Voorschrift Geheime Berrichtenwisseling

Par Daniel TANT

Voici la brochure complémentaire au code hollandais.

Nº. 54.

VOORSCHRIFT

GEHEIME BERICHTENWISSELING

VOOR DE

LANDMACHT.

(V. GEH. BER. ~~XX~~).

(Aanschrijving D. v. O. d.d. 28 October 1927, IIe Afd., No. 21).

BREDA.
DE KONINKLIJKE MILITAIRE ACADEMIE.
1927.

N°. 54.

VOORSCHRIFT

GEHEIME BERICHTENWISSELING

VOOR DE

LANDMACHT.

(V. GEH. BER. ~~XX~~).

(Aanschrijving D. v. O. d.d. 28 October 1927, IIe Afd., No. 21).

BREDA.
DE KONINKLIJKE MILITAIRE ACADEMIE.

1927.

INHOUD.

Punt.			Bl.
I—V.		INLEIDING	1
VI.		Bekendheid met het voorschrift	2

HOOFDSTUK I.

Gebruik van geheimschrift.

1— 7.	A.	Algemeen	3
8—13.	B.	Tactisch gebruik van geheimschrift	5
14—21.	C.	Technisch gebruik van geheimschrift	9

HOOFDSTUK II.

22—32.	A.	Oproepseinen voor radio- (en aardtelegraaf-) posten	14
33—38.	B.	Schuilnamen	17
39—40.	C.	Golflengten	21

HOOFDSTUK III.

41—44.	A.	Gebruik van afkortingen	22
45—52.	B.	Gebruik van den XAA-code	23
53—64.	C.	Het cijfervierkant	27
65—66.	D.	Vercijfering van den U-seinlapcode	32
67—70.	E.	Vercijfering van radio-opdrachten van artillerie aan vliegtuigafdeelingen (vliegtuigen)	33
71—73.	F.	Geheime berichten, waarbij niet of slecht gebruik kan worden gemaakt van Morse-code	35

Blz.

BIJLAGEN. (Opgenomen in voorschrift No. 54*a*).

I. Afkortingen 1
II. Morse-code en Spellingsalfabet. 21
III. Tabel van de meest voorkomende verminkingen van lettergroepen 24
IV. Code voor den U-seinlap. 32
V. Tabel der codegetallen van den U-seinlap. . . 40
VI. Schema voor oproepseinen 42
VII. Schema voor schuilnamen 44
VIII. XAA-Code. 46

INLEIDING.

I. Dit voorschrift vat onder den term *geheimschrift* samen: *geheime code's* en *cijferschrift*. §

II. Onder *code* wordt verstaan een lijst van cijfers, letters, lettergrepen, woorden of zinnen, welke eenvoudig stuk voor stuk en meestal verkort, kunnen worden vervangen door een groep (*codegroep*) bestaande uit letters, cijfers of teekens.

Indien de beteekenis der codegroepen geheim is, spreekt men van *geheimen code* en anders van *open code*. Open code (bijv. de Morse-code, de code voor den U-seinlap, de XAA-code, enz.) is *geen* geheimschrift, doch slechts een soort van verkort schrift.

III. *Cijferschrift* is een stelsel van geheimschrift, waarbij men de letters, cijfers of teekens van den klaren tekst of van den codetekst wijzigt in beteekenis, in waarde, in volgorde, enz., volgens een overeengekomen formule, schema, sleutel, enz.

Cijferschrift behoeft niet steeds uit cijfers, doch kan ook uit letters bestaan. In hun meest eenvoudigen vorm naderen cijferschrift en code elkaar in wezen.

IV. Men verstaat onder:

klaar (in uitdrukkingen als *klaar schrift, klaar woord, klare tekst,* enz.): niet in geheimschrift, doch in de gangbare taal gesteld.

codeeren: het in code omzetten van klaar schrift.

vercijferen: het in cijferschrift omzetten van klaar schrift of van open code.

ontcijferen: het in klaar schrift weder omzetten van cijferschrift of code. Wenscht men echter bepaaldelijk onderscheid te maken tusschen het terugzetten eenerzijds van cijferschrift, anderzijds van code in klaar schrift, dan kan men de laatstgenoemde bewerking instede van ontcijferen ook *decodeeren* noemen.

---

§ Het rekent niet daartoe het z.g. *latent* of *verborgen schrift*, dat verkregen en weder leesbaar wordt door middel van chemische processen, tenzij het *verborgen schrift* eveneens in *geheimschrift*, (geheimen code of *cijferschrift*) is gesteld.

dubbele vercijfering: het (ten tweede male) vercijferen van een tekst reeds in cijferschrift of in geheimen code gesteld.

sleutel: een getal, een woord, een zin, een schema, enz., waarop een stelsel van geheimschrift is opgebouwd. Het is in het algemeen de kern van het geheimschrift, *welks geheimhouding tot het uiterste moet worden verzekerd*, daar het kennen of vinden van den sleutel tevens insluit het kennen van het geheimschrift in zijn geheel.

ontsluieren: het langs analytischen weg vinden van den sleutel van een geheimschrift, zonder tevoren daarmede ingewijd te zijn.

Onder *bericht* wordt in dit voorschrift verstaan elke mededeeling zoowel bericht als bevel, instructie, aanwijzing, enz.

V. Geheimschrift kan zijn openlijk, indien het als zoodanig onmiddellijk is te herkennen; dan wel *verborgen,* indien men het ter verzekering van eigen veiligheid of van eene veilige berichtenwisseling verbergt in een onschuldig lijkenden tekst met behulp van sympathische inkten, door puncteeren van woorden of letters, welke de dragers zijn van den geheimen tekst, enz.

Bekendheid met het voorschrift.

VI. Alle beroepsofficieren en de voor indeeling bij eene verbindingsafdeeling bestemde verlofsofficieren moeten op de hoogte zijn van dit voorschrift; de overige verlofsofficieren en de sergeanten (wachtmeesters) bij eene verbindingsafdeeling der infanterie (wielrijders), der cavalerie en der artillerie, alsmede de sergeanten-telefonist, idem-telegrafist, idem-radiotelegrafist en idem-optisch seiner, opgeleid bij het regiment genietroepen, moeten op de hoogte zijn van hetgeen in het voorschrift met een groot lettertype is gedrukt.

Het gestelde in Hoofdstuk III sub E is uitsluitend van belang voor het wapen der artillerie en voor den luchtvaartdienst.

HOOFDSTUK I.

Gebruik van geheimschrift.

A. Algemeen.

1. Alle verbindingen kunnen een gevaar vormen voor eigen troepen, indien niet steeds rekening wordt gehouden met de mogelijkheid, dat de aan deze verbindingen toevertrouwde berichten door onbevoegden worden opgevangen. Dezen kunnen zelfs uit onschuldig lijkende mededeelingen belangrijke gegevens samenstellen met betrekking tot onze militaire maatregelen, voornemens, opstellingen, enz.

2. Het gevaar, dat zou kunnen voortspruiten uit het onbevoegd opvangen der eigen berichten, moet worden gekeerd, deels door het gebruik van geheimschrift, deels door maatregelen, welke op andere wijze beoogen de mogelijkheid van opvangen zooveel mogelijk te beperken.

3. Het gebruik van geheimschrift heeft ten doel het ontcijferen der daarin gestelde berichten door on-ingewijden niet mogelijk te maken, of slechts ten koste van zooveel tijdverlies, dat de ontcijfering geen waarde meer heeft.

4. De eischen, waaraan een voor *militaire* doeleinden bestemd stelsel van geheimschrift moet worden getoetst, kunnen worden omschreven als volgt:

a. Het stelsel mag, zoo niet wiskundig, dan toch praktisch door derden niet ontsluierd kunnen worden.

b. Het bezit van een bericht in dat geheimschrift en van zijn letterlijken, klaren tekst mag geen aanleiding zijn, dat daardoor het stelsel ontsluierd kan worden.

c. Met uitzondering van den sleutel mag het geheimschrift desnoods in zijn geheel aan den vijand bekend zijn, zonder dat hierdoor het stelsel tevens onbruikbaar wordt.

d. De sleutel moet overgegeven en onthouden kunnen worden zonder de hulp van schrifturen en kunnen worden gewijzigd naar het believen der correspondenten.

e. In zijn praktische toepassing moet het eenvoudig zijn, geen hoofdbreken en niet veel tijd kosten, noch de kennis vereischen van vele toe te passen regelen: als regel moet één persoon in staat zijn met dat stelsel te werken.

f. De vercijferde berichten moeten geschikt zijn voor overseining door middel van Morse-teekens. Waar geen Morse-teekens voor de overseining kunnen worden gebezigd, moet het geheimschrift aan die andere wijze van overbrenging voldoen (bijv. voor seinen met den U-seinlap).

Deze eischen moeten als ideale eischen worden beschouw uit praktische overwegingen als: mate van geheimhouding, omstandigheden waarin en het personeel waardoor het cijferwerk zal worden verricht, de bijzondere eischen van het verbindingsmiddel, enz., zal dikwijls de eene eisch ter wille van den andere geheel of gedeeltelijk moeten worden opgeofferd.

5. De beantwoording van de vraag, *wanneer* van geheimschrift moet worden gebruik gemaakt, hangt af van

— den inhoud der mededeeling en (of) van

— de mate van het gevaar, dat zij door onbevoegden kan worden opgevangen.

6. Afhankelijk van den *inhoud* kan òf geen òf slechts een kortstondige òf wel een meer langdurige, dikwijls zelfs een blijvende geheimhouding noodzakelijk zijn.

Indien de inhoud geen geheimhouding vereischt, dan wel gevaar voor onderschepping practisch uitgesloten kan worden geacht, beteekent het gebruik van geheimschrift slechts tijdverlies.

Berichten kunnen hunne waarde voor derden reeds hebben verloren, nadat zij te bevoegder plaatse hun nut hebben gesticht. In deze gevallen is geen geheimschrift noodig of wel voldoet een geheimschrift, dat het geheim gedurende dat korte tijdsverloop verzekert.

In militair-diplomatiek verkeer, bij den inlichtingsdienst, voor mededeelingen van en aan groote eenheden, enz., moet het gebruik van geheimschrift een langdurige of een blijvende geheimhouding waarborgen.

7. Bij alle verbindingsmiddelen bestaat min of meer het *gevaar dat* de daaraan toevertrouwde *berichten* door onbevoegden *worden opgevangen*; de mate van dit gevaar verschilt slechts naar gelang van het te gebruiken verbindingsmiddel.

Verreweg het meest is dit gevaar te duchten in het radioverkeer en wel voornamelijk van de zijde van den vijandelijken luisterdienst.

Bij de aardtelegraaf kunnen de seinen technisch even gemakkelijk worden opgevangen als bij radio; storende gevechtsinvloeden bemoeilijken echter het cijferonderzoek der opgevangen berichten.

Bij telefoon en telegraaf vermindert het gevaar met toenemenden afstand tot den vijand. Bij langdurige gevechtsaanraking moet de strook binnen 3000 M. van de eigen voorste lijn vooral voor het telefoonverkeer als het gevaarlijkste gebied worden beschouwd. Doch ook zelfs ver achter het eigen front blijft bij deze verbindingsmiddelen het gevaar van het opvangen door onbevoegden van eigen nationaliteit bestaan.

Optische seinen kunnen in vele gevallen door den vijand worden medegelezen.

Bij berichthonden en bij postduiven beperken goede africhting en doelmatig gebruik de mogelijkheid, dat een bericht in handen valt van den vijand.

Ordonnansen en vliegtuigen, de laatste voor zooverre zij zich niet boven vijandelijk gebied bewegen, verzekeren nog het best de berichten tegen onderschepping.

B. Tactisch gebruik van geheimschrift.

8. De in punt 5, 6 en 7 genoemde omstandigheden met betrekking tot den inhoud der berichten en den aard van de daarvoor te bezigen verbindingsmiddelen moeten in onderling verband worden nagegaan.

Schriftelijke bevelen worden bij voorkeur zoodanig overgebracht, dat vercijfering onnoodig is.

De afzender is verantwoordelijk voor het al dan niet in geheimschrift stellen van zijn bericht. De commandant, onder wien de verbindingspost ressorteert, beslist nochtans of de door dezen post te verzenden berichten, welke in klaarschrift zijn aangeboden en niet voorzien zijn van de bijzondere aanwijzing: NCY (zie punt 10), al dan niet moeten worden vercijferd.

9. Indien de afzender dan wel de vorenbedoelde commandant er niet zeker van is, dat een voor den vijand belangrijk bericht steeds langs veilige verbindingswegen zal kunnen worden doorgezonden, dan dient hij dit bericht zekerheidshalve vóór de verzending te vercijferen of te doen vercijferen. Hij kan het bericht echter ook onvercijferd verzenden, doch moet het alsdan voorzien van de *bijzondere aanwijzing:* ZNCY (afkorting voor: zoo noodig vercijferen).

Berichten, welke voorzien zijn van deze bijzondere aanwijzing ZNCY, kunnen op hun verbindingsweg onvercijferd blijven, indien het voor de verzending of doorseining te bezigen verbindingsmiddel veilig kan worden geacht. Voor de al of niet vercijfering van zulk een bericht zijn alsdan verantwoordelijk de troepencommandanten, wier verbindingsposten met de doorzending van het bericht zijn belast. De bijzondere aanwijzing ZNCY mag eerst dan uit het bericht worden doorgeschrapt, indien het vercijferd is.

10. *In beginsel* mag geheimhouding niet worden opgeofferd aan snelheid van overbrenging.

Uit den aard der zaak brengt echter het gebruik van geheimschrift tijdverlies en bij een weinig geoefend cijferpersoneel kans op verminkingen en onleesbaarheid van het bericht mede. Er kunnen zich daarom omstandigheden voordoen, dat men voor veel spoed eischende en voor den vijand belangrijke berichten besluit geen geheimschrift te gebruiken. Voor deze beslissing en de daaruit mogelijk voortvloeiende gevolgen is de afzender verantwoordelijk.

Deze berichten voorziet de afzender van de bijzondere aanwijzing NCY (afkorting voor: niet vercijferen), ten teeken dat hij snelheid van overbrenging verkiest boven geheimhouding. Hierbij is vercijfering verboden.

11. Lange bevelen worden in den regel niet vercijferd

(zie ook punt 8, tweede zinsnede, punt 9 en punt 10). Dit heeft slechts plaats bij zeer korte bevelen of bij bevelen, waarbij voor de overbrenging zeer veel tijd beschikbaar is, terwijl geheimhouding dringend geboden is (voorbereidingen in den stellingoorlog, uitvoeringsbevelen).

12. Naar gelang van den inhoud van berichten moeten de volgende regelen worden in acht genomen:

a. Een bericht in geheimschrift moet steeds in geheimschrift worden beantwoord, indien dit antwoord, als het in klaar schrift ware gesteld, aan derden aanwijzingen zou kunnen geven omtrent den waarschijnlijken inhoud van het eerste bericht.

b. Een verzoek om herhaling van een vercijferd bericht, dat geheel of gedeeltelijk niet ontcijferbaar is gebleken, moet in geheimschrift worden gesteld. Blijkt de onontcijferbaarheid te berusten op verminking bij de overbrenging van het bericht, dan mag dit in zijn eersten vorm door den afzender worden herhaald. Is echter door hem een fout begaan bij het cijferwerk (gebruik van een verkeerden sleutel, enz.), dan moet het te herhalen bericht in eenigszins andere bewoordingen worden gesteld en daarna opnieuw vercijferd.

c. Voorschriften of aanwijzingen omtrent het gebruik van geheimschrift en omtrent het gebruik of de beteekenis van sleutelwoorden of sleutelgetallen, schuilnamen, oproepseinen, geheime codegroepen, mogen slechts schriftelijk of mondeling langs veiligen verbindingsweg worden gegeven.

Uitzonderingen op den voorgaanden regel en wel ten behoeve van bijzondere geheimschriften (voor militaire attachés, kondschappers, enz.), waarbij de correspondenten zonder veel tijdverlies moeilijk schriftelijk of mondeling te bereiken zijn, moeten uitdrukkelijk in de bijzondere gebruiksaanwijzingen van het betrokken geheimschrift worden toegestaan.

d. Namen van eenheden, van commandanten van groote

eenheden, enz. kunnen den vijand reeds belangrijke aanwijzingen geven omtrent onze voornemens, troepenopstelling, enz. Hunne vermelding in klaar schrift of in open code in berichten, welke opgevangen kunnen worden, dient te worden vermeden. Het gebruik van oproepseinen en schuilnamen voor de vermelding van adres en van afzender is dan regel.

13. Uit den aard der verbindingsmiddelen met betrekking tot het gevaar van opvangen, vloeien de volgende verplichtingen voort.

a. Onafhankelijk van den afstand tot den vijand mag — behoudens in het geval, voorzien in de laatste zinsnede van punt 10 — geen bericht, waaruit de tegenpartij eenig nut kan trekken (over aflossingen, verliezen, eigen troepenopstelling, enz.), in klaar schrift of open code per radio worden gezonden; evenmin met optische seinmiddelen, indien gevaar bestaat dat de vijand de seinen medeleest. Evenmin mogen binnen 3000 M. van de eigen voorste troepen, wanneer deze reeds gedurende eenigen tijd in gevechtsaanraking zijn, belangrijke berichten per lijn- of aardtelegraaf (uitgezonderd geheimtelegraaf) of telefonisch worden gewisseld, anders dan met gebruikmaking van geheimschrift. Belangrijke berichten per postduif of berichthond, dikwijls ook per ordonnans, worden vercijferd of door gebruik van schuilnamen voor derden onbegrijpelijk gemaakt.

b. Gebruik van schuilnamen en oproepseinen is verplicht:
in het radioverkeer te allen tijde,
in het optisch seinverkeer, indien de vijand de seinen kan medelezen,
in het telefonisch en in het lijn- en aardtelegrafisch verkeer binnen de in punt 13 *a* bedoelde strook.

C. *Technisch gebruik van geheimschrift.*

14. De wijze, waarop geheimschrift moet worden gebruikt, is, onverminderd de voor een bepaald stelsel gemaakte bijzondere gebruikseischen, onderworpen aan de hieronder volgende regelen.

Veronachtzaming dezer regelen brengt niet alleen de waarde van het geheimschrift, doch daardoor ook wellicht de veiligheid der eigen troepen in gevaar. De ervaring leert, dat zelfs schijnbaar nietige fouten in het technisch gebruik van geheimschrift den sleutel ervan kunnen onthullen.

15. *a.* Alvorens een geheimschrift toe te passen dienen de bijzondere gebruiksaanwijzingen daarvan grondig te worden gekend.

b. Alle voorzorgen moeten worden genomen om den sleutel ongeschonden te bewaren. Eenig vermoeden, dat het geheim geschonden is, moet onmiddellijk worden gemeld.

Zooveel mogelijk worden steeds dezelfde personen voor het cijferwerk aangewezen; zij mogen slechts die gegevens ontvangen, welke betrekking hebben op de geheimschriften, welke zij voor hun taak noodig hebben.

Kladpapieren afkomstig van het cijferwerk worden onmiddellijk na gebruik vernietigd (verbrand). Alle bescheiden, welke den sleutel in gevaar kunnen brengen (ontvangen cijferberichten, geheime codes, bijzondere gebruiksaanwijzingen betreffende den sleutel, enz.) moeten veilig worden bewaard en onmiddellijk worden vernietigd, indien gevaar dreigt dat zij den vijand in handen zullen vallen.

c. Cijferberichten mogen nimmer te zamen met hunne ontcijferingen worden opgelegd. De ontcijferingen kunnen worden opgelegd in het archief, waarin zij behooren. De cijferberichten, die niet verbrand kunnen worden,

moeten afzonderlijk, zoo veilig mogelijk, worden opgelegd.

De vercijferde teksten van berichten, *door middel van het cijfervierkant* in geheimschrift gesteld, moeten evenwel 2 uren nà de ontcijfering worden verbrand.

Indien bijzonder belangrijke cijferberichten langs veiligen weg door een bevestiging in klaar schrift worden gevolgd, dan mag alleen indien bepaaldelijk noodig de tekst van beide berichten dezelfde zijn. Alle zinspeling in klaar schrift op deze bevestiging dient in beide berichten te worden vermeden.

d. De ontvanger van een cijferbericht moet — behalve bij dringende noodzakelijkheid — zorgen, dat bij het verwerken en verder bekend maken van dit bericht de tekst niet letterlijk overeenstemt met dien van het cijferbericht.

e. *Het is uitdrukkelijk verboden eenzelfde bericht gedeeltelijk in geheimschrift, gedeeltelijk in klaar schrift op te stellen.*

De tijdwinst, welke men hiermee beoogt, valt in het niet bij het gevaar voor ontsluiering, waaraan men het geheimschrift hierdoor zou blootstellen. Onder dit verbod van gelijktijdig gebruik van geheimschrift en klaar schrift in eenzelfde bericht vallen ook de als klaar schrift te beschouwen afkortingen, open code en leesteekens.

Slechts *schuilnamen* en *oproepseinen,* hoewel ook deze een soort van geheimen code zijn, mogen gezamenlijk met klaar schrift of met open code worden gebruikt. Evenzoo vormt de vercijfering als aangegeven in punt 69 van bijzondere radioberichten van artillerie aan vliegtuigafdeelingen (vliegtuigen) eene uitdrukkelijk toegestane uitzondering op dit verbod.

Vordert een gedeelte van den klaren tekst van een bericht geen bijzondere geheimhouding en zou een vercijfering daarvan gelijk staan met nutteloos tijdverlies, dan wordt dit gedeelte als een afzonderlijk bericht in klaar schrift of open code gezonden. Dat het daarbij aansluitende gedeelte vercijferd zal worden, moet worden verzwegen. In het vercijferde gedeelte van het bericht kan zoo noodig — van zelf sprekend eveneens vercijferd — verwezen worden naar het in klaar schrift gestelde gedeelte.

Vermenging van open code met klare taal is toegestaan.

f. Eenige openlijke zinspeling, hoe gering ook, ten aanzien van het vercijferd ontvangen of verzenden van een bericht, is verboden. Herhaling of verduidelijking in klare taal, ook zelfs van een enkele groep in een cijferbericht, moet geheel worden vermeden.

g. Zooveel mogelijk moet worden nagelaten den tekst van cijferberichten met eenzelfden aanhef aan te vangen of met eenzelfde slot te beëindigen. Indien dit de tegenpartij bekend is, zou het haar de ontsluiering van het geheimschrift dikwijls zeer vergemakkelijken.

h. De vermelding van adres en afzender, alsmede van nummer en tijd van den afzender van het bericht, moeten vergeleken bij den eigenlijken inhoud van het bericht, min of meer als afzonderlijke groepen worden beschouwd en mogen nimmer worden vercijferd.

De groepen voor adres en afzender worden, indien geheimhouding daarvan noodig is, met schuilnamen (c.q. oproepseinen) gecodeerd in de eerste plaats door den afzender, zoo noodig door de zorg van den ver-

HOOFDSTUK II.

A. Oproepseinen voor radio- (en aardtelegraaf-) posten.

22. De beteekenis van radio-oproepseinen is geheim; de lijsten dezer oproepseinen met hun beteekenis zullen slechts de voor een bepaalden post, dienst, enz. noodige oproepseinen mogen bevatten.

23. Radio-oproepseinen bestaan uit samenvoegingen van normaal 2 letters, welke met behulp van het schema als in Bijlage VI is gegeven, worden verkregen. De samenvoegingen FT, OK, RP, SL en ZD mogen echter niet worden gebruikt als oproepseinen voor radioposten, aangezien zij reeds eene beteekenis hebben als afkorting.

24. Daartoe wordt een vierkant in 25 horizontale rijen en 25 verticale kolommen verdeeld, elke rij en elke kolom te benoemen met een letter uit het alfabet *(zonder de letter Q)*.

Elk der 625 op deze wijze verkregen kleinere vakjes stelt een oproepsein voor van 2 letters, waarvan de *eerste* letter overeenkomt met die van de *verticale kolom*, de *tweede* letter met die van de *horizontale rij*, waarin het oproepsein ligt.

De benoeming van rijen zoowel als van kolommen geschiedt met behulp van een alfabet (zonder de Q), waarvan de volgorde der letters door een sleutelwoord (of -zin) wordt vastgesteld.

De volgorde der letters ter benoeming van rijen mag niet dezelfde zijn als die van kolommen.

In het schema van Bijlage VI is als sleutelwoord aangenomen:

PRINS WILLEM.

Met weglating der letters, welke meer dan één keer daarin voorkomen, doch met behoud van hare volgorde, geeft dit sleutelwoord tot *sleutelletters* en volgorde hiervan:

PRINSWLEM

(in voorkomend geval wordt de IJ als sleutelletter steeds als de *enkele letter* Y beschouwd).

Men schrijft daarna onder de sleutelletters de overige letters van het alfabet (zonder de Q) in hare alfabetische volgorde van links

naar rechts in rijen, even groot als het aantal sleutelletters; de onderste rij kan eventueel minder letters tellen. Aldus:

Fig. 1.

P R I N S W L E M
A B C D F G H J K
O T U V X Y Z

De aldus opgeschreven letters, kolomsgewijze afgeschreven, in elke kolom van *boven naar beneden,* de kolommen resp. van *links naar rechts,* geven het benoemingsalfabet voor de *bovenzijde* van het vierkant nl.

PAORBTICUNDVSFXWGYLHZEJMK (in het vierkant in te schrijven van links naar rechts).

Voor het benoemingsalfabet van de linker zijde van het vierkant gebruikt men hetzelfde sleutelwoord, doch thans worden de 25 letters geschreven in een vierkant van 5 maal 5 letters, aldus:

Fig. 2.

A B C D F
G H J K O
T U V X Y
Z P R I N
S W L E M

Namelijk, te beginnen met links boven achtereenvolgens van links naar rechts, de rijen achtereenvolgens van boven naar beneden worden in het vierkant van 5 × 5 eerst de letters van het alfabet (zonder de Q en zonder de sleutelletters) in haar alfabetische volgorde ingeschreven, daarna de sleutelletters in hare sleutel-volgorde.

Fig. 2, kolomsgewijze afgeschreven, in elke kolom van *boven naar beneden,* de kolommen resp. van *links naar rechts,* geeft het benoemingsalfabet aan voor de *linkerzijde* van het vierkant van bijlage VI, nl.:

AGTZSBHUPWCJVRLDKXIEFOYNM (in het vierkant in te schrijven van boven naar beneden).

Elk der 625 vakjes stelt schematisch een oproepsein van 2 letters voor, waarvan de *eerste letter* die is van de *kolom,* te nemen uit het *bovenste* benoemingsalfabet; de *tweede letter* is die van de *rij,* te nemen uit het *linker* benoemingsalfabet.

25. De O.L.Z. stelt vast (wijzigt) de benoeming der kolommen en rijen door de uitgifte van een (nieuw) sleutelwoord.

26. Als beginsel geldt dat aan radio-(aardtelegraaf-) posten van een bepaalde eenheid geen bepaalde groep van oproepseinen mag worden gegeven, welke dusdanig onderscheiden is van andere groepen, dat ook de vijand daaruit gegevens zou kunnen ontsluieren met betrekking tot bevelsverhouding, troepenindeeling, opstelling, enz.

27. Teneinde den vijand zooveel mogelijk te beletten eenig verband te vinden tusschen de oproepseinen en de daarmede aan te duiden posten of eenheden, worden in beginsel ten behoeve van eenzelfde eenheid daaraan toegewezen die oproepseinen, welke in het schema van Bijlage VI liggen in een *diagonaalrij*, d.i. een rij evenwijdig aan den diagonaal, welke den linkerbenedenhoek met den rechterbovenhoek verbindt. De diagonaalrijen hebben in tegenstelling met de kolommen en rijen een vaste nummering van 1 tot en met 25 en van 1a tot en met 24a (zie Bijlage VI); de nummers der diagonaalrijen geven tevens voor het gemak het aantal aan der in die diagonaalrijen gelegen oproepseinen.

28. De O.L.Z stelt, na voor het gebruik van het A.H.K., enz. de noodige diagonaalrijen te hebben gereserveerd, de overblijvende diagonaalrijen of eenige daarvan ter beschikking van den C.V., van C. van duurzame stellingen, van Territoriale Bevelhebbers, enz.

De C.V. stelt op gelijke wijze hem toegewezen diagonaalrijen of gedeelten daarvan ter beschikking van het H.K.V., de D.G., de Lt.B., enz.

De C. der D.G., der Lt.B., enz. handelen op overeenkomstige wijze bij de verdeeling der hun toegewezen oproepseinen.

29. Herhaalde verandering van oproepseinen — in den stellingoorlog bovendien onafhankelijk van aflossingen — is noodig om de tegenpartij het onderzoek naar de beteekenis van of het verband tusschen de oproepseinen te bemoeilijken en haar te gewennen aan het in werking treden van nieuwe oproepseinen, hetgeen bij het optreden van nieuwe troepen niet is te vermijden.

In beginsel zal voor radio- en aardtelegraafposten een verandering van oproepsein gepaard gaan aan eene wijziging van hunne golflengten of toonhoogten.

30. Verandering van oproepseinen geschiedt door eene wijziging in de benoeming van de kolommen en rijen in het schema van Bijlage VI (slechts op last van den O.L.Z.) of door een wijziging in de verdeeling der toegewezen oproepseinen (op last van elken

commandant, doch slechts met betrekking tot de aan dezen ter verdeeling toegewezen oproepseinen). Teneinde deze laatste wijze van verandering der oproepseinen mogelijk te maken is het gewenscht bij de toewijzing ervan met een zeker surplus rekening te houden.

Bij verandering van oproepseinen is het gewenscht deze voor een bepaald troependeel niet alle gelijktijdig te wijzigen, doch gedeeltelijk.

31. In den stellingoorlog mogen oproepseinen van het eene gedeelte van een operatietooneel in geen geval naar een ander gedeelte worden medegenomen; oproepseinen zijn alsdan aan hun plaats gebonden; bij troepenaflossingen mogen zij niet worden veranderd, doch worden zij aan de aflossende troepen overgegeven.

32. In den bewegingsoorlog moet aan den vijand worden belet het verblijf onzer troepen op te maken uit de verplaatsing der bij deze troepen ingedeelde radioposten. Hiertoe zal het noodig zijn reeds tevoren maatregelen te treffen, opdat deze posten bij elke belangrijke verplaatsing hunne oproepseinen kunnen veranderen.

B. Schuilnamen.

33. Indien de openlijke vermelding van namen van troepeneenheden, van staven, commandanten, belangrijke terreinvoorwerpen, enz. den vijand reeds nuttige gegevens kan verstrekken, moeten deze worden aangeduid met schuilnamen. Zij behoeven niet uitsluitend uit namen te bestaan, maar men kan daarvoor ook andere woorden, letters, getallen of een combinatie daarvan bezigen.

Oproepseinen vormen een soort van schuilnamen en mogen als zoodanig worden gebruikt. In radioberichten mogen de bij de oproepseinen behoorende schuilnamen voor „adres" en „afzender" niet worden geseind, maar gebruikt men uitsluitend de oproepseinen.

34. Schuilnamen mogen tegelijk met open code of met klaar schrift worden gebezigd.

In beginsel worden schuilnamen steeds gebezigd ter ver-

melding van adres en van afzender in berichten, welke door den vijand kunnen worden onderschept. Dit geschiedt in de eerste plaats door den afzender zoo noodig door de zorg van den verbindingspost, met de verzending van het bericht belast. *De groepen voor adres en afzender worden nimmer vercijferd;* zijn de schuilnamen niet bekend dan worden adresseering en afzender vercijferd, vooraan *den inhoud* opgenomen en het bericht gezonden aan den commandant, die voor de doorzending kan zorg dragen.

35. De punten 22, 26, 29 en 31 gelden ook ten aanzien van schuilnamen.

36. Als schuilnamen voor het versluieren van namen als bedoeld in punt 33 1e zin, worden de samenvoegingen van eigennamen met getallen, b.v. KAREL 16, ~~MARINUS~~ MARIE 97, enz. gebezigd.

Voor het vormen en het uitgeven dezer schuilnamen wordt gebruik gemaakt van een soortgelijk vierkant als is aangegeven in punt 24, met dien verstande echter, dat het vierkant behalve aan de boven- en de linkerzijde, ook benoemd wordt aan de onder- en de rechterzijde met behulp van een sleutelwoord (-zin), hetwelk een ander moet zijn dan dat voor het alsdan geldende schema van oproepseinen.

In Bijlage VII is als sleutelwoord genomen:

MITRAILLEUR

gevende tot sleutelletters: MITRALEU.

Het alfabet, geschreven in den vorm als aangegeven in fig. 1 en fig. 2 van punt 24, geeft als overeenkomstige figuren:

Fig. 1a.

M I T R A L E U
B C D F G H J K
N O P S V W X Y
Z

Fig. 2a.

B C D F G
H J K N O
P S V W X
Y Z M I T
R A L E U

Fig. 1a, kolomsgewijze afgeschreven, in elke kolom van *boven naar*

In het schema van Bijlage VII stelt het gearceerde vakje schematisch de schuilnamen voor: PIETER 38, JAN 3, ANNA 56 en NICO 61.

De O.L.Z. stelt vast (wijzigt) de benoeming der kolommen en rijen door de uitgifte van een (nieuw) sleutelwoord.

Ten aanzien van de uitgifte dezer schuilnamen geldt het bepaalde in punt 28; rekening dient daarbij te worden gehouden, dat bij de toewijzing van diagonaalrijen of gedeelten daarvan met elk vakje, althans zonder nadere beperkingen, steeds 4 schuilnamen worden toegewezen.

37. Schuilnamen kunnen ook voor andere doeleinden worden gebruikt dan voor het versluieren van namen bedoeld in punt 33.

In een schuilnaam kunnen korte doch belangrijke mededeelingen worden neergelegd als het al dan niet voortzetten van den aanval, het tijdstip van den aanval, het overschrijden van een bepaalde lijn door bepaalde troepen, enz. Uit den aard der zaak kunnen deze schuilnamen door de betrokken commandanten zelf worden uitgegeven.

Ook kunnen voor de meest spoedeischende meldingen aan kondschappers schuilnamen (schuilzinnen) worden medegegeven, waardoor in oogenschijnlijk onschuldige berichten belangrijke mededeelingen kunnen worden verborgen. De veiligheid der kondschappers laat meestal het gebruik van als zoodanig onmiddellijk herkenbaar geheimschrift niet toe.

Voor de in dit punt bedoelde schuilnamen kan *zoonoodig* een andere vorm worden gekozen dan die in punt 36 aangegeven. Zij kunnen bestaan uit zinnen, woorden, letters, getallen of een combinatie daarvan, mits daarbij rekening wordt gehouden dat zij geen aanleiding geven tot verwarring met hun gewone dan wel de daaraan van hooger hand reeds toegekende beteekenis. Evenmin mag daarbij een geringe, doch veel voorkomende verminking van 1 letter of van 1 cijfer aanleiding kunnen geven tot ernstige gevolgen.

Een keuze van schuilnamen als bijv.:

A 1 LOOSDUINEN bezet
A 3 LOOSDUINEN niet bezet
15 richting A. verkennen
35 richting B. verkennen

is onjuist.

38. Daar schuilnamen in wezen geheime code zijn, is het, indien voor een bepaalde berichtenwisseling behoefte blijkt aan een min of meer uitgebreide lijst of stelsel van schuilnamen, in verband met punt 19 noodzakelijk, dat van deze behoefte door de D.Cn., C.Lt.B., overeenkomstige of hoogere commandanten kennis wordt gegeven, opdat door de door den O.L.Z. ter beschikking te stellen cijfer-experten een stelsel kan worden ontworpen.

C. Golflengten.

39. Bij de toewijzing van golflengten of series van golflengten geldt als leidend beginsel, dat zij door regelmaat den vijand geen inzicht mag geven in de samenstelling en in de indeeling van de strijdmacht.

Het beperkte golfbereik der verschillende soorten radiotoestellen kan nochtans een indeeling in groepen noodzakelijk maken. Binnen deze groepen moet echter de toewijzing van golflengten of series daarvan geheel onregelmatig zijn.

40. Ter misleiding van den vijand worden de golflengten tijdens den loop der operatiën veelvuldig gewijzigd in beginsel zoo mogelijk gelijktijdig met de oproepseinen.

HOOFDSTUK III.

A. Gebruik van afkortingen.

41. Teneinde een eenvormige regeling in het leven te roepen is in Bijlage I de wijze van afkorting vastgesteld voor bepaalde commandanten, staven, troepeneenheden, enz., gesplitst in:

a. benamingen van eenheden, commandanten en staven van de landmacht op voet van oorlog, zoomede algemeene afkortingen;

b. afkortingen te gebruiken bij de vuurleiding der art.;

c. afkortingen te gebruiken in radioberichten bij de samenwerking van art. met vliegtuigen;

d. afkortingen te gebruiken in het dienstverkeer;

e. afkortingen voor bijzondere aanwijzingen.

42. Ter besparing van tijd moet in het berichten-verkeer te velde zooveel mogelijk worden gebruik gemaakt van deze afkortingen. Elke officier en elke seiner dient de voor zijn dienst bestemde afkortingen te kennen.

Behalve de in Bijlage I vermelde afkortingen mag ook worden gebruik gemaakt van die uit het dagelijksch leven, voor zoover deze geen aanleiding geven tot misvattingen.

43. Andere afkortingen dan die, voorkomende in dit voorschrift (zie bijlage I ad *a*) en de in punt 42 laatste zinsnede bedoelde, mogen in schriftelijke bevelen niet worden gebruikt. Van de schrijfwijze en punctuatie mag in schrift en druk niet worden afgeweken. Overigens geldt ten aanzien van het gebruik van de afkortingen in Bijlage I ad *a* het gestelde in de Toelichtingen daarvan. (bldz. 6).

44. Bij het vercijferen van afkortingen worden alle letters in afkortingen met hoofddrukletters aangegeven (zie punt 16); lees- en zinteekens kunnen (behalve in schrift en druk) worden weggelaten, *voor zoover althans het weglaten ervan geen misvatting teweeg kan brengen.* Bij de ontcijfering wordt door den ontcijferaar de voorgeschreven schrijfwijze der afkortingen weder hersteld.

B. Gebruik van den XAA-code.

45. Deze code (Bijlage VIII) is een *niet* geheime code; het is een lijst van in militaire berichten te velde het meest voorkomende woorden, uitdrukkingen en getallen, welke verkort kunnen worden weergegeven met codegroepen bestaande uit 3 letters, waarvan de beginletter de letter X is; de beide daarop volgende letters vindt men onmiddellijk *links* van het klare woord, getal of uitdrukking.

46. *Inrichting van den XAA-code.* De code bevat $24 \times 24 = 576$ codegroepen, d.i. het aantal combinaties 2 aan 2 van 24 letters, daar de letters Q en X niet als slotletters in de codegroepen mochten worden opgenomen. (Het cijfervierkant laat de vercijfering van de letter Q niet toe; de letter X moest uitsluitend dienen ter aanduiding van het begin van een XAA-groep).

Deze codegroepen, waarvan Bijlage VIII in de kolommen „Code" slechts de 2 slotletters vermeldt, zijn alfabetisch gerangschikt.

Naar de beteekenis der codegroepen (kolommen „Klaar" in Bijlage VIII) zijn deze te onderscheiden in:

a. bijzondere groepen,
b. getallen,
c. leesteekens,
d. het woordenboek.

44. Bij het vercijferen van afkortingen worden alle letters in afkortingen met hoofddrukletters aangegeven (zie punt 16); lees- en zinteekens kunnen (behalve in schrift en druk) worden weggelaten, *voor zoover althans het weglaten ervan geen misvatting teweeg kan brengen.* Bij de ontcijfering wordt door den ontcijferaar de voorgeschreven schrijfwijze der afkortingen weder hersteld.

B. Gebruik van den XAA-code.

45. Deze code (Bijlage VIII) is een *niet* geheime code; het is een lijst van in militaire berichten te velde het meest voorkomende woorden, uitdrukkingen en getallen, welke verkort kunnen worden weergegeven met codegroepen bestaande uit 3 letters, waarvan de beginletter de letter X is; de beide daarop volgende letters vindt men onmiddellijk *links* van het klare woord, getal of uitdrukking.

46. *Inrichting van den XAA-code.* De code bevat $24 \times 24 = 576$ codegroepen, d.i. het aantal combinaties 2 aan 2 van 24 letters, daar de letters Q en X niet als slotletters in de codegroepen mochten worden opgenomen. (Het cijfervierkant laat de vercijfering van de letter Q niet toe; de letter X moest uitsluitend dienen ter aanduiding van het begin van een XAA-groep).

Deze codegroepen, waarvan Bijlage VIII in de kolommen „Code" slechts de 2 slotletters vermeldt, zijn alfabetisch gerangschikt.

Naar de beteekenis der codegroepen (kolommen „Klaar" in Bijlage VIII) zijn deze te onderscheiden in:

a. bijzondere groepen,
b. getallen,
c. leesteekens,
d. het woordenboek.

47. Als bijzondere codegroepen vindt men de codegroep:

1. XAA = XAA-code.
2. XEZ = (letter) Q.

   Van deze codegroep moet worden gebruik gemaakt bij vercijfering met behulp van het Cijfervierkant van woorden, waarin de letter Q niet of moeilijk kan worden weergegeven met K of KW (bij namen, enz.).
3. XFA = nu volgt codegroep U-seinlap.

   Met behulp van deze codegroep kan men van de codegetallen van den U-seinlap (~~overgenomen~~ Opgenomen in Bijlage IV) gebruik maken, zoowel bij berichtenwisseling anders dan met den U-seinlap als in te vercijferen berichten.

   Een bericht: Wij zijn niet gereed op het vastgestelde uur aan te vallen,

   kan bijv. optisch geseind worden als:

   XFA 135.
4. XFB = verleden deelwoord v/h voorafgaande woord.

   Voorbeeld:

   Klaar: Gevecht afbreken
   Code: XJW XFR
   Klaar: Gevecht afgebroken
   Code: XJW XFR XFB

48. *Getallen* of reeksen van getallen kunnen worden weergegeven met de codegroepen XAB, XAC, enz. tot en met XEF; Romeinsche cijfers door de codegroepen XEG tot en met XEP. Men kan daarbij al dan niet gebruik maken van de codegroepen voor de *leesteekens:* XER tot en met XEY.

De codegroepen XAB tot en met XEY worden *alleen* gebruikt ten behoeve van de vercijfering van getallen met behulp van het cijfervierkant.

Bij het codeeren van een reeks van cijfers moet alleen

ermede rekening worden gehouden of een cijfer (getal) een afzonderlijk begrip vormt dan wel of die reeks van cijfers tezamen één enkel begrip omvat.

In het eerste geval worden de afzonderlijke cijfers (getallen) ook als afzonderlijke groepen gecodeerd, met als onderlinge afscheiding gecodeerde leesteekens; in het laatste geval worden de codegroepen eenvoudig achter elkander gegeven en is het onverschillig, hoe men die reeks van cijfers ontbindt.

Voorbeelden:

Klaar: 12000
Code: XAO XAB XAC of XAD XAY XAC of XAO XAC XAB
Klaar: 359
Code: XAF XCN of XBN XAL
Klaar: 3/4
Code: XAF XEY XAG
Klaar: 1,2 — III — 8 R.I.
Code: XAD XES XAE XEI XAK RI

49. Het eigenlijke *woordenboek* omvat de codegroepen XFE t/m XZZ. De klare groepen zijn alfabetisch gerangschikt; in beginsel zijn slechts de in militaire berichten te velde meest gebruikte of als zoodanig geachte woorden opgenomen en wel die, waarvoor *geen afkortingen* bestaan en welke *meer dan 4 letters* tellen. Vier of minder letters tellende woorden als: in, aan, door, enz. zijn in het woordenboek niet opgenomen, evenmin woorden als: Jachtvliegtuigafdeeling (afkorting: Ja.V.A.), Hoofdkwartier van het Veldleger (afk. H.K.V.), enz., wel bijv.: Jachtvliegtuig of Jachtvliegtuigen (XLU), U-seinlap (XVI), enz.

Waar een klare groep een tweeledige beteekenis heeft, bijv.

XWJ = verkennen (-ing)

moet uit het bericht blijken of de eerste (verkennen) dan wel de tweede (verkenning) is bedoeld.

In den regel kunnen de werkwoordsvormen (tijden en wijzen) zonder gevaar voor misvatting worden weergegeven met de onbepaalde wijs; bestaat dit gevaar, dan is toevoeging noodig van hulpwerkwoorden, persoonlijke voornaamwoorden, uitgangen, enz.

Klaar: Marcheer onmiddellijk af.
Code: U XFT XPO
Klaar: Bevind mij blad 33, vierkant 7—56, 45—25.
Code: IK XHE BL XBL VT XAJ XEV XCK XES XBZ XEV XBD

50. De XAA-code wordt gebruikt in die gevallen, waarin men verplicht is of behoefte heeft berichten zoo kort mogelijk weer te geven en in deze behoefte niet op andere wijze is voorzien (door afkortingen of anderen code); derhalve:

a. bij optisch-, telegraaf- of radio seinen in Morse-code;
b. bij schriftelijke berichten (voornamelijk voor postduiven);
c. bij vercijfering met het cijfervierkant.

51. Bij het seinen als open code wordt elke codegroep als een afzonderlijke groep gerekend en geseind.

Bij gebruik van den XAA-code wordt de tekst van het bericht zooveel mogelijk aangepast aan de in dezen code gegeven woorden.

52. De XAA-code is *niet geheim;* niet vercijferd vormen de codegroepen slechts een soort van verkort schrift. Als zoodanig zal het toepassing vinden voor berichten, welke geen geheimhouding vereischen, daarbij al of niet vermengd met klare taal, afkortingen en schuilnamen.

Is geheimhouding noodzakelijk, dan wordt de gecodeerde tekst alsnog vercijferd.

C. *Het cijfervierkant.*

53. Het CIJFERVIERKANT is een stelsel van vercijfering, waarbij met behulp van een sleutelwoord (c.q. sleutelzin) de letters van den klaren of van den open code-tekst *2 aan 2* worden vervangen door andere groepen van 2 letters (vercijferde of kortweg *cijfergroepen* genoemd). Een daarbij overblijvende enkele letter uit den klaren tekst wordt eveneens door een andere letter vervangen.

54. Het *sleutelwoord* is geheim en wordt vastgesteld door den O.L.Z., die deze bevoegdheid echter al dan niet blijvend kan overdragen aan den C.V., aan commandanten van duurzame stellingen of aan andere, rechtstreeks onder zijne bevelen staande commandanten.

De bedoelde bevoegdheid kan weder worden overgedragen:

1e. door den C.V. aan de D.G.Cn., aan den C.Lt.B. en aan commandanten van zelfstandige divisiën of andere onderdeelen;

2e. door de stellingcommandanten aan door dezen aan te wijzen Front- of Groepscommandanten.

Van het uitgegeven sleutelwoord wordt zoonoodig aan neventroepen kennis gegeven.

Het sleutelwoord moet *minstens vijf* verschillende letters *(sleutelletters)* bevatten; de letter Q mag er niet in voorkomen, de IJ wordt in het sleutelwoord steeds als de *enkele letter* Y beschouwd.

Het sleutelwoord moet herhaaldelijk worden gewijzigd (nimmer echter op geregelde tijdstippen); wijziging ervan is reeds geboden, indien slechts een vermoeden bestaat, dat de vijand ermede bekend is. *Het is verboden het sleutelwoord dan wel het ingevulde cijfervierkant op schrift te bewaren.*

55. Het cijfervierkant wordt, door de zijden elk in 5 te

verdeelen, onderverdeeld in 25 vakjes. In elk dier vakjes wordt volgens een bepaalden regel één der letters van het alfabet *(zonder de letter Q)* ingeschreven. Het sleutelwoord stelt den regel van inschrijving vast.

Is het sleutelwoord bijv.: BEVERWIJK, dan levert het met weglating der letters, welke meer dan één keer daarin voorkomen, doch met behoud van hare volgorde in het sleutelwoord de volgende *sleutelletters:* B E V R W Y K.

De vakjes in het cijfervierkant worden nu ingeschreven elk met een letter, te beginnen met het *linker bovenste* vakje achtereenvolgens van *links naar rechts*, de rijen achtereenvolgens van *boven naar beneden.*

Eerst schrijft men de letters van het *alfabet* in (zonder de Q en zonder de sleutelletters), *daarna de sleutelletters* in de volgorde, zooals het sleutelwoord die aangeeft.

Aldus ingeschreven geeft het sleutelwoord BEVERWIJK het volgend cijfervierkant:

A	C	D	F	G
H	I	J	L	M
N	O	P	S	T
U	X	Z	B	E
V	R	W	Y	K

56. Om een bepaalden klaren (code-) tekst met behulp van dit cijfervierkant te vercijferen, wordt die tekst volgens een in punt 61 aan te geven regel verdeeld in groepen van 2 letters. Vóór de vercijfering wordt de letter Q zoo

mogelijk eerst door K of KW vervangen, dan wel aangegeven met XEZ; alle cijfers worden eveneens vóór de vercijfering voluit in letters geschreven of, indien het getal te veel letters zou bevatten, weergegeven met XAA-codegroepen (zie punt 48).

57. Bij het *vercijferen* van een groep van 2 klare letters kunnen zich met betrekking tot hare onderlinge plaats in het cijfervierkant de volgende 4 gevallen voordoen:

a. de beide letters bevinden zich in *dezelfde horizontale rij;*
b. zij liggen in *dezelfde verticale kolom;*
c. zij liggen noch in dezelfde rij noch in dezelfde kolom;
d. de beide letters zijn *dezelfde.*

ad a. De beide letters worden één voor één vervangen door de letter onmiddellijk *rechts* daarvan gelegen, een letter, welke in een rij in het meest rechtsche vakje ligt, te vervangen door de letter gelegen in het meest linksche vakje uit dezelfde rij.

De klare groep AF wordt aldus CG.
FG „ GA.

ad b. De letters worden één voor één vervangen door de letter onmiddellijk *eronder* gelegen, waarbij een letter, welke in een kolom het meest beneden ligt, wordt vervangen door de bovenste letter uit diezelfde kolom.

De klare groep JZ wordt aldus PW.
JW „ PD.

ad c. Hierbij liggen de letters in de hoekpunten van een rechthoek. De letters worden één voor één vervangen door de letter, welke het andere hoekpunt vormt van denzelfden rechthoek en gelegen is in dezelfde rij.

De klare groep AJ wordt dan DH.
RG „ KC.

ad d. De verdubbeling van een letter wordt vervangen

door de verdubbeling van de letters onmiddellijk *rechts* daarvan gelegen, waarbij een letter, die in een rij in het meest rechtsche vakje ligt, vervangen wordt door de meest links gelegen letter uit diezelfde rij.

De verdubbeling VV wordt vercijferd tot RR.
KK „ VV.

58. Een bij de verdeeling in groepen van 2 letters overblijvende *enkele letter* wordt vervangen door de letter, welke in het cijfervierkant onmiddellijk *rechts* daarvan vermeld staat en indien rechts daarvan zich geen letter meer bevindt, door de letter in het meest linksche vakje uit diezelfde rij.

Nimmer mogen echter andere dan z.g. overblijvende letters op deze wijze, letter voor letter, worden vercijferd.

59. Vóór de overseining wordt de cijfertekst van links naar rechts in groepen van *vijf* letters verdeeld; de slotgroep kan een minder aantal letters tellen.

60. Bij vercijfering van een tekst, waarin naast klare taal ook afkortingen en XAA-codegroepen voorkomen, behoeft, indien geen gevaar voor misvatting bestaat, geen afscheiding te worden aangebracht (met behulp van XAA-groepen voor leesteekens) tusschen afkortingen en XAA-groepen of tusschen deze onderling; in het bevestigend geval daarentegen wel.

Voorbeeld:

Klaar: U marcheert onmiddellijk met 2,3 — I—36 R.I.;
1 — I—36 R.I. per auto.

Te vercijferen codetekst:

U XNO XPO MET XAE XES XAF XEG XBO
RI XET XAD XEG XBO RI PER XGI

61. Met inachtneming van de vercijferingsregelen hiervoren in de punten 57 en 58 gegeven, wordt het cijfervierkant toegepast in zijn meest eenvoudigen vorm. Hierbij

worden de letters van den klaren tekst, van *links naar rechts* gaande afgedeeld in groepen van 2 letters, vervangen door de 2-lettergroepen, welke het cijfervierkant volgens het punt 57 geeft. Een eventueel aan het slot overblijvende enkele letter kan met een willekeurige letter worden aangevuld en daarna vercijferd als 2-lettergroep, dan wel vercijferd als enkele letter volgens punt 58.

Voorbeeld:

te vercijferen: oprukken tot voorste lijn 10 R.I.

gecodeerd in XAA-code (zie punt 50 c.)	:	XRJ TOT XYO XAM RI
ingedeeld in groepen van 2 letters	:	XR JT OT XY OX AM RI
vercijferd	:	RC MP PN BR XR GH CO
over te seinen cijfertekst	:	RCMPP NBRXR GHCO

62. De in het vorige punt voorgeschreven vorm waarborgt het geheim der berichten, *mits* deze kort zijn, steeds gebruik wordt gemaakt van een afkortingscode of van reglementaire afkortingen en veelvuldige wijziging van het sleutelwoord den vijand verhindert veel cijfermateriaal te verzamelen, dat vercijferd is met hetzelfde sleutelwoord.

63. Andere vormen van het cijfervierkant zijn denkbaar; deze zijn in den regel moeilijker te ontsluieren, de vercijfering daarmede eischt daartegenover een weinig meer tijd. Wanneer deze vormen in bijzondere gevallen zullen worden toegepast, wordt zulks door den O.L.Z. bepaald.

64. De regels voor de *ontcijfering* van met behulp van het cijfervierkant vercijferde berichten worden kortheidshalve in dit Voorschrift niet gegeven; zij volgen logisch uit die voor de *vercijfering* gegeven in punt 57 en 58.

Er dient slechts rekening mede te worden gehouden dat

een bericht eerst als ontcijferd kan worden beschouwd, indien het vlot leesbaar is (alle afkortingen juist gepunctueerd en geschreven, alle XAA-groepen vervangen door de klare beteekenis).

D. Vercijfering van den U-Seinlapcode.

65. Voor de vercijfering dezer codegroepen met behulp van het cijfervierkant wordt gebruik gemaakt van de groep XFA (zie punt 47 ad 3).

Het daar veronderstelde bericht: „Wij zijn niet gereed op het vastgestelde uur aan te vallen",
wordt eerst gecodeerd tot: XFA 135; dit vervolgens verder gecodeerd tot: XFA XAP XAH
en bijv. volgens punt 61 van het cijfervierkant met BEVERWIJK als sleutelwoord vercijferd tot: BCCUD NUCI

66. De vercijfering van een codegroep van den U-seinlap zoo, dat het vercijferde sein weder met den U-seinlap kan worden gegeven (met gebruikmaking van een halfronden lap: „Het uitgelegde bericht is vercijferd") geschiedt als volgt:

Instede dat het werkelijk bedoelde codegetal wordt geseind, wordt dat codegetal blootgelegd, dat in de tabel van Bijlage V wat zijn *plaats* betreft zooveel getallen *hooger* ligt boven het werkelijk bedoelde sein, als wordt aangegeven door het rangnummer in het alfabet van den beginletter van het sleutelwoord voor het cijfervierkant, dat aan dien U-seinlappost s verstrekt.

Is BEVERWIJK het geldende sleutelwoord (beginletter B heeft rangnummer), dan seint hij het te vercijferen bericht: „Wij hebben geweerpatronen noodig" (codegetal 247)

[zonder de letter Q]

met het codegetal 245 met een halfronden lap als bijsein, (codegetal 245 ligt in de tabel van Bijlage V twee plaatsen hooger dan codegetal 247).

Bij het doorseinen per radio van een dergelijk bericht moet het worden voorafgegaan door de bijzondere aanwijzing : CY.

E. Vercijfering van Radio-Opdrachten van Artillerie aan Vliegtuigafdeelingen (Vliegtuigen).

67. Indien deze opdrachten niet in voorgeschreven, zeer karakteristieken vorm gesteld behoeven te worden, doch men daarin geheel vrij is, moeten zij, indien noodig, worden vercijferd en wel met behulp van het cijfervierkant.

Naderen deze opdrachten om bepaalde redenen den vorm als aangegeven in Bijlage IV van No. 71a. Voorschrift voor het gebruik van Luchtstrijdkrachten, dan *mag* het cijfervierkant *niet* daarvoor worden gebruikt.

68. Instede daarvan moet uitsluitend worden gebruik gemaakt van z.g. *vercijfering met behulp van een optelgetal.*

Dit optelgetal wordt gevormd met behulp van het voor den afzender geldende sleutelwoord voor het cijfervierkant.

Daartoe wordt het sleutelwoord bijv. BEVERWIJK ontbonden in zijn sleutelletters : B E V R W I J K.

Deze sleutelletters worden naar haar alfabetische volgorde genummerd van 1 tot en met 10 (10 door 0 voor te stellen), te beginnen met A, indien er geen A is de daaropvolgende letter B, anders C, en zoo vervolgens.

Met de sleutelletters B E V R W Y K krijgt men dan het z.g. *sleutelgetal :* 1 2 5 4 6 7 3.

Telt het sleutelwoord meer dan 10 sleutelletters, dan neemt men als sleutelgetal alleen de volgorde der 10 alfabetisch eerste sleutelletters.

Het aldus gevormde sleutelgetal kan men naar behoefte naar rechts verlengen met een 2e sleutelgetal, waarvan de cijfers achtereenvolgens 1 grooter zijn dan de overeenkomstige cijfers van het eerste sleutelgetal, dit 2e getal evenzoo verlengen met een 3e sleutelgetal waarin de cijfers weder 1 grooter zijn dan het 2e, enz. (met dien verstande dat wanneer de uitkomst 10 zou zijn, daarvoor wordt geschreven 0).

Men krijgt op die wijze het *optelgetal*, zijnde:

1254673 2365784 3476895 4587906 5698017 6709128 enz.

69. Dit optelgetal wordt cijfer voor cijfer van links naar rechts geschreven onder *alle* cijfers van de opdracht.

Voorbeeld: (Opdracht II uit bijlage I VV.Luchtstr. kr. '25)

Klaar: —.—.— BCD, VT 26 — 73, 80 — 20 WG, AA,

Optelgetal: 12 54 67 32

Vercijferd: —.—.—CY BCD VT 38 — 27, 47 — 52 WG, PETRUS §,

Klaar: VT 25 — 68, MK 4 brug 70 — 10, 9 uur 30 —

Optelgetal: 36 57 8 43 47 6 89

Vercijferd: VT 51 — 15, MK 2 VOGEL § 13 — 57, 5 uur 19 —

Klaar: 10 uur 15 .—.—.

Optelgetal: 54 58

Vercijferd: 64 uur 63 .—.—.

Men telt nl. van links naar rechts gaande klaar cijfer en optelcijfer bij elkander op, verwaarloost bij die optelling het cijfer der tientallen en schrijft alleen het getal der eenheden als optelsom (vercijferde tekst) op. Indien men

§ Noot. Aangenomen is dat doelen, merkpunten, enz. kunnen worden aangeduid met schuilnamen.

beschikt over schuilnamen voor soorten van doelen, merkpunten, uurindeeling, enz., dan wordt hiervan gebruik gemaakt; anders laat men die afkortingen (woorden) onvercijferd.

Om aan te geven dat het bericht vercijferd is, wordt aan het begin daarvan de afkorting CY = Vercijferd gevoegd.

70. Bij het *ontcijferen* wordt het optelgetal uiteraard afgetrokken, daartoe evenzoo cijfer voor cijfer van links naar rechts geschreven onder de cijfers van het vercijferde bericht.

Hierbij wordt de bewerking ook beschouwd als een serie van afzonderlijke aftreksommen, waarbij rekening is te houden met het niet vermelden van het cijfer der tientallen.

F. Geheime berichten, waarbij niet of slecht gebruik kan worden gemaakt van den Morse-Code.

71. Behalve met den U-seinlap kunnen deze berichten worden gegeven met behulp van vuurwerkseinen, grondlappen, spiegels, enz. en met geluidseinen.

Gebonden als deze seinmiddelen zijn aan het geringe aantal variaties der daarmede te geven seinen, bovendien nog beïnvloed door atmosferische en plaatselijke toestanden (nevel, gebrek aan een bepaalde soort vuurwerkseinmiddelen, enz.) kunnen deze seinen slechts worden bestemd voor de meest belangrijke en dringende mededeelingen en is het vooral bij de vuurwerkseinen verboden eens voor al de seinen vast te stellen.

Welke beteekenis aan bepaalde vuurwerkseinen zal worden gehecht, wordt geregeld door de autoriteiten vermeld in punt 54.

72. Bij de vaststelling van een code voor vuurwerkseinen moeten de meest zichtbare en meest karakteristieke seinen worden bestemd voor de meest belangrijke berichten. Seinen die onderling kunnen worden verwisseld, moeten worden bestemd voor berichten, waarbij verwisseling geen ernstige gevolgen kan veroorzaken.

Het verschil in beteekenis bij vuurwerkseinen met seinpotten baseere men meer op het verschil in vorm dan op dat in kleur.

De verschillende kleuren kan men gebruiken om de seinen als eigen seinen te herkennen.

73. Tot de geheime vuurwerkseinen moeten ook worden gerekend het *attentiesein*, het *contrasein* en de *verkenningsseinen*, te wisselen tusschen marinevaartuigen, vliegtuigen en den wal onderling; deze worden vastgesteld door den Minister van Marine.

ARCSI - Association des Réservistes du Chiffre et de la Sécurité de l'Information
Association régie par la loi de 1901 - N° SIRET : 511 069 569 00016
Tous droits de propriété intellectuelle réservés à l'ARCSI, association loi 1901, selon les règles du droit français