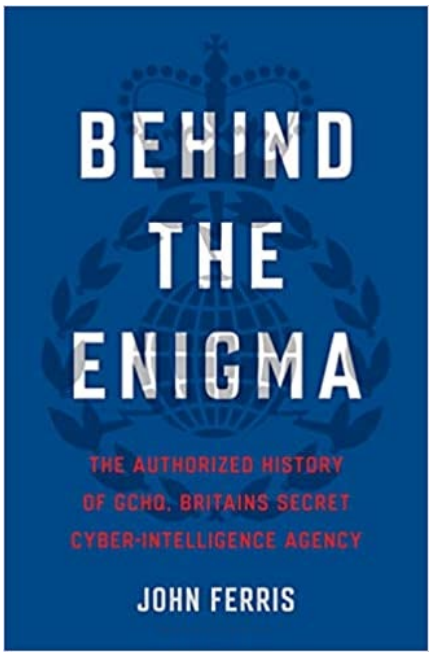
Journal of Military and Strategic Studies

VOLUME 20, ISSUE 3



Commentary

Behind the Enigma: The Authorized History of GCHQ, Britain's Secret Cyber-Intelligence Agency (London: Bloomsbury Publishing, 2020).

Dr. John Ferris

I was asked to write the authorized history of GCHQ (Government Communications Headquarters) because not that many people work in the history of

ISSN : 1488-559X

signals intelligence, which practitioners call *sigint*. In fact, I may have been studying the history of that topic longer than any other scholar. Beyond that, over the years I've built up a reputation among siginters who are interested in history, as actually understanding the techniques of their craft, of being able to make sense of what they do and, above all, of being able to do something that was uncommon, to answer the *so what?* question. In this case the *so what* question is, all right, you've produced this material through some complex means, which may be extremely difficult, time-consuming, and sophisticated, but so what? Once you've generated that material, who cares? Who uses that material, how is it used and how can you assess how is it used? Those are questions which I've been dealing with as a historian since the 1980s, but which few other scholars have tried to tackle. So, when in 2014-15, Government Communications Headquarters decided that it needed to have an authorized history, I was the obvious candidate, in all due modesty.

Why did GCHQ decide that it needed an authorized history? Signals intelligence agencies, especially Anglophone ones, have been very reticent - I might almost say anal - about maintaining secrecy for their practice. Really up until the 1990s, their aim was not to be known by anyone. But from 1990, gradually those inhibitions declined. They released a lot of material, in fact, ultimately all of the material from before the end of the Second World War, with the exception of some stuff on the technicalities of codebreaking. NSA (National Security Agency), GCHQ's American counterpart, began to be remarkably open by past standards. It was willing to have its people talk to journalists or academics and it began to sponsor a demi official history conference every couple of years which proved to be very important to civilian students, including myself. Beyond that, siginters, after 2000, began to realize that they needed some kind of public acceptance for their work because it was expensive, was being used by government, and was touching on public spheres in ways which it had not done before, in what I call "the second age of sigint." The first age of sigint involved struggles between states versus states, focused primarily on military communications carried by radio. The second age of sigint involves relationships, many of them competitive, between states and societies versus states and societies over communications carried by telephone lines, maritime cables, cellphones and satellites, via the Internet, through what we describe by the loose term, *cyber*. Organizations like NSA, GCHQ or their Canadian equivalent, the Communication Security Establishment (CSE), were advising

individual people and companies about how to protect themselves against cyber threats, which they could not do if they remained absolutely secret.

Finally came the shock of the Snowden disclosures in 2013 when a contractor working for NSA, exploiting its poor security practices, copied a wide swathe of material which he then leaked to the press. Now, I believe that nothing in the Snowden disclosures proved illegal or immoral behaviour by any Western sigint agency, but every civilian analyst, including me, was shocked to see exactly how sigint was practised. Thus, GCHQ decided that it must be more open than it had been before. GCHQ was hitting the moment of its centenary. It had existed in various forms for about 100 years and, following the examples of its sister secret services, MI5 and MI6, decided to commission an authorized history to explain to civilians what it had done.

When they gave me the opportunity, I was given lots of previously classified records, but also there were limits on the material I could use. GCHQ didn't want me to talk about any technical issues involving cryptanalysis from after 1945, which didn't bother me because, frankly, I didn't think I could really understand them, and I didn't think that most of my audience really cared either. GCHQ didn't want me to talk about diplomatic codebreaking after 1945; in other words, reading the codes of neutral governments or friendly governments, because it is politically embarrassing. Any partners of GCHQ could take out anything which I wrote about them. In other words, if I said something about another British agency or about a Canadian agency, under the principle of *equities* which works in the intelligence world, those agencies could take themselves out of my story, if they wished. Some did though, fortunately, the most important of these partners, NSA, was generous on these matters. But subject to these conditions, I was given access to the main range of GCHQ policy files. I received complete access to a number of case studies, in other words, instances where signals intelligence affected issues like the Falklands conflict, for example. I was allowed to conduct what journalists would call research on *deep background*, to interview people and to use what they said without being able to identify them. I received more access to the records of any signals intelligence agency than any civilian historian, had ever done, and there would be no interference with what I wrote. In fact, GCHQ never did interfere. Some of the people I worked with closely gave me advice, which I found very useful, and it saved me from making many errors in interpretation, but it was my story.

Also, as time went by, GCHQ offered me more material than they'd originally promised. The history was originally supposed to close in 1992, with the end of the Cold War, but we agreed that I should try to take it forward to the present day, that is, 2020, although after 1992, my access to documents declined significantly and I was relying heavily on open-source material and interviews.

All right, so what is my story and why does it matter? It matters because no one has been able to write about any sigint agency in the long term because access for any evidence after 1945 was denied. To tell the whole story was very difficult. Instead, I could marry all the material I already had from before 1945 with classified material going up to 1992. That gave me a perspective on signals intelligence that no one had. Sigint practitioners don't know their own history. Because of their focus on secrecy, they hid their own history from their own people, which meant that very often 10 or 20 years down the line, people would have to rediscover the wheel. They confront eda problem that their predecessors had handled quite well 20 years before, but they didn't know how so, and had to relearn how to do it. The perspective that I developed was broader than that which sigint professionals or civilian historians had.

Here is a pocket history of the Ferris view of sigint. That history begins in 1914, with the First World War. It didn't exist in 1913. Signals intelligence involves an amalgam of the ability to intercept modes of communications, which could be post, cable, radio, or internet traffic normally carried on the telephone lines, combined with techniques of analysis; cryptanalysis, which means breaking codes; and traffic analysis, which means gathering material from the external features of communications. Modern sigint uses traffic analysis to a great extent. If you're intercepting communications between terrorists, you try to see which IP address interacts with which others and then, by focusing on those external features, you find describe networks, which may define your targets. I discovered that about a year into the history of sigint, suddenly extraordinarily sophisticated and powerful practices were developed. Traffic analysis emerged in spring 1915 when the British Royal Flying Corps found that the call signs of German aircraft reflected the organization of the German Air Force. Since the primary function of aircraft was to spot for guns, this aerial intelligence revealed the location of enemy artillery pieces and thus the epicenter of enemy power on the Western front. The British conducted economic warfare in the First World War, and also intercepted all

forms of communication across the Atlantic via sea mail, cable, or wireless. In the first world war, the British intercepted about 1 billion messages carried by these forms of communication. This is a massive amount of material. No intelligence agency, indeed, no agency of any kind in history before, had ever confronted this much material. But the British created an organization called the War Trade Intelligence Department, led by academics, essentially, historians and economists from Oxford, who deployed extraordinary modes of information processing, which, in effect, indexed every proper name mentioned in every message. And if any individual was interested in, for example, the life history of a Norwegian manufacturer of banjos, they can gather all that material in two hours. Data retrieval was extraordinarily fast and precise from an extraordinarily wide range of material. When I first described these findings to professional siginters, they were astonished , because they were using exactly the same techniques against Internet traffic. Meanwhile, signals intelligence became the most important form of military and naval intelligence. Military forces used radio all the time, usually with poor security. Any good sigint agency could pick up lots of material. There was as much sigint in the First World War as there is in the second. The only difference is that the enemy was better throughout the First World War than is the case in the Second World War. Ultra in the Second World War was so successful is because at a certain point, the German simply fall further and further behind the British and the Americans and Canadians, who had a solid run of victories gained from good intelligence, but in the first world war, the Germans are better, so there is a constant struggle between one side gaining an advantage in the other side gaining a counter advantage.

At the end of the First World War, every major state and many secondary ones saw sigint as a necessity. Our military and diplomatic establishments will need code breaking agencies to give us material on a daily basis. Really, from 1914, there's never been a moment when leading governments have not collected signals intelligence on neutrals, their enemies and sometimes their allies. It's simply a normal part of the way governments work. We don't understand that simply because governments tried to keep that story secret from us for a long time, which is another reason why my story matters.

I provide a detailed analysis of how signals intelligence helped Britain and the western allies in the Second World War. The Germans and also Italians get some successes from signals intelligence, but in the long run we get more, and it matters a lot. It doesn't allow us to survive or win. It doesn't guarantee victory but it does make victory much easier to achieve. At the end of the war, Dwight Eisenhower, the commander-in-chief of Allied forces in Western Europe, thanked British code breakers for providing intelligence, which saved countless thousands of Allied lives. Western decision-makers are astounded by the performance and quality, especially of British sigint, and again want to replicate it.

From this moment on, everything I discuss comes from material that I was the first civilian to see. Often, I was the first person to look at those files in 40 years. I had a very different position to interpret this material than anyone else had done. The bulk of my story, about two thirds of it, is the history of GCHQ and more broadly of Western signet from the end of the Second World War down to the end of the Cold war. I try to explain, exactly who are the people who conduct signals intelligence? There's a great deal of social history here. I spent a lot of time talking about what women do in sigint, and assessing the largest group of western siginters in the Cold War. These were radio intercept personnel, almost universally male, almost always ex servicemen, sitting with headphones listening to Morse code or voice communications, and providing material for senior decision-makers. I talk a lot about how the process of sigint works. In many areas, my account is perhaps more technical than most people want to read and I suggest that if you find me too technical on some issue, skip it. But I wanted to provide a complete record which would enable anyone interested in the topic to really understand what it was. I talk about how sigint is collected, how it is processed, how you make sense of it. I was allowed to interview some British codebreakers who gave me unique insights into how they thought, how they approached their problems, and how they broke codes.

Above all, I was able to generally assess the nature of the signals intelligence struggle in the Cold War. Here let me just generally give a few simple observations, because it is too detailed to try to do anything further. When it comes to reading neutral traffic of secondary powers, the Cold War is a great time. Any competent code breaking power and by that I mean the Soviets, the Israelis, and western sigint agencies, are able

to read the communications of a very large number of neutrals, particularly in the Middle East and Asia but across the world as a whole. There is a wide variation of what you can do with diplomatic sigint. Sometimes you can really pick the pocket of the person you are bargaining with. Sometimes diplomatic codebreaking gives you material, you cannot use. All I would say is that it's part of the daily background for decision-making, and let me make a point here for Canadians. Lester Pearson is *the* go-to man for British code breaking from 1942. He's one of the most experienced consumers of sigint in the world by the end of 1945. Lester Pearson is famous for being the most effective Foreign Minister in the history of Canada. But what is rarely mentioned is that he also receives a very large amount of material from sigint generated by Canada and its allies. Pearson is successful in part because he's bright, but also perhaps in part because he is very well informed. Yet, studies of Pearson as statesman never discuss sigint as a factor in his success.

Sigint alliances become normal in the Cold War. Canada is part of the most important of them which normally is called UKUSA, or the *Five Eyes*. The *Five Eyes* are Australia, Canada, Britain, New Zealand and the United States, i.e. all the Anglophone ex-dominions plus the United States. The term *Five Eyes* simply refers to a standard security classification. A sigint product that can be distributed between all members of the *Five Eyes*, is labelled for *Five Eyes* only. If it's only supposed to go to your own people, it might be for British eyes only or for US eyes only. The *Five Eyes* is an international organization of the sigint agencies of those five countries. It is not a formal treaty, but rather a process of administration and organization known and accepted by all the governments of those states. Those five countries cooperate very, very closely in most forms of sigint collection and analysis, and spread the material and the workload among each other. To belong to the *Five Eyes,* you must bring something to the pot. If you don't provide material, people won't let you continue to take from the pot. For Canada and the Cold War, we focused on Soviet traffic in the Arctic or the North Atlantic. Since the end of the Cold War, CSE has been forced to find other targets and has move out more broadly into terrorism involved targets or economic target, s as all the *Five Eyes* had to change their targeting. But for Canadians, we're part of an organization which is the strongest players in sigint in the world. They help protect our security. They don't attack our traffic and in return we and they cooperate in the tracking of the traffic of anyone we think is of interest or threat.

Here, let me say something which I know many people think is a terrible thing. Reading the traffic of neutral governments is not evil, it is normal. It's what states do all the time. To read the traffic of your friends is also normal and useful. After all, if you are negotiating on trade issues, the states whose position you want to know best of all, that of the people you're negotiating with, very often are your friends .That's part generally of the diplomatic side of the Cold War, which currently cannot be written fully.

When I looked at the main struggle between NATO and the Warsaw Pact, what I discovered was something which confirmed my own suspicions and that of a few other people working in the field. In the signals intelligent struggle between the *Five Eyes* and the soviet block, there was no Ultra. We could not regularly read the highest level of communications of the Russian government. As a general rule, Soviet cryptography was pretty good, with a series of exceptions linked to Soviet multi channel voice encryption systems, i.e. if I'm speaking Russian to another Russian, our communications go through an encryption system which turns my voice communications into something else and returns it to plain language Russian. Alas, for the USSR, the Soviet system fails to encrypt all the channels by mistake. They don't understand that and the British and Americans exploit that weakness for 30 years. Moreover, in West Berlin, the British, French and Americans have massive sigint installations right in the middle of the largest conventional force on earth, The Group of Soviet Forces in Germany. They're using voice communications all the time. Much of which the British and Americans are reading. Now, most of us, when we think of Berlin and Cold War intelligence, think of checkpoint Charlie and the exchange of spies, but the real story is that the British, French and American sigintors are perfectly positioned to read and break into the most important traffic of the most important Army of the enemy, but only in some areas.

Most Soviet cyphers are unbreakable, but beyond that you do traffic analysis. The British, Canadians and Americans have personnel who spend all of their lifetimes living within the communications systems of a single Soviet division or corps, day in, day out for 25 years. They actually have a very clear understanding of normality and can see anything that is out of place. Added together, you've got a huge amount of material on the normal working of Soviet military forces, which allows you to say

World War Three will not break out today, or tomorrow. That provides a fair amount of certainty in a world where things are potentially very dangerous. Although sigint in the high Cold War doesn't break into the highest levels of Soviet communications, for both sides, it provides a fair degree of certainty that the other side is not actually preparing for real war imminently, including during the Cuban missile crisis or the Hungarian crisis rf the Czech crisis. By providing a very clear picture of what the other side is doing, sigint tends to calm the waters.

When you get to other kinds of bilateral conflicts in the Cold War, however, say the Americans in Vietnam, the British during Konfrontasi with Indonesia in the 1960s, or in the Falklands conflict, the Israelis in their war with Arab countries., what happens with sigint varies dramatically. In the case in Vietnam, astonishing to most people ,the Americans lose more than the they gain simply because they have to use radio much more than the North Vietnamese do. The North Vietnamese have a lot of English speakers who just listen to American voice communications and pick up a lot of useful intelligence. The North Vietnamese don't use radio very often, and their personnel are pretty well trained. Without success in sigint, conversely,Britain culd not have won the Falklands conflict. Sigint is an important part of Israeli superiority in the Arab-Israeli wars of the 60s and 70s. These issues are going to be dealt with by historians for a very long time. What I do for the Cold War largely is to provide a framework and give some insights on certain issues. Much material on these issues is wide open and it is now possible for civilian historians to study it.

Finally, I turned toward what happens after the Cold War, where I argue that we have entered a second age of sigint. At the end of the Cold War, many of the fundamental elements of the way communications and signals intelligence work change. High-frequency radio becomes increasingly a tertiary form of communications, military organizations, intelligence ones and foreign offices start to use normal civilian forms of communication which focus on the Internet, increasingly, normally carried over telephone lines, but also by multi channel maritime cables and radiotelephone or satellite communications. The targets for state sigint agencies no longer used a specialized form of communications like radio, but normal communications systems, and if you are going to follow them, you must intercept these normal communications. Unfortunately, it's very difficult when you are observing the movement of billions of

telecommunications events a day, to know which ones come from a target and which come from a civilian you don't care about. Sigint agencies automatically intercept civilian communications, including that of their own people. Now let me emphasize that to *intercept* does not mean to *read*. It simply means that you can temporarily hold copies of a given transmission. You can't read most of them, because so much encryption is involved, but you can try to identify your targets and then try to break them. In that process, however, you are also tracking communications from normal people like you or I. Even worse, if I'm sending an email to a person sitting in another room in my office, that communication may be routed through Beijing. If Russian intelligence in Petersburg sends a message to Russian intelligence in Moscow, it may be routed through London or oddly enough, even Calgary. Thus, now you no longer can easily discern the difference between an internal national communication, which the *Five Eyes* are not supposed to touch, i.e. CSE is not supposed to intercept or attempt to read Canadian communications, but it is free to intercept and read anything else outside of the territory. Nowadays, it is actually really hard to distinguish between those places. Beyond that, signals intelligence organizations used to only be owned by governments because no one else had the technical expertise or the ability to intercept traffic. On the Internet, that's no longer the case. Millions of entities have some primitive sigint capabilities. Cyber criminals can read a lot of your communications. Phishing is an extremely elementary form of sigint, but it can compromise the entire cryptography of a medium-sized organization, like Western universities, which in many cases, essentially have had to download and turn into paper form all of their internal communications to ensure they're not destroyed, and then ransom back their digital forms.

So suddenly, normal people are caught up in sigint. The problem is not really foreign governments or our own, because my government doesn't care about my email traffic and is bound by law, which makes it very difficult for sigint to attack my communications unless a judge authorizes it, which is true across the *Five Eyes*. That's one reason why not I'm one of those who worries about *1984*, and our own governments reading all of our mail. There's too much mail and there too many laws which are obeyed--among the *Five Eyes*. The real problem for us as individuals are cyber criminals. They exist in large numbers. They are out to get us, or more precisely, the most vulnerable members of our society, the people they can hit. And the only people

who can protect us against them are our government sigint agencies, or in some cases, private communications security organizations, which for their sake of their own goodwill often help individuals or to provide public knowledge. But we're now caught up in a world where each of us as individuals is a target for sigint, in which our government cannot easily protect us from being attacked by foreign sigint organizations whether they are state run or criminal run. Now again, terrorism, which is important but and unfortunately also gets more attention than it really deserves, also creates problems if you're trying to track it down through signet, which is the most effective way to try to track it down. If you going to bring them to court, you need to have an agent in place, but if you're going to try to track down generally who they are, sigint is the easiest way to do it. Alas, terrorists sometimes have good communication security techniques but they all use normal modes of communication. If the government is going to track them down, it must go through internal traffic that might come from Canada, or might involve Canadian passport holders.

Under the old rules of the game which governed sigint from 1914 to 1992, in Western countries, there is little reason to believe sigint agencies were involved in internal politics, because that wasn't their job. They focused on foreign government communications. Nowadays we're actually living in an environment where our communications can be intercepted and attacked by foreign cyber criminals, foreign governments and monitored by our own government. And I do not blame anyone for being unhappy about the circumstances, and it makes me feel icky to know that some analyst might indeed be perhaps touching one of my communications, boring as in fact they would be if they could read them. But that world is what it is. It's not going to change. When we use the Internet, most of us deliberately volunteer huge amount of data about ourselves. We deliberately publicize things about ourselves and make ourselves targets for sigint. Now, the people who most make use of that opportunity are of course corporations. Corporations who run Internet services, or try to keep track of their customers and find ways to make money are using our freely volunteered data more than any government sigint agency is.

Sigint once was this esoteric issue which was relevant only to governments collecting intelligence on each other. Now, it is part and parcel of the way we live and that really means, I suggest, that any rational person should know something about

communication security and sigint, because that's part of your environment. All that's an important part of my story, which I presented but it wasn't one that I expected to be writing when I started.

John Ferris is a professor of history at the University of Calgary, where he is also a fellow at the Centre for Military, Security and Strategic Studies. He received a PhD in war studies from King's College London. He is the author of numerous academic articles on diplomatic intelligence and military history, as well as on contemporary strategy and intelligence. He lives in Calgary, Canada.

*Behind the Enigma*is available for purchase at all bookstores and online at Amazon.