doctoral work, published in the *Astrophysical Journal*, provided tangible evidence of quantum behaviour in complex systems. Teaching students about scientists such as Imes broadens their image of who can be a physicist. This is one strategy to transform STEM curricula and to demonstrate how faculty members can respect the contributions of women and people of colour. In short, students should see scientists who look like them reflected in classroom content. Researchers such as Christopher Emdin, a scholar of science education at Columbia University in New York City, have used this approach to attract students from historically under-represented groups into STEM fields. Called culturally relevant pedagogy, it merits more detailed discussion than it gets in this book.

Early in her narrative, Posselt asks a crucial question: how much should graduate programmes reform "to accommodate the diverse career pathways in their fields"? There are simply not enough tenure-track positions, and most PhD holders don't work in academia. STEM fields have been slow to empower graduate students who choose to use their training to improve or uplift their communities.

Departments and faculty members need to provide safe spaces for students interested in careers outside academia. Students in Michigan's applied-physics programme said they wanted to secure employment and make a difference in society. The programme involves collaborations with many different departments, showing how physics can improve people's daily lives. This approach can resonate with and empower graduate students from historically under-represented groups.

There are many more successful doctoral programmes than Posselt can cover. For example, Louisiana State University in Baton Rouge is the leading producer of African Americans with PhDs in chemistry. The university has succeeded through targeted recruitment, mentoring and support.

Equity in Science does a good job of highlighting some of the barriers and challenges to equity in graduate programmes, and provides examples of what some do right and wrong. The book supplies specific guidance on inclusive practices. What we need now is a companion volume on getting and keeping scientists of colour in the next section of the pipeline: faculty. As I found after securing that PhD, rising through the ranks of academia as a Black woman chemist is tremendously hard work. What kept me going? Inspired by Saint Elmo Brady's legacy, I knew I too deserved a seat at the table.

Sibrina N. Collins is executive director of the Marburger STEM Center at Lawrence Technological University in Southfield, Michigan.
e-mail: scollins@ltu.edu

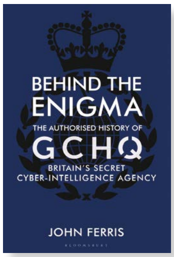
The code-breakers who led the rise of computing

World wars, cold wars, cyberwars – marking a century of state surveillance at GCHQ. **By Andrew Robinson**

"Most professional scientists aim to be the first to publish their findings, because it is through dissemination that the work realises its value." So wrote mathematician James Ellis in 1987. By contrast, he went on, "the fullest value of cryptography is realised by minimising the information available to potential adversaries."

Ellis, like Alan Turing, and so many of the driving forces in the development of computers and the Internet, worked in government signals intelligence, or SIGINT. Today, this covers COMINT (harvested from communications such as phone calls) and ELINT (from electronic emissions, such as radar and other electromagnetic radiation). Ellis and Turing are just two of the many code-breakers and code-builders in *Behind the Enigma*, the first authorized history of one of the world's pre-eminent secret intelligence agencies, GCHQ, the United Kingdom's Government Communications Headquarters. Famous for its Second World War decryption of the German Enigma cipher at Bletchley Park, there is so much more to this secrecy-shrouded outfit, reveals Canadian historian John Ferris.

Fielding formidable research, Ferris tells a global tale of mathematics, engineering, data sciences and linguistics in the service of politics, diplomacy, war and security. Spanning a century, it ranges from telegraphic intercepts to malware that can bring down infrastructure. After a brief introduction to pre-1914 intelligence based on letters, cables and wireless messages, his story begins with First World War cryptography and the foundation of GCHQ in 1919 as the Government Code & Cypher School. It ends with the agency's current, not-so-secret incarnation as a protector of the cyber commons. In September 2001, the director of GCHQ crossed the Atlantic on the only aircraft allowed into the United States immediately after the al-Qaeda attacks, to work with his US opposite number.



Behind the Enigma: The Authorised History of GCHQ, Britain's Secret Cyber-Intelligence Agency
John Ferris
Bloomsbury (2020)

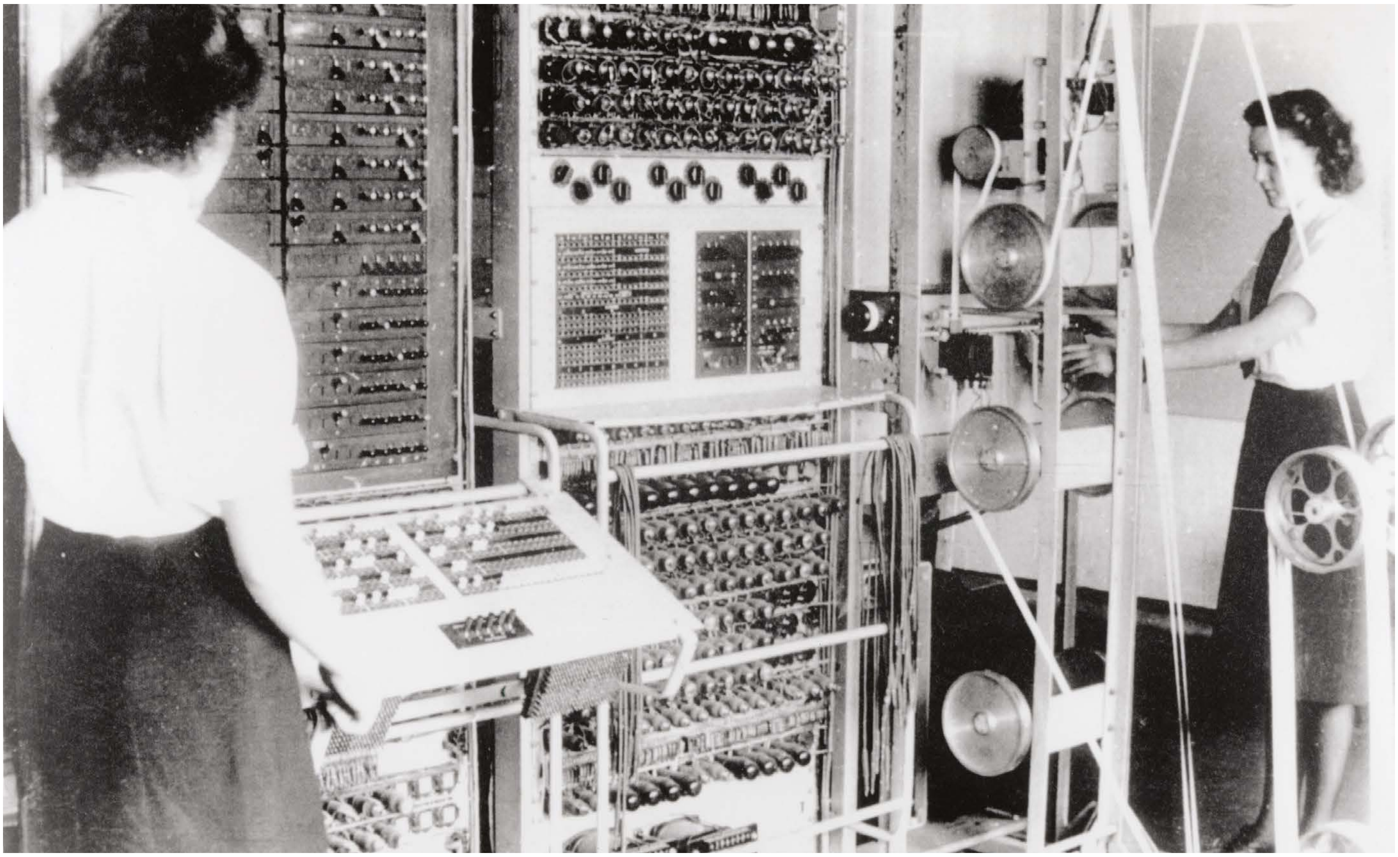
What emerges is that SIGINT has ranged from highly effective to almost useless. In July 1962, a few months before the Cuban missile crisis, GCHQ picked up enciphered Soviet messages suggesting that two Soviet passenger and cargo ships were "possibly en route Cuba" and that their voyages might be "other than routine". But there was no hint of the ships' purpose and content. Then, in mid-October, a US U-2 spy plane detected the first proof of Soviet missiles in Cuba, triggering the crisis. Two weeks later, soon after US president John F. Kennedy's announcement of a naval blockade of Cuba, GCHQ detected a flurry of urgent enciphered messages sent from Moscow to Soviet ships. Thus, SIGINT helped to alert and inform governments, but the US political decision depended on ground observations by the military.

By contrast, at the end of the Falklands War against Argentina in 1982, the commander of the British task force declared that, without GCHQ's advance penetration of the Argentine plan of attack, mainly through COMINT in Spanish, the invasion would have failed at sea. But once the soldiers landed on the Falkland Islands, SIGINT failed them in battle, because of the improvised nature of the chain of command.

Central to these events was UKUSA, or 'Five Eyes' – which receives frequent mention in the book. This is the still-operative multilateral agreement for cooperation in SIGINT between Australia, Canada, New Zealand, the United Kingdom and the United States. It was inaugurated between GCHQ and the US National Security Agency in 1946, at the beginning of the cold war, but its existence was concealed from the public until 2005.

Intriguing are the backgrounds and mindsets of past and present GCHQ staff – today 6,000 in number, compared with 10,000 at its wartime peak – and their working conditions, breakthroughs and varied relationships with peers in other countries. Of their US counterparts, retired GCHQ director David Omand joked to the BBC in 2013: "We have the brains. They have the money. It's a collaboration that's worked very well."

Certainly, GCHQ mathematicians were often secretly ahead of the academic game. For example, in 1970 Ellis came up with the possibility



SSPL/GETTY

Cryptographers at Bletchley Park use a Colossus computer to decrypt German military communications during the Second World War.

of "secure non-secret digital encryption", but could visualize no way to implement it. In 1973, a younger colleague, Clifford Cocks, later chief mathematician at GCHQ, realized Ellis's concept by inventing the public-key system now known as the RSA encryption algorithm. Its name derives from Ron Rivest, Adi Shamir and Leonard Adleman, who invented it independently in 1977 in the United States.

In 1974, another GCHQ mathematician, Malcolm Williamson, devised the technique for public exchange of a common secret key between two parties that later became the basis for all secure transactions on the Internet. This one is also named after US cryptographers – Whitfield Diffie and Martin Hellman – who discovered it independently in 1976. Only in 1997 were these two crucial GCHQ discoveries declassified. Even in 2020, writes Ferris, "Siginters feel disquiet when they see the name GCHQ in press headlines".

Often recruits were linguists, sometimes with unusual skills. During the Second World War, many were gifted academics from Oxford and Cambridge universities (although GCHQ turned down Oxford's J. R. R. Tolkien, despite his mastery of languages). One notable was the young Cambridge classicist John Chadwick. He took a crash course in Japanese in 1944 to help decrypt messages sent by Japanese naval representatives working in wartime Berlin and Stockholm. Post-war, Chadwick, with architect and philologist Michael Ventris, deciphered Europe's earliest readable script, Minoan Linear B, an archaic form of Greek.

Bletchley's staff was famously more than 75% women. Compared with "virulent sexism" in the computing industry, Ferris notes of GCHQ in the 1930s that, "once inside, the standards were those of flair, not gender". But the stories of notable women from those days are still only now coming to light, as witness the dearth of female portraits in the book's plate sections. Staff included linguist Emily Anderson, a former professor of German who became a world-leading cryptanalyst in the 1930s, and mathematician Joan Clarke, who used Bayesian statistics to speed decryption at Bletchley, where she collaborated with (and was briefly fiancée of) Turing. These days, the organization – like most in cybersecurity – realizes that it has a sizeable gap to close on gender balance in its workforce; Ferris doesn't dwell on that.

Inevitably, official secrecy limits this analysis – as do the author's academic interests (more military than scientific). In inviting Ferris, GCHQ ruled out discussion of diplomatic-communications intelligence from after 1945 and the technicalities of current methods. Other intelligence agencies, such as the US National Security Agency, had power of veto over details of joint projects. Also off limits were records of the period after the end of the cold war in 1991. For these decades, Ferris had to interview current staff, mostly under 'deep background'.

Thus, the 1990–2020 era is covered less critically. In a discussion of the 2013 leaks about UKUSA surveillance by National Security Agency contractor Edward Snowden, which were followed by a UK government inquiry into GCHQ, Ferris rejects the charge that the agency collects intelligence on everybody, regardless of their risk to UK security. His unsatisfying take is that their sins are more of omission than commission. He writes: "GCHQ did not openly address the operational and legal elements of bulk collection because it did not know how to do so, rather than having anything to hide."

Today, a secure cage in GCHQ's basement archives contains the vetting records of each member of staff, collected from interviews with friends and families before hiring. These were unavailable to Ferris. Each record is destroyed when the member dies. "Nothing better typifies GCHQ than this focus on privacy for people who strip secrecy," he writes. Perhaps this is why even the deceased in this pioneering history seldom come alive as individuals. For all Ferris's scholarly sleuthing, not even Turing – a key contributor to decrypting Enigma, and a globally compelling human enigma – really emerges from the shadows.

Andrew Robinson's many books include *Lost Languages: The Enigma of the World's Undeciphered Scripts* and *Einstein on the Run: How Britain Saved the World's Greatest Scientist*. He is based in London.
e-mail: andrew@andrew-robinson.org