

De grote drie in de vroeg twintigste-eeuwse Nederlandse crypto

Radboud University Nijmegen
NISA/iHub Symposium, 15 sept. 2023

Bart Jacobs
bart@cs.ru.nl



De grote drie

Welke drie?



Henry Koot
1883 – 1959
denker



Jacobus Verkuyl
1890 – 1967
doener



Johannes Nuboer
1901 – 1984
strateeg

Deze voordracht bevat een overzicht van bekende wetenswaardigheden over deze drie cryptologen, met een enkele nieuwigheidje.



Outline

Henri Koot

Jacobus Andries Verkuyl

Johannes Frans Willem Nuboer

Ten slotte



Iets over cryptologie / geheimschrijving

- ▶ Cryptologie bestaat uit twee onderdelen:
 - defensief: **cryptografie**: ontwerp van versleutelingsmethoden
 - offensief: **cryptoanalyse**: breken van versleutelingIn de praktijk is "crypto" een korte aanduiding voor allebei
- ▶ Eeuwenlang vooral gebruikt door diplomaten en militairen
 - ontsleutelingspogingen in "geheime kamers"
 - in 20ste eeuw grotendeels ondergebracht bij geheime diensten
 - vanaf jaren 1970 academisch onderwerp, nu leidend
- ▶ Ontwikkeling van gebruikte technieken:
 - (1) handcijfers, vaak combinatie van substitutie en transpositie
 - (2) mechanische cijfers, via rotors
 - (3) digitale cijfers, onkraakbaar, tenzij foutief gebruikt
- ▶ Crypto is meermaals historisch doorslaggevend geweest
 - Zimmermann telegram, Enigma, Purple (Midway, Yamamoto)
 - toegang tot informatie bepaalt machtsverhoudingen



Rol van NL op crypto gebied (in 20ste eeuw)

- ▶ Rotormachine is NL-uitvinding (1915, Spengler, Van Hengel)
 - uitnutting door anderen: Enigma, Hagelin, Sigaba, Typex, Fialka, ...
- ▶ NL las Duitse, Engelse en Franse codeberichten in WWI
 - belangrijk voor handhaving neutraliteit
- ▶ NL las Japanse geheime berichten in jaren 30
- ▶ NL las Indonesisch versleuteld verkeer
 - bijv. tijdens onderhandeling over onafhankelijkheid
 - bij verdediging van NL-Nieuw-Guinea (slag bij Vlakke Hoek, 1962)
- ▶ Strategie om cryptologisch autonoom (of relevant) te zijn na WWII
 - defensief: CCB / NBV, nu onderdeel van AIVD
 - offensief: WKC / TIVC, eerst bij Marine, nu JSCU bij AIVD/MIVD
- ▶ NL had/heeft eigen crypto industrie (maar met beperkte markt)
 - Philips USFA, Fox, Compumatica, Pijenburg, ...
- ▶ Academisch actief op crypto & computer security gebied



Koot bio

- ▶ Geboren in 1883 in Singaradja (Bali), met NL vader, Chinese moeder
- ▶ Volgt HBS, dient in KNIL-infanterie, doet gevechtservaring op, komt naar NL voor officiers opleiding aan KMA
- ▶ Kan niet terug naar Indië vanwege WWI, werkt bij geheime dienst: GS IV, later GS IIIc
- ▶ Verdiept zich als autodidact in cryptoanalyse, breekt eigenstandig Duitse, Franse, Engelse codes
- ▶ Leidt aan HKS tientallen cryptologen op, incl. Verkuyll & Nuboer
 - is **directeur van het cijfer** bij BuZa, ontwerpt nieuwe codes
 - is ook lector Maleis aan Univ. Utrecht
- ▶ Wordt Commandant Binnenlandse Strijdkrachten aan eind WWII
 - aanwezig bij capitulatie, als Gen.-Maj. tegenover Reichelt
- ▶ Erefuncties na WWII, introduceert Greet Hofmann aan het hof
 - overlijdt in 1959; kazerne in Stroe naar hem genoemd
 - crypto bijdragen blijven onvermeld in overlijdensadvertenties



Where we are, so far

Henri Koot

Jacobus Andries Verkuyll

Johannes Frans Willem Nuboer

Ten slotte



Koot herinneringen



Algemeen Handelsblad,
21 januari 1959



Kazerne omgedoopt door
Prins Bernard, 21 april 1978



Historici over Koot — hij schreef zelf niks

- ▶ G.J. van Ojen Jr. *Leven en Werken van Henri Koot*, 1978
 - informatief, zonder kritische afstand, haast idolaat
 - mede-gebaseerd op gesprekken met echtgenote & leerlingen
- ▶ K. de Leeuw, *Koot, Henri (1883-1959)*, in: Biografisch Woordenboek van Nederland 5, 2002. (online bij [Huygens Instituut](#))
 - korte, feitelijke beschrijving van Koot's leven en werk, inclusief crypto
- ▶ Koot wordt kort genoemd door Engelen / de Graaff / Klinkert
- ▶ David Kahn, *The Code Breakers: The Story of Secret Writing*, 1966
 - schrijft niet over Koot, wel over Verkuyl (& Petersen)
- ▶ NSA Daily – History Today – 24 Aug. 2011 (vrijgegeven in 2015)
 - The Netherlands had its counterpart to Herbert Yardley ...
 - ... in Henri Koot, the “godfather” of Dutch military cryptology ...
 - ... one of the greats in cryptology, albeit little known outside of his homeland.



De Meijer / Van Woelderen over Koot

Van Woelderen (rechts op foto) leidde GS III met Fabius (links), gedurende WWI, hield dagboek bij, waaruit uitgebreid geciteerd wordt in De Meijer's *Geheime Dienst in Nederland, 1912 – 1947*



- ▶ DM, p.25: Onder leiding van kapitein H. Koot werden zowel de Engelse als de Duitse code voor de telegrammen-wisseling ontcijferd. Ook een later door de Duitsers in gebruik genomen code, de 'Waco-code', werd gebroken.
- ▶ DM, p.25: Op de plaatsing bij GS III en het behoud van de “onvolprezen” en “geniale” Koot werd door GS III zeer veel prijs gesteld.



De Meijer / Van Woelderen over Koot, vervolg

- ▶ VW, 8/2/1918: Onze eigen installatie voor radio-telegrafie vangt tegenwoordig de draadloze telegrammen op, die op bepaalde uren van de Duitse duikboten worden verzonden, wij zullen nu wel spoedig de geheime code ontcijferen door de handigheid van den genialen Koot.
- ▶ VW, 8/6/1918 Door het oplossen van den Engelschen code ontvangen wij thans ook van die zijde hoogst belangrijke gegevens.
- ▶ VW, 28/4/1919 De Duitse “Waco”-code is gevallen, waaruit wij nauwkeurig de machinaties lezen van de Amerikanen, die de Duitschers aanzetten, om de vredesvoorstellen niet aan te nemen.
- ▶ VW, 4/7/1919: De positie van kapitein Koot moet dringend worden vastgesteld, anders dreigt het gevaar dat deze allereerste kracht in het ontcijferen van codes toch nog door vertrek naar Indië voor GS III verloren gaat.

(Over de genoemde Duitse Waco code ontbreekt informatie.)



Koot, als “geniale leermeester”, volgens leerlingen

- ▶ de Vos van Steenwijk: “... dat het Koot was, die ons land in 1917 van een Duitse oorlogsverklaring heeft gered, door een gecodeerd telefonisch gesprek (??) tussen Duitsland en Den Haag te ontcijferen. Het betrof de z.g. zand en grintkwestie” (geciteerd in Van Oyen, p.35)
- ▶ Van der Schrieck: “Generaal Koot had een fantastisch brein, dat zo snel en diep dacht dat weinig mensen hem konden volgen. Zijn lievelingsonderwerp en werk was cryptografie. Volgens mij was hij een van de meest vooraanstaande crypto-analysten ter wereld.”
- ▶ Van der Schrieck citeert ook Amerikaanse collega: “If you give Koot a telegram in a code unknown to him, he just sniffs it and tells you what's in it.”



Where we are, so far

Henri Koot

Jacobus Andries Verkuyl

Johannes Frans Willem Nuboer

Ten slotte



William Friedman over Verkuyl

Bron: Recommendations for **Legion of Merit and Medal for Merit Awards**, 27 sept. 1943.

*The next most valuable source of intelligence was the Japanese transposed code system known as "J-18" and "J-19". Its solution represented a high cryptanalytic achievement, for initially the system appeared to be impregnable. [...] For continuity in cryptographic operations, credit belongs to the group under the direction of **Colonel J.A. Verkuyl**, including Mr. Eugene Waltz, Mr. William O. Bryan, Mr. Joseph S. Petersen, Jr., Mr. (now Sgt.) George Hurley, Miss Isabel M. Murdock, and Miss Elisabeth Stevens.*



Verkuyl bio

- ▶ Geboren in 1890, te Amsterdam, KMA in 1909, vanaf 1914 in Indië
- ▶ Cursus cryptografie op HKS in 1927 bij Koot, die hem noemde: nauwkeurig, vasthoudend, maar zonder veel cryptografische aanleg 😊
- ▶ Hoofd "zwarte" **Kamer 14** in Bandoeng
 - kraakte Japanse diplomatieke code, samen met **Van der Beek**
 - later actief met **Henning** — die Duitse diplomatieke code in Azië kraakte, via klare tekst opgeprikt in Duitse club
- ▶ VS Gen. Brett wil in 1942 crypto-samenwerking met NL; Verkuyl naar **Arlington Hall** (Washington), waar oa. Purple gekraakt wordt
 - werkt onder **Friedman**, samen met **Petersen**
 - leert daar zwakte van Hagelins, gebruikt door NL
- ▶ In 1946 eerste hoofd van CCB (niet Koot) en ook van Marid VI
 - crypto successen tegen Indon. opstandelingen / diplomatie
 - aanzet tot reorganisatie CCB in 1953, wordt NBV in 1960
 - in 1951 bij Marid opgevolgd door Spanjaard
- ▶ Laatste (actieve) jaren zijn mysterieus / onopgehelderd



David Kahn over Verkuyl, en Petersen, in 1967

- ▶ Liason officer Verkuyl had een buro naast Petersen op **Arlington Hall**
 - ze werkten allebei aan Japanse codes — van 3/1942 tot 12/1943
 - "a field in which Verkuyl had considerable prewar experience"
 - "one of Holland's finest cryptanalysts"
- ▶ Ook betrokken: **Giacomo Stuyt**, verbindingsofficier op NL ambassade
 - NL gebruikte Hagelin, Verkuyl wist dat VS die gebroken hadden
 - na vertrek Verkuyl bleven Petersen & Stuyt in contact
 - in 1948 gaf Petersen geheim materiaal aan Stuyt, o.a. over Hagelin, dat gecopieerd werd op ambassade
- ▶ Kahn: "Verkuyl thinks that Petersen was motivated . . . to help secure the communications of his friends from other nations prying"
- ▶ Petersen gepakt en veroordeeld, in een geheim proces, onder druk gezet om te bekennen; heeft uiteindelijk 4 jaar gezeten

Zie ook: **Cees Wiebes**, *Operation Piet*, 2008 — met NL-nietjes anecdote



Verkuyl & Kahn, voor American Hotel, A'dam'62



(Foto op website US National Cryptologic Museum)

Kahn's aantekeningen, van gesprek met Verkuyl

Bron: US Nat. Cryptologic Museum, met dank aan Florentijn van Kampen

Verkuyl, J.A.
inf. ofcr. b. Amsterdam, 4 July 1890. 19 May 1962
Amsterdam
The word 'beer' = beer, was word
that helped solve (A code for Dutch
in NEI, somebody thought
a certain codegroup might be stand
for beer, which ^{Jacks} imported a great deal
because it is not a climate.



Kahn's aantekeningen, van gesprek met Verkuyl, vervolg

Dutch staff too small to solve purple.
Bandung was where ^V purely crypto
staff worked - after '33 - w Vander
Beck, 2 other boys & ² girls
to type it out. V got ^{in Holland} from
General H. Koot, an ofcr of Colonial
Army who a student in war college in
Holland in 1914. Students were made
censors when war broke out. Couldn't

"Dutch staff too small to solve Purple ..."

Einde

Volstrekt enige kennisgeving.
Tot onze grote droefheid overleed heden, in de
leeftijd van 76 jaar, mijn beste, zeer zorgzame
Man, onze Broer, Zwager, Oom en Oudoom
JACOBUS ANDRIES VERKUYL
Kolonel K.N.I.L. b.d.
Officier in de Orde van Oranje-Nassau.
Uit aller naam:
L. S. Ch. Verkuyl—Jonker
Amsterdam, 11 april 1967.
Weteringschans 131.
Thuis liever geen bezoek.
Geen toespraken.
Voor hen die afscheid willen nemen, bestaat
daartoe gelegenheid donderdagmiddag van 2—3
uur in de rouwkamer „Sax” (P. C. Hooftstraat
38—40). De crematie zal plaatshebben vrijdag
14 april op „Westerveld”, na aankomst van de
trein te 15.29 uur halte Driehuis-Westerveld

Telegraaf, 13 april 1967



Where we are, so far

Henri Koot

Jacobus Andries Verkuyf

Johannes Frans Willem Nuboer

Ten slotte

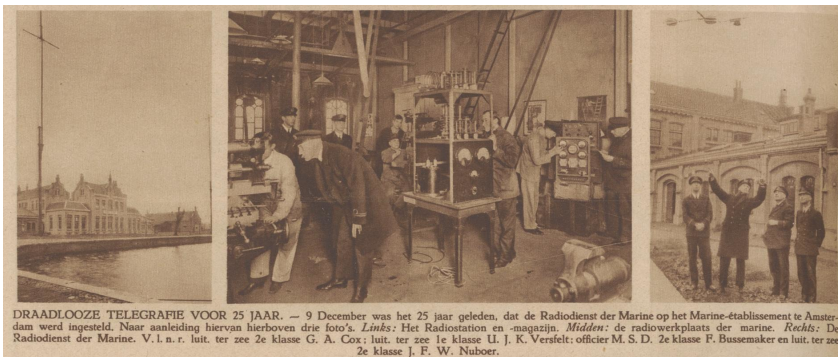


Nuboer bio

- ▶ Geboren in 1901 in NL-Indië, opgeleid tot marine-officier aan KIM
 - ingedeeld bij verbindingen, i.h.b. radiodienst
 - ontwierp kortegolf communicatie voor kruisers & onderzeeërs
 - volgde internationale ontwikkelingen, schreef strategische visies
- ▶ Deed privé cursus cryptografie bij Koot in 1930
 - nauwkeurig, werklustig, intelligent
 - schreef dictaat van cursus & opgaven — in NIMH archief
 - introduceerde Enigma chiffreremachines bij de Marine
- ▶ Organiseerde Marine-inlichtingen in Batavia, als 'Afdeling I'
 - brak ±1935 met Schalkwijk "punt-code" van Japanse marine
 - relevant (crypto) materiaal bij NIMH, uitgewerkt door Rijneveld
- ▶ Vertrok op 14 mei 1940 naar Engeland met Marinestaf
 - werd strategisch adviseur van MvO Furstner & MP Gerbrandy
- ▶ (Leeftijds)ontslag in 1953, overlijden in 1984
 - heeft zelf veel gepubliceerd, ook over cryptoanalytisch werk.



Marine Radiodienst jubileert: 25-jarig bestaan in 1929



Arnhemsche Courant, 14 dec. 1929
(en ook in andere kranten)



Leden radiodienst uitgelicht, met Nuboer rechts



Fittie Nuboer – De Jager

- ▶ Nuboer publiceert *De verdediging van Nederlandsch Indië een maritiem vraagstuk*, Marineblad, aug. 1939
 - pleidooi voor investering in schepen, niet in vliegtuigen
- ▶ Oud-vice-admiraal **De Jager** was een andere mening toegedaan.
 - Nuboer: "Slechts één enkele schrijver, zoals met name Mr. J.C. de Jager, *gelukkig reeds lang gepensioneerd*, blijft de oude misvatting propageeren." (p. 902)
- ▶ Op 22 dec. 1939 spreekt Nuboer bij de Marinevereniging over "Versterking der vloot met kapitale schepen"
 - debat met de Jager wordt aangekondigd, maar die blijft weg
- ▶ De oude-vice-admiraal is *not amused*
 - hij verdedigt zijn debat weigering in het openbaar, en spreekt van "vlegelachtigheid" van Nuboer
 - de pers smult er van (in dec. 1939).

Na de oorlog bij de NAVO, op TV, in de krant



De Telegraaf, 1 aug. 1953

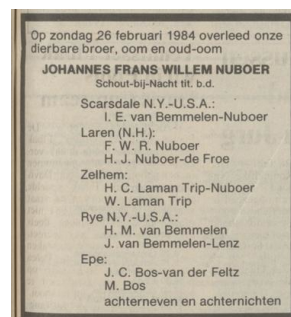
Uitgebreid opinie artikel
in Het Vaderland, 26/11/59
"West-Europese defensie staat
of valt met de Navo-zeemacht"



De Telegraaf, 9 sept. 1958
"rustig redenerend"



Einde, NRC 28 feb. 1984



Where we are, so far

Henri Koot

Jacobus Andries Verkuyll

Johannes Frans Willem Nuboer

Ten slotte



Eindwoord

- ▶ Historische status van “de grote drie” van eerste helft 20e eeuw:
 - over **Koot** is redelijk wat bekend, maar helaas niet over zijn belangrijke cryptoanalytische werk in WWI
 - **Verkuyl** is de meest mysterieuze, over wie nog weinig gevonden / uitgezocht / gepubliceerd is
 - over **Nuboer** is ook veel bekend (beschikbaar), door zijn eigen publicaties en gearchiveerde nalatenschap
- ▶ Ze verdienen een serieuze biografie, individueel of gezamenlijk
 - institutionalisering van cryptologie / verbindingsinlichtingen
 - belang voor (lang) handhaven NL-neutraliteit
 - generatie van hoog-opgeleide, intellectuele officieren
- ▶ Intrigerende vraag:
 - wie zijn de grote crypto-drie in de **tweede helft** van de 20e eeuw?



Opmerkingen / toevoegingen / vragen?

