistical, administrative, and bureaucratic systems in place to support them meant he was keen to make sure that the design, construction programme, and utilization of Rockex II would be a different story. Welchman recognized that, to ensure that Britain had a long-term and robust security system, the Rockex II needed to be the subject of considerable planning, meticulous design, and developed with suitable factory facilities capable of swift mass-production.[70]

Welchman clearly succeeded in his effort to turn the development of Rockex II into the model for the future approach to machine research and development. 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'.[71] While RM(26), despite its early promise, was jettisoned before it left the prototype stage because it proved incompatible with US cipher systems,[72] the approach

[69] TNA, HW 62/6, A.D.(Mech) [Gordon Welchman] to Director [Edward Travis], 10 July 1944.

[70] Ibid.

[71] TNA, CAB 21/2522, Future Machine Development, Unknown [illegible signature] to Sir Edward Bridges, 27 June 1945.

[72] Joel Greenberg, *Gordon Welchman: Bletchley Park's Architect of Ultra Intelligence* (London, 2014), p. 98.

to work on the system demonstrates the significance of the agency's new, professionalized approach to the development of technology, which if well designed and implemented had the potential for years of service before obsolescence. Had that approach not been taken, it seems likely that more time and effort would have been expended on the abortive RM(26).

It is clear that other senior officials with a stake in secure communication had 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.[73] 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.[74] By October 1945, Welchman's prescription that a dedicated group manage cipher machine development was coming still closer to realization with the formation of the Cypher Machine Development Committee (CMDC). The CMDC comprised numerous senior officials tasked with communications matters from across the service ministries, the Cypher Policy Board, and GC&CS – and included Welchman.[75]

As noted, security had become an increasingly important concern throughout the war. Looking at the issue retrospectively in September 1945, Menzies, in his capacity as chair of the Cypher 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 notably in 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' of applying that expertise and experience to the 'security of British communications as a whole'. This was a gap that must be filled, so that GC&CS could not only provide advice to its client ministries but also ensure that, in future, the agency's store of knowledge and experience be available to 'planners and operators of Britain's Communications'.[76]

Clearly the hitherto problematic methods of ensuring British communications security had, at last, been acknowledged in Whitehall. Like Welchman, the Cypher Policy Board recognized that the measures and organizational apparatus that had hitherto been

[73] Aldrich, *GCHQ*, pp. 56–7.

[74] Ibid., p. 57.

[75] For examples of attendees, see: TNA, CAB 21/2522, Minutes of the Fourth Meeting of the Cypher Development Committee, 14 September 1945.

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

employed to secure Britain's communications had emerged as the product of circumstance, as opposed to careful planning. Indeed, the 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 itself indicative of the wider failure to appreciate the benefits of centralized professional communications security planning across Whitehall until remarkably late in the day.

IV. Conclusions

The development of the Rockex system, and its much improved successor Rockex II, was a lengthy process that had necessitated inter-service and departmental cooperation in the development of a complex and revolutionary cipher system. The design and manufacture of Rockex II was the result of an unprecedented planning process by GC&CS. In turn, the agency 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 utilized in some British embassies at least until the 1970s.[77] As Ferris notes, in developing and adopting the machine in the final stages of the Second World War, the British state established a situation in which Britain would emerge as a world leader in cipher security at the outset of the Cold War.[78]

Prior to the development of Rockex, machine design and research had been a fraught process instigated as a last resort to resolve pressing problems caused by mounting wartime pressures. Frank Birch, a senior figure within the agency and in the early 1950s the author of its internal history, complained in that history that the agency's general administration and organization in 1940 had been like 'a rudderless vessel'. This, he explained, was because in the face of 'a succession of emergencies, only hand-to-mouth empirical improvisations are possible'.[79] His diagnosis of GC&CS's general organizational difficulties was also very much true of its machine development initiatives. By 1944 the agency had come to (realize and) accept that this relatively last-minute and ad hoc approach to developing its machine sections, though unavoidable at the time, could not be allowed continue. The machines developed under this approach, while enormously successful, were fragile solutions that could easily be 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 crucially also on long-term planning, bureaucratic oversight, and the building of logistical structures.

These were lessons that had been 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.[80] Furthermore, GC&CS had evolved into a large, professional, and mechanized bureau, complete with teams of expert machine designers and builders and contacts with experts

[77] TNA, FO 850/134, Note from Foreign Office Archivist, 16 April 1973.

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

[79] Birch, *Official History*, vol. 1 (pt 1), p. 90.

[80] Smith, 'How I Learned to Stop Worrying', pp. 214–16.

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 through the formation of inter-service and ministry committees dedicated to oversee and direct the development of cipher security. Without this collaboration across the services and GC&CS, it is impossible to see how a system such as Rockex II could have been developed in the way that it was. It is clear that GC&CS had transformed from a collegiate agency that had rapidly, and sometimes unwillingly, adopted mechanized 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 cipher system further catalysed the processes of change and was, ultimately, the first major beneficiary of that transformation.

For the historian seeking to understand how and why GC&CS transformed itself from an archaic and beleaguered organization 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, the point at which the agency ceased to invest in technology as a last resort to address what had hitherto been unassailable problems comes clearly into view. 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 strategy for its post-war operations. Second, the development of Rockex highlights the importance of the under-recognized connections made by the agency with bodies such as BSC. The agency's ability to recognize invaluable expertise in other quarters, and to cultivate connections with key specialists such as Bayly, was central to its success.[81] Third, the development of the system showcases 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 professionalizing cultural changes within GC&CS that historians are only beginning to unravel.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

[81] 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.*