



OPERATIONEEL

# CRYPTO

Paars, veilig en in beweging



Majoor J.A.C. (Jochem) Kooistra,  
COMMIT/JIVC/ITCC/OSEUD/  
Hoofd Bureau Crypto

▶TR/010N ▶TR/01▶03  
▶TR/010N ▶TR/01▶03

▶RS/0211 SEARCH... A01  
▶RS/0211 SEARCH... A01



▶SEARCH▶TR/01▶03  
▶SEARCH▶TR/01▶03

Crypto. Iedereen weet ervan. Niet iedereen weet er het fijne van. Dit artikel geeft een impressie van de geschiedenis van het huidige bureau Crypto door de ogen van Majoor Kooistra, overdragend Hoofd. →



## OPERATIONEEL

Crypto is een randvoorwaarde om ons werk veilig te kunnen doen. Ons vakgebied kenmerkt zich door in opdracht van commandanten de eenheden snel en veilig te voorzien van voldoende informatie om de juiste besluiten te kunnen nemen. Daarnaast dient die informatie afgeschermd te worden onze vijanden om voordeel te creëren dan wel te behouden. Beveiliging is daarbij essentieel. Niet alleen hoe wij als collega's met de informatie omgaan die ons in vertrouwen wordt toevertrouwd, maar ook het beveiligen van onze hoog gerubriceerde netwerken en (radio) systemen.



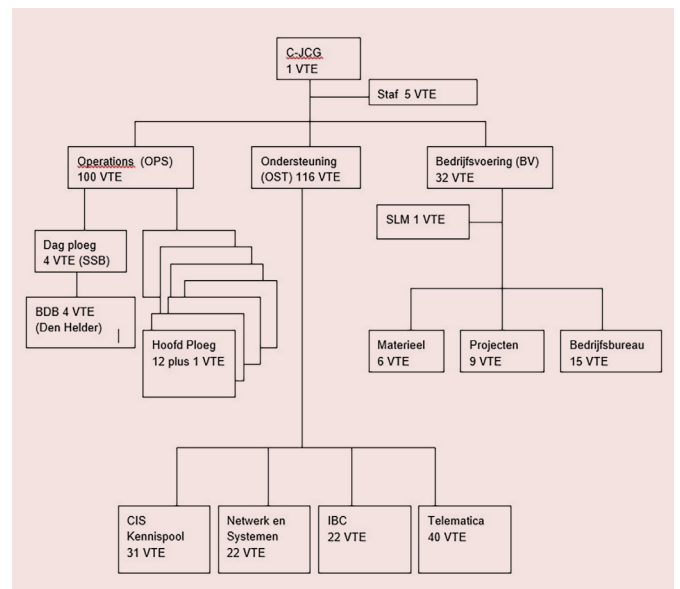
Camp New Amsterdam, Gebouw A118

Tot aan ongeveer 2005 had elk Operationaal Commando (OPCO) dit nog in eigen beheer. De krijgsmacht was nog vele malen groter dan nu en er was ruim voldoende werk binnen elk OPCO om de eigen algehele crypto beheer en distributie te rechtvaardigen. In die tijd was het zeker nog het geval dat elk OPCO haar eigen (radio) systemen had en elk OPCO dus zijn eigen crypto. In de beginjaren van deze eeuw kwam er langzaam een kentering. Netwerken waren niet meer OPCO specifiek (bv TITAAN) en ook andere behoeften aan hoog gerubriceerde informatie werd binnen verschillende OPCO's identiek benaderd (NSWAN, BICES etc.).

In deze tijd speelden reorganisaties en krimp ook nog eens mee en er werd in de zomer van 2005 een Concept Voorlopig Realisatieplan (CVRP) geschreven, waarbij er 4 CIS organisatiedelen van defensie werden omgevormd naar 1 Joint CIS Groep (het JCG). Ook de verschillende cryptodistributie organen maakten hier deel van uit. Als locatie voor het JCG werd Gebouw A118 op Camp New Amsterdam gekozen. Een gebouw, met een grote kluis. In de tijd van de Amerikanen, was dat de opslaglocatie van de dollars waarmee de troepen werden betaald. Deze was geschikt om alle cryptostroken, codeboeken, naslagwerken etc. op te slaan en te behouden. Centraal in het land, om van daaruit ook de fysieke distributie te kunnen uitvoeren naar alle defensielocaties in binnen- en buitenland.

Deze reorganisatie / oprichting JCG (met als doel krimp en *efficiency*), leverde een reductie van zo'n 30 functies op met inbegrip van functies in het vakgebied crypto. Het grootste voordeel was de afname van vervoersbewegingen. Heel veel informatie is er niet terug te vinden over de precieze invulling van de crypto-functies. Wel vielen deze allemaal onder de tak Ondersteuning (OST) in de afdeling Informatie Beveiligingscluster (IBC). Deze afdeling (inclusief management) kwam toen neer op 22 VTE. Onderdeel hiervan was een Bureau Crypto Distributie (BCD) van negen functies.

Voor de cryptodistributie (CD) was dit prima, echter in de loop der jaren werd het beheer en de zero-tolerance steeds belangrijker. We moesten in control komen van het totale (CCI en crypto) beheer en deze met audits kunnen controleren. Zo rond 2010 is de eerste Medewerker Audit aangesteld en uiteindelijk werd in 2015 het Crypto Sleutels en Publicaties Monitor team (CSPM) operationeel. Hiermee werd elk zelfstandige crypto-organisatie jaarlijks aan een audit onderworpen om zo het beheer bij de operationele eenheden te controleren. Uiteindelijk resulteerde deze wijziging in een zelfstandig Bureau Crypto, met een BCD verantwoordelijk voor het beheer van de landsvoorraad cryptosleutels defensie en het verstrekingspunt richting alle OPCO'S en een Bureau Crypto Audit (BCA, die namens DOPS J6 (in de rol van Chef Verbindingsdienst Defensie (CVBD)) en de Beveiligingsautoriteit (BA) deze audits ging afnemen. Dit in samenwerking



Organisatie JCG 2005

met de Audit Dienst Rijk (ADR) omdat nu eenmaal niet alle organisatieonderdelen door BCA konden worden ge-audit (bijvoorbeeld het Bureau Crypto zelf).

De huidige organisatie bevat 19 functies: 6 landmacht, 5 marine, 4 luchtmacht en 3 burgerfuncties. Dit was ook de samenstelling (op papier) zoals ik die aantrof bij het begin van mijn functievervulling in 2021. De Defensieorganisatie was nog steeds niet toe aan groei en er werd nog steeds gezocht naar mogelijkheden tot bezuinigingen.

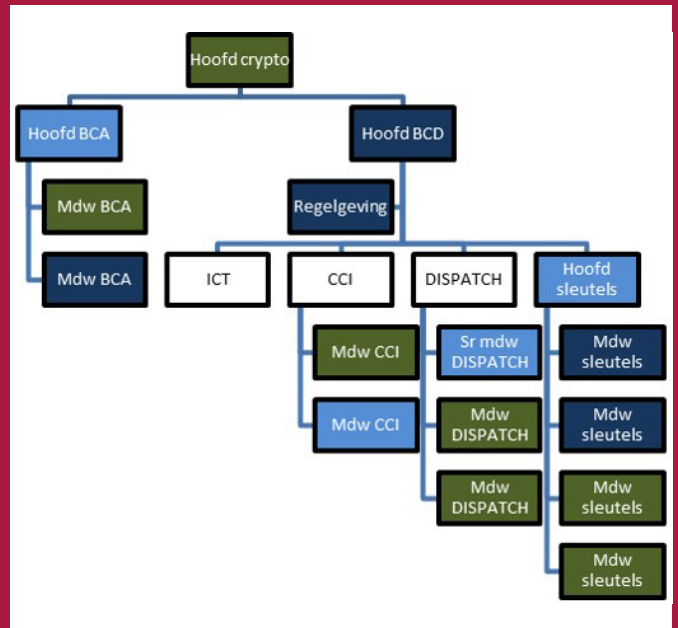
Reeds in 2018 had men al wel geconstateerd, dat de cryptoketen binnen het JIVC als los zand aan elkaar zat. Er was geen synergie en de samenwerking en afstemming was daardoor niet optimaal. Tevens waren er te weinig functies om daadwerkelijk alles op crypto gebied te kunnen volgen en gericht te zijn op de toekomst. In 2018 is er toen een Nota beschreven, waar er gesproken werd over een twintigtal extra benodigde functies om dit te verhelpen. Iedereen was het erover eens, dit moest gebeuren. Een expertisecentrum bij het al bestaande Bureau Crypto om kennis en ervaring te borgen, mee te denken in projecten en defensiebreed te kijken naar opleidingen en NATO-standaarden. Daarnaast een nieuw op te richten bureau met ontwikkelaars, (technische) beheerders, systeemmanagers e.d. om intern het specialisme crypto te borgen en er ook gedegen naar te handelen en specifieke systemen te kunnen beheren.

Echter: Geen geld, jarenlang geen geld. Zodra er ergens geruchten waren dat er extra geld zou kunnen komen richting defensie, werd de Nota weer afgestoft. Om vervolgens weer ergens op een stapel te belanden.

En dan ineens voelt Europa de noodzaak weer te moeten investeren in defensie. Het is onrustig aan de oostkant van de grenzen en we moeten ons weer richten op een grote boze vijand. Zo vlak aan de vooravond

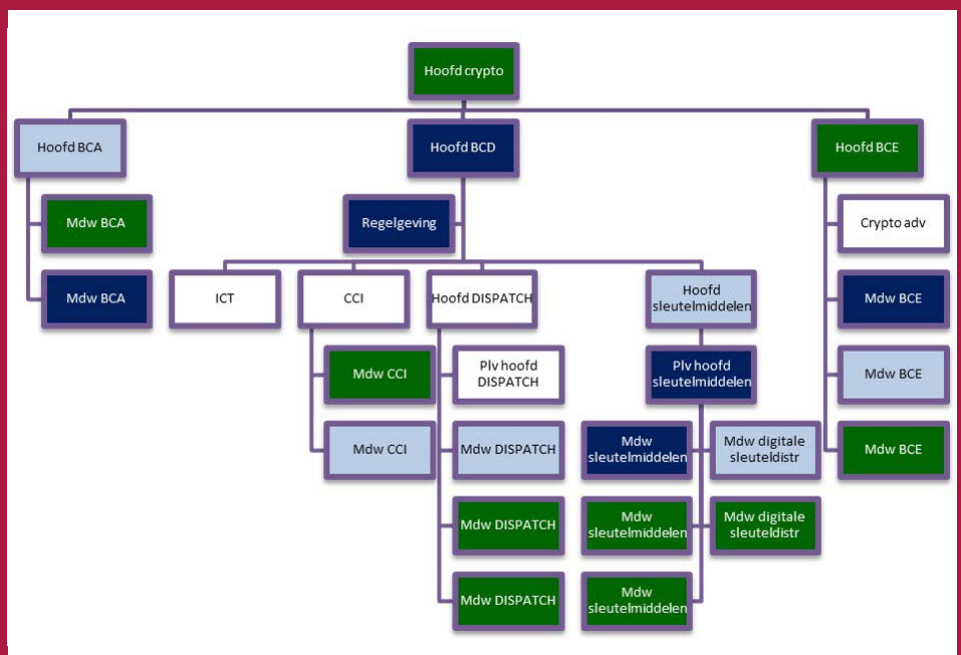
van reorganisatie 2b van het JIVC komt er geld beschikbaar. In Den Haag is politica Sophie Hermans dermate doortastend, dat er in de al lopende reorganisatie onder andere geld beschikbaar komt voor de Nota uit 2018. Met spoed worden er functies gezocht die toch in de reorganisatie "functie neutraal" deze 20 functies kunnen compenseren. Dat lukt en sinds mei 2024 ziet de afdeling crypto er als volgt uit:

Wie goed kijkt, valt op dat er onder de afdeling sleutelmiddelen nog eens 2 functies zijn gekomen. Tijdens het schrijven van dit artikel wordt de laatste hand gelegd aan het formaliseren van deze functies.



Organisatie JCG 2015

Wie ooit dacht dat de digitalisering van de sleuteldistributie (EKMS, *electronic key management system*) meer capaciteit zou vragen dan er nu in huis is. Met het huidige CD-noods-cenario zijn er afspraken gemaakt om het een "insider" lastig te maken hier misbruik van te maken. Als je digitaal sleutels gaat distribueren, zullen in dat proces taken en verantwoordelijkheden gescheiden moeten worden en door verschillende personen moeten worden uitgevoerd. Dit is veiligheid technisch gewoon een harde eis. Daarbij komt ook nog eens, dat elk zichzelf respecterend systeem tegenwoordig zijn eigen crypto genereert met een eigen key managementsysteem met de daarbij behorende taken en verantwoordelijkheden.



Organisatie JCG 2024



Locatie Eemnes

De afdeling Bureau Crypto Expertise (BCE) adviseert in cryptogerelateerde projecten om nieuwe crypto (en CCI) tijdig en met de juiste procedures binnen defensie te krijgen. Voorheen gebeurde het met enige regelmaat dat er een nieuw systeem gekocht en wel al op de plank lag en dan pas de afdeling crypto het verzoek kreeg de crypto te leveren. Nieuwe systemen, andere bedrijven, buitenlandse producten, allemaal zaken die een aanvraag van de juiste crypto in een vroegtijdig stadium verlangen. Reden hiervoor is, dat defensie zelf geen ontwikkel capaciteit heeft. NATO of *US crypto* krijgen we alleen na toestemming van de *Controlling Authority* en als we dan ook nog eens nationaal crypto willen, dan zal de Nationale Distributie Autoriteit (NDA) toch echt meer informatie (systeemconfiguraties) moeten hebben om de crypto te kunnen maken. Dáár zit wel ontwikkelcapaciteit en verder is de NDA voor bureau crypto de leverancier van alle crypto aan defensie.

Daarnaast wordt er eindelijk gewerkt aan een basis crypto/infosec opleiding die voor elk OPCO gaat gelden. Alle OPCO's schrijven ook mee en aan dit lopend traject. Met de komst van het EKMS kunnen gelijk veranderingen worden meegenomen die dan van toepassing gaan zijn, vanwege de veranderingen in cryptodistributie en beheer na invoering van het EKMS. Ook de manier van auditen gaat veranderen. Verder zit men vanuit het BCE in meerdere overleggen gericht op de toekomst van crypto. Zaken m.b.t. quantum, NATO, GriT, Foxtrot, Tactische Data Linken, etc. zijn allemaal onderwerpen, waar dit expertisecentrum in duikt en beziet welke consequenties dit heeft op beheer, op cryptografie en dus ook op de bezetting van de gehele afdeling.

Bovenop de uitdagingen m.b.t. ARBO-richtlijnen is ondertussen Gebouw A118 op Camp New Amsterdam te klein geworden. Echter, verandering van infra is nog steeds een lastig en tijdrovend verhaal binnen defensie. Te weinig geld om de huidige groei van defensie te kunnen volgen en te voorzien van de daadwerkelijk benodigde infra. Vrij snel na mijn start zijn wij een Opgave Tekortkoming Vastgoed (OTV)- proces

begonnen. Op Camp New Amsterdam zijn er te weinig kantoorruimtes, te weinig beveiligde ruimtes, geen ruimte voor kasten (PGU van militair personeel), geen eigen douchegelegenheid (elk gebouw heeft naast de wacht aan de poort nog een eigen toegang tot hun eigen gebouw, incl. wachtpersoneel, cardreaders en andere procedurele zaken om erbinnen te kunnen komen) etc. In deze OTV is er een opgave gedaan wat de totale behoefte aan infra (vastgoed) is om de huidige werkzaamheden goed en veilig uit te voeren en daarbij ook verdere groeimogelijkheden te hebben voor de toekomst.

Momenteel werkt een deel van de afdeling al op locatie Eemnes en liggen er plannen om uiteindelijk met de hele afdeling daarnaartoe te gaan verhuizen. Daarnaast worden er op meerder vlakken haalbaarheidsonderzoeken doorlopen om dit mogelijk te maken. Te denken valt aan onder andere het realiseren van een 24/7 wacht, wat daar nu nog niet is, capaciteiten om met zowel MULAN als hoog gerubriceerde netwerken daar te kunnen werken, verwarmen/verkoelen van de kantoren etc.

**“Er is geld,  
we hebben prioriteit,  
nu doorpakken.”**



Sinds de zomer van 2023 is er op verzoek van de BA en de DOPS J6 (In de rol als CVBD) gekeken hoe we als defensie willen omgaan met militaire crypto buiten ons bedrijf. Hoe moet je dit zien? Andere ministeries (en Nederlandse attachés in het buitenland) maken gebruik van gerubriceerde netwerken met onze crypto. Vaak beheerd door de crypto organisatie van de bestuursstaf. Echter is dat niet het enige.



*Bureau Crypto is een paars team*

Ondertussen zijn vele bedrijven steeds meer verweven met onze organisatie en van daaruit ontstaan daar behoeften om ook op gerubriceerd niveau met ons informatie te kunnen delen. Nu kun je die bedrijven hun eigen crypto organisatie gaan geven en deze jaarlijks ook auditen en daarmee grip houden op wat er buiten defensie mee gebeurt. Dat betekent dan wel, cursussen geven aan mensen buiten defensie, inzichten delen met deze bedrijven en meer werk voor bureau audit en versnippering van het totaaloverzicht.

Als plan ligt er nu wederom een ophoging van de afdeling crypto met een nieuw bureau van 4 man (2 burgers en 2 militairen) die alle externe crypto gaan beheren. Defensie gaat zelf het beheer over het CCI en de sleutels voeren vanuit een vast bureau behorend aan de afdeling crypto. Dit Bureau Crypto eXtern (BCX, de E was al vergeven aan Bureau Crypto Expertise) gaat erbij komen.

Wat de toekomst verder nog gaat brengen is niet helemaal duidelijk. Wat wel duidelijk is, is dat de cryptowereld verandert en dat defensie daarin mee moet. Momenteel zien we ook een groei in het aantal key managementsystemen. Vrijwel elk apart (communicatie) systeem voorziet straks in haar eigen sleutel distributie. Deze staan los van het eerdergenoemde EKMS, maar gaan wel komen en staan fysiek in principe bij Bureau Crypto. Voor ons *Long Range Communication* Systeem (LRC) doen we nu de eerste ervaringen op met hun *Key Management Systeem* (KMS). Het Verbeterd Operationeel Soldaat Systeem (VOSS) heeft ook een eigen KMS en ook die komt binnenkort ook bij ons te staan. In een strategisch partnerschap met FOX crypto wordt er gewerkt aan de opvolger van de huidige TCE, ook met een eigen KMS, inderdaad straks ook geplaatst bij Bureau Crypto.

Komende augustus, na 3,5 jaar deze functie te hebben mogen draaien, ga ik hier weg. Ik heb BCE mogen opstarten en mogen zien dat er al heel veel gebruik van wordt gemaakt. We moeten zelfs een beetje op de rem trappen om niet te vergeten dat ze net nieuw zijn en er geen tijd meer is om zelf ook de paden nog goed weg te zetten om die te borgen voor



*Nieuwe auto's*

de toekomst. Ik riep aan het begin van mijn functie bij Bureau Crypto dat het EKMS in mijn tijd uitgerold zou gaan worden. Helaas ga ik dat net missen. Ik was toch te optimistisch. De cryptowereld is een bijzondere wereld met meer krachten dan je vooraf had kunnen bedenken. Ik zal deze functie niet snel vergeten. Een mooie, paarse eenheid, met betrokkenheid van al het personeel bij de operationele eenheid en altijd bereid een stap extra te zetten als het nodig is. Een mooie club met mooi en belangrijk werk. 