Recap – Combat Cloud

Plenair I

De plenaire ochtendsessie stond in het teken van de Combat Cloud en de rol van IT, data en connectiviteit binnen de toekomstige informatievoorziening van Defensie. Defensie en marktpartijen gingen met elkaar in gesprek over de uitdagingen en kansen van een steeds complexere, multidomeinomgeving.

Tijdens de sessie werd toegelicht hoe digitale technologie een steeds belangrijkere rol speelt in het versterken van de operationele slagkracht. Daarbij werd ingegaan op de ontwikkeling naar een datacentrische manier van werken, waarbij informatie veilig, snel en op het juiste moment beschikbaar moet zijn voor verschillende gebruikers en samenwerkingspartners.

Ook werd stilgestaan bij de betekenis van Combat Cloud: een samenhangend digitaal ecosysteem waarin data, connectiviteit en informatieverwerking bijdragen aan effectieve besluitvorming en ondersteuning van operaties. Praktijkvoorbeelden benadrukten het belang van robuuste en veilige digitale infrastructuren als randvoorwaarde voor moderne defensieoperaties.

Plenair I

<u>Sleutelpunten</u>

- **Combat Cloud is geen losse technologie, maar een operationeel ecosysteem** van data, cloud, connectiviteit en besluitvorming over alle domeinen heen.
- **Betrouwbare en veerkrachtige connectiviteit is mission critical**: uitval of verstoring heeft direct gevolgen voor commandovoering, veiligheid en strategische communicatie.
- **De verschuiving van netwerkcentrisch naar datacentrisch werken vraagt om nieuwe keuzes** in classificatie, beveiliging, interoperabiliteit en samenwerking met de markt.

<u>Belangrijkste key takeaways</u>

1. Data is de **kern van moderne militaire operaties**, maar alleen als die data tijdig, betrouwbaar en in de juiste context beschikbaar is.
2. **Resilience** is cruciaal: systemen moeten blijven functioneren bij verstoring, uitval, jamming of verlies van verbinding.
3. Defensie heeft een **hybride cloudlandschap** nodig, waarin public, private, secret en sovereign cloud elk een rol spelen.
4. Classificatie en beveiliging moeten **slimmer en flexibeler** worden ingericht, zodat operationele snelheid niet onnodig wordt geremd.

5. **Samenwerking** tussen Defensie, krijgsmachtdelen en industrie is onmisbaar om Combat Cloud daadwerkelijk werkend te krijgen.
6. De grootste uitdaging is niet alleen technologie, maar **integratie en toepasbaarheid in de operatie** – van hoofdkwartier tot tactische edge.

Break-out 1: Datastromen, classificatie en betrouwbaarheid

De eerste break-out-sessie ging over de uitdagingen van het veilig en effectief omgaan met data in een complete operationele omgeving. Deelnemers bespraken hoe data optimaal kan worden gedeeld, verrijkt en ingezet, met aandacht voor betrouwbaarheid, classificatie en informatiebeveiliging.

Een belangrijk thema was de ontwikkeling naar een meer datacentrische manier van werken, waarbij data op verschillende niveaus en in uiteenlopende contexten beschikbaar moet zijn. Daarbij werd benadrukt dat de waarde en gevoeligheid van data afhankelijk zijn van de context en het gebruik, wat vraagt om zorgvuldige governance en duidelijke afspraken over eigenaarschap en classificatie.

Daarnaast werd gesproken over het belang van samenwerking, standaardisatie en een toekomstbestendige inrichting van de informatievoorziening. De sessie benadrukte dat een goede balans nodig is tussen samenwerking met de markt en het behouden van voldoende eigen kennis en regie binnen Defensie.

<u>Sleutelpunten</u>

- **Dataclassificatie is dynamisch**: ruwe data kan laag geclassificeerd zijn, maar door combinatie en context een hoogwaardig en gevoelig informatieproduct worden.
- **Netwerkcentrisch en datacentrisch moeten naast elkaar bestaan**: Defensie heeft zowel robuuste netwerken als flexibele datagedreven processen nodig.
- **Governance en context zijn cruciaal**: niet alleen technologie, maar ook eigenaarschap, standaardisatie, samenwerking en kennisopbouw bepalen het succes.

<u>Belangrijkste key takeaways</u>

Break-out 1 laat zien dat Defensie voor een fundamentele ontwerpvraag staat: niet “welke cloud kiezen we?”, maar “hoe bouwen we een infrastructuur en governance die realtime kan meebewegen met context, classificatie en operationele behoefte?”. De oplossing ligt waarschijnlijk niet in één totaalontwerp, maar in het uitwerken van concrete use cases per operationele context, met een generiek fundament daaronder. Daarbij zijn vertrouwen, traceerbaarheid, datakwaliteit en eigen regie minstens zo belangrijk als technologie zelf.

Break-out 2: Werken zonder stabiele connectiviteit

De tweede break-out-sessie stond in het teken van de vraag hoe Defensie digitale technologieën zoals cloud, data en AI effectief kan inzetten in operationele omgevingen waar connectiviteit beperkt of tijdelijk niet beschikbaar is. Deelnemers bespraken de impact van uiteenlopende operationele omstandigheden op de inrichting van de digitale informatievoorziening.

Een belangrijk thema was de noodzaak om systemen en applicaties zo te ontwerpen dat zij ook kunnen functioneren bij beperkte of verstoorde verbindingen. Daarbij werd het belang benadrukt van flexibele architecturen, veilige data-uitwisseling en oplossingen die informatie lokaal kunnen verwerken en beschikbaar houden wanneer continue connectiviteit ontbreekt.

Daarnaast werd ingegaan op de rol van software, AI en edge computing bij het vergroten van de operationele effectiviteit. Tot slot benadrukten de deelnemers het belang van een wendbare aanpak, waarin Defensie en de industrie gezamenlijk experimenteren, kennis ontwikkelen en innovatieve oplossingen sneller kunnen toepassen.

<u>Sleutelpunten</u>

- **Always connected is geen realistisch uitgangspunt meer**: Defensie moet ontwerpen voor D-DIL-omstandigheden met beperkte, verstoorde of afwezige verbindingen.
- **De oplossing ligt niet alleen in netwerken, maar juist ook in software en architectuur**: edge computing, lokale AI, caching, synchronisatie, prioritering en graceful degradation zijn cruciaal.
- **Sneller experimenteren en kleiner beginnen is noodzakelijk**: cultuur, samenwerking en regie zijn minstens zo belangrijk als technologie.

<u>Belangrijkste key takeaways</u>

1. **Disconnected first** moet het nieuwe ontwerpprincipe worden voor militaire IT, applicaties en data-uitwisseling.
2. **Edge-capaciteit** is essentieel: verwerking, analyse en besluitondersteuning moeten zo dicht mogelijk bij de gebruiker of sensor plaatsvinden.
3. Defensie moet af van netwerkcentrisch en meer sturen op **data, interoperabiliteit en flexibele architecturen**.
4. Applicaties moeten **adaptief** zijn en kunnen terugvallen op lichtere vormen van communicatie en functionaliteit.
5. **Kleine, praktische experimenten in realistische omstandigheden** zijn effectiever dan grote, trage programma's.
6. De grootste uitdaging is niet alleen technisch, maar ook **organisatorisch en cultureel**: durf, eigenaarschap, opleiding en samenwerking bepalen het succes.

Break-out 3: Interoperabiliteit

De derde break-out-sessie stond in het teken van interoperabiliteit en de vraag hoe Defensie informatie beter kan delen en benutten binnen een omgeving waarin krijgsmachtdelen, bondgenoten en partners nauw samenwerken. Daarbij werd gesproken over de ontwikkeling naar een datacentrische benadering, waarin data veilig, gecontroleerd en contextafhankelijk beschikbaar wordt gesteld.

Deelnemers bespraken de technische, organisatorische en semantische aspecten van interoperabiliteit en benadrukten het belang van gemeenschappelijke standaarden, heldere governance en een zorgvuldige omgang met classificatie en informatiebeveiliging. Ook werd stilgestaan bij de uitdagingen van informatie-uitwisseling in operationele omgevingen waar connectiviteit niet altijd gegarandeerd is.

De sessie benadrukte dat verdere stappen richting interoperabiliteit vragen om een gefaseerde aanpak, gebaseerd op samenwerking, praktische toepassingen en aansluiting bij bestaande (internationale) standaarden.

<u>Sleutelpunten</u>

- **De kernambitie is de overgang van netwerkcentrisch naar datacentrisch werken**, zodat informatie veilig en contextafhankelijk beschikbaar is, ook in operationeel verstoorde omgevingen.
- **NAVO-standaarden moeten leidend zijn**, maar de grootste blokkades zitten niet in techniek alleen. Vooral organisatie, governance en implementatievermogen vormen de uitdaging.
- **Begin klein en concreet**, bijvoorbeeld met een afgebakende use case zoals meteo-data, en bouw van daaruit verder aan data-eigenaarschap, classificatie, ontsluiting en veilige uitwisseling.

<u>Belangrijkste key takeaways</u>

1. Interoperabiliteit is niet alleen een technisch vraagstuk, maar ook een organisatorisch, semantisch en bestuurlijk vraagstuk.
2. Data moet losser worden georganiseerd van netwerken, zodat beschikbaarheid en beveiliging op dataniveau geregeld kunnen worden.
3. Defensie moet niet opnieuw zelf standaarden uitvinden, maar veel consequenter aansluiten op bestaande NAVO-standaarden.
4. De basis moet eerst op orde zijn: inzicht in datasets, eigenaarschap, labeling, governance en minimale infrastructuur.
5. Werk met kleine, concrete stappen en pilots, zodat de ambitie tastbaar wordt en vertrouwen in de aanpak groeit.