# 7
# Signals Intelligence and the Battle of the Atlantic

In discussing Ultra and the part that it played in the Battle of the Atlantic, it is important to understand not only what it was and how it was obtained but also to realise how it fitted into a number of contexts, especially communications, the enemy's efforts in the same field and intelligence as a whole. Unless these are absorbed to some extent, then the tendency to mythologise Ultra becomes nearly irresistible, to the detriment both of appreciating its true worth and of understanding its part in the whole history of the Battle of the Atlantic.

Initially, it helps to define a number of commonly used terms. Sigint is properly speaking the exploitation by reception of any transmissions made by an enemy in the electromagnetic or acoustic spectra; it does not just refer to emissions in these media used for communications. To be correct, this is Comint. There are, of course, instances of radio emissions used for non-communications purposes which are of intelligence interest. Most notably, there are the German radio navigation systems such as the *Knickebein* air bombing aid and the *Sonne* oceanic navigation system.[1] While describing terms, it is appropriate to look at the language of the decryption process and its product. *Enigma* is the name for the cipher machine used by the Germans. It had many variations, both in the electro-mechanical machine itself and in the systems of use, by the various selection of wheels, plug connections and the settings of these components. The various systems were known by different codenames by the two sides. Thus the Atlantic U-boats for most of 1942 used a system known to the Germans as Triton and the Allies as Shark. Ultra is a term which has caused some difficulty. It has been contended that originally it referred to what was only a security caveat on signal messages carrying information derived from the decryption of Enigma-encoded materials and not to the product itself.[2] Whatever

the truth of the matter, it is now fairly common to refer to the output itself by the name of Ultra and this could hardly have been avoided when the original work published in English on the subject bore the title that it did.[3] However, it is important to note that there were other terms in use such as 'Z', 'Special Intelligence (SI)' and 'Boniface'. But perhaps the most important thing to remember is that Ultra by whatever name it was known was only a part of Comint, in itself a subset of Sigint and even that was a component of the whole range of intelligence available to the Allies.[4] This will be expanded on later in this chapter. But before returning to Sigint, it is necessary to examine some aspects of radio and its use that Sigint exploits.

## Radio – basic characteristics

Radio permits long-range communication. This is such a platitude simply because it has been taken for granted in an age when speech and images from the furthest part of the world and from outside it are transmitted either directly or via space into our homes; when it is possible to talk from almost anywhere to almost anywhere; where aircraft, ships and even weapons can navigate themselves with great precision to almost anywhere in the world. Under these circumstances it is easy to forget two things: the simplicity of the presentation now overlays considerable complexity and that it was not always quite so easy as it now seems to be. It is therefore useful to describe some fundamental properties of radio as they applied to submarine warfare in the 1940s.

The first point to note is that the selection of frequency band, that is the number of vibrations or cycles per second that were used was of critical importance for ensuring communication.[5] In broad terms the highest frequencies which are of use for communications have excellent characteristics but for one problem – their range. In practical terms their limit under most conditions is about 25 miles for two stations attempting communication when both are on the earth's surface.[6] Such technology was not generally available at the outset of the war in any case and its applicability to submarine warfare would have been dubious.[7] The most reliable frequencies for long-haul communications are those of the Low and Very Low Frequency (LF/VLF) bands which travel great distances. But these tend to be much more suitable for shore installations than for units at sea for two simple reasons: size and power requirements. A typical shore LF/VLF shore transmitter might easily occupy an area measurable in hundreds of yards or more. It would also use a great deal of power. What became

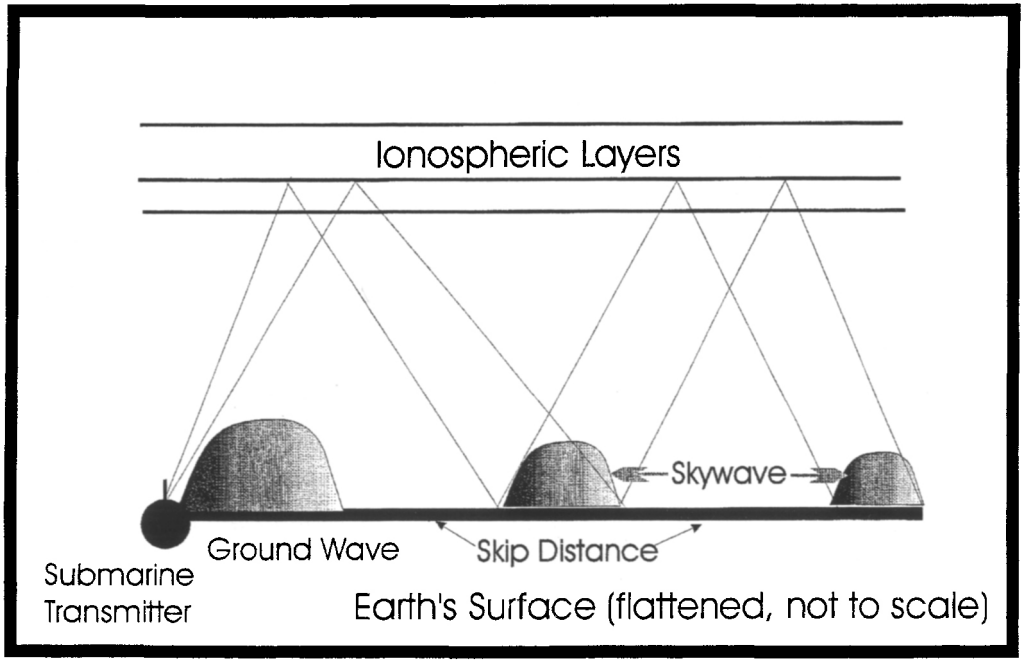


Figure 7.1

*Figure* 7.1 **High frequency (HF) propagation**

known as shortwave or High Frequency (HF) radio appeared to be much more attractive for submarine communication. It made no inordinate demands on aerial size for either reception or transmission and it only required relatively low power for long-range communication. Here, it would appear, was the answer to the passing of information to and from submarines at sea in the deep Atlantic from Europe and the passing of orders back to these U-boats.

But there was a problem, too. Whereas LF and other frequencies below HF worked by having a considerable groundwave, that is, a signal path which followed the curvature of the earth for very considerable distances, HF did not behave in this fashion. What it tended to do was to behave less uniformly. Firstly, there was a ground wave extending some tens of miles from the transmitter. Although this was to have important consequences for the Battle of the Atlantic, the groundwave is not described in this chapter.[8] Secondly, the signal would move upwards until it hit the layers of the ionosphere, which are found some 50–400 miles above the earth's surface. Then, in general, they would be bounced back to earth in a footprint of some size some hundreds or even thousands of miles from their originator. The first problem with this phenomenon is that there is a gap, often of considerable distance, between the outer limit of the groundwave and the first of the returning skywave or between the first and second or subsequent skywave footprints. None of this would be very troublesome were it not for the next difficulty, that of predicting the effect of ionospheric bouncing. The effect is also subject to variation with location, time of year, frequency selected and, most notably, time of day. Sometimes, too, transmitter power would be insufficient. As a result, although it would be desirable to exploit the effect by bouncing it to where a known and friendly receiver was stationed, this was quite simply not practicable and thus interception by unintended receivers was all but inevitable. The problem was most marked for units at sea whose transmission options were most limited. It was much easier to cover a range of options from shore transmitters by means of transmitting on more than one frequency within the HF band and also by use of the other long-haul bands. The net result of all this was that submarines often had difficulty in communication, resulting in the need to transmit messages more than once and thus giving more interception opportunities to the Allies. For the purposes of this book, and to a readership largely weaned on instantaneous and reliable communications, this is an important point to remember.

## Radio communications – a two-edged sword

For much of the Battle of the Atlantic, radio communication was both an essential part of the German submarine system and its greatest vulnerability. This rather bald statement needs both qualification and explanation. The proviso is that, of course, for very considerable periods submarines worked in effect as more or less independent units. Under these circumstances, much of the rationale for copious signalling disappeared. This occurred at different times and for different reasons. The first exclusion should perhaps be made for those submarines operating singly in distant waters. As they did not have to coordinate their activities with any of their brothers, except in a very general sense, there was no need for frequent signalling. Indeed, their *modus operandi* militated against it.[9] Next, there were long periods even in the main Atlantic battlegrounds when closely coordinated action was neither desirable nor, latterly, possible. Such action related to the early part of the war when the numbers of submarines were too low to allow group operation and independent targets were both easy and plentiful. A further period occurred in early 1942 when *Paukenschlag* took submarines to the east coast of the United States and the ready availability of targets meant that there was no necessity for group operations. A different rationale informed the decision in 1944 to engage in inshore operations around the United Kingdom. Here it was the impracticality and unprofitability of attempted anti-convoy operations which predicated submarines being used singly.

However, for the group operations – the *Rudeltaktik* – which predominated in several periods, largely from the autumn of 1940 through to the end of 1941, and again from mid-1942 to mid-1943, plentiful radio communication was not just desirable but essential to the conduct of operations. This arose from a combination of Dönitz's own experiences of submarine command in the First World War where he learned in the hardest way possible that a single submarine opposed by a number of escorts was at a disadvantage. It also took account of pre-Second World War tactical exercises and trials when despite the promise of group attack it became obvious that control would be a central problem of this tactic.[10] Originally it had been thought that a seagoing senior officer in a submarine himself could coordinate and control such attacks but this quickly proved impractical. As a result a method of command evolved in which this function was assumed by the BdU headquarters ashore in Europe. Such a method, whilst it could be effective, put an enormous premium on the flow of information from U-boats at sea and

thus created a very large demand for radio communication. There can be little doubt that the *Rudeltaktik* could be every effective at its best and that the Allies paid dear for those cases when it was working at peak efficiency, such as with the attacks on convoys SC42, TM1 and HX229/SC122.[11] But what is also clear is that all such operations – even when no convoy contact was made – generated a great deal of signal traffic in both directions. This was to be one of the submarine force's most vulnerable points.

## Reaping the communications harvest I – direction-finding

Although the system of submarine communications used by the Germans was an integral part of their pattern of anti-shipping warfare, it also presented the Allies with a major potential source of information. A casual student of the Battle of the Atlantic might assume that all of this came from Ultra but even before and besides this, there were other useful products too. In the limited sense of what might be extracted from a single signal, clearly decryption represented not only the most difficult technical feat but also the most thorough exploitation too. Such a statement, however, tends to ignore the other Sigint products that were available. This is to some extent interrelated with hypotheses and, at best, knowledge about how an enemy is either conducting himself or would like to.

It should never be forgotten that the mere act of intercepting an enemy signal provides information in itself, however rudimentary. The existence of a number of broadcasts or other transmissions by a shore authority may suggest scale and type of activity. Clearly, without too much technical analysis, frequencies selected and power of transmission may suggest, for example, whether the intended recipient is likely to be close to the transmitter or further away. From sea, the very least that can be deduced is that some seagoing unit is there. At the next level it may well be possible, without any significant deep analysis, to count the number of units at sea. This may be made more difficult if either total or partial radio silence is enforced – a circumstance which rarely obtained during *Rudeltaktik* operations. A good example of the opposite is the surprise obtained by the Japanese carriers on their long transit to Pearl Harbor in conditions of almost total radio silence.[12] But even if total silence is not adopted then the composition of a group of ships, which may transmit only selectively, might well be difficult to deduce from mere intercept alone. Dönitz's semi-autonomous submarines, however, used radio a great deal.[13] Initial British facilities for

this were adequate rather than luxurious but the advent of American participation improved the potential for interception.

Beyond doing little more than listening to German radio transmissions lay a series of techniques, the greatest of which in terms of both technical achievement and utility was almost certainly Ultra. But before discussing it, there are several other processes that are worth discussing. The foremost among these is almost certainly direction-finding of transmissions from ships and submarines at sea. Here the subsequent discussion is entirely concerned with this skill as practised on land; taking HF DF to sea took longer, was more limited and an account of its significance belongs elsewhere.[14] In the first few months of the war, the considerable geographical limitations of the British system – with its stations confined to the British Isles – was largely offset by the fact that many German operations were in any case restricted to the North Sea. However, once the Germans overran Norway, the Low Countries and France in 1940, the submarine genie was able to leave the bottle with ease and the inadequacies of the British direction-finding system were exposed. The Germans at this point correctly assessed this situation. However, what they failed to do was to keep pace with subsequent improvements in the system. These came about partly through physical extension of submarine operations into the Atlantic where direction-finding could be done, by better coordination of the product and eventually and most importantly, by the ability to use western hemisphere stations, not only in the USA but also in Canada.[15]

Although the interception and taking of rapid bearings eventually became commonplace and the collation of such information to produce locational information when the data supported it was a routine activity, there were elements of both science and art involved in getting the best out of the system. Perhaps the most important aspect was the simple one of the angle of intersection of the bearings.

Determining position depended in the first instance on obtaining at least two intercepts from at least two different stations. The greater the baseline distance the better, as this might permit improved triangulation. However, it was not just the distance between two intercepting stations that mattered but also their location relative to both each other and the signal source. Figure 7.2 illustrates this point. When the angle between the bearings is relatively narrow then the area of probability in which the target is likely to be is made much larger. This is, of course, partially a function of bearing accuracy. Were this parameter to be totally accurate and reliable then the angular orientation would not matter but, in practice, bearing measurement is subject to a number of

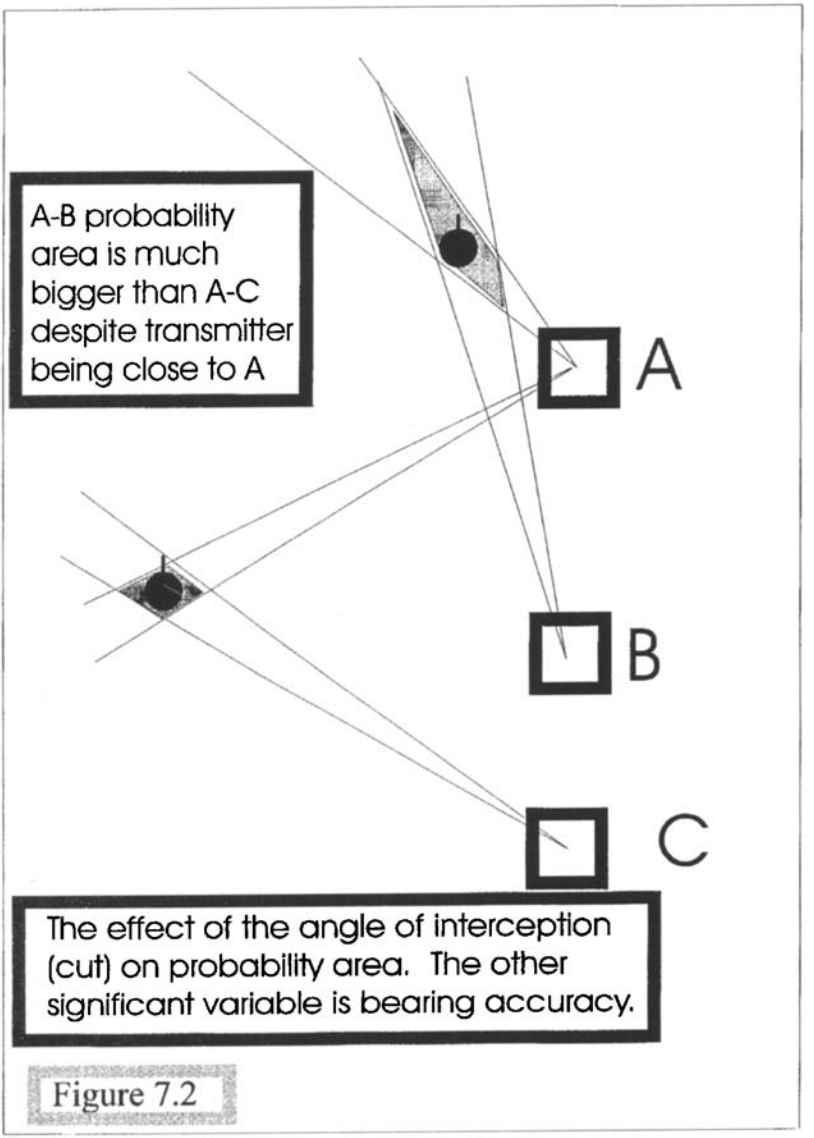


*Figure* 7.2 Direction-finding accuracy

errors and any given bearing is likely to be correct within a tolerance of several degrees. The factors which affect this include environmental ones along the signal path, the characteristics of the receiving equipment and local factors related to the placement of the aerial system. A further problem was that, in general, signals tended to follow the shape of the earth and thus HF DF bearings could not easily be plotted directly on standard, that is Mercator, projection charts. That said, those whose business it was to work with HF DF regularly, at intercepting stations and within such places as the NID and American organisations, rapidly became adept in extracting the best information possible from imprecise data. It is difficult to say exactly how good HF DF was as a locating device, as it could vary very considerably with circumstances. A broad American study taking in two years' worth of data concluded that average accuracy was in excess of 100 miles with the median figure some distance below this.[16] This might suggest that HF DF was not particularly useful for intelligence purposes but that does not square with both experience of the correlation of imprecise information and the anecdotal evidence.

Even imprecise information may yield a far more accurate product if there is enough of it to permit correlation and smoothing of several data points. This is a technique which is routinely employed in many fields of signal processing and although perceived today as a matter of electronic techniques and computer algorithms, it is also amenable to human perception and calculation. A simple example would be the visual interpolation and placement of a trend line in an ordinary graph with either missing data points or a degree of scatter in order to extract best-fit or trend lines as is done elsewhere in this book. This is hardly either unduly mathematical or high-technology although the more advanced ways of doing this might be. In the context of HF DF during the Second World War, a number of individual HF DF positions which might be of only moderate accuracy singly could yield less imprecise and much more useful assessments when considered together. This is supported by the evidence of the OIC carrying out evasive routeing – often successful – for a considerable period before timely Ultra information became available.[17] Direction-finding was thus extremely valuable inasmuch as at its best it provided reasonable positional information and some trend of the movement of a submarine or a group of U-boats. Assuming that the particular movement continued to follow the pattern previously observed, this was obviously valuable. However, once the pattern was departed from, then such information was of lesser value until a new trend could be discerned.

## Reaping the communications harvest II – other techniques

But direction-finding was not the only Sigint technique of value other than Ultra. There were a series of different exploitation methods, not every one of which was usable all of the time. Some of these complemented direction-finding directly; some did not. Similarly Ultra, too, derived support from or contributed to these at times. The idea that any of these three general fields – Ultra, HF DF and other Sigint techniques – existed in some form of hermetically separate compartments has to be dispelled. A distinction should be drawn between the handling of any sensitive material – especially intelligence – as it moves from place to place – and its processing. It is certainly true that many activities were by their specialised nature dealt with by a single organisation. But it was also important that there was adequate cross-fertilisation between these strands, otherwise important connections would not be made. It is unlikely that anyone who worked in intelligence organisations would ever claim that such communication always worked perfectly or that it was never so excessive as to endanger security. Such tensions will always exist in any intelligence system. This will be alluded to later in this chapter in the context of the two opponents' relative intelligence systems.[18] Conversely, if such communication is working properly it may create difficulties for the analysis of the effect of individual factors.[19] Although there were many other techniques used, it is intended to concentrate on three here: codebreaking short of Ultra, technical identification and traffic analysis (TA).

There can be no doubt that Ultra – the decryption of machine ciphers – was an achievement of the highest intellectual and technical order. However, it should not conceal the fact that it was not the only activity of its kind and that other systems were read consisting of codes and ciphers technically less secure than Enigma.[20] The German Navy probably made less use of such systems than did other German entities, but they did not avoid them all together. These were often much easier to read and their exploitation was, on the whole, much more reliable than Ultra. Their use was often for what would be regarded by many as irrelevant and mundane matters such as coastal waters information (such as shipping lanes cleared of mines), administration, merchant-ship movements and weather reports. Certainly such information in individual packets was rarely significant for its own sake; even when formed into a body of data it only provided a low level of background information. But it did have two great benefits, the

provision of an insight into German organisation and methods, and as a window into the higher-grade ciphers.[21] The latter worked because of a German propensity for putting the same literal information into signal messages sent in both low- and high-grade systems. As a result the relatively routine decryption of a low-grade signal might produce the partial text of a high-grade one, thus providing an opportunity for a more general decryption at the higher level.

A shore radio station might have several radio transmitters at its disposal; a major warship too could deploy a number but the constraints of space in a submarine rendered such luxuries infeasible. In most boats, there was one main transmitter operating in the HF band.[22] Although these sets were manufactured to a high standard and German radio technology was as good as any other nation's, at least at the outset, there were small variations in the performance of sets, because of manufacturing tolerances being relatively wide by late-twentieth-century standards. To some extent these were measurable by an intercepting station using a technique known as Radio Finger Printing (RFP). This was done by photographing the signal and analysing its characteristics. However, this was probably only capable of indicating the broad type of submarine, i.e. the supply and minelaying craft.[23] A similar process to RFP was TINA.[24] In this the Morse 'fist' of individual operators was the characteristic studied. Although a submarine would carry more than one operator, the number was limited, especially when compared with a surface ship. This was even more marked as the latter only went to sea comparatively rarely. Both of these were useful supplementary techniques.

Moving on from there is Traffic Analysis (TA). In one sense this is a ragbag of techniques, disciplines and borrowings from other parts of the Sigint spectrum. In broad terms it is the study of an enemy's communications as a system and the conclusions which may be drawn from such an investigation. Although it might be argued that it includes decryption – and it can certainly benefit from it – it is normally taken to exclude that particular skill.[25] Traffic analysis looks at patterns of communication. If, for example, a particular form of shore broadcast has been associated with a certain type of operation then its re-activation may suggest the imminence of another such operation. From sea, it may be possible to recognise certain procedures, such as those used in enemy reporting to realise that an anti-convoy operation is in the process of being initiated. Such characteristics as the frequencies of these transmissions may also give more than an inkling of the intensity of operations. Sometimes, too, signals carried clear indications of

the type of message they were and this too had significance for those intercepting, even if the full meaning of the enciphered text that followed was not rapidly made clear, if ever. This was especially so of the so-called E-Bar and B-Bar messages, whose prefix used the German Morse forms of these letters. These might indicate either a further signal book from which the body of the following message came or even the type of report being made. Thus in 1942 and 1943, the most common U-boat short signals (other than weather reports) used the *Kurzsignalheft* (Short Signal Book) and were called B-bars by the British (beta signals by the Germans). Although other subjects, such as fuel reports were sent in this format, their most frequent use was for convoy-sighting reports. Although these examples indicate the type of questions answered by TA, they do little to describe the skill as a whole. It is more than a little difficult to indicate more fully how TA was carried out. It depended much on not just observing radio signals but also of gaining the greatest possible understanding of the system that was being studied. It also suggested flexibility of thinking and of being prepared to abandon favourite hypotheses when new information came to hand. Further it paced a premium on developing the ability to discriminate between new developments in a communications system and understanding more of an unchanged system in which a large accession of knowledge has just been made. As a conceptual study, TA is probably the most difficult area of Sigint to grasp and certainly the most difficult to evaluate. In practical terms, however, it contributed greatly to assessments of U-boat numbers at sea, submarine casualties and realising that the enemy was experiencing problems of ambiguous orders or reports.[26] However, it would not be going too far to say that TA and Ultra enjoyed a symbiotic relationship.

## Decryption – the Peak of Sigint

The decryption of the signals involved in the German attack on shipping by submarines represented one of the greatest achievements of the Second World War in a number of different ways. Whatever may be said elsewhere in this book that suggests that its reputation has been somewhat overdone in the last quarter of this century, there can be little doubt that it was an intelligence achievement of significance. Further its execution pioneered mathematical, electronic and computing techniques which have a considerable impact on the world we live in today. It is not too fanciful to see this undistinguished redbrick English country-house as an intellectual hothouse comparable to the

Massachusetts Institute of Technology or Silicon Valley. But this is looking ahead. To understand the business of Bletchley Park in the 1940s it is necessary to look instead at the fundamentals of codes and ciphers to gain some idea of what its inhabitants were trying to achieve. It may be helpful to dispose of one linguistic point initially – the difference between codes and ciphers. There are many different definitions of these, often overlapping. Perhaps that adopted by David Kahn in his book on the Battle of the Atlantic is most useful for clarifying the issue.[27] Here he talks of codes using words and ciphers letters. This is broadly correct and illustrates the point well. Code-names are widely used in military operations, either for clarity, brevity or as a means of obtaining a degree of secrecy, usually in the short term. This is usually best suited to spoken communication. Once important communications are entrusted to radio this method becomes not only relatively insecure but also cumbersome in operation. In this, the Second World War occupies an intermediate position between the cleft stick with a message in secret writing of some form and the late-twentieth-century secure communication which needs no or little operator intervention other than to pass a message.

In mid-twentieth century, the system normally employed was to use a cipher in which one character is substituted for another. Clearly if this was done on a simple basis, say always *a* for *b*, *b* for *c* and so on, there would be little difficulty in attempting to extract the meaning from the coded text; there is thus a necessity for a system which changes every coded letter each time it is used. This could be done by a variety of methods, such as randomly generated one-time pads in which the sequence is worked out by hand and both sender and receiver of the message have access to the same encrypt/decrypt pad which, as the name implies, is used only once. Assuming that the tables in the pad are truly random, that they have not been compromised by capture and that they are (as intended) only used once, then this is the most secure method possible. This comes about because the key is used just once, thus making it impossible to use cryptographic methods against it, since the key (that is, the one-time pad) never repeats, unlike some other code systems in which a high volume of traffic may use the same setting. But for all their considerable theoretical advantages, such systems suffer from a severe practical disadvantage. While they may be ideal for running a small espionage circle with a limited number of stations and infrequent transmissions, they are completely impractical for a complex military machine with hundreds of potential transmitters and the possibility of each one generating a

significant signal traffic at any one time. In the case of submarines, which undertake relatively protracted operations, there are also difficulties of logistics to consider. These would be merely awkward but the problems of the reception station, too, have to be considered and the sheer scale would be a constant headache. One solution would be to use a similar system but to make continuing use of the same key or settings. This would have many disadvantages, not least security. A machine system on the other hand, such as Enigma, at least in theory, would appear to be the ideal solution.[28] Once set up, the scope for human error is greatly reduced and the machine's security is very high.

How was this achieved? It is difficult to give a short, thorough and correct account of the Enigma machine, but a simplified explanation can be given.[29] Cryptography did not begin with the Enigma machine; it has a history extending back over centuries. What, however, machines such as this did was to mechanise and automate the complex business of ciphering or deciphering a signal message. This was an important consideration, for the growing complexity of cipher systems resulted in two undesirable implications: time for the process and likelihood of error, leading to messages rendered incomprehensible to the addressee. Once a machine such as the Enigma was set up, it was very simple in operation. Pressing a keyboard key for the plain language message lit up a letter for the coded version. By the standards of the late-twentieth century, this was clearly awkward because the resultant stream of letters still had to be transcribed before being sent by hand-keyed Morse, but for the 1930s and 1940s this was advanced technology. But this was arguably not the most important implication of the Enigma machine.

Enigma's great utility lay initially in its ability to produce a cipher which was derived in a complex way and, without extraordinary aid, one which was very difficult to decrypt. Beyond this lay a system, or rather a series of subsystems, which gave Enigma such a large number of possible settings that even if an enemy had a complete working machine it would still be very difficult to work out the correct setting. Before moving on to see how this problem was solved, it is helpful to look at some of these complications. The Enigma was an electro-mechanical device whose heart was a number of rotor wheels. Described in its simplest form, their rotation produced the cipher text letter. But there was very much more to it than this. To begin with, the rotors themselves were not simple mechanical wheels; they carried internal wiring with different cross-connections between their electrical contacts to other parts of the machine. At the start of the war

German army and air force Enigma machines only used three rotors out of a total set of five, and the next level of complication was introduced by the selection of rotors and the order in which they were fitted into the machine. In the case of naval Enigma, a further cryptanalytical problem was caused by the main naval systems using four rotors out of a range of up to eight available rotors. Even had there only been three possible rotors, each always placed in the same position relative to each other, the probabilities for initial settings start to mount up suggesting around 17 500 possible combinations: with the possible choice being four from eight rotor types, and a free choice of rotor position relative to each other, the numbers mount further. But the rotor complications do not end there. Each rotor as well as having its fixed electrical connections also had a rotatable outer ring, which was set in position by the operator before inserting the rotor into the machine. It might be thought that this was sufficient to give a feeling of security to the users but there was a final complication. Many of what had been the internal electrical connections were instead broken and terminated in a series of sockets on the front of the machine. Obviously, these would have to be reconnected, but by using the socket system it became possible to reconnect them in a different order than the one they had been in originally, using a system of leads with plugs rather like the telephone exchanges of the period and in use for some decades after, and thereby introducing a further layer of probability to a system already with very many combinations. Setting up an Enigma machine for use involved setting all these variables plus one further step. This was to advance each rotor to a specified start position for each signal, thus producing a different set of coded text than had this start position been in a different place.

It was fully recognised by the Germans that it was possible, likely even, that at least one machine, possibly with a complete set of rotors, could fall into enemy hands. Their worst case would occur when it happened in such a way that the machine was captured with the day's current settings set on the machine and a list of the settings for the remainder of the month in question. But even this would not necessarily be a disaster in the medium and long-term. This was because, as a matter of routine, settings were changed daily. This introduces the subject of the administration of the system used by the Germans.

The Enigma machine was widely employed by the Germans, not just for submarines, not just by the Navy and it was widely used in the communications systems of organisations beyond the armed forces as normally perceived by the Allies. Thus the SS, the *Abwehr*, the police