The Typex Scare of 1943:
How Well Did the British React to a Cypher-Security Scare?

Dermot Turing
Visiting Fellow
Kellogg College
62 Banbury Road
Oxford OX2 6PN, UK
dermotturing@btinternet.com

Abstract

The response of German Naval Intelligence, at various points in World War Two, to suspicions that the Enigma cipher had been broken is well known. In 1943 the British were faced with evidence about the possible compromise of the Typex machine, the highest-level communications device in use across their armed forces. This paper compares the response of the British to the Typex scare to the German investigations concerning Enigma.

Reconstructing the story, it seems that the Germans had, in fact, read some Typex messages. Although Allied code-breaking during the war operated on a higher plane than Germany's, it was inappropriate to assume that the Germans could not do so. Various similarities between the German and British responses emerge: the British were ill-adapted to investigating their own security; they were reluctant to chase down the truth, using arguments to justify their desire to be reassured that all was safe.

1 Introduction

The British answer to high-security enciphered radio communication was the Typex machine. Typex has been discussed elsewhere (Erskine, 1997; Ferris, 2005). Suffice it to say here that was an electro-mechanical machine, whose principle, as with the more famous Enigma machine, was a set of wired rotors each of which switched a letter of text for another, with the rotors stepping on to create a different cipher overlay each time a key was pressed. Additional security features included settable entry and exit 'stators', rotor-cores which could be inserted backwards so as to invert their left-right behaviour, a set of ten rotors from which to choose five, and in some versions a plugboard (like the German military version of Enigma).

All this was good for British communications security, but there were still vulnerabilities. First, the British armed services were not universally equipped with the plugboard version of Typex. Then there were elementary errors of cryptographic security, such as (in particular) the operational error where the machine operator chose as his start-position for encipherment a non-random orientation of rotors based on the end-position of the preceding message – facilitating a cryptanalytical attack known to Bletchley Park as 'Herivelismus'.[1] Together with the risk of capture of a machine, its operating instructions, and rotors, there was a high risk that the German code-breaking organisations in the Oberkommando der Wehrmacht (German Armed Forces General Staff), the Oberkommando des Heeres (German Army General Staff) or the Luftwaffe Chi-Stelle (German Air Force Cipher Bureau) would be able to crack messages sent in Typex.

Despite this, the idea has persisted that the Germans never broke Typex (Hinsley et al., 1981; TICOM, 1946, vol 4). That received view is not clearly wrong, but there was certainly a point

[1] TICOM document D-83, UK National Archives (TNA) HW 40/87.

during the war when it appeared that the Germans could read Typex messages and had done so. This paper examines the evidence which the British had before them, and how the British reacted. A comparison can then be drawn to the – perhaps notorious – lack of effective response on the German side to a series of equivalent scares about the security of Enigma (cf. Mulligan, 1985; Ratcliff, 1999, 2006).

2 The Typex Scare of 1943

The news came out, as news does, in bits and pieces. First there was an alarming message from Bertie. 'Bertie' was the name given to Commandant Gustave Bertrand, the signals intelligence officer from the French Army's 'Deuxième Bureau' who had managed somehow to re-establish himself under the Vichy régime and run a small code-breaking operation, which despite everything remained in contact with the British Secret Intelligence Service, the parent of the Government Code & Cypher School at Bletchley Park. As well as running a team of Polish, Spanish and French code-breakers, Bertie had his ear to the ground in many ways, receiving news relating to radio communications security and similar issues from a range of sources.

On 19 July 1942, Bertie signalled to the British that there were reports that the German Air Ministry was using adapted versions of two 'English cipher machines' captured at Dunkirk.[2] It is not difficult to imagine that the British had lost a Typex machine in the chaos of the Dunkirk evacuation, and indeed they had.[3] However, Typex would be difficult to crack without the rotors, and with a set of ten rotors from which to choose five (as opposed to the three when Marian Rejewski achieved his feat of reverse-engineering the Enigma machine in 1932) the reconstitution of the wiring of Typex rotors would have been a herculean task without a physical capture; it seems that the Germans did not manage to capture Typex rotors at Dunkirk. (This probably reflects the fact that the Typex equipment was too bulky to be easily moved, so had to be left behind, whereas the rotors could be much more easily transported or disposed of.)

Whether Bertie's message needed to be taken seriously, amid all the noise of contrary intelligence heard in the cacophony of war, is difficult to judge even with hindsight. But in the same month there was another snippet of news. A certain Dr Vögele had, according to a German signal intercepted and decrypted at Bletchley Park, been sent to visit cipher material captured following the fall of Tobruk to Rommel: the signal was sent only five days before Bertie's telegram, and only just over three weeks after the capture of Tobruk. The British probably did not know at that stage that Vögele was a senior cipher specialist ('Regierungsrat') in the Luftwaffe's Chi-Stelle, thus establishing a link to Bertie's note which showed that German Air Force intelligence could be engaged in an attack on Typex security. A note on the telegram, apparently in the handwriting of Lt Cdr Russell Dudley-Smith RNVR, the officer at Bletchley Park tasked with cipher security questions, says 'no typex machines forward of Gambut [a military airfield complex in Libya] during recent fighting': maybe, then, this was more noise.[4]

The third tiny piece of the jigsaw-puzzle came on 15 August. 'The following message in code has been received from a British Prisoner of War in GERMANY… COLONEL STEVENSON C.S.O. S. AFRICA DIVISION REPORTS THAT ALL CODES CIPHERS TELEX MACHINES AND DRUMS DESTROYED TOBRUK BEFORE JERRY'S ENTERED.'[5] Why would a prisoner go to such lengths to report that what ought to have been done, had been done, unless perhaps there was a question about it?

3 The British response

Whatever the immediate cause, something seems to have prodded the British into action on Typex security. It may have been an intercept. On 20 January 1943, the commanding officer of a signals intelligence regiment, believed to be stationed in Greece, wired 'OKH/In 7/VI' asking whether the recipient dealt with a certain kind of British five-letter traffic. 'In 7/VI' was the cryptanalytic division of the Oberkommando des Heeres, and it was noted that this was the first mention in secret signals of what seemed to be a programme of interception of Typex messages.

[2] TNA HW 40/88.

[3] There are many TICOM interviews which stated this, for example, D-83 (TNA HW 40/87), D-40 (US National Archives and Records Administration (NARA) RG 457 HMS P11 Box 24).

[4] TNA HW 40/88.

[5] TNA HW 40/88.

To begin with, Alan Turing was asked to advise on the maximum secure message length for a Typex signal – on the basis that long signals should be split into pieces, each enciphered using a different rotor start-position, thereby reducing the exploitability of 'cribbing' to reveal the settings in use. Turing reported on 10 July 1943, 'it seems that 1000 letters would not be too long with the form of the machine with a pluggable Umkehrwalze [reflector rotor], but that with the other form of the machine the question turns on the crib-avoiding discipline'. [6] The problem which this short sentence reveals was that the British Typex machine was fundamentally insecure unless they were using the pluggable reflector. In any case, Turing's assessment was hardly a thoroughgoing examination of security relating to Typex.

What the sentence from Turing's paper does not reveal is that the Typex machine existed in a form which lacked not just a pluggable reflector, but any kind of plugboard at all. At least some of the time, the British Army in North Africa was using only the simplest version of the Typex machine without the all-important plugboard. Alan Turing – who had worked on the Enigma problem in the earliest years of the war had just confirmed the ease of breaking a rotor-based cipher machine based on cribbing. Dilly Knox had broken such machines from the mid-1930s onwards. Post-war German interviews and documents confirm that the Germans knew how to do this too.[7] Worse still, Commander Edward Travis, then deputy head of the GC&CS, had explained in 1940 that he had concerns about Typex.[8] The central problem with Typex in 1943 was that the British were ignoring what they themselves knew about rotor-machine security: allowing the services to use a bad machine with lax operational practice, a combination of affairs which surely ought to have rung alarm bells.

The bells were not going to ring, though, without an accumulation of evidence which was overwhelming, and that would only happen if the Germans had actually broken Typex and then told the British that they had done so. This is, in practice, what happened when the Allies got notice that Colonel Fellers's 'black code' messages back to Washington from Cairo were being read, and when the Allies got notice that the Royal Naval Cypher number 3 was being read by the German Navy's B-Dienst with appalling consequences for the security of convoys in the North Atlantic (Tighe, 1945). Thus, by 1943 there was a growing body of concern that not all was well in the world of Allied signals security. The most damning case regarding Allied army and air force signals was presented by the Germans themselves, when their field signals security regiment NFAK (Nachrichtenfernaufklärung) 621 was captured in Tunisia. Not only did the prisoners explain that American signals security on the battlefield (where lower-grade ciphers were in use) was rotten, but there was a fresh set of indications that Typex itself might have been read. It only required the Germans to keep quiet about their successes for the British complacency to continue.

During the final stages of the battle for Tunisia in May 1943 the German signals unit NFAK 621 was among those who surrendered to Allied forces. NFAK 621 had a difficult history. On the one hand, the unit had been immensely successful at providing Rommel with real-time signals intelligence, based on both traffic analysis and in-the-field cryptanalysis, but on the other hand its star officers and much of the unit had been captured in July 1942 during the early stages of the second Alamein battle. Now even more men from the rebuilt unit had once again fallen into Allied hands. Leutenant Bode was interrogated in June 1943, and revealed that he had been engaged on translating and emending British machine messages from 1937 until June 1940. The interrogator asked what kind of a machine; Bode said 'a sort of typewriter. A man just typed the nonsense stuff, and the English came out on a tape.' That sounded rather like a Typex. The intelligence captain from MI8(a) who interrogated Bode added that 'Unfortunately, BODE, at that time, was a very junior N.C.O., and the knowledge of the machine was very restricted. It was in fact treated very much as our own CX/MSS knowledge.' (CX/MSS was the designation to intelligence received from 'most secret sources', in other words decrypts resulting from cryptanalysis.)[9]

But 'the trouble with BODE is that he is trying to tell us more than he knows and is only too

[6] TNA HW 40/87.

[7] OKH In 7-VI Kriegstagebuch for July 1941, Politisches Archiv Berlin, TICOM collection S8 (PA-S8), nos T-2755 to T-2764; TICOM document D-83, TNA HW 40/87.

[8] TNA ADM 223/505.

[9] TNA HW 40/88.

ready to agree with anything one says.' On the other hand, 'there is a possibility of obtaining confirmation of BODE's story from other members of 621 Intercept Coy. when they arrive in this country for interrogation.' So, another pair of prisoners were interrogated on 23 August 1943. One – Leutnant Haunhorst – had been a divisional intelligence officer working closely with NFAK 621. The other – Oberleutnant Possel – was a senior radio officer in the 10th Panzer Army Intelligence Regiment. [10] Independently, these two officers said that one or more Typex machines had been captured at Tobruk, and a certain 'Warrant Officer Wagner' using 'reference books' containing settings had been able to set the machine and decode messages. Some of the reference books came from the 'Haupt Chiffrier Stelle OKH' – the Head Cipher Office of the Oberkommando des Heeres.[11]

Obviously, further action was needed. But the investigation was, almost perversely, directed in the wrong way. Rather than look at the vulnerability of Typex, it seems that evidence to confirm the security of Typex was sought out.

4 Confirming confirmation bias

So the first thing actually done was to track down what had happened to the Typex machines at Tobruk. Questionnaires were sent out and an inquiry as to destruction procedure was undertaken. 'Navy report no typex equipment held by RN ships or staffs using Tobruk. RAF report no machines or drums [rotors] held RAF in Tobruk relevant dates. They add all drums held RAF during retreat to Alamein safely returned.' 'Your [question] five One set black drums Number 1270 handed over on authority CSO 8 Army to Captain MacFarlane Cipher Officer 2 SA Division reported by latter destroyed night before Tobruk file reference 8Army X2/883 of 20 June 42. Destruction certificate black drums 1270 based on this cipher message which stated all cipher equipment except one "W" Book one local recyphering table destroyed.'[12]

Another task was to locate the other members of NFAK 621 who might be able to cast further light on the alleged reading of Typex in North Africa, as revealed by Possel and Haunhorst – ideally the Warrant Officer called Wagner. After some months, ex-NFAK 621 prisoners Habel and Bremer were located, but there was no trace of any Wagner. Habel, who had been the commander of NFAK 621 at the time of its capture, was transferred from the United States to London together with Bremer, where they arrived on 22 December 1943, and interrogated. 'Although every means possible were used to induce these two men to talk, their inherent security which is of an abnormally high standard has completely defeated normal methods of approach.'[13] So the British were none the wiser. Plus, the proper procedures had been followed at Tobruk: destruction certificates had been prepared, which should not have happened if the Typex equipment had not been properly destroyed, so clearly prisoners like Bode, Haunhorst and Possel must be mistaken or attempting to mislead.

Indeed, it was quite possible that they had been mistaken. Various forms of rotor-based cipher equipment was being used in North Africa. If Typex were being read regularly, through cryptanalysis rather than capture of a few weeks' worth of settings, surely a more robust response to Allied plans would have been experienced on the ground, whereas it had been possible to take the Axis by surprise in relation to major operations like TORCH (the landings in French North Africa) and HUSKY (the invasion of Sicily). By the spring of 1944, with the preparations for the main invasion of continental Europe well under way, those events seemed a long time ago, and the Typex scare of 1943 something one could stop worrying about.

It was therefore, perhaps, not surprising to find Gordon Welchman of Bletchley Park reaching that conclusion, even before Habel and Bremer had been grilled. Welchman was not only highly intelligent and highly persuasive but he also carried the confidence of Commander Travis, who by this time was head of Bletchley Park. Travis appointed Welchman to lead a Machine Coordination and Development Section in September 1943, which meant that among other things Welchman was (occasionally – there was a question over his terms of reference) in charge of security of cipher machinery. Welchman's memo is interesting:

[10] TICOM document I-16, TNA HW 40/89.

[11] TNA HW 40/88.

[12] TNA HW 40/88.

[13] TNA WO 208/5109.

> This story about the mysterious Wagner sounds like a garbled account of something true. I imagine that, having captured a few Type X machines, the Germans would have the sense to maintain a forward decoding party to take full advantage of any captured keys, but it seems unlikely that we should have lost any Type X keys in Tunisia and the story suggests that there is far more in it than that….
>
> As regards breaking, I have always felt that the Germans could not be breaking any of our Type X traffic because, if they were, they would take steps to prevent us breaking their enigma traffic….
>
> I have never thought seriously about possible methods of breaking Type X, but should have guessed that the equipment necessary would be pretty bulky unless the problem is being simplified by extreme carelessness….
>
> On the whole I feel that a thorough investigation would be a good thing, but I don't see who could do it. However it may be possible to shoot down the Wagner story after further discussion here and further interviews with P.O.W's. It is quite possible that Haunhorst was merely shown how the Type X machine worked, and it would be interesting to know whether he actually saw an English message decoded.[14]

So the idea of an investigation into Typex security was not pursued. Despite being told that the Typex project was clothed with the utmost secrecy within the German radio intelligence regiment, the idea that 'Wagner' might have been a cover-name for the Warrant Officer actually involved does not seem to have occurred to those involved in the interrogations. The British had decided to look away from the possibility of 'extreme carelessness' and rely on the specious idea that 'if they were, they would take steps to prevent us breaking their enigma traffic'. But this argument was nonsense: putting it in reverse, the British were taking no cryptanalytical steps (despite the success against Enigma) to check up on Typex, and using that as an illogical excuse to take no steps to protect Typex.

In a note of 3 June 1944, Lt Cdr Dudley-Smith stated that 'Five months of interrogation has produced no additional information on German exploitation of Typex in N. Africa.' He sounds weary of the whole business. And that was how things stood, until after the war was over.[15]

5 TICOM

As is now well known, a 'Target Intelligence Committee' (TICOM) was set up in the summer of 1944 to track down German codebreakers and interrogate them as to their successes or otherwise (Rezabek, 2017; Jackson, 2013; TICOM, 1946). Over the course of the months and years following the invasion of Germany, many German individuals were asked to describe their attacks on Typex and the successes which they had had.

Some of the answers were confusing, and some prisoners seem to have changed their testimony. However, the consistent story from the team at OKH In 7/VI (who had had Typex on their to-do list for years) was that they had initially put a great deal of effort into the attack on Typex, knowing that they could reconstitute the keys through cribbing, if they knew the wiring in the coding rotors; that they could reconstitute the stepping arrangement of the rotors, if they knew the key; and that partial cribs were available because through statistical analysis they knew that RAF messages began stereotypically with the letters AIRX and ended with a series of Xs as filler to make up to a round multiple of five characters for a group. They had Hollerith machinery in abundance and were adept at using it for sorting and statistics – as indeed had been done at Bletchley Park. They had captured keys for May and June 1940 and a memorandum from the War Office (MI1(b)) which remonstrated against lax cipher discipline. They were using 'Herivelismus' to predict rotor start-positions. All in all, they had had a good start on Typex.[16]

But later on, the Typex experts – notably Dr Erich Hüttenhain, Regierungsrat in the OKW's cipher research division – had abandoned work. Recovering the rotor wirings through statistical analysis would demand excessive amounts of Hollerith time, relative to the resources available and other priority work which was using the machinery to good effect. What is more, it is not clear that they had any answer to the more challenging problem of the plugboard – by contrast to the attack in Britain on Enigma, for

[14] TNA HW 62/5.

[15] TNA HW 40/88.

[16] TICOM document D-83, TNA HW 40/87.

which Alan Turing's Bombe had specifically been designed. Yet Hüttenhain's boss, Oberstleutnant Mettig, who at the time of the Tobruk capture was in command of OKH In 7/VI, said under interrogation that Typex was read in North Africa in 1942.[17] But Mettig's evidence seemed to be contradictory. He had said, only five days before, that the official in charge of the British section of In 7/VI, Referat Zillmann, 'despite great efforts was unable to break the English cypher machine'.[18] Mettig later retracted the statement about North Africa, but doubt lingered.

None of the OKH codebreakers interrogated seem to have been personally present in North Africa in 1942. Dr Vögele had been there, and he was accompanied to Africa by Inspektor Harms, from Mettig's team in OKH In 7/VI. Our knowledge of this visit comes partly from a bugged discussion between Hüttenhain and another German codebreaker, Dr Fricke, which took place in the evening of 25 September 1945. Harms, aged 50, was not happy in Africa, and came home after two weeks complaining of the heat. It seems that Harms didn't think too highly of Vögele: Vögele had 'done nothing' while they were there, except that he had filled two suitcases with material and taken them back to Germany while, apparently, Harms came back empty-handed. Furthermore, Hüttenhain was certain that Harms had seen nothing of Typex in North Africa – he would have said so, and he hadn't. Perhaps, hinted Hüttenhain, Vögele (of the German Air Force's Chi-Stelle) had had his own Typex operation in Potsdam?[19]

The basics of what Hüttenhain was telling the TICOM interrogators are confirmed by the war diary of Inspektorat 7/VI.[20] Harms certainly went to Africa in July 1942, when there was much excitement about the finds at Tobruk. The war diary also confirms that Zillmann had made no progress on Typex cryptanalysis in OKH. But lack of success on the part of Zillmann, as confirmed by Mettig, did not confirm lack of success in every place and by every agency. What is more, there were liaison meetings at various times between OKH In 7/VI and the Luftwaffe's Chi-Stelle, with Vögele in particular, while Mettig was commanding In 7/VI;[21] at the time of Tobruk and after he was in a position to control the liaisons with other services. These liaisons included a link-up connecting the intercept team of the Luftwaffe in Athens and the NFAK 621 outpost in North Africa.[22] The missing part of the Typex puzzle was in the Chi-Stelle, and held by Dr Vögele in particular.

Luckily the TICOM group had captured Dr Ferdinand Vögele in August 1945. Vögele was a reluctant captive.[23] Vögele wrote an extensive CV, and catalogued numerous breakthroughs on various American code and cipher systems; as it was a British system, Vögele did not mention Typex.[24] Vögele's colleague Lieutenant Pick wrote about British systems and repeated the mantra that an attempt had been made against Typex in 1940 but abandoned. Although Vögele was interrogated specifically about Typex, the interrogation took place on 25 September, the same day that Hüttenhain and Fricke were discussing the Typex question under the British microphones. So the interrogation of Vögele about Typex lacked the input from Hüttenhain and Fricke, and was superficial:

> VOEGELE stated that he would certainly have heard had Typex been broken, and reiterated most emphatically his belief that Typex was never broken. His considered opinion was that the breaking of Typex was impossible… He ceased taking the messages in 1940. When informed that a P.O.W. taken in Cyrenaica had described what appeared to be the registration of Typex traffic at Athens in 1942 or 43, VOEGELE said that one of his staff there, a cryptographer named ROSSKATH, had unofficially arranged that they take Typex traffic again for 4-6 weeks.[25]

Despite this feeble examination, the evidence was beginning to fall into place. Even that old telegram from the early days of the scare, when In 7/VI had been asked by Athens about Typex, could be seen to be part of the picture, if someone went through the war diary and joined the pieces up.

[17] TICOM document I-48, TNA HW 40/166.

[18] TICOM document I-78, TNA HW 40/167; TNA HW 40/89.

[19] Transcript of bugged conversation between Hüttenhain and Fricke, TNA HW 40/89.

[20] See fn 7; also PA-S8 T-2762.

[21] PA-S8 T-1620.

[22] PA-S8 T-2762.

[23] TICOM document I-87,NARA RG 457 HMS P4 Box 35.

[24] Seabourne Report, Vol XIII, NARA RG 457 HMS A1-9032 Boxes 974-6.

[25] TICOM documents I-87, I-119, NARA RG 457 HMS P4 Box 35.

Yet, oddly, the conclusion on 22 September had been that it was Hüttenhain who was misleading the interrogators on the story of Typex. 'Great emphasis is laid on the idea that they considered enigma, and therefore Typex insoluble.' By the next month, it was thought that Vögele was 'the problem' – he had been caught out on the business of Typex interception in Greece, and 'again we have no definitive evidence but the whole story does not ring true.'[26] Vögele was a civilian and the time was up; the TICOM team could not hold him indefinitely, and by the time of that report it is likely that Vögele had gone back to Germany. The secret of Typex in North Africa would remain just that.

The conclusion? It seems that the Eighth Army had left behind a Typex machine, complete with rotors and keys, at the time of the capture of Tobruk. Both OKH and the Chi-Stelle had sent someone over, but it was Vögele who had filled two cases with the materials and it was his agency, not OKH's Harms, which had exploited it. For some period after that, decryption of Typex messages was possible by figuring out the message settings being used by the British. Mettig was in the loop, but his subordinates and OKW colleagues seem not to have been: the to-and-fro between NFAK 621 and Berlin, noted by Prisoner Haunhorst, may not have involved OKH, especially if it concerned RAF issues. The main cryptanalytic player was Vögele of the Luftwaffe's Chi-Stelle. The TICOM interrogators do not seem to have picked up on the differences, or the rivalries, between the German agencies. The limited duration of the German success against Typex was probably due to the gradual adoption of the plugboard model of Typex, against which even Vögele's Chi-Stelle had no answer.

So Typex messages probably had been read, although on the basis of battlefield captures rather than as a result of Bletchley-style general cryptanalysis. Even so, that poses the question whether the British should have reacted differently when confronted with evidence that their most secure communications device was either compromised or under cryptanalytic attack.

6 Comparing German and British responses to security scares

The German Marine-Nachrichtendienst (naval intelligence service) is widely perceived to have scored not just one but three own-goals in failing to detect the Allied breaks into naval Enigma during the Battle of the Atlantic. Investigations took place in 1941, 1943 and 1944 into the security of Enigma. On each occasion, too-good-to-be-true coincidences were drawn to the attention of those in charge of signals security, and on each occasion alternative explanations, fantastic if not wholly absurd, were preferred to the simple, obvious, and correct interpretation that Enigma messages were being read by the Allies (Tighe, 1945; Ratcliff, 2006; Mulligan, 1985). German intelligence preferred its own narrative that Enigma was secure, so it had (consciously or unconsciously) to be shown to be so, and all evidence was interpreted in that sense. The consequences for German, and Allied, losses in the North Atlantic are well known.

To quote Dr Rebecca Ratcliff (1999):

> In concluding that Enigma was not the source of enemy information, the investigators set out to prove only what could not have been the leak, Enigma. They did not set out to prove what *was* the source and did not produce a scenario which explained the [British] Admiralty's information… German intelligence assumed the enemy would either be able to read the ciphers completely – and within a three to five day period or not at all.

In parallel, though on a smaller scale, the British were shown evidence in 1942 and 1943 which indicated that (as predicted by Travis in 1940) Typex was not secure. Gordon Welchman's memo seems to have many of the same errors as the German investigations, as explicated in Dr Ratcliff's analysis. Welchman should not carry the blame for British failings, though: in 1942 the number of personnel in charge of own-systems security at Bletchley Park was one – the diligent Lt Cdr Dudley-Smith – and he a non-specialist to boot (Erskine, 2002). The Admiralty appointed Lt Cdr George Bull RNVR as adviser on cipher matters to the Naval Intelligence Department's Security Panel in the spring of 1942;[27] by 1943 Alan Turing had also taken on a communications security role (Turing, 2015, p 164), so things were slowly beginning to

[26] TNA HW 40/89.

[27] TNA ADM 223/505.

improve on the British side at the time of the Typex scare, but a security mindset was not yet embedded. (By contrast, when the British spotted defects – through decrypts of German messages – in American cipher security in North Africa, they were quick to point them out, and the Americans as quick to implement change.[28])

Perhaps because of the paucity of personnel available for the task, the British reaction to the Typex scare of 1943 was almost as weak as that of the Marine-Nachrichtendienst. Confirmation bias seems to have influenced the decision to pursue further investigations – trying to prise more details out of more German prisoners, and checking for destruction certificates – rather than looking at the actual security issue, which was already known and ought to have been better understood. Surely it was wrong to own up to a problem with Typex only after it had been firmly established that the Germans had actually exploited Typex – to wait for sight of the horse bolting before checking the fastening on the stable door?

It seems that if they had been equipped with what Dr Vögele came away with from Africa in 1942, the talented team of German codebreakers in OKH or OKW might have been able to make some headway with the Typex problem. They might have been defeated by an earlier adoption of plugboard-equipped Typex and with more rigorously enforced operating discipline, but that does not seem to have been the outcome of the British examination of the post-Tobruk evidence. In fact, what saved the British from a potentially devastating reading of Typex messages in the months following Tobruk was the organisational split between the armed services' own cryptanalytical organisations, OKW, OKH and the Luftwaffe's Chi-Stelle. Vögele did not, apparently, have direct access to Hüttenhain, whose know-how on Typex was not shared.

7 Concluding comments

The British response to the Typex scare of 1943 has similarities to the German responses to the Enigma alarms throughout the war. Neither side wanted to know that its high-security communications machine was insecure. Neither side wanted to investigate properly or to implement changes which would fix a risk without overwhelming evidence which would arrive too late, in other words after breach – potentially a breach with monumental consequences – had actually occurred. A risk-based assessment was done by neither side.

There the similarities stop. Fortunately for the Allies, the British machine was more secure than the German one, and with the use of secure indicator procedures and the plugboard, significantly so; Bletchley Park was ahead of the game on mechanical cryptanalysis, thanks to the work of the Poles before the war and the invention by Turing and Welchman of the new cryptanalytic bombe; and the Germans had not managed to invent cryptanalytic techniques which could crack a plugboard-adapted rotor cipher machine. Much of the difference was a mismatch in brilliant inventiveness. Some of that brilliance might just as easily have been on the other side; it was the Allies' good fortune that they possessed it in greater measure.

References

Erskine, Ralph. 1997. *The Development of Typex*. Enigma Bulletin No.2 p 69-86.

Erskine, Ralph. 2002. *The Admiralty and Cipher Machines during the Second World War: Not so Stupid After All*. Journal of Intelligence History Vol 2 (2) p 49-68.

Ferris, John. 2005. *The British "Enigma": Britain, signals security and cipher machines, 1906-1953*. Chapter 3 in 'Intelligence and Strategy – Selected Essays'. Routledge.

Hinsley, F.H., et al. 1981. *British Intelligence in the Second World War*, vol 2, appendix 1. Cambridge University Press.

Jackson, John. 2013. *Hitler's Codebreakers – German Signals Intelligence in World War 2.* BookTower Publishing.

Mulligan, Timothy P. 1985. *The German Navy Evaluates Its Cryptographic Security, October 1941*. Military Affairs Vol 49 (2) p 75-79.

Ratcliff, R.A. 1999. *Searching for Security: The German Investigations into Enigma's Security* in Alvarez, D. (ed), 'Allied and Axis Signals Intelligence in World War II'. Frank Cass, p 146-167.

Ratcliff, R.A. 2006. *Delusions of Intelligence.* Cambridge University Press.

Rezabek, Randy. 2017. *TICOM: the Hunt for Hitler's Codebreakers.* Privately published.

TICOM (Target Intelligence Committee). 1946. *European Axis Signal Intelligence in World War II*

[28] TNA HW 40/92.

as Revealed by 'TICOM' Investigations and by Other Prisoner of War Interrogations and Captured Material, Principally German. https://www.nsa.gov/news-features/declassified-documents/european-axis-sigint/

Tighe, W.G.S. 1945. *Review of the Security of Naval Codes and Cyphers – September 1939 to May 1945*. Unpublished, TNA ADM 1/27186.

Turing, Dermot. 2015. *PROF: Alan Turing decoded.* The History Press.