How the Dutch broke the Japanese Blue Code in the late 1930s

Joost Rijneveld
Supervisor: prof. dr. B.P.F. (Bart) Jacobs
Radboud University
joostrijneveld@gmail.com

ABSTRACT

In a prelude to the Second World War, Japan sought to expand its territories, using intricate cipher systems to encrypt its communication telegrams. By breaking these ciphers, Johannes Frans Willem Nuboer was able to provide the Dutch East Indies with valuable tactical insight. In this paper, we will explore the inner workings of the '.' code, its weaknesses, and how the Dutch intelligence department in Batavia ended up deciphering it. We then present evidence that indicates that this is the same code that the United States Navy refers to as the BLUE BOOK or BLUE CODE.

Author Keywords

Johannes F.W. Nuboer, Blue Code, Blue Book, cryptography, Second World War, Japanese Imperial Navy

INTRODUCTION

In the late nineteen thirties, the Japanese Imperial Navy was using an intricate cryptographic system to secure their communications — all the while, the Dutch were reading along. Through this research, we will see how.

In times of war, it can provide an immense tactical advantage to be able to listen in on the channels of the enemy, especially when this enemy believes he is communicating securely. This can be achieved using cryptanalysis. For the Royal Netherlands East Indies Navy, an officer named Johannes Nuboer played the key role in this. In the years leading up to the Second World War, it was Nuboer's work that allowed the Dutch navy to read a large part of the Japanese telegrams. This work, as accounted in the manuscripts available in Nuboer's archives at the Netherlands Institute of Military History, has provided the raw material for this paper.

Based on these notes, we unravel how the Japanese codes worked and how Nuboer was able to exploit their weaknesses. Finally, we consider evidence that the main code that Nuboer described is in fact the same code that the United States Navy broke and refers to as the BLUE CODE. In this paper, however, the code will be referred to by the name Nuboer gave it: the '.' code.

HISTORIC CONTEXT

The Japanese economy had been growing steadily throughout the first thirty years of the twentieth century. Until the rise of militarism in 1930, natural resources were never a pressing issue [9]. Japan was prosperous. However, the growing military influence on the domestic economy (along with the aftermath of the 1929 Great Depression) was fuelling a sentiment of military expansionism. This soon caused a shortage of oil and coal, and set the scene for a series of occupations in Northern China and Mongolia, eventually culminating in the Second Sino-Japanese War and lasting until well into the 1940s.

As the Dutch East Indies had large depots of oil, rice and tin (and a poorly equipped army), the growing Japanese occupation could become a serious threat to the southern islands. In order to be able to remain neutral and avoid Japanese influence, the Dutch constantly had to plan one step ahead and organise a strict diplomatic campaign [1]. For this, they needed an intelligence service. Johannes F.W. Nuboer, a Netherlands Naval War College graduate who had followed courses in cryptography, was selected to set this up [5].

In command of the newly formed navy Department 1 (*Intelligence*), Nuboer intended to supply the other departments of the navy with monthly reports of his findings. As the Japanese society was very closed and private at the time, human intelligence (such as through espionage) was considered to be practically impossible [6]. This meant that Nuboer was especially dependent on other sources, such as signal intelligence.

The staff in Batavia kept a close watch on the information that was published in the Japanese press. The work of Department 1 was also greatly aided by photographs of various Japanese military vessels and snippets of information from the letters sent by the Dutch diplomatic mission in Tokyo. Initially, Nuboer's newly formed department was greatly understaffed and unable to sufficiently focus on decrypting intercepted telegrams as well. However, when lieutenant at sea J.M. Schalkwyk was detached to the Dutch Indies, Nuboer gained a valuable colleague. Together they would be able to decipher many of the encryption schemes the Japanese navy used to conceal its communication.

SRC 2014, November 26, 2014, Amsterdam, The Netherlands.

JAPANESE TELEGRAMS

The Dutch intelligence services soon started intercepting several Japanese telegrams each night. These telegrams consisted of plain-text address information and grids of 10 by 10 Kana[1] symbols representing the message [6]. Some telegrams were plainly readable, but others were unintelligible. In case of these unreadable telegrams, a recurring symbol at the end of each line would indicate what encryption scheme was used. Nuboer soon noticed that messages from naval sources often included a single dot, indicating a code he would come to refer to as the '.' code.

BREAKING THE '.' CODE

On February 20th, 1935, a Japanese training squadron left port at Yokosuka. After brief visits to Keelung, Hongkong, Manilla and Bangkok, it visited Singapore on March 28th and Batavia on April 5th. After leaving the port of Singapore on April 1st, and again when leaving the port of Batavia on April 5th, the squadron sent out a remarkable encrypted telegram containing many repetitions. Nuboer soon noticed two lines that contained a nearly identical set of symbols [2]. These two lines read:

```
Hi  Shi He  Tsu So  Yu  Ke  Ta  Wa
Ta  Ke  Hi  Shi He  Wa  Se  Tsu So
```

Eight symbols occur in both lines; Yu only occurs in the first, while Se occurs in the second. This could indicate a cipher system that permutes nine columns of plaintext, and this is exactly the lead Nuboer pursued. In his memoires, Nuboer does not precisely detail how he found the permutation, but he describes placing the unique Yu symbol last and working from there. With some further deduction, one can indeed confirm that by applying the permutation 5-2-6-3-7-9-1-4-8 to both lines, the following pattern emerges:

```
Ke  Shi Tsu Ta  Hi  He  So  Wa  Yu
Se  Ke  Shi Tsu Ta  Hi  He  So  Wa
```

After Nuboer had found a candidate permutation that might have been used to encipher the telegrams, he applied it to the entire ciphertext. He soon found that his suspicions had been correct: suddenly, groups of symbols started recurring throughout the ciphertext at a spectacular rate. At first it seemed like the symbols were paired together, but upon closer inspection the repetitions turned out to affect groups of four Kana symbols, indicating a recipherment of existing code groups [2].

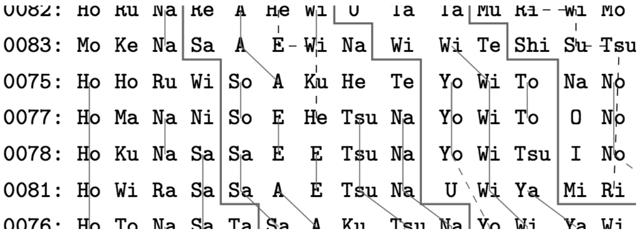
The '.' code book

After discovering the permutation that lay at the base of the '.' code, the crypto-analysts of Department 1 were able to decipher an immense mass of material that had been intercepted over the past months. This allowed for the reconstruction of a significant part of the code book[2] [6].

The '.' code is formed by groups of four Kana symbols, of which the last symbol is a control symbol. The control symbol can be found by adding the numerical value of the other Kana symbols (A = 1, E = 2, Ha = 3, He = 4, etcetera), subtracting one and converting the value back to a Kana symbol (modulo 44). This checksum allowed for the reconstruction of the group in case one of the symbols was lost [3]. As the code used 44 different symbols (omitting N and Nu), this meant there was room for roughly 85.000 groups. This space was used efficiently by including table-like structures to list the names of ships, various authorities and geographical locations, as well as systems to represent numbers and timestamps. By combining this with information from other sources (such as leaked naval records), large parts of the code book could be uncovered.

THE RECIPHERED '.' CODE

In August 1935, all '.' code telegrams suddenly became completely undecipherable. When applying the permutation, the resulting messages would contain unknown code groups and combinations of known code groups that did not form a coherent message. However, based on frequency analysis of the symbols, Schalkwyk and Nuboer were able to conclude that it did concern yet another transposition of the same base code. Luckily, only a few months later, a ship off the coast of Taiwan broadcasted an odd series of telegrams that allowed Nuboer to gain a new foothold. These telegrams contained many recurring symbols, but new ones were added in seemingly random places as they grew in size. By sorting the telegrams by length and connecting identical symbols with pencil lines, Nuboer discovered an interesting pattern.



```
0082: Ho Ku Na Ke A  He Wi  U   Ta  Ta Mu  Ki  Wi Mo
0083: Mo Ke Na Sa A  E  Wi  Na  Wi  Wi Te  Shi Su Tsu
0075: Ho Ho Ru Wi So A  Ku  He  Te  Yo Wi  To  Na No
0077: Ho Ma Na Ni So E  He  Tsu Na  Yo Wi  To  O  No
0078: Ho Ku Na Sa Sa E  E   Tsu Na  Yo Wi  Tsu I  No
0081: Ho Wi Ra Sa Sa A  E   Tsu Na  U  Wi  Ya  Mi Ri
0076: Ho To Na Sa Ta Sa A   Ku  Tsu Na Yo  Wi  Ya Wi
```

Based on the groups and patterns that emerged from these telegrams (as well as other clues [4]), Nuboer was able to conclude that they were dealing with an eleven-column grid that was transcribed vertically. Wherever a jump in the pattern occurred, a column ended.

More columnar permutation

Going on the assumption that the groups of symbols indeed represented columns in a grid, Nuboer searched for the correct permutation; simply writing them sequentially had proven to be fruitless. By marking the symbols that appeared to be added when the messages grew larger, Nuboer noticed that the four 'new' symbols could be arranged in such a way that they would form a valid[3] code group. Not only were these groups valid, but they would also frequently occur in previously decrypted '.' code telegrams. As Nuboer was familiar with these groups, he quickly recognised their anagrams. Each of these anagrams produced a four-symbol permutation

[1] Kana is a concise Japanese alphabet. Each character corresponds to one sound in the Japanese language.

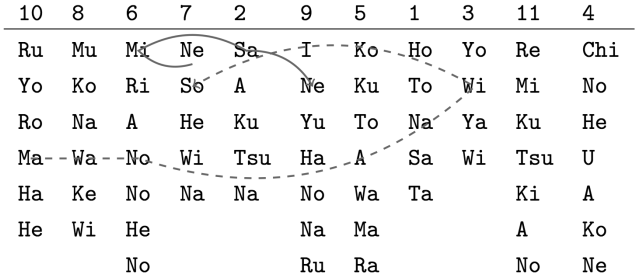
[2] A sorted list of predefined code groups and their meanings.

[3] After verifying the checksum symbol, only one out of every forty-four random combinations would prove to be valid.

when it was properly arranged, effectively ordering the four columns that had contained the newly added symbols. By combining these small four-symbol permutations and linking them together, a complete permutation of the columns could now be construction.

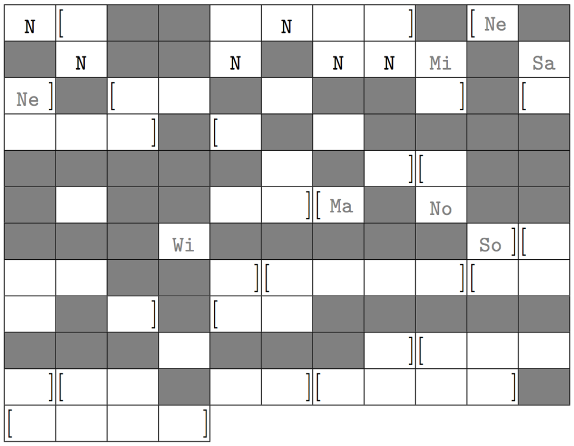
Finding the figure

In the diagram below, the columns from one of the telegrams have been arranged according to the found permutation. The columns are remarkably varying in length, and Nuboer notes that there were only few in-tact code groups to be observed. To Nuboer, this indicated that the underlying figure that was used to transcribe the telegrams contains many blank fields, obfuscating the code groups.



10	8	6	7	2	9	5	1	3	11	4
Ru	Mu	Mi	Ne	Sa	I	Ko	Ho	Yo	Re	Chi
Yo	Ko	Ri	So	A	Ne	Ku	To	Wi	Mi	No
Ro	Na	A	He	Ku	Yu	To	Na	Ya	Ku	He
Ma	Wa	No	Wi	Tsu	Ha	A	Sa	Wi	Tsu	U
Ha	Ke	No	Na	Na	No	Wa	Ta		Ki	A
He	Wi	He			Na	Ma			A	Ko
		No			Ru	Ra			No	Ne

Many frequently occurring code groups (such as the Ne Mi Sa (Ne) group) were in fact distinguishable, but spread out all over the figure, often across various lines. Nuboer left little information on how he then proceeded. However, the above figure is heavily annotated in his manuscripts, and littered with various markings. From these notes, it appears that, by linking frequent code groups, Nuboer drew conclusion about their relative positions. This then allowed him and Schalkwyk to piece together the appropriate spacing [4]. The figure for November 1935 is included below[4]. N-symbols (negation symbols) indicate fields where random symbols were inserted for obfuscation. This, combined with the obscurity created by the blank fields, made the code groups especially hard to isolate. See for example the Ma No Wi (So) group in the diagram above, connected by a dashed line.



N	[	▨	▨		N		]	▨	[Ne	▨
▨	N	▨	▨	N	▨	N	N	Mi	▨	Sa
Ne]	▨	[		▨		▨	▨	]	▨	[
		]	▨	[	▨		▨	▨	▨	▨
▨	▨	▨	▨	▨		▨	]	[	▨	▨
▨		▨	▨		]	[Ma	▨	No	▨	▨
▨	▨	▨	Wi	▨	▨	▨	▨	▨	So]	[
		▨	▨	]	[			]	[	
	▨	]	▨	[		▨	▨	▨	▨	▨
▨	▨	▨		▨	▨	▨	]	[		
]	[		▨		]	[			]	▨
[			]							

While the permutations of the columns changed frequently, these grids typically remained constant for a longer period. This allowed Nuboer to use an already known grid to find new permutations more easily; a feat Nuboer soon mastered. Once again the process depended on finding frequent code groups. By applying a tactic that a modern-day cryptanalyst might recognise as differential analysis, Nuboer would verify that, by permuting multiple telegrams according to the same permutation, each telegram would produce a common and valid code group. As by now Nuboer was able to recognise these groups on sight, this proved very effective. Through a series of deductive steps based on the relative distances between the symbols in the groups he found, Nuboer would then crack new permutations "over lunch". While it still consists of a set of technical intricacies, this became very much a logic puzzle. By carefully trying to squeeze the groups into the correct places in the grid, a telegram would line up and 'unlock'. And when the permutation was found, all of that day's telegrams could be read.

THE AMERICAN EFFORT

As early as World War I, the United States has been involved in military cryptanalysis (most notably through illustrious groups called Black Chambers). In the late twenties and early, the American navy began to see the crucial advantage that cryptanalysis could provide, and began training selected radio operatives. In the following decade, they would yield results very similar to those of Nuboer's Department 1, allowing them to closely follow the movements of the Japanese navy during the conflict in Northern China and revise their own strategic positions.

In American sources, two Japanese code systems from the 1920s and 1930s stand out. The first system is dubbed the Red Book. It appears to have been in use since 1918, and was broken by Agnes Meyer Driscoll in 1928 [7] – years before Nuboer would begin his work in Batavia. The American success followed a feat of what is referred to as 'practical cryptanalysis' [8]; breaking and entering into the Japanese consulate in New York City to obtain a copy of the (red-covered) Kana code book. Unfortunately, the technical details of the Red Book do not match those of any of the systems Nuboer stumbled upon, and the system appears to have been discontinued in November 1930.

Superseding the Red Book, the Japanese navy employed a system the American cryptanalysts called the Blue Book (named after the blue binders that they would use to carry the telegrams in). Of this new system, an American cryptographer notes that *"it employed a [..] columnar transposition involving both nulls and blanks. The garble table, [..], reduced the number of code groups to 85,184."* [8]. Using frequency analysis based on the Red Book, the Americans were able to make guesses about the meaning of the most common four-symbol code groups.

What is striking about the details above is that the system described is extremely similar to the '.' code that was decrypted by Nuboer and has been the main focus of this paper. As noted before, the '.' code consists of the same number of

[4] The figures were alternated every month and discarded after six months, and (generally) fresh permutations were used every day.

code groups, and also employs an intricate transposition of nulls and blanks.

The American codebreakers Safford, Dyer and Driscoll manage to break the code in late 1933, two years ahead of Nuboer, while the Japanese navy is still using the weak variant of the '.' code as well. On this breakthrough, Parker writes: ".. *their success had followed what was possibly the most difficult cryptanalytic task ever undertaken by the United States up to that time."* [7]. Additionally, they were aided in their work by a set of IBM tabulating machines. If it is indeed the same system, this puts the work of Nuboer in a remarkable perspective, especially considering the fact that the Dutch did not have access to the Red Book.

Another mention of the Blue Book states that a cryptologist named Arnold Conant was tasked with the daily duty of recovering the transposition, much like Nuboer had been after he had recovered the grids. By revealing that the code groups were written in the blank spaces from left to right and read from top to bottom [8], this anecdote further adds to the growing set of evidence.

The exact date when the Blue Book was discontinued remains slightly unclear: both June 1939 and October 1938 are mentioned [7, 8]. In any case this confirms to Nuboer's memoirs, where he describes how the work on the '.' code still continued when he left for the Netherlands in the summer of 1938 [6].

CONCLUSIONS

Nuboer stresses that the main gain from the Dutch cryptanalytic efforts was the amount of general tactical data that was gathered about the Japanese Imperial Navy. This included organisational structures of the various squadrons and fleets, but also positioning and even production information concerning the various Japanese vessels. In 1936, a vast part of all Japanese Naval communications was being read and carefully indexed by Department 1 in Batavia. This enabled many strategic successes, such as the timely evacuation of Dutch diplomats from the Hangzhou Bay area. While the escalating hostilities let to more rigorous use of cryptography and more frequently changing keys, the Dutch were consistently able to keep up.

In this paper, we have briefly explored how the Japanese '.' code worked and how it was broken. While at first glance the code might appear simple in hindsight, it had stumped radio operatives all around the Pacific theatre for years. Consisting of a code book substitution (which was initially closely guarded secret) and an intricate transposition involving nulls and blanks for further obfuscation, the cipher was truly a tortuous puzzle. This also shows in the assessments by the American naval intelligence services, assuming the code they refer to as the Blue Book is in fact the same code. In the previous section, we have seen a brief summary of the evidence that supports this. While the proof is not quite complete (as we have yet to find a telegram referred to as part of the Blue Code), it provides for interesting conclusions. Consider for instance the scale at which the United States Navy operated; an organisation much larger than Nuboer and his Department 1 could have ever hoped to rival.

All in all, it is remarkable to see how such a system can be unravelled by a slight tug on the correct loose ends.

ROLE OF THE STUDENT

While researching material for a study on the history of Dutch cryptography, prof. dr. Jacobs came across Johannes F.W. Nuboer's archives at the Netherlands Institute of Military History. The manuscripts from these archives promised a unique insight in the state of Dutch cryptanalysis in the 1930s and 1940s. Joost Rijneveld worked his way through the documents in order to uncover what Nuboer had known some eighty years ago. By means of his thesis, Joost provides an analysis of how the Japanese systems worked and how the Dutch were able to break them, as well as embedding it in the appropriate historical context. This paper serves as a summary thereof.

REFERENCES

1. R. D. Haslach. *Nishi no kaze, hare. Nederlands-Indische inlichtingendienst contra agressor Japan*. Van Kampen, Weesp, 1985.

2. J. F. W. Nuboer. Bijlage 2: Het vinden van de hervercyfering van de Japanse marine-code 1 in juni 1935. In *collectie 070, inv.nr. 4.18*. Nederlands Instituut voor Militaire Historie, Den Haag, 1977.

3. J. F. W. Nuboer. Bijlage 4: De Japanse marinecode no. 1. In *collectie 070, inv.nr. 4.18*. Nederlands Instituut voor Militaire Historie, Den Haag, 1977.

4. J. F. W. Nuboer. Bijlage 5: De ontcyfering van de sleutels van augustus 1935. In *collectie 070, inv.nr. 4.18*. Nederlands Instituut voor Militaire Historie, Den Haag, 1977.

5. J. F. W. Nuboer. Oprichting en beginjaren van de Afdeling 1 van de Marinestaf te Batavia. In *collectie 070, inv.nr. 4.17*. Nederlands Instituut voor Militaire Historie, Den Haag, 1977.

6. J. F. W. Nuboer. A history of Afdeling I (Intelligence), Naval staff, Batavia, Netherlands East Indies, from August 1934 to January 1938. volume 47. The Cryptogram, 1981.

7. F. D. Parker. *Pearl Harbor Revisited: United States Navy Communications Intelligence 1924-1941*, volume 6. Center for cryptologic history, National Security Agency, 1994.

8. A. Pelletier. Cryptography – Target Japan. In *U.S. Naval Cryptologic Veterans Association*, pages 27–32. Turner Publishing Company, 1996.

9. Y. Yasuba. Did Japan ever suffer from a shortage of natural resources before World War II? *The Journal of Economic History*, 56(03):543–560, 1996.