Ultra Information Management – an enigma

Martin White Managing Director, Intranet Focus Ltd

martin.white@intranetfocus.com

A visitor surveying the main ceiling-height bookcase in our dining room and knowing my background would not be surprised to see books on American political history, the history of science and the music of J.S.Bach. A substantial number of books on Richard Feynman (my hero!) might come as a bit of a surprise but certainly not as great as a section on the use of cryptography, especially in World War Two. This has long been a subject of great interest to me since buying David Khan's book The Codebreakers in a second-hand bookshop in San Francisco in the early 1980s. At the time that Khan wrote this book in 1974 the full story of the way in which Turing and others had been able to read the Enigma-encrypted German radio messages had not been made public, though Khan does hint at what was going on. However, my interest is not so much in the way in which the Enigma and Lorenz cyphers were decrypted but in the processes through which the information and intelligence was then communicated to senior battlefield commanders.

The exact source of the information was never disclosed to even the most senior commanders but was handled by Special Liaison Units (SLU), consisting of a few officers and enlisted men; low in rank to avoid drawing attention and often situated some distance away from the battlefield HQ, to maintain security. This process was masterminded by Frederick Winterbotham and was known as Ultra. In effect this was the prototype of the way in which information specialists started to work directly with research scientists in the 1970s to make use of the availability of online computer access to scientific information.

I have just finished reading a superb book by Sir Max Hastings entitled The Secret War, which is notable for presenting not just the work of Allied cryptographers but also similar work being undertaken by the German, Russian, American and Japanese armed forces. A sub-theme of this book is the challenges common to all these operations in managing the enormous number of messages that had to be deciphered, assessed, interpreted and distributed each day, especially once America and Japan entered the war. This work was all about information management, though it was never described in those terms.

Reading *The Secret War* some common elements of managing the information flows emerge, all of which apply right now to the challenges of handling information inside organisations to ensure that decisions are made on the basis of the best available information. Without going into detail about the processes involved, some of the issues that arose included:

Timeliness - the decoded information had to be transmitted on to the SLUs quickly enough for commanders to consider what actions they should take. At many times during World War Two the cryptographers found that codes and routines had changed which resulted in delays of many days in breaking back into the messages.

Context – it was all very well knowing that the 3rd Mechanised Brigade were moving from Marseille to Bordeaux, but without knowing what equipment and role the Brigade had this information had no value at all. To try to overcome this problem vast card indexes were built up of every military unit, commander and capability. By the end of World War Two, the card indexes in the main analysis section in London ran to around four million cards.

Veracity – commanders had to make decisions based on sources of information they were not aware of. This required the commanders to have great faith in the skills of often very junior staff in the SLU unit.

Completeness – quite often the picture gained of a battlefield (and I include here land, sea and air operations) was not complete. The lack of information might not even be obvious and so commanders had to trust their own judgement in making the optimum decision. Another factor here was that although air and sea operations were carried out by radio messages, army operations also used telephone lines.

Trust – there was not time to double-check every piece of information. Sometimes there was a mistake in the decryption, or the message was corrupted. Once a commander had made a decision which in retrospect was not a "correct" one they might well stop trusting the information they had been provided with.

Prioritisation – with so many messages being decrypted, especially when the early mechanical devices (the Bombes and Collosus) became available, the initial triaging of messages by importance was a very difficult challenge as the teams in Bletchley Park often had little idea of the current battlefield situation. On many occasions what seemed to be of little importance turned out to be a significant misjudgement of priority.

Feedback – only rarely did the decryption teams have any feedback from the battlefield. Winston Churchill was very supportive, but the day-to-day work had to be a labour of personal commitment. Yet the secrecy had to be total, and that meant that even staff working in different sections of Bletchley Park could not talk about the work they were undertaking. Indeed, many had no idea of what they were doing and why – a good example would be the staff in the Y Service spending all their time writing down meaningless sets of five characters as they intercepted radio communications.

Post-1945 the history of the development of computers is well documented, and without doubt, the decryption work was of the greatest importance in catalysing the development process. The techniques of managing very large card indexes also continued to be developed, many using edge-notched cards. It is quite interesting to read a report on Nonconventional Technical Information Systems published in 1958. It reads as though these all suddenly sprang into life but in fact, they were all introduced during World War Two to manage decrypted information. When I started work in 1970 at the BNF - (see *The Evolution of UKeiG*) - a ten-thousand-hole optical coincidence card system was being used for information retrieval; a technique developed by Polish cryptographers in the 1930s as they, for the first time, worked out how to decode the German Enigma machine traffic. Gradually these were supplanted by computers and in particular the development of

computer phototypesetting that generated computer-readable tapes for use in information retrieval systems.

When it comes to the techniques of managing information, there was no need for these after the end of World War Two. Computers did not have a major impact managing text information until the arrival of IBM STAIRS in 1973 and "enterprise search" applications only came on to the market in the 1980s. Going back to the start of my career the most technically sophisticated device in the BNF (apart from a foundry and several diecasting machines) was the IBM golf-ball typewriters being used by the team preparing BNF Abstracts.

Certainly, the volume of published scientific information increased substantially after World War Two and this led to the formation of the Institute of Information Scientists in 1958. I have always wondered how many of the founders and initial members of the IIS were aware of the Enigma and Ultra work, but of course could say nothing about it. If they had, perhaps the importance of information as an organisational asset and the techniques of information management tested out for real in a global conflict could have been more widely recognised and adopted.