~~RESTRICTED~~

SECURITY OF RADIO TRAFFIC

Lecture given by Major W. F. Friedman,
Sig-Res., at the Signal School
January 14, 1935

SECURITY OF RADIO TRAFFIC

A lecture given by

Maj. William F. Friedman, Sig-Res.

Cryptanalyst,

Office of the Chief Signal Officer

at

The Signal School,

Fort Monmouth, New Jersey

January 14, 1935.

To those present today it is almost unnecessary to mention that secrecy in the preparation of plans for, and the preliminary or initial phases of, military operations is a vital element in the success of those operations. Since, in modern warfare, the latter can hardly be conducted without signal communication, it follows that the degree of secrecy or security with which such communication is accomplished contributes very materially to the success or failure of the operations. This brings me directly to the subject of signal communication security, the aim of which is to nullify as completely as possible the efforts of the enemy to intercept and learn the meaning of the messages transmitted by any of the agencies of signal communication.

Passing over a long, and interesting history of the development of electrical signaling, we come at once to the statement that if signal communication security has been a factor in the results of warfare in the past, it is today more vital to success than ever before, because more than ever before has the art of electrical signaling become an essential factor in the art of warfare.

I shall have here little to say concerning the subject of signal communication security as regards wire methods of communication. Were it possible to restrict military signal communication to wire methods exclusively, the problems of security would be much simplified. But radio methods are here to stay, and while the use of radio in war may not be so extensive as was visualized by the overenthusiastic Army devotees up to 1932, it is certain that radio will be an absolutely indispensable means of communication for certain elements of a command (aircraft, mechanized forces, and rapidly moving units) and will be a reliable, very useful means of emergency communication

for other elements. It is possible that, within the discretion of an army commander, it will be used as a regular means of communication, and not only as an emergency means. Only time and real action will tell. But the very nature of radio is such that enemy interception of messages transmitted by its means is more feasible, and therefore it is in radio communication that the principles of security are most applicable. How can we or rather how should we conduct radio communication so that we may prevent information conveyed by its means from falling into the hands of unauthorized persons no matter how remote from connection with potential enemy services?

Getting down to fundamentals, today we know three and only three basic methods for maintaining secrecy in radio communications. First, we can manipulate or do something or other directly to the signaling elements themselves to disguise the impulses corresponding to the letters transmitted. Secondly, we can, to a greater or lesser degree, control or guide the electrical signals to their proper destination by appropriate apparatus so that interception outside the path of transmission is impracticable or impossible. Thirdly, we can use cryptographic methods to disguise the text transmitted.

As to the first means, although I am not a communication engineer, nevertheless I have made some study in this field. More or less complicated methods of disguising, changing, or hiding the electrical signaling elements have been devised but none of them, so far as I am aware, will yield more than a relatively minor degree of security -- that sufficient to prevent casual listeners-in from hearing, intercepting, recording, or understanding the signals. They will not stand up under organized attack by persons having

an incentive to read the messages and provided with the necessary equipment to intercept the signals, whatever the characteristics of the latter may be. Of all these methods it may be said that they will only cause some annoyance - they will not yield true secrecy. Among such methods I include those which reduce the letters to plural-unit-code elements (Baudot) and shift these units about; multiplex methods which require accurate synchronism between transmitting and receiving stations; methods which superimpose variable superaudio frequencies upon basic, shifting carrier frequencies; in telephony, especially, inversion methods using side band transmission; band inversion methods, and so on. Phonographic and oscillographic equipment is available today which, in the hands of experts, renders the detection, recording, and interpretation of such signals possible. It is clear that while methods of this category yield sufficient secrecy for commercial or social use, they do not and can not render the degree of security required for military, naval or diplomatic communications which are to be kept secret for any considerable length of time against the organized attack of the cryptanalytic services of foreign governments.

As to the second basic method mentioned above, namely that involving the use of special apparatus such as directive antenna and directional radiating systems, we all know that at the present stage of development the secrecy features of such methods are only of relatively small value. Broadly speaking, the directive antenna of today are associated only with large, fixed stations; the art as regards small mobile or portable stations such as the majority of military stations must be, is just in its infancy. As to what will be the outcome of the ultra-high frequency methods using microrays (1 cm. to 1 meter),

I think it too early to say. These methods achieve some degree of secrecy because these radio waves behave very much like light rays. They can be reflected and refracted; and they can be directed to specific spots by means of narrow beams of rays. But at the present moment not only is the size of the necessary reflectors a prohibitive factor in portable sets, but also the art in general awaits farther development of radio tubes permitting of high output with microrays. And even assuming the present difficulties to be overcome, there still remains some question as to whether 100 per cent or complete directivity can be attained, for it appears that any sort of reflecting obstacle in the path of the beam will reflect and disperse a certain amount of the energy. With amplifiers capable of amplifying a millionfold, can we be sure that such stray reflected waves will not afford sufficient energy to be detected, amplified, and recorded? In this connection I would like to quote a paragraph from a recent article[1] by Mr. W. D. Hershberger, Associate Physicist at the Laboratories here:

> "Also it should be borne in mind that although a radio-optical system may be made highly directional, only relative secrecy is secured. Of necessity, a beam has a finite width even in the most highly favored case of a well-constructed searchlight. Once a transmitter radiates power into space there is no method for checking the presence or absence of unwanted listeners. If such a listener should possess better receiving equipment than that possessed by those for whom the message is intended he could operate either considerably off the

---

[1] "A Survey of Radio-optics" by W.D. Hershberger, Associate Physicist, Signal Corps Laboratories, The Signal Corps Bulletin, July-August, 1934, No. 79.

axis of the beam or at a greater range. It has been by no means demonstrated that 9-centimeter waves are limited to the direct line of sight any more than 70- or 50-centimeter waves. True no one has ever signaled beyond the horizon with such waves, but not until we actually have sufficient power to even reach the horizon should we venture opinions as to what might happen beyond it if we had the power."

Mr. Hershberger concludes his article as follows:

"The latent possibilities of the radio-optical waves are most promising, but their fuller realization is conditioned on continued technical advances. If the progress made during the past 5 years is indicative of what may be expected in the future, the field will assume an increasing importance for the Signal Corps. The use of radio-optical equipment for portable beacons for aircraft, for limited range directional signaling in all varieties of atmospheric conditions, as well as other uses which suggest themselves, can readily be forseen."

Leaving this phase of the subject, we come now to the third basic method mentioned above, for achieving secrecy in radiocommunication, viz., the use of cryptography. In a report dated October 19, 1934, to the Research and Deve opment Division, OCSigO, on the subject of "Transmission secrecy," Major Richard H. Ranger, Sig-Res., an acknowledged expert in the radio field, after considering secrecy methods applied to signaling elements (the first method mentioned by me above), says:

"By all odds the most complete and satisfactory method of obtaining secrecy in telegraphic communication consists in using cipher. There are all grades of codes of such type requiring more and more labor

in translation. In addition to the letter by letter substitution there is of course the word and phrase substitution which gives a wide latitude to secreting messages in this form."

Major Ranger concludes his report in the following words:

"It is felt that secrecy for telephonic transmission would involve terminal equipment much more involved than the work would justify. This would be particularly true of anything for airplane or front line use and it would seem that the necessary secrecy would have to be obtained by code even for telephonic work. For telegraphic work it seems that straight ciphering is by all means the most effective method, because it requires no special equipment in the communication channel. Furthermore, with the development of printers, it is felt that the enciphering and deciphering equipment may readily be inserted at each terminal so that the operational becomes practically automatic with very quick and efficient service for the service intended and very difficult of interpretation by any other. It would therefore seem that this latter method is the proper method of attack on secrecy."

Before taking up in detail the question of codes and ciphers, I think it advisable to discuss for a few moments certain other phases of radio communication more or less directly connected with the question of secrecy in space telegraphy. I refer to the matter of radio frequencies, radio calls, procedure, addresses and signatures.

Radio differs from wire communication in many respects, but there is one difference which is of great importance in connection with secrecy. It is this: in the case of wire telegraphy, if you see a wire line and want to locate the source of the electrical impulses guided by the wire, you must

actually and physically follow the wire to the point where the signals are fed into it; but in the case of radio telegraphy, you can locate the transmitter without actually seeing it, though it be many miles away. I put the matter in simple language so that you may more readily visualize the military consequences of the possibility of radio direction finding. It means that without even attempting to read the messages transmitted by radio, if they are in cryptographic form, valuable information can be obtained merely by locating the transmitting stations, studying the characteristics of the transmissions, the stations with which they communicate, when and how much they transmit, and so on. What this valuable information is, I hardly need point out to you: the location, disposition and grouping of the enemy forces; in other words, his order of battle, and his intentions.

This is an aspect of radiocommunication which I should enlarge upon at this point. Let us assume that the stations AB, CD, EF, GH call one another, and that the enemy radio intelligence service has intercepted the calls. At the moment we will assume that these calls mean little or nothing to the enemy. But as traffic among these stations proceeds the situation clears. The location of the stations become known, of course; but the actual volume of traffic, even if the subject matter is not understood, will enable the enemy signal intelligence service to determine certain facts. An increase in volume of traffic may indicate the movement of troops, or again, an attack. In fact, an outstanding instance of the usefulness of this source of information is found in the case of the so-called ADFGVX Cipher System employed by the German Army on the Western Front in 1918. (Cite story of chart of activity.) Another extremely important instance, was in connection with the American St. Mihiel drive. Just before this attack there were many indications that the Germans had withdrawn and the advisability of advancing the infantry without artillery preparation was ser-

iously considered. The final decision to make the attack as originally planned was based on the evidence of the radio-direction finders, which conclusively indicated that the enemy radio stations were still active in their old locations. How many American soldiers owe their lives to this one case of alertness on the part of the Signal Corps intercept and goniometric service, it is impossible to say. You may gain some idea of the importance which General Nolan, Chief of G-2 in the AEF, placed upon the value of the goniometric service when he said, in the dispassionate tone of his final report: "From the goniometric service it was possible to get much valuable information, obtainable from no other source, in regard to enemy intentions."

Now in collecting this information, the data upon which it may be based consist of radio frequencies, calls, procedure, addresses and signatures. These are intimately, directly, and unavoidably connected with the technical operation of the stations, with the handling of the traffic, and with the origins and destinations of the individual messages. Let us take them up in the order mentioned.

Regarding the matter of radio frequencies and its relation to security, I can say but little at this time. It is obvious that a complete knowledge of the frequencies employed by the different units is of great and immediate help to the enemy in intercepting the messages. Can these frequencies be shifted about as often, for example, as we can shift call signs? If so, a greater degree of security will be afforded in proportion to the frequency and thoroughness of the shifting. Approximately 180 different channels separate by 20 kc. are available for Army use under the present set up of assigned frequencies and equipment, and,

with the exception of the sets assigned to forward infantry and cavalry units, all Army sets are of the universal type, so that frequency-shifts can readily be made among the latter. It is my understanding that certain limitations introduced by the present fixity in frequency of the sets used by front line infantry and cavalry units makes a thorough shuffling of the available frequencies impracticable; but even a partial shuffling of frequencies is better than none. The important principle to note in this connection is that the most thorough changes and shifts should be made among the most mobile units, with other shifts as thoroughly and as frequently as practicable, and certainly each time a unit moves to a new position. If mechanized cavalry, for example, have used frequencies a, b, c, and d in the last engagement, they should not use the same frequencies in the next action. Again, for example, if the 1st Division is today occupying a position on the front as a part of the I Corps, and tomorrow is moved to a new position and forms an element of the III Corps, a complete change in frequency and calls used by the Division net is indicated, otherwise the enemy, by taking bearings upon the transmitters of the 1st Division, noting the same frequency and the same calls, will know at once that the division has been moved and can draw definite conclusions from this fact.

In short, a knowledge of radio frequencies, if the latter are not changed, not only facilitates the interception of the traffic, but also leads rapidly to identification of radio nets; the latter rapidly leads to identification of types of units and their groupings, finally to the actual identification of numerical designation, when other information is at hand.

In the foregoing remarks, I have already more than alluded to the part played by changing radio calls. If they are not changed frequently, they lead not only to an easy identification of units, their location, and groupings, but

also they assist the enemy cryptanalysts in the attacks upon the text of the messages. For instance, it is easy to see that if an intercepted message carries with it not only the text but also indications as to the location of the transmitting station, its call sign, and the call sign of the receiving station, this information will assist the enemy cryptanalysts to identify the communicatants, where they are, and to what group or superior unit they belong. This often then affords some basis for assumptions as to the general tenor of the message and gives clues to the possible presence of certain words in the message. It is often the case that without these clues, solution is delayed or rendered impossible.

You will immediately ask: how practicable is it to make such wide and frequent changes in frequency assignments and call signs? Is this not going to place a tremendous and impossible burden upon the signal officers of the units concerned? Those of you who have ever had experience in the mere physical labor involved in getting up lists of frequencies and lists of call signs for one field army will probably answer the foregoing question postively, saying that it will be impossible to make these frequent changes. But I will ask you to suspend your final judgment until I have outlined to you a mechanical method which can be employed in the production of these lists, which we have but recently worked out in connection with the production of codes. I think you will find it of considerable interest, but at this point in my talk I will stop only to say that I think the mechanical method can be applied successfully to this problem, so that frequent and thorough shifts in frequency assignments and in radio calls will be quite practicable.

A few minutes back the matter of radio procedure was mentioned as being connected with the question of security. Basically, the purpose of radio procedure is to facilitate the movement of traffic by reducing the amount of conversation exchanged between operators and by standardizing the reduced

conversation so as to avoid ambiguities and questions. From the secrecy point of view the importance of a strict adherence to authorized procedure is to be emphasized. Every time a transmitter is operated means a time when bearings may be taken on the emission. That is one point. Another point is that if operators are permitted to engage in mere gossip, they will be certain to disclose information of value to the enemy. And finally, a strict adherence to authorized procedure is to a certain degree an aid in authenticating the transmission of our own messages and will make the transmission, by the enemy, of false and "decoy" messages harder.

The last of the subsidiary preliminary considerations to radio security is the matter of address and signatures. It is obvious that these must be hidden or disguised. Various methods suggest themselves for the purpose. They may be cryptographed in the same code or cipher that is used for the text of the messages; but if this is done it greatly weakens the code or cipher. They may be cryptographed in a special code or cipher, adapted only to this purpose; but this adds one more system to an already burdensome list of systems. Finally, the radio calls themselves may be employed to serve not only for their own specific purpose but also as addresses and signatures. To this proposal I can see no serious objections, but the matter is still under consideration. At this time, I can only quote the appropriate paragraph from the recently issued Tentative Cryptographic Security Manual:

> "18. Addresses and signatures. - a. Much important tactical and technical information can be obtained by an alert enemy merely from a study of the addresses and signatures of cryptographed messages. For this reason these indispensable parts of every message must be disguised or hidden.

b. Cryptographed messages within the military establishment will not be addressed to specific individuals by surnames of addresses, nor will they carry as signatures the surnames of specific individuals as the senders of the messages. They will be addressed only to and signed only by (or in the name of) the commanding officers concerned, using their official designation or title of office. In the case of received messages, the specific officers to whom copies are to be distributed will be determined by the commanding officer of the headquarters concerned or by his administrative officer.

c. In the theater of operations, in messages which are transmitted in normal or abbreviated form between field units in tactical nets (radio, wire, telephone, visual), the tactical call signs of the units concerned, as given in the heading of the message, will also serve as the address and the signature. In no case will the address or the signature appear in the text of the message, either in plain or in secret language, except in the special case cited in subparagraph d. At the receiving message center the official designation of the addressee and of the sender (as indicated by the call signs appearing in the heading) will be inserted in the positions reserved for these items on the authorized field message blank.

d. When a message is intended for an individual not permanently assigned to the headquarters to which the message is sent, it will nevertheless be addressed to the commanding officer of the headquarters concerned and the first few words of the text will indicate for whom the message is intended. If the text of the message is to be cryptographed, information as to the addressee will be cryptographed in the same code or cipher as that used for the text; the surname of the person for whom the message is

intended and the surname of the sender may be used in these cases. The plain text of such a message may be as follows: "For Lieut. Col. John Doe stop You are directed to return to permanent station at once signed Richard Roe".

e. In the case of code or cipher messages in the zone of the interior, a special address and signature code will be used in accordance with the instructinns governing the employment of that code."

I cannot close these preliminary remarks without directing brief attention to the opportunity which radio communication affords for organized, coordinated attempts at conscious deception of the enemy. If it is possible to gain information from a mere study of radio calls and traffic volume as well as traffic direction, it is just as possible to deceive the enemy by deliberate dissemination of false calls and false traffic. But this is a subject which requires much thought and extremely careful control, otherwise it will either be wholly unsuccessful or it will defeat its own purpose. I know of only one or two cases of successful deception of this sort. (AEF mobile dummy stations; Allenby in Palestine.) It seems to me that by and large it is much safer merely to take cognizance of the part played by radio calls, the direction and volume of traffic in the derivation of important information and so far as possible keep the traffic at a perfectly even level at all times, rather than to try to deceive the enemy by radio camouflage measures and take a good chance of overplaying one's hand. The job of keeping the traffic at an even level is sufficient to keep all hands busy! If radio camouflage is to be tried, it should be left to specialists under the direction of the highest commander involved, just as the imposition and lifting of radio silence is left to him.

Having referred to the matter of radio silence, I will point out that this is a very important means of achieving radio security. The greatest problem in connection with it is not so much when to impose it as when, how, and why to break it. During silent periods the signal officer must understand the general tactical as well as the special radio situation in order to know when and for what kinds of messages the silence will be annuled at his command. He must be guided by doctrine and the special instructions in effect during the operation. The period of radio silence is often assumed to be a period of relaxation for communication personnel but it should, on the contrary, be one of watchfulness and preparation for all communication personnel.

Having disposed of these preliminary matters, we come now directly to the question of codes and ciphers.

Let us note the list of systems now authorized for use in the military service. (Par. 39 CSM) This is quite a formidable list and one may question the practicability of handling so many different systems. But a study of Par. 33 of the Cryptographic Security Manual soon shows the reasons for such an extensive list. (Read Par. 33.)

It will be admitted that at the present stage in the art of cryptography, for such a far flung organization as our military establishment, the necessity for wide distribution of methods and for systems to cover the three categories of secrecy dictates the use of all the systems listed.

You may inquire as to the possibility of cryptographic machinery supplanting certain of the codes mentioned. You are perhaps aware that all over the world there is at present more or less feverish activity along the lines of the development of mechanical and electrical cipher apparatus. Most of these devices, I feel sure, have come to the attention of the Chief Signal Officer and we have studied them with great care. None of them have been found to be wholly suitable for our service. If the Chief Signal Officer could have had only 1 per cent of the money that civilian agencies have spent in this country

alone during the past 20 years in their efforts to produce a suitable cryptographic device, I am sure our developments along this line would have been completed long ago. The basic reason for the failure on the part of these civil agencies to produce a really good machine is that the inventors that have worked on the problem have all been excellent mechanics, excellent draftsmen, excellent fabricators - but not cryptanalysts, or at least not with sufficient experience in modern cryptanalytic theory and practice. (Here relate one or two recent experiences with cipher machines.)

For your own information I will tell you a bit about our confidential developments in this field. (Here tell of Cipher Device Type M-134 T1 and T2.)

The successful completion of this project (and I foresee no difficulties in this respect) should provide us with appropriate machinery for secret intercommunication between our large, fixed headquarters both in the Zone of the Interior and in the Zone of Communications. If this is done, we may find it possible to discard our War Department Staff Code, War Department Confidential Code, and War Department Telegraph Code, for the same machine, with different cipher keys, can serve the purposes of these three codes, without any danger of compromising the most secret communications, for which the War Department Staff Code is intended. How far down this machine can be taken in the combat zone remains to be determined. The complete apparatus consists of a cryptographic unit and a printing unit, but the system is flexible as regards the presence or absence of the printing unit of the mechanism. I see no reason why the complete machine cannot function successfully at GHQ, and at Army Headquarters. Without the printing element, it is entirely feasible to take it down to Division Headquarters, in which case it can replace Army Field Code. I am not so sure that it will be possible to take this machine below Division Headquarters. If not, can we develop a smaller automatic device for secret communication within the

Division? Can we develop any small device which will give the equivalent security of our Division Field Code? For I must say to you that at the present state of the art, a code such as our Division Field Code, if frequently changed and properly handled, yields a greater degree of security and is faster than any small, practicable cipher device that has come to my attention. The development of a device to replace the Division Field Code will take considerable time, and may not be practicable in the end. In the meantime we must rely upon this code for communications within the Division.

The question arises now: how frequently can new editions of the Division Field Code be prepared? I will recall to your mind that this code is a two-part, cross-reference code, each part containing approximately 6000 lines of text. Our latest copy comprises 100 pages of printed matter. With our present methods it takes five men approximately one month to produce the manuscript for such a code and the manuscript in this case consists of the text typed on 3 x 5 filing cards which then go to the Government Printing Office. But I have recently developed a method for producing code manuscript by machinery and this method can give us a complete manuscript in not more than five or six days using the full-time services of but two men for the job. You will no doubt be interested in this method of code production and I think it well worth explaining in some detail. (Here go into the details, using scheme formulated in presenting matter to The Adjutant General.)

There is no doubt whatever in my mind but that in case of emergency this automatic method would be the one we would find most useful, and most practicable. It has all the advantages of speed, accuracy, and safety. Moreover, in the field the manuscript could be reproduced photolithographically by our Engineers, or, if GHQ is provided with a printing plant, by whatever agency controls that plant. Perhaps the Signal Intelligence Service GHQ would

be provided with such facilities purely for the purpose.

In discussing the production of lists of frequency assignments and radio call signs, I referred to the possibility of devising a mechanical method for their production. You will no doubt see now what I have in mind. Here again I see no obstacle to the use of these very efficient machines for the purpose and you, in turn, can appraise the proposal from your point of view. I shall be glad to discuss this matter further and answer questions which may occur to you.

The production of code books, cipher tables, cipher alphabets and keys is but the first step in a rather long and somewhat complicated chain. You know that by recent changes in AR 105-5 and 105-25, the Chief Signal Officer now has the responsibility not only for the production of manuscript for codes and ciphers, but also for their printing, storage, issue, and accounting. The safeguarding of the final documents is a problem in itself. Without adequate control over these phases it is useless to expect much of a degree of security. Proper storage space at the production center is vital, but no more so than at the headquarters to which the codes and ciphers are issued. Definite, detailed, and quite specific regulations governing the handling of the documents by all personnel concerned are also necessary. And finally, without a properly instructed and carefully indoctrinated using personnel, even the very best cryptographic systems can be readily and quickly compromised. In this matter of instruction and indoctrination we have recently made an important step forward when the Chief Signal Officer prepared the Cryptographic Security Manual already mentioned. This manual, approved by the Secretary of War, has thus far been given only a very limited distribution because it contains certain matters which are secret and which therefore cannot be widely disseminated. But

it is contemplated that another edition, in which these secret parts have been deleted, will be prepared and will then be given a comprehensive distribution. Its study should materially assist in maintaining security in regard to the storage and handling of the documents themselves, and in the handling and filing of cryptographic messages and their translations. In the latter connection, under the new regulations these matters in the field and at all fixed posts fall under the jurisdiction of the signal officer of the headquarters staff. Heretofore it has been the case that at some headquarters codes and ciphers were handled by the Adjutant General, at others, by G-2, at still others by the Signal Officer. There was no uniformity of procedure or regulation. All this was, of course, not conducive to security. By definitely placing responsibility for these matters under one head, and it was logical that the signal officer be that head, it is certain that cryptographic security as a whole will be strengthened.

Furthermore, with increasing attention to matters of security it is possible that the time will come when there will be maintained at every headquarters a rotating roster of "security officers" such as we now have in the War Plans and Training Division. Their duties in this regard, which are, of course, in addition to their regular duties, are to make daily inspections of the quarters where codes and ciphers are stored, to see that safes and cabinets containing them are properly safeguarded and so on. I will remind you at this point that under the proper tables of organization, the signal intelligence services at Army and GHQ provide for a "communication security unit", the function of which is to study our own radio traffic and report on violations of the principles of radio security. This unit works upon messages furnished it by

our own intercept service. It has nothing to do with solving enemy intercepts but of course its experience is directly correlated with the experience gained by the code and cipher solving personnel of the signal intelligence service. It is obvious, without my going into the subject in detail, that we should fail pretty seriously in our duty, if we did not take advantage of the experience of the solving personnel to gain hints for the security of our own methods. Close cooperation between these units is therefore very necessary.

All this is but a modest beginning, it is true, and there remains much to do by way of further instruction and study. It is only by keeping everlastingly at such a job that real progress in security and radio discipline can be made.

It is my understanding that these talks with the Advanced Class are more of the nature of round-table discussions. I have made a hasty survey of the subject and will now be glad to try to answer such questions as present themselves to you as a result of my remarks.

~~RESTRICTED~~