TOEZICHTONDERZOEK

De cybercapaciteit bij de militaire inlichtingendienst

Notitienummer 2025.317 – 5 februari 2026

Comité R | I
Contrôle des services de renseignement
Toezicht op de inlichtingendiensten

EXECUTIVE SUMMARY

Halfweg oktober 2022 richtte het ministerie van Defensie het Cybercommando op. Dat werd ingebed binnen de Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht (ADIV) met de bedoeling deze dienst toe te laten zijn opdrachten in cyberspace uit te voeren. Voorliggend onderzoek heeft aangetoond dat de interne zeggenschapsstructuren en beheersinstrumenten deze wettelijk voorziene inbedding van het Cybercommando binnen de ADIV in de praktijk bevestigen.

Met de oprichting van het Cybercommando werd een eerste stap gezet in de verdieping en verbreding van de cybercapaciteit van Defensie, waarbij uiteindelijk vanuit deze eenheid een volwaardige Cybermacht werd gecreëerd, één van de vijf machten van de Belgische Krijgsmacht.

De cybercapaciteit van het Cybercommando staat thans in voor de exploitatie van cyberspace ten voordele van de ADIV en van Defensie en biedt in bepaalde gevallen steun aan de Natie. Afhankelijk van haar opdracht, valt de cybercapaciteit onder een verschillend juridisch kader: de Wet houdende regeling van de inlichtingen- en veiligheids-diensten (W.I&V) – in dat geval berust de verantwoordelijkheid bij het Cybercommando van de ADIV) – dan wel het Koninklijk besluit Structuur Defensie en de Wet Aanwending en Paraatstelling Defensie en zijn uitvoeringsbesluit, in dat geval berust de verantwoordelijkheid bij de Cybermacht. Hoewel vanuit juridisch oogpunt het Cybercommando en de Cybermacht twee afzonderlijke entiteiten zijn binnen de Krijgsmacht, is dit op organisatorisch vlak niet zo. De commandant van het Cybercommando is tevens de commandant van de Cybermacht en er is één organisatie waarbinnen alle personeelsleden, desgevallend, ten dienste (moeten) staan van beide hoedanigheden. Waar de cybercommando-opdrachten en -bevoegdheden wettelijk zijn vastgelegd in de W.I&V, is dit niet het geval voor de opdrachten van de Cybermacht. Anderzijds verschillen de gezagslijnen naargelang de cybereenheid optreedt als uitvoeringsorgaan van de ADIV (chef ADIV) of als Cybermacht (Chef van Defensie).

Deze dualiteit in juridische structuur, hoewel begrijpelijk en verantwoord, houdt het risico in op onduidelijkheid bij de uitvoering van de opdrachten en bij de aanwending van bevoegdheden, alsook op discussies omtrent de bevoegdheid van het Comité R/I als toezichtorgaan op de activiteiten van de cybereenheid. Het Comité formuleert dan ook aanbevelingen met betrekking tot (1) de verduidelijking van de opdrachten van de Cybermacht, (2) de verdere inkapseling van het Cybercommando binnen de ADIV en (3) het verlenen van de bevoegdheid aan de Kamer-commissie Opvolging Militaire Missies om het Comité te gelasten met een toezichtonderzoek naar de cybercapaciteit handelend als Cybermacht. De overige aanbevelingen hebben betrekking op de noodzaak tot voldoende aandacht voor de financiële middelen voor de cybercapaciteit, de steunverlening aan de Veiligheid van de Staat (VSSE) en een mogelijke herziening van de 'tegenaanval'-bevoegdheid van de ADIV in cyberspace.

1.
INTRODUCTIE

1.1. AANLEIDING VOOR HET ONDERZOEK

1. Op 19 oktober 2022 richtte het ministerie van Defensie zijn 'Cyber Command' op, voorgesteld als "*een eerste stap naar de oprichting van een vijfde component in het Belgische leger, de Cybercomponent*"[1], naast de Land-, Lucht, en Medische componenten, en de Marine.[2]

2. Dit nieuwe commando ('Cybercommando') werd ingebed binnen de ADIV[3] zodat het Comité R/I bevoegd is om hierop zijn wettelijke toezichtsbevoegdheid uit te oefenen. Met het oog op een efficiënte en effectieve uitoefening van dit toezicht was het voor het Comité van primordiaal belang om dit nieuwe commando grondig te leren kennen in al zijn facetten. Daarbij stelde het Comité van meet af aan vast dat beoogd werd om het Cyber Command, als onderdeel van de ADIV, te laten evolueren tot een volwaardige Cybercomponent / Cybermacht (Cyber Force). In dit verband verklaarde de toenmalige minister van Defensie in haar beleidsverklaring van 4 november 2020: "*Vertrekkende van deze cybercapaciteit binnen de ADIV kan een Cybercomponent ontwikkeld worden binnen een horizon van vijf jaar, zonder de capaciteit cyberinlichtingen van de ADIV te verzwakken. De operaties van de toekomstige Cybercomponent kunnen gaan boven cyberdefensie en*

---

1 Vrije vertaling uit MATRICHE, J., "Cyberespace, le nouveau champ de bataille de l'armée belge", *Le Soir*, 18 oktober 2022 (*« une première étape vers la création d'une cinquième composante dans l'armée belge, la composante CYBER »*) .

2 Het Koninklijk besluit van 2 december 2018 tot bepaling van de algemene structuur van het Ministerie van Landsverdediging en tot vaststelling van de bevoegdheden van bepaalde autoriteiten (*B.S.* 18 januari 2019), zoals het op dat moment van toepassing was, vermeldde in artikel 1, 5° slechts vier componenten.

3. Eind december 2024 werd door de ADIV een presentatie gegeven aan het Comité R/I over de structuur van de dienst. Bij deze presentatie werd bij een onderdeel over "Cyberspace" toegelicht dat het Cyber Command, dat onder de leiding staat van de Commandant Cyber Command (CyC), is geïntegreerd binnen de structuur van de ADIV, en dat dit Cyber Command verantwoordelijk is voor de uitvoering van opdrachten die zijn opgenomen in de W.I&V. De ADIV omschrijft deze opdrachten met de termen Cyber Intel en Cyber Security. Zie ook het verslag van de hoorzitting van de Commissie Landsverdediging met de commandant van het Cyber Command, *Parl. St.*, Kamer, 2022-2023, DOC 55 3323/001.

noodzaken een wettelijk kader dat zal aangemaakt worden tijdens deze legislatuur".[4]

3. Deze voorgenomen evolutie naar een Cybercomponent/Cybermacht werd ook in de daaropvolgende beleidsverklaringen inzake defensie telkens bevestigd[5], alsook in de eerste contacten tussen het Vast Comité I en de eerste commandant van het Cyber Command, generaal-majoor Michel VAN STRYTHEM.[6] In een interview verklaarde generaal-majoor VAN STRYTHEM dat het commando van het Cyber Command "*waarschijnlijk (sic)*" binnen de ADIV zal blijven.[7] Tijdens zijn presentatie voor het Vast Comité I op 18 januari 2023 stelde hij ook een visie voor op het 'Cyber Command' dat weliswaar deel uitmaakt van de ADIV, maar ook een volwaardige component binnen Defensie moet worden in een transversale, ondersteunende dimensie vergelijkbaar met de medische component. Op 2 maart 2023 stelde generaal-majoor VAN STRYTHEM in de Koninklijke Militaire School[8] het draaiboek voor van het Cyber Command, dat uiteindelijk een 'Cybercomponent' moet worden en als dusdanig enerzijds valt onder de organieke Wet houdende regeling van de inlichtingen- en veiligheidsdienst van 30 november 1998 (W.I&V) en anderzijds onder het kader van de 'CHOD Ops Order' en zijn '*rules of engagement*'.[9]

4. Deze evolutie van Cyber Command als onderdeel van ADIV tot een Cybercomponent/Cybermacht zou *prima facie* gevolgen kunnen hebben voor de uitoefening van de bevoegdheden door het Vast Comité I en roept enkele fundamentele vragen op, o.m. met betrekking tot de uitoefening van de opdrachten van de ADIV in cyberspace. Dit gegeven vormde een bijkomende aanleiding om een toezichtonderzoek te openen naar het Cyber Command.

5. In het federaal Regeerakkoord 2025-2029 wordt dan weer geen melding gemaakt van de

---

4 *Parl. St.*, Kamer, 2020-2021, DOC 55 1610/017, p. 25.

5 *Parl. St.*, Kamer, 2021-2022, DOC 55 2294/008, p. 31; *Parl. St.*, Kamer, 2022-2023, DOC 55 2934/020, p. 42 en *Parl. St.*, Kamer, 2023-2024, DOC 55 3649/022, p. 45.

6 Bij KB van 23 oktober 2022 werd generaal-majoor Michel VAN STRYTHEM aangeduid om het ambt van commandant van het Cyber Command uit te oefenen. Michel VAN STRYTHEM werd bij KB van 20 juni 2025 benoemd in de graad van luitenant-generaal (*BS*, 18 augustus 2025).

7 CLEVERS, A., "L'armée belge se dote d'un Cyber Command", La Libre Belgique, 19 oktober 2022.

8 Koninklijk Hoger Instituut voor Defensie, Avondconferentie 'Waarom heeft België een Cybercommando nodig?', 2 maart 2023. "*Wat zijn de opdrachten van dat Cyber Commando? De eerste opdracht [= Intelligence, Security & military operations in Cyberspace] is het voeren van operaties. En dat kan, en dat moet binnen twee afzonderlijke wettelijke kaders. Dus, eerst is het wettelijke kader van de organieke wet inlichtingen- en veiligheidsdiensten en waar eigenlijk de operaties in de security operaties en de operaties, de intelligence operaties gevoerd worden onder de organieke wet SGRS-ADIV. De anderen zijn de militaire operaties die uitgevoerd worden op mandaat van de regering, met rules of engagement en met een CHOD OP ORDER onder de gekende procedures en systematiek die geleid wordt door het Departement Operaties van Defensie. [Daar zijn?] de twee frameworks dat erin gewerkt wordt. In vredestijd is de focus, het volume het percentage het grootst voor het eerste wettelijke kader, maar er zijn voorbeelden van operaties in het kader van de inzet van de krijgsmacht, met rules of engagement die nu al bestaan",* aldus generaal-majoor Van Strythem.

9 Zie onder meer de Wet Aanwending en Paraatstelling Krijgsmacht van 20 mei 1994 (*infra*).

oprichting van de Cybercomponent. Volgende passages komen erin voor met betrekking tot Defensie en de cyberproblematiek :

"Defensie neemt een centrale rol in bij het afweren van hybride dreigingen en dreigingen gelieerd aan Great Power Competition (inclusief economische risico's), zowel uitgaande van statelijke als niet statelijke actoren. Om op dit vlak een rol van betekenis te spelen, zetten we onder meer in op de verdere uitbouw van onze verdedigingscapaciteit en onze cyberverdediging, waarbij we ook ***investeren in middelen voor elektronische oorlogsvoering en in artificiële intelligentie. Zo heeft de verdere uitbouw van ons Cybercommando onder meer tot doel om onze weerbaarheid tegen buitenlandse inmenging op te schroeven en om ons desgevallend voor te bereiden op offensieve operaties****. Een versterkte samenwerking tussen de verschillende actoren moet ons toelaten onze capaciteiten op dat vlak te verbeteren. We investeren meer in nieuwe technologieën.*[10]

We zetten in op een multidimensionale aanpak, opgebouwd rond militaire veiligheid, cyberveiligheid en informatiezekerheid. We voeren onze cyberbescherming op via het investeren in ***nieuwe capaciteiten voor ons Cybercommando****, maar ook via samenwerkingen met kennisinstellingen en door de* ***synergiën tussen de inlichtingendiensten verder te versterken en een grotere mobiliteit voor het personeel te verzekeren binnen de bestaande wettelijke kaders****. Dit met respect voor de onafhankelijkheid en eigenheid van de verschillende diensten. We focussen op verdere hervorming van ADIV, evenwel zonder haar topfunctie te demilitariseren. In het kader van de Defensiecodex werken we aan de modernisering van de wetten rond militaire inlichtingenvergaring, zoals een* ***Wet Tactische Inlichtingen****.*[11]

We versterken de samenwerking met de inlichtingendiensten van onze partners binnen de NAVO en de EU. In het kader van onze maatschappelijke weerbaarheid, laten we relevante informatie beter doorstromen naar andere belanghebbenden. ***De inwinning van inlichtingen in het buitenland wordt versterkt, zowel op vlak van defensie en cyber als op economisch vlak.***[12]

De ***Algemene Dienst Inlichtingen en Veiligheid beschikt over voldoende middelen om zijn taken in dit domein ten volle te kunnen vervullen*** *met respect voor haar specificiteit als een militaire inlichtingendienst".*[13]

6. Uit deze passages zou kunnen worden begrepen dat de federale regering ervoor opteert om het Cyber Command de komende jaren te behouden binnen de structuren van de ADIV. Een uitdrukkelijke bevestiging van deze keuze wordt teruggevonden in artikel 42 van het Koninklijk besluit van 30 juni 2025 tot bepaling van de algemene structuur van het

10 Federaal Regeerakkoord 2025-2029, blz. 183.

11 *Idem*, p. 184-185.

12 *Idem*, p. 185.

13 *Idem*, p. 185.

Ministerie van Landsverdediging en van de bevoegdheden van bepaalde autoriteiten[14], dat bepaalt: *"Bij de Algemene Dienst Inlichting en Veiligheid bestaat een Cybercommando dat optreedt in het domein van cyberspace en dat de opdrachten uitvoert die bepaald zijn in artikel 11 van de wet van 30 november 1998. Het Cybercommando staat onder leiding van de cybercommandant. Hij is ook de commandant van de cybermacht."*

7. In de beleidsnota van de minister van Defensie van 17 april 2025 wordt gesteld dat de componenten van Defensie vanaf 21 juli 2025 opnieuw Machten worden genoemd, waaronder "*de nog op te richten Cybermacht*"[15], hetgeen kort nadien gebeurde. Artikel 1 van voornoemd K.B. van 30 juni 2025 bepaalt dat de Cybermacht een onderdeel is van de strijdkrachten.[16]

1.2. BEVOEGDHEID VAN HET COMITE R/I

8. De bevoegdheid van het Comité R/I binnen zijn generieke toezichtopdracht wordt niet op functionele maar op organieke wijze bepaald.[17] Het Comité controleert de ADIV (en de VSSE) als organisatie. Het organiek criterium als bevoegdheidsafbakening houdt in dat het Comité een controle uitoefent op de ADIV (en de VSSE) als aparte structuren, bestaande uit een geheel van mensen en middelen, een geheel aan opdrachten en werkzaamheden en een eigen hiërarchische zeggenschapsstructuur. Het Comité controleert hierbij alle activiteiten van de onder toezicht staande diensten, dus zowel de operationele werkzaamheden als de beheersmatige taken.

9. Zoals dit verslag verduidelijkt, verricht de ADIV diverse activiteiten en werkzaamheden ter uitvoering van verschillende soorten opdrachten. In de Toezichtwet heeft de wetgever duidelijk de wil veruitwendigt dat alle door eenzelfde organisatie uitgevoerde activiteiten en werkzaamheden door het Comité R/I gecontroleerd moeten worden. Dat een dienst, eenheid of capaciteit, naargelang het soort activiteiten dat deze verricht, onder verschillende gezagsoverheden staat of onder een verschillende benaming handelt, verandert niets aan de draagwijdte van de wettelijke controleopdracht van het Comité. Anders stellen zou neerkomen op het verdedigen van de stelling dat de uitvoerende macht, bij reglement (KB, MB of interne dienstnota), de wet aan de kant kan en mag schuiven.

10. De door de wetgever bepaalde organieke bevoegdheidsafbakening heeft betekenis voor de controle op de cybereenheid. Zoals verduidelijkt, is deze eenheid als organisatie belast

---

14 *BS*, 15 juli 2025, p. 59443.

15 *Parl. St.*, Kamer, 2024-2025, DOC 56 0856/022, p. 30. Eerder (3 juni 2025) vermeldde de Koning "*geschiedenis [werd] geschreven binnen Defensie door het embleem van de Cybermacht te overhandigen. Deze ceremonie vormde het hoogtepunt van de oprichting van deze nieuwe macht, die onmisbaar is gezien de actuele dreigingen*". (https://x.com/BECybercom/status/1930164947209629768).

16 *BS*, 15 juli 2025.

17 *Cf.* artt. 33, 34, 40, 48, 50 en 51 Toezichtwet.

met twee soorten opdrachten: de Cybercommando-opdrachten (m.n. ter uitvoering van de ADIV-opdrachten) en de Cybermacht-opdrachten (m.n. als strijdkracht). Zoals gezegd, worden deze activiteiten door dezelfde structuur verricht. Indachtig de wettelijke keuze voor het organiek criterium als bevoegdheidsafbakening, is het Comité bevoegd toezicht te houden op de activiteiten binnen de uitvoering van beide soorten opdrachten. Dat binnen de uitvoering van de Cybercommando-opdrachten de cybereenheid onder het rechtstreeks gezag staat van de Chef ADIV maar binnen de uitvoering van de Cybermacht-opdrachten onder deze van de Chef Defensie, heeft geen invloed op de toezichtbevoegdheid van het Comité.

11. Voor de draagwijdte van de wettelijke controleopdracht van het Comité maakt het ook geenszins een verschil uit of de militaire cybercapaciteit de benaming Cybercommando of Cybermacht draagt.[18] Het Comité stelt vast de ADIV hierover een andere mening is toebedeeld.[19]

12. Het Comité is evenwel niet bevoegd een controle te verrichten op de instructies van de minister van Defensie, de Chef Defensie of, desgevallend, de onderstafchef paraatstelling en operaties die gericht zijn aan de Cybereenheid. Het Comité houdt geen toezicht op de regering noch op andere gezagsoverheden van de te controleren organisaties.[20] Het Comité heeft logischerwijs wel een toezichtbevoegdheid op de instructies van de Chef ADIV aan de Cybereenheid.

13. Tot slot brengt het Comité in herinnering dat de aanwending van het budget van de Cybermacht nooit enige bevoegdheidsrechtelijke gevolgen kan hebben. Ingeval de installatie van cybermedewerkers binnen de andere machten (de zgn. 'gedecentraliseerde capacitaire modules') geschiedt met behulp van het budget van de Cybermacht, betekent dit dat betrokkenen zich in de eerste plaats bezig dienen te houden met de uitvoering van

---

18 Noch maakt het verschil uit of de militaire inlichtingencapaciteit ADIV of ACOS IS wordt genoemd."

19 De ADIV ging niet akkoord met de stelling over de controlebevoegdheid. Zoals gezegd, is het Comité van oordeel dat het feit dat een dienst, eenheid of capaciteit, naargelang het soort activiteiten dat deze verricht, onder verschillende gezagsoverheden staat of onder een verschillende benaming handelt, geen invloed heeft op de draagwijdte van de wettelijke controleopdracht van het Comité. Anders stellen zou immers neerkomen op het verdedigen van de stelling dat de uitvoerende macht, bij reglement (*i.c.* bij KB Structuur Defensie van 30 juni 2025), de wet (*i.c.* de Toezichtwet) aan de kant kan en mag schuiven.

20 In dezelfde zin is het Comité niet bevoegd controle uit te oefenen op de activiteiten van de Chef ADIV vanuit zijn hoedanigheid van Vleugeladjudant van de Koning. De Vleugeladjudanten van de Koning maken immers deel uit van het Militaire Huis, een aparte organisatie die de Koning bijstaat bij het uitoefenen van zijn constitutionele bevoegdheden op vlak van Defensie. Ook is het Comité niet bevoegd controle uit te oefenen op de activiteiten van de adviseur(s)-generaal van de ADIV vanuit hun hoedanigheid van lid van de Directieraad van het ministerie van Landsverdediging. Organiek bekeken vormen zowel het Militaire Huis als de Directieraad aparte structuren die zich juridisch en feitelijk onderscheiden van de unieke structuur ADIV & ACOS IS.

Cybermacht-opdrachten. Anderzijds wil dit geenszins zeggen dat het Comité van rechtswege geacht wordt aan te nemen dat betrokkenen louter dergelijke activiteiten uitoefenen, noch dat het Comité geen toezichtsbevoegdheid zou hebben op dergelijke cybermedewerkers.

1.3. DOELSTELLING VAN HET ONDERZOEK

14. Het doel van dit toezichtonderzoek is om de organisatie en activiteiten van het Cyber Command in kaart te brengen en te analyseren.[21] Daarbij is het met name van belang om duidelijkheid te verschaffen over de precieze positie van het Cyber Command binnen de ADIV, daarbij de precieze verantwoordelijkheden te bepalen, en de gevolgen die dit heeft voor de commandostructuur. Minstens even belangrijk is na te gaan welke de gebeurlijke impact is van de creatie van de Cybermacht, waarvan de commandant tevens de commandant van het Cyber Command is, op de uitoefening van de opdrachten van de ADIV in cyberspace. In dit verband rijst m.n. de vraag of het risico bestaat dat bepaalde (inlichtingen)activiteiten die voorbehouden zijn aan de ADIV voortaan onttrokken worden aan het toezicht door het Comité R/I.

15. Dit risico van gebrek aan controle vormt een potentiële bedreiging voor de bescherming van de rechten van personen krachtens de Grondwet en de wet, en voor de coördinatie en doeltreffendheid van de diensten. Het instellen van een toezichtonderzoek zal het Comité R/I in staat stellen om de bevoegde overheden zo nauwkeurig mogelijk te informeren over de reële risico's van inlichtingenactiviteiten die daadwerkelijk ontsnappen aan de democratische controle en alle nuttige aanbevelingen te doen om deze risico's te beperken.

16. Recent gaf de Premier een inkijk in de Belgische cybersecuritystrategie.[22] Daarin was onder meer sprake van de samenwerking tussen het Cyber Command en het Centrum Cybersecurity Belgium (CCB) of nog, de interacties met de Belgische Permanente Vertegenwoordigers bij de EU en de NAVO.[23] Ook de mogelijkheden die het Platform Cybersecurity van het Coördinatiecomité voor Inlichtingen en Veiligheid (CCIV) biedt aan de inlichtingen- en veiligheidsdiensten om het beleid inzake cyberveiligheid te bespreken

---

21 De volledige titel van het onderzoek luidt: 'Toezichtonderzoek naar de organisatie en de activiteiten van het Cyber Command van de Algemene Dienst Inlichting en Veiligheid (ADIV)'.

22 *QRVA*, Kamer, 56 020, 29 juli 2025 (Vraag nr. 61 van De Heer Volksvertegenwoordiger Kjell Vander Elst van 19 juni 2025 aan de eerste minister over de 'Belgische cybersecuritystrategie' (DO 2024202504357).

23 Naast deze structurele samenwerking werken het CCB en het Cyber Command ook op *ad hoc* basis samen aan specifieke dossiers, zoals de NATO Cyber Defense Pledge, de EU Cyber Census en het EU Cyber Defence Coordination Centre (EU CDCC).

en informatie uit te wisselen over de *situational awareness* waren aan de orde.[24] In voorliggend rapport werden deze samenwerkingsvormen niet onderzocht. Desgevraagd kan dit het voorwerp uitmaken van een vervolgonderzoek.

17. Het ontwerprapport van het toezichtonderzoek werd voor opmerkingen en verzoek tot declassificatie voorgelegd aan de ADIV. De opmerkingen werden verwerkt in onderhavig verslag.

[24] De leden van het platform zijn: het CCB, de FOD Buitenlandse Zaken, de VSSE, het OCAD, het Openbaar Ministerie, het College van de federale procureurs, de Federale Politie, de Federal Computer Crime Unit, het Nationaal Crisiscentrum (NCCN), Defensie en Cyber Command.

2.

GRONDSLAG VOOR DE OPRICHTING VAN HET CYBER COMMAND (CYCOM)

18. In de Beleidsverklaring van de toenmalige minister van Defensie van 4 november 2020 werd aangekondigd dat Defensie haar cybercapaciteit aanzienlijk zal verdiepen, hetgeen zich op termijn moest vertalen in de creatie van een volwaardige component. Hiertoe zou in eerste instantie de cybercapaciteit binnen de ADIV moeten versterkt worden, waarna vanuit deze cybercapaciteit een volwaardige Cybercomponent zou kunnen ontwikkeld worden binnen een horizon van vijf jaar, zonder de capaciteit cyberinlichtingen van de ADIV te verzwakken.[25]

19. Hiertoe werd binnen Defensie midden 2021 een projectteam samengesteld met als opdracht de oprichting van de nieuwe Cybercomponent uit te werken. Dit resulteerde in het in kaart brengen wat er op het vlak van cybercapaciteit reeds voorhanden was binnen de schoot van de Belgische Defensie en het uitvoeren van een internationale *benchmark*.[26]

20. Het Cyber Command van de ADIV werd opgericht op 19 oktober 2022, en was op dat moment een fusie van de directie Cyber van de ADIV, het 'Project Office Cyber & Influence', de dienst ELINT/SIGINT (voorheen 'C3'), de dienst OSINT/SOCMINT (voorheen 'C5') en het platform "Information Warfare" (voorheen 'PF10'). Deze feitelijke gebeurtenis werd slechts *post factum* geformaliseerd in artikel 42 van het KB van 30 juni 2025 tot bepaling van de algemene structuur van het Ministerie van Landsverdediging en van de bevoegdheden van bepaalde autoriteiten.[27] Het enige basisdocument dat het Vast Comité I heeft verkregen en dat dateert uit de periode van de oprichting van het Cybercommando waarin hiernaar expliciet wordt verwezen, is het reeds vermelde KB van 23 oktober 2022, waarbij (toenmalig) generaal-majoor VAN STRYTHEM vanaf 19 oktober 2022 werd aangesteld als Commandant van het Cyber Command.

21. Uit de bovenvermelde beleidsverklaring blijkt aldus dat de ontwikkeling van een Cybercommando in de schoot van de ADIV een dubbele finaliteit had. Ten eerste moest

---

25 *Parl. St.*, Kamer, 2020-2021, DOC 55 1610/017, p. 25.

26 *Parl. St.*, Kamer, 2022-2023, DOC 55 3323/001, p. 4 (hoorzitting Commissie Landsverdediging van 1 maart 2023 met de commandant van het Cybercommando).

27 Zie hoger. In dit verband verklaarde de minister van Defensie in haar algemene beleidsnota van 31 oktober 2022: "*Eventuele aanpassingen aan het Koninklijk Besluit betreffende organisatie van Defensie en zijn staf na de oprichting van het Cyber Command zullen worden opgenomen in het herzieningstraject van de Defensiestaf*" (*Parl. St.*, Kamer, 2022-2023, DOC 55 2934/020, p. 43).

hiermee de cybercapaciteit van de ADIV versterkt worden om deze dienst toe te laten haar opdrachten in cyberspace uit te voeren, en ten tweede moest vanuit dit Cybercommando een volwaardige Cybercomponent ontwikkeld worden[28] zonder dat evenwel afbreuk zou worden gedaan aan de cyber(inlichtingen)capaciteit van de ADIV.

22. In de beleidsnota Defensie van 31 oktober 2023 werd gesteld dat de oprichting van het Cybercommando o.m. tot doel had toezicht te houden op het proces om de volgende doelstellingen te bereiken: (1) het versterken van de bestaande cybercapaciteit binnen de ADIV, (2) het ontwikkelen van de zoektocht naar talent en vorming, (3) het initiëren van cyberinnovatie, onderzoek en technologische ontwikkeling, in samenhang met de 'Defense, Industry and Research Strategy (DIRS)', en het ondersteunen van het ontwikkelingsproces van de nieuwe Cybercomponent. *"Het Cyber Command vormt daarmee de kern van wat een volwaardige Cybercomponent bij Defensie zal worden"*.[29]

---

28 Zie ook *Parl. St.*, Kamer, 2022-2023, DOC 55 2934/020, p. 42 (algemene beleidsnota Defensie van 31 oktober 2022).

29 *Parl. St*., Kamer, 2023-2024, DOC55 3649/022, p. 45. Uit de interviews op het Comité bleek dat 2032 als streefdatum wordt vooropgesteld om volledig 'uitgerold' te zijn.

3.

MISSIE EN ACTIVITEITSDOMEINEN VAN CYBER COMMAND (CYCOM)

23. Informatie over de missie, opdrachten en activiteiten van het Cyber Command (CyCom) kunnen worden gevonden in diverse bronnen: de door het Cyber Command gegeven briefings aan het Vast Comité I, de website van het ministerie van Landsverdediging en van de ADIV, de verslagen van parlementaire zittingen, de Nationale Cyber Strategie, het *'ADIV – Jaarverslag 2024'*, alsook enkele andere geclassificeerde documenten, waaronder het *'Stuurplan 2023-2027 van de ADIV*[30]*'*.

3.1. DE BEVOEGDHEDEN VAN CYBER COMMAND IN HET STUURPLAN 2023-2027

24. Het operationele deel van het "Stuurplan van de ADIV 2023-2027" maakt melding van de creatie van een Cyber Command, en omschrijft de bevoegdheden hiervan als volgt[31]:

"Het Cyber Command heeft een dubbele verantwoordelijkheid. Enerzijds neemt het de inlichtingen- en veiligheidsopdrachten van de ADIV in de cyberspace en het elektromagnetisch domein op zich. Anderzijds heeft de Cyber Commander, als hoofd van de nieuwe Cybercomponent, de rollen en verantwoordelijkheden van een steuncomponent in het domein van de cyberspace voor de andere componenten en de rest van Defensie. In dat opzicht is de Cybercomponent verantwoordelijk voor het verzekeren van de maneuvervrijheid van de Strijdkrachten in de cyberspace en het genereren van militaire cybereffecten ter ondersteuning van de operaties van Defensie.

Zijn operationele taken zijn in vier punten samen te vatten:

- *"Conduct Cyber Operations": De opdrachten van de ADIV uitvoeren en die van de*

30 Het Stuurplan werd openlijk door de minister van Defensie aangekondigd (*Parl. St.*, Kamer, 2022-2023, DOC 55 2934/020, blz. 32): *"Een van de geïdentificeerde prioriteiten was de voorbereiding van een stuurplan voor de dienst. Begin dit jaar werd het Stuurplan 2022 van de ADIV uitgevoerd na voorstelling aan de Kamer van Volksvertegenwoordigers. In het verlengde van dat stuurplan is een meerjarig stuurplan voor de periode 2023-2027 in voorbereiding om begin 2023 uitgevoerd te worden."*

31 De omschrijving van de bevoegdheden werd overgenomen uit het GEHEIM geclassificeerde Stuurplan. Op verzoek van het Comité R/I ging de ADIV akkoord met de declassificatie hiervan.

Strijdkrachten ondersteunen in de cyberspace en het elektromagnetisch domein. Deze zijn opgenomen in de vier luiken van het Cyber Operations Framework: Cyber Security Operations (PROTECT), Defensive Cyber Operations (DEFEND), Cyber Intelligence, Surveillance and Reconnaissance Operations (COLLECT & ANALYSE) and Cyber Offensive Operations (FIGHT).

- *"Cyber readiness of the Forces": Toezicht uitoefenen op de paraatstelling en de operationele voorbereiding van heel Defensie om in de Cyberspace en het elektromagnetisch domein te kunnen werken.*

- *"Readiness of the Cyber Forces": De paraatstelling en de operationele voorbereiding van de gespecialiseerde cybermiddelen van de ADIV uitvoeren; andere diensten van de ADIV, buiten het Cyber Command, zijn verantwoordelijk voor de digitale infiltratie via virtuele agenten, de exploitatie van gegevens afkomstig van telefonische onderschepping op het nationaal grondgebied, de relaties met telefoonoperatoren en de vergaring van informatie op sociale netwerken voor veiligheidsonderzoeken.*

- *"Homebase Support": Overeenkomstig de richtlijnen van de Nationale Veiligheidsraad, zich klaarhouden om de capaciteiten van de ADIV in het kader van opdrachten van hulp aan de Natie in te zetten, met name in geval van nationale cybercrisissen. Zo nodig, deze capaciteiten inzetten. Deze taak spruit voort uit de versterking van de digitale veerkracht van België en omvat, indien nodig, steun aan de operatoren van kritieke infrastructuur.*

3.2. DE BEVOEGDHEDEN VERDER TOEGELICHT

25. De cybercapaciteit van het Cyber Command staat in voor de exploitatie van cyberspace ten voordele van de ADIV en Defensie en biedt in bepaalde gevallen steun aan de Natie. De cybercapaciteit valt, afhankelijk van haar opdracht, onder twee verschillende juridische kaders: de organieke Wet betreffende de inlichtingen- en veiligheidsdiensten – in dat geval berust de verantwoordelijkheid bij het Cyber Command van de ADIV – of het juridische kader voor de inzet van de Belgische strijdkrachten – in dat geval berust de verantwoordelijkheid bij de Cybermacht.

26. De minister van Defensie verklaarde in zijn beleidsnota van 17 april 2025 dat het Cybercommando zijn veiligheidsopdrachten in cyberspace blijft uitvoeren, met name ter bescherming van Defensiepersoneel, communicatie-infrastructuur en wapensystemen, alsook zijn inlichtingenopdrachten (collecte en analyse) om een nauwkeurig beeld te behouden van de buitenlandse dreiging die zich richt op België in de elektromagnetische, digitale en informatieruimte.[32]

---

32 *Parl. St.*, Kamer, 2024-2025, DOC 56 0856/022, p. 11.

27. Als commandant van het Cybercommando formuleerde de toen nog generaal-majoor VAN STRYTHEM de missies van zijn dienst als volgt tegenover de Commissie Landsverdediging: (1) het uitvoeren van operaties in de cyberruimte (inlichtingen, veiligheid, defensieve operaties), (2) steun aan de andere componenten en activiteiten (defensief en offensief), en (3) versterking van de nationale weerbaarheid.[33]

28. De activiteitsdomeinen werden door de commandant van het Cybercommando omschreven als volgt: (1) preventieve werking[34], (2) actieve monitoring van netwerken, (3) inlichtingenvergaring, en (4) militaire inzet (defensief en offensief, *cyber force protection*)[35].

29. De missie en de opdrachten van het CyCom zijn in belangrijke mate gebaseerd op de NAVO-doctrine, die is neergeschreven in de *'NATO Allied Joint Publication (AJP) – 3.20 Allied Joint Doctrine for Cyberspace Operations'*. In dit document vindt men onder andere een definitie terug van cyberspace, zoals die door de NAVO en dus ook het CyCom van de ADIV wordt gehanteerd. Deze definitie luidt als volgt: *"Het wereldwijde domein dat bestaat uit alle onderling verbonden communicatie-, informatie- en andere elektronische systemen, netwerken en hun gegevens, met inbegrip van die welke gescheiden of onafhankelijk zijn, die gegevens verwerken, opslaan of verzenden."*[36]

30. Nog volgens de NAVO-doctrine bestaat de cyberspace uit drie "lagen": 1/ een fysieke laag, 2/ een logische laag, en 3/ een "cyber-persona" of sociale laag, ook nog "virtuele" laag genoemd.

    - De fysieke laag is verbonden aan een geografische locatie, en bestaat uit tastbare componenten als computers, servers, routers, hubs, bedrading en apparatuur die wordt gebruikt voor gegevensopslag, -verwerking en -overdracht. De fysieke laag kan ook wapensystemen en kritieke infrastructuur bevatten.
    - De logische laag bestaat uit elementen die zich manifesteren in code of in gegevens, zoals besturingssystemen, protocollen, software- en gegevenscomponenten. De logische laag zorgt er, samen met de fysieke laag, voor dat een cyberpersoon (cyber persona) kan communiceren en handelen.
    - De "cyber-persona" of sociale laag bestaat uit elementen die geen werkelijke personen of organisaties zijn, maar een representatie van hun virtuele identiteit. Een virtuele identiteit kan bestaan uit een e-mailadres, een gebruikersidentificatie, een sociale media-account of een alias. Eén persoon of organisatie kan dus

---

33 O.a. inzake activering van het cyber crisisplan van CCB en van het Nationaal Crisiscentrum *Parl. St.*, Kamer, 2022-2023, DOC 55 3323/001, p. 5 (hoorzitting commissie Landsverdediging van 1 maart 2023 met de commandant van het Cybercommando).

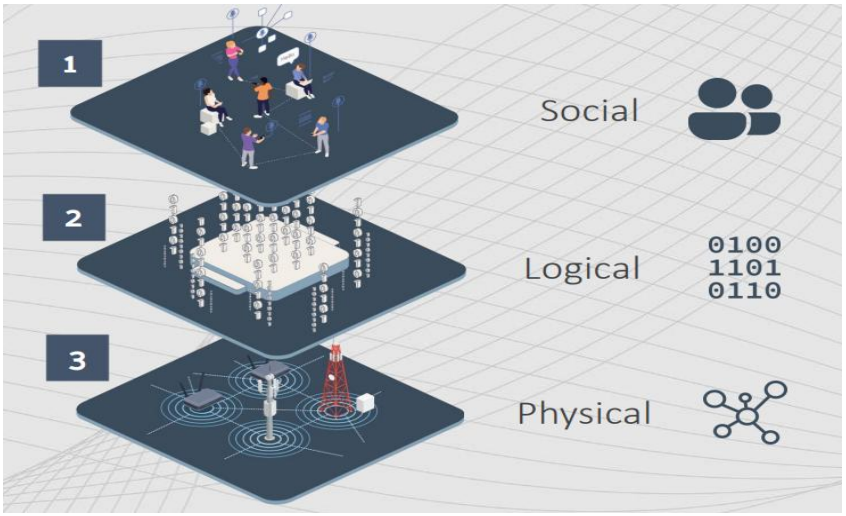
34 Zoals homologatie van netwerken, richtlijnen van goede praktijken, bewustmaking van risico's.

35 Met o.m. de bescherming van de nieuwe geïnterconnecteerde wapensystemen doorheen de verschillende componenten.

36 Vrije vertaling uit *"NATO Allied Joint Publication (AJP) – 3.20 Allied Joint Doctrine for Cyberspace Operations"*, p. 4.

meerdere "cyber-personas" hebben. Omgekeerd kunnen meerdere personen of organisaties ook één gedeelde "cyber persona" creëren.

31. De uitvoering van cyberoperaties vindt altijd plaats in de logische laag, en kan ook plaatsvinden binnen de twee andere lagen.



32. Binnen de verschillende 'lagen' van de cyberspace heeft het Cyber Command volgende vier kernopdrachten:[37]

1/ PROTECT: Om de vrijheid van handelen tijdens militaire operaties te garanderen, moet Defensie al haar communicatie, informatie- en wapensystemen beschermen. Het optimaliseren van de veiligheid en weerbaarheid van alle systemen vereist een gecoördineerde aanpak op verschillende niveaus.

2/ DEFEND: Zelfs de beste cyberbeveiliging kan een succesvolle cyberaanval nooit helemaal uitsluiten. Defensie moet beschikken over een robuuste set van maatregelen om adequaat te kunnen reageren op cyberincidenten en continuïteit in de uitvoering van opdrachten te garanderen. Daarom ontwikkelt Defensie voortdurend haar capaciteiten voor detectie, analyse en remediëring, evenals attributie en communicatie.

3/ COLLECT: Defensie blijft haar inlichtingenexpertise in cyberspace uitbreiden. Daarbij ligt de focus op de capaciteiten en intenties van cyberactoren in de regio's waar het aanwezig is. Cyber Command gebruikt specifieke methodes om relevante informatie te verzamelen over de spionage- en sabotageactiviteiten van onze tegenstanders.

4/ FIGHT: De inlichtingencapaciteit kan ook worden ingezet om zelf cyberaanvallen voor te bereiden en te ondersteunen. Dit kan door te zoeken naar kwetsbaarheden in de

37 https://www.mil.be/nl/evolutie-van-defensie/protect-defend-collect-and-fight-in-cyberspace/

communicatie-, informatie- en wapensystemen van onze tegenstanders.

33. De verschillende onderdelen van het Cyber Command zijn, al naargelang hun specifieke rol, actief binnen één of meerdere van de hierboven beschreven “lagen” van de cyberspace, en leveren hun bijdrage aan de uitvoering van één of meerdere van de hierboven vermelde opdrachten (zie *infra*).

4.
BEHEER VAN DE CYBEREENHEID

34. De Inlichtingenwet schrijft voor dat het land twee inlichtingen- en veiligheidsdiensten heeft: de VSSE, burgerlijke inlichtingen- en veiligheidsdienst, en de ADIV, militaire inlichtingen- en veiligheidsdienst.[38] Hoewel de wet niet expliciet definieert wat dan wel een inlichtingen- en veiligheidsdienst is, blijkt dit duidelijk uit de wettelijke omschrijving van de inlichtingen- en veiligheidsopdrachten in artikel 7 W.I&V (VSSE) en artikel 11 W.I&V (ADIV). Uit deze bepaling vloeit het wettelijk verbod voor de uitvoerende macht voort om – zowel *de iure* als *de facto* – nieuwe inlichtingen- en veiligheidsdiensten op te richten.

35. Van belang voor voorliggend toezichtonderzoek is dat de Krijgsmacht geen bevoegdheid heeft om binnen de ADIV een nieuwe inlichtingen- en veiligheidsdienst op te richten die, juridisch gezien (via KB), weliswaar een onderdeel uitmaakt van de ADIV doch die *de facto* autonoom zou zijn wegens de wijze waarop de interne zeggenschapsstructuren en beheerinstrumenten binnen en van de Krijgsmacht en de ADIV zouden zijn georganiseerd (bv. regels omtrent hiërarchie, evaluatie, tucht, personeelsbeheer, budget).

36. Zoals gezegd, stelt het KB Structuur Defensie dat het Cybercommando ingericht wordt binnen de ADIV.[39] Vanuit de doelstelling om na te gaan of het Cybercommando werkelijk een onderdeel van de ADIV uitmaakt, heeft het Comité de ADIV en zijn Chef en het Cybercommando en zijn chef bevraagd rond de concrete interne zeggenschapsstructuur en beheersinstrumenten. Omdat zowel de ADIV als het Cybercommando worden geleid door een opperofficier van dezelfde graad, was bij het Comité de vraag gerezen of de Chef ADIV werkelijk een (afdoende) zeggenschap heeft over het Cybercommando. Het Comité stelde ter zake vast dat er geen problemen aanwezig zijn. Het Comité kreeg een omstandig antwoord op zijn vragen, die zonder meer overtuigen dat er geen inbreuk wordt gepleegd op het wettelijk verbod bedoeld in artikel 2, §1 W.I&V.

37. Volgende elementen duiden erop dat het Cybercommando een integraal onderdeel is van de ADIV:

    - Voor wat betreft *de jaarlijkse evaluaties van de twee directeurs van het Cybercommando* (m.n. Directie Cyber Operations en Directie Development & Readiness) is de Cybercommandant de betrokken evaluator, maar bestaat de

38 Art. 2, §1, eerste lid W.I&V.

39 Art. 42, tweede lid, eerste zin KB Structuur Defensie.

mogelijkheid in beroep te gaan bij de hiërarchische meerdere van de evaluator, zijnde de Chef ADIV.[40] Hun verantwoordelijkheden worden in detail vastgelegd in het reglement DGHR-REG-EVAL-001[41];

- Binnen *het militaire tuchtreglement voor het militaire personeel*[42] worden de zware straffen in eerste aanleg opgelegd door de ten opzichte van de betrokken militair bevoegde korpscommandant. Binnen het Cybercommando wordt deze functie ingevuld door de drie unit commanders (eenheidscommandanten), zijnde de chef CSCU, de chef DCOU en de chef DICU, alsook door de twee directeurs voor de overblijvende elementen binnen het Cybercommando.[43] Indien een tussenkomst boven het niveau van de korpscommandant noodzakelijk is, wordt de Cybercommandant en ten slotte ook de Chef ADIV betrokken in een tuchtprocedure;[44]

- Voor de medewerkers is er interne mobiliteit mogelijk tussen de ADIV en het Cybercommando (in beide richtingen);[45]

- De Chef ADIV beschikt over meerdere sturingsinstrumenten tegenover het Cybercommando:

  — Op individueel niveau: zie bovenstaande bevoegdheden van de Chef ADIV op vlak van tucht en evaluatie.
  — De Chef ADIV beschikt over volgende andere sturingsinstrumenten[46]:
    - Het (meerjaarlijkse) Stuurplan van de ADIV waarin een deel omtrent het Cybercommando is opgenomen;
    - Net zoals aan de andere diensten binnen de ADIV, geeft de Chef ADIV via jaarlijkse objectieven richtlijnen aan het Cybercommando;
    - De (jaarlijkse) lijsten van zogenaamde 'speciale methoden' (o.m. interceptie van buitenlandse communicatie) worden voorgelegd aan de Chef ADIV waarbij hij punctuele instructies kan geven;
    - Op tweewekelijkse basis houdt de Chef ADIV een bilateraal overleg met de Cybercommandant met als focus de synchronisatie tussen het Cybercommando onder de ADIV en de Cybermacht;
    - Op tweewekelijkse basis houdt de Chef ADIV een overleg met zijn

40 Nota van ADIV gericht aan Comité R/I nr. 25-00159405 van 1 oktober 2025, p. 8.

41 Reglement DGHR-REG-EVAL-001 van 26 juli 2023 'De professionele evaluatie van de militair' (ed. 1).

42 Reglement DGHR-REG-CARDI-001 van 15 juli 2014 'Tucht' (ed. 1).

43 De taakomschrijving van vernoemde diensten komt in een volgend onderdeel aan bod.

44 Nota van ADIV gericht aan Comité R/I nr. 25-00159405 van 1 oktober 2025, p. 9 en Reglement DGHR-REG-CARDI-001, p. 25.

45 Nota van ADIV gericht aan Comité R/I nr. 25-00159405 van 1 oktober 2025, p. 8.

46 Nota van ADIV gericht aan Comité R/I nr. 25-00159405 van 1 oktober 2025, pp. 3, 7, 10 en 11.

Commando – waarbij o.m. de Cybercommandant en de twee directeur binnen het Cybercommando aanwezig zijn – waarbij de Chef ADIV de mogelijkheid heeft zijn instructies te geven aan de betrokken diensten onder zijn gezag, waaronder dus het Cybercommando;

- Eveneens heeft de Chef ADIV een tweewekelijks bilateraal overleg met onder meer de Directeur Cyber Operaties, de Directeur Cyber Development & Readiness, alsook de Directeur Inlichtingen en de Directeur Veiligheid;
- De Chef ADIV krijgt *ad hoc* briefings bij de start van operaties alsook frequent update briefings over lopende operaties, waar de cyber operaties in opdracht van het Cybercommando deel van uitmaken, waarbij hij de mogelijkheid heeft punctuele instructies te geven;
- De binnen de ADIV gebruikte tools voor het '*staffen*' van dossiers voorzien in een hiërarchisch te volgen structuur, waarbij de Chef ADIV als hoogste autoriteit hernomen is. Dit geeft de Cybercommandant de mogelijkheid zijn standpunt te communiceren aan de Chef ADIV die finaal de beslissing neemt;
- Bij een conflict van beschikbare cybercapaciteit tussen enerzijds informatieverzoeken van de ADIV en anderzijds informatieverzoeken van derden (*i.c.* de federale politie, de VSSE) dient de Chef ADIV de finale beslissing te nemen.

— Het Cybercommando is gehuisvest in het blokkencomplex van de ADIV (met dezelfde toegangscontrole);
— Cyber Intel is als platform geïntegreerd in het 'collection management' van de ADIV;
— Het personeel van het Cybercommando neemt deel aan de korpsmaaltijd van de ADIV.

5.
BUDGETTAIRE SITUATIE

38. Uit het antwoord van de ADIV op de door het Comité gestelde vragen, kan besloten worden dat de budgetstructuur van Defensie, de ADIV en de Cybereenheid op heden geen probleem vormen voor de inkapseling van het Cybercommando binnen de ADIV. Daarnaast rees bij het Comité de vraag naar de actuele budgettaire situatie van de militaire cybercapaciteit, en of dit afdoende is om tegemoet te komen aan de vele verwachtingen van de betrokken politieke overheden, militaire en civiele stakeholders.

39. De beslissing van de NAVO in 2016 tijdens de Warsaw Summit om – naast land, lucht en zee – cyberspace als apart operatiedomein te erkennen[47], rechtvaardigt onverkort de beslissing van de regering om de Cybermacht als aparte strijdkracht reglementair op te richten en om het Cybercommando als apart juridisch onderdeel van de ADIV in te richten. Uit dergelijke beslissing vloeit logischerwijs de verantwoordelijkheid in hoofde van de regering en het ministerie van Landsverdediging om ter zake afdoende mensen en financiële en materiële middelen ter beschikking te stellen, om op deze wijze de militaire cybercapaciteit gedegen uit te bouwen en ten dienste te stellen van de nationale veiligheid en de Belgische internationale engagementen.

5.1. ALGEMEEN[48]

40. In zijn antwoord aan het Comité stelt de ADIV: "Het toegekende budget wordt binnen het Ministerie van Defensie verdeeld over de verschillende organen en onderafdelingen waaronder zowel de ADIV alsook de verschillende machten: Landmacht, Luchtmacht, Marine, Medische Dienst en sinds 21 juli 2025 ook de Cyber Force." Verder wordt gesteld: "Cyber Command ontvangt een vast deel van het defensiebudget, dat intern wordt verdeeld volgens strategische en operationele noden."

41. Op de vraag van het Comité wie er beslist in geval van conflict bij het beheer van de beschikbare capaciteit van Cyber Command ten behoeve van, enerzijds, de opdrachten van ADIV en, anderzijds, de opdrachten van Cyber Force, antwoordt de ADIV:

    — "Als hoofd van Cyber Command heeft de Cyber Commander een hiërarchische lijn via de Chef ADIV, rechtstreeks naar de minister. Anderzijds heeft de Cyber Force

47 In 2019 erkende de NAVO de ruimte als vijfde operatiedomein.

48 Nota van ADIV gericht aan Comité R/I nr. 25-00159405 van 1 oktober 2025, pp. 5, 6 en 12.

Commander een hiërarchische lijn via de CHOD naar de minister. In theorie zal het dus aan deze laatste zijn om een dergelijke beslissing te nemen."

— En "In de praktijk behoren alle middelen op dit moment toe aan de ADIV, dus is het hoofd van de ADIV die beslist over de prioriteiten. Het doel is om de bestaande interne processen binnen Defensie te verfijnen die bepalen hoe capaciteiten worden geïmplementeerd in dienst van de ADIV en/of de Cyber Force en op welke criteria de prioriteiten moeten worden gebaseerd."

42. Zowel in het schriftelijk antwoord van de ADIV als in de mondelinge interviews van de Cybercommandant werd aan het Comité meegedeeld dat het de bedoeling is om personeelsleden aan te werven binnen de Cybermacht die tewerkgesteld zullen zijn bij de andere machten. In het verslag aan de Koning bij het KB van 30 juni 2025 wordt dit als volgt verwoord: *"De cybermacht, behorende tot de strijdkrachten, stuurt coherent gedecentraliseerde capacitaire modules aan die in staat zijn om militaire opdrachten uit te voeren*."

5.2. BUDGET IN CIJFERS

43. De ADIV heeft geen specifiek toegekend budget (personeelskredieten, werkingskredieten, investeringskredieten). De budgetten van de ADIV zijn geventileerd doorheen de begroting van Defensie in volgende domeinen: personeel, operaties & training, investerings- en werkingskredieten in het kader van de *material resources*, kredieten in het kader van de vorming, en residuaire functioneringskredieten.

44. Cijfergegevens over de budgetten van de ADIV, Cybercommando en Cybermacht werden als VERTROUWELIJK Wet 11.12.1998 geclassificeerd.

6.
EXTERNE ORGANISATIE VAN DE CYBEREENHEID

6.1. CYBERCOMMANDO *VS.* CYBERMACHT

45. Krachtens het Koninklijk besluit dat de algemene structuur van het ministerie van Landsverdediging bepaalt, bestaat binnen de ADIV een *Cybercommando* (Cyber Command) dat optreedt in het domein van cyberspace en dat de opdrachten uitvoert die bepaald zijn in artikel 11 van de Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.[49] Het Cybercommando staat onder leiding van de Cybercommandant.[50]

46. De ADIV in zijn geheel bestaat uit een Algemeen Commando (Comdo) – samengesteld uit: de Chef ADIV (C), de adjunct-chef ADIV (DCOM), de hoofdcommissaris (HCC) en de adjunct-hoofdcommissaris (HCC Adj) – alsook uit (de directeurs van) de directie Inlichtingen (Dir Rens), de directie Veiligheid (Dir S), de directie Plans & Policy (Dir P&P) en de directie Steun (Dir Sp). Naast een Algemeen Commando is er een Cybercommando, geleid door de Cyber Commander (CyC) en bestaande uit de directie Cyber Operations (Dir Cy Ops) en de directie Cyber Development & Readiness (Dir Cy D&R).

47. Tijdens een (tweewekelijkse) commandomeeting – *de facto* het directiecomité van de ADIV – zit de Chef ADIV samen met zijn adjunct, de hoofdcommissaris en de adjunct-hoofdcommissaris, de Cybercommandant alsook de directeurs van genoemde directies.[51]

48. Het Cybercommando moet onderscheiden worden van de *Cybermacht* (Cyber Force). Dit is een van de vijf machten (strijdkrachten) binnen de Belgische Krijgsmacht.[52] Net zoals de andere machten staat de Cybermacht onder een eigen commandant.[53] Van betekenis is dat

---

49 Cf. art. 42, eerste lid KB van 30 juni 2025 tot bepaling van de algemene structuur van het Ministerie van Landsverdediging en van de bevoegdheden van bepaalde autoriteiten (*BS* 15 juli 2025; hierna: KB Structuur Defensie).

50 Art. 42, tweede lid, eerste zin KB Structuur Defensie.

51 Nota van ADIV gericht aan Comité R/I nr. 25-00159405 van 1 oktober 2025, pp. 2 en 10.

52 Naast de Landmacht, Luchtmacht, Marine en Medische dienst (*cf.* art. 1, eerste lid, 5° KB Structuur Defensie).

53 Art. 37, tweede zin KB Structuur Defensie.

de commandant van het Cybercommando tevens de commandant van de Cybermacht is.[54] In de Belgische krijgsmacht wordt het ambt van hoofd van het cyber-uitvoeringsorgaan van de militaire inlichtingen- en veiligheidsdienst en het ambt van hoofd van de macht bevoegd voor cyberspace aldus in één persoon verenigd.

49. Vanuit juridisch oogpunt zijn het Cybercommando en de Cybermacht twee afzonderlijke entiteiten binnen de Krijgsmacht. Vanuit organisatorisch vlak is dit geenszins het geval. Er is één hiërarchische structuur, met aan het hoofd één leidinggevende, die zowel de hoedanigheid van uitvoeringsorgaan binnen de militaire inlichtingen- en veiligheidsdienst inneemt alsook een van de strijdkrachten en die alle betrokken opdrachten uitoefent. Ook binnen deze eenheid bestaan er geen afzonderlijke afdelingen belast met de opdrachten van de ADIV dan wel met de opdrachten van de Cybermacht. Er is één organisatie waarbinnen alle personeelsleden, desgevallend, ten dienste (moeten) staan van beide hoedanigheden.

50. In de praktijk leidt deze dubbele hoedanigheid soms tot verwarring. Indicatief op dat vlak is dat zelfs op de website van het ministerie van Landverdediging bij de uitleg over de Cybermacht wordt gesteld dat "*Cyber Force is part of ACOS IS*".[55] Dit klopt echter geenszins. Cyber Force is immers een van de vijf strijdkrachten en ACOS IS een van de vier stafdepartementen.[56] Juist was geweest dat "*Cyber Command is part of ADIV/SGRS*".

51. De dubbele hoedanigheid van de cybercommandant heeft gevolgen zowel op vlak van de geldende gezagsstructuren ten aanzien van de eenheid als op vlak van de taakuitvoering en het hierbij toepasselijke wettelijk kader. Treedt de eenheid op als uitvoeringsorgaan van de ADIV, valt deze onder de rechtstreekse hiërarchie van de Chef ADIV, die op zijn beurt onder het rechtstreekse gezag van de minister van Defensie valt voor wat betreft de uitvoering van de inlichtingen- en veiligheidsopdrachten.[57] Handelt de eenheid als Cybermacht, dan staat ze onder het rechtstreekse gezag van de Chef Defensie.[58] Afhankelijk van de hoedanigheid waarin opgetreden wordt, zijn er derhalve andere gezagslijnen voor de Cybereenheid en bijgevolg andere gezagsoverheden waaraan de cybercommandant verantwoording moet afleggen.

---

54 Art. 42, tweede lid, tweede zin KB Structuur Defensie.

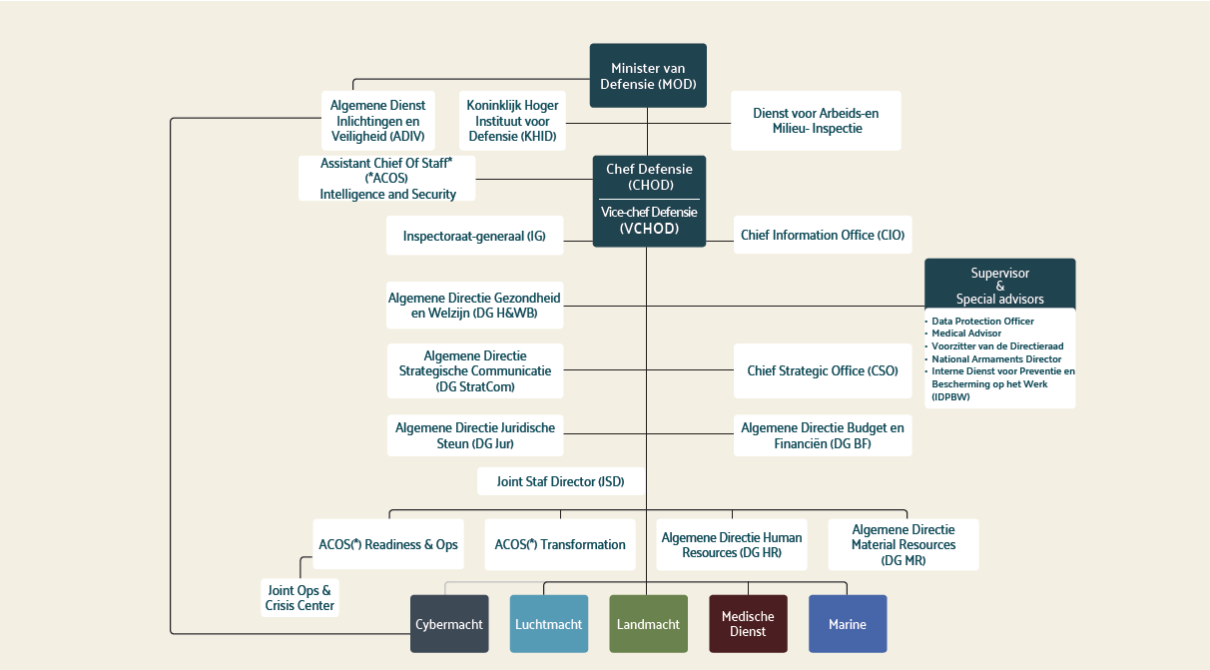
55 www.mil.be/nl/over-defensie/ (consultatie op 20 oktober 2025).

56 Voor de vergissingen kan begrip getoond worden. In de praktijk bestaat organisatorisch immers geen verschil tussen de Cybermacht en het Cybercommando enerzijds en tussen ADIV en ACOS IS anderzijds.

57 Vermeldenswaard is dat de Chef ADIV tevens de hoedanigheid heeft van onderstafchef inlichtingen en veiligheid (ACOS IS) en vanuit deze hoedanigheid onder de rechtstreekse hiërarchie van de Chef Defensie valt.

58 *Cf.* art. 6, §1, eerste lid, *in limine* en 4° en art. 7, §3, tweede lid KB Structuur Defensie.

Schema Ministerie van Landsverdediging[59]



52. Dit geheel maakt duidelijk dat het wettelijk kader en de hoedanigheid van waaruit de Cybereenheid zijn activiteiten en werkzaamheden ontplooit, betekenis heeft. De afbakening van de opdrachten tussen het Cybercommando (m.n. de ADIV-opdrachten in cyberspace) en de Cybermacht, bepalen de in een concreet geval toepasselijke gezagslijnen tegenover de eenheid en de hiermee gepaard gaande verantwoordelijkheid in hoofde van de Chef ADIV, van de Chef Defensie en van de minister van Defensie.

53. Als organisatie heeft de eenheid twee categorieën van opdrachten: de activiteiten waar de eenheid optreedt als onderdeel van de ADIV en dus als uitvoeringsorgaan van de militaire inlichtingen- en veiligheidsdienst (hierna: de Cybercommando-opdrachten) en de activiteiten waar opgetreden wordt als Cybermacht en dus als een van de Belgische strijdkrachten (de Cybermacht-opdrachten). De Cybercommando-opdrachten worden geregeld door de Inlichtingenwet[60] en de Classificatiewet.[61] De Cybermacht-opdrachten worden dan weer geregeld door het KB dat het ministerie van Landsverdediging inricht (het zgn. KB Structuur Defensie) alsook door de Wet Aanwending en Paraatstelling Defensie en zijn uitvoeringsbesluit.[62] Voor beide soorten opdrachten moet in belangrijke

---

59 Bron: https://www.mil.be/nl/over-defensie/#

60 Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten (W.I&V).

61 Wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, de veiligheidsadviezen en de publiek gereguleerde dienst (W.C&V).

62 Wet van 20 mei 1994 betreffende de perioden en standen van de militairen van het reservekader alsook betreffende de aanwending en de paraatstelling van de Krijgsmacht (*BS* 21 juni 1994; hierna:

mate teruggegrepen worden naar NAVO-regelgeving, beleids- en doctrinale documenten[63] voor een nadere toelichting en verduidelijking.[64, 65]

54. Er zijn gegronde redenen om het Cybercommando te integreren binnen de ADIV. Als onderdeel van de militaire inlichtingen- en veiligheidsdienst kan de eenheid namelijk voluit gebruik maken van de ruime aan de ADIV wettelijk toegekende taakstelling en bevoegdheden. Vooral de mogelijkheden op vlak van bijzondere inlichtingenmethoden (bv. *legal hackings*, opvragen metadata) en SIGINT-activiteiten (bijv. gebruik van het vorderingsrecht tegenover telecomoperatoren binnen het intercepteren van buitenlandse communicatie) zijn nodig voor een gedegen digitaal inlichtingenwerk. Hiernavolgend worden de ADIV-opdrachten opgesomd waarin het Cybercommando een rol te vervullen heeft.

6.2. CYBERCOMMANDO-OPDRACHTEN

6.2.1. Inlichtingenopdrachten, inclusief in cyberspace

55. De ADIV heeft volgende inlichtingenopdrachten, inclusief in cyberspace:

(a) het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op elke activiteit die de onschendbaarheid van het nationaal grondgebied of de bevolking, de militaire defensieplannen, het wetenschappelijk en economisch potentieel m.b.t. de actoren verbonden met defensie, de vervulling van de opdrachten van de strijdkrachten of de veiligheid van de Belgische onderdanen in het buitenland bedreigt of zou kunnen bedreigen,

---

Wet Aanwending en Paraatstelling Defensie) en het KB van 6 juli 1994 houdende bepaling van de vormen van operationele inzet, hulpverlening en militaire bijstand, en van de voorbereidingsactiviteiten met het oog op de aanwending van de krijgsmacht (*BS* 20 juli 1994; hierna: KB Aanwending en Paraatstelling Defensie).

63 De Allied Joint Publication (Doctrine) (AJP) van de NAVO is een verzameling publicaties die de basisprincipes en doctrine voor gezamenlijke operaties vastleggen. De kernonderdelen zijn AJP-1 die de overkoepelende doctrine voor alle gezamenlijke operaties bevat. Het schetst de strategische context en basisprincipes van gezamenlijke operaties. En AJP-6, die de doctrine voor operaties op operationeel niveau beschrijft, inclusief de coördinatie tussen verschillende entiteiten.

64 Het NAVO-document AJP-2 (Allied Joint Doctrine for Intelligence, Counterintelligence and Security) is de hoeksteen van de NAVO-doctrine voor inlichtingen. Het biedt de fundamentele principes en richtlijnen voor inlichtingenondersteuning bij gezamenlijke operaties. In diverse subsidiaire publicaties worden meer details gegeven, bijvoorbeeld (1) op niveau Joint Functional Doctrine: AJP-2.1 Intelligence Procedures, AJP-2.2 CI & Security Procedures, AJP-2.3 HUMINT, AJP-2.4 SIGINT, AJP-2.7 JISR, en (2) op een nog gedetailleerder niveau (Level-3-Intel Publications): AInP-16 IRM&CM, AInp-10 Technical Exploitation, AInP-5 HUMINT TTPs, AInP-10 Technical Exploitation, AInP-14 JISR TTPs.

65 Andere relevante AJP-documenten zijn o.m.: AJP-10.1 (Information Operations) en AJP-3.20 (Cyberspace Operations), AJP-3.6(B) (Electronic Warfare).

en er de bevoegde ministers onverwijld over in te lichten.[66]

Het bevoegdheidsbereik van de ADIV binnen dit onderdeel van de inlichtingenopdracht laat zich bepalen door de te beschermen belangen in combinatie met de te beheersen dreigingen. De vraag of de militaire inlichtingendienst bevoegd is in een concreet geval dient m.a.w. beantwoord te worden door na te gaan of er een aanknopingspunt te vinden is met minstens één belang alsook met minstens één dreiging.

(b) het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op de factoren die de nationale en internationale veiligheid beïnvloeden of kunnen beïnvloeden in die mate dat de Krijgsmacht betrokken is of zou kunnen worden om inlichtingensteun te bieden aan hun lopende of eventuele komende operaties, en er de bevoegde ministers onverwijld over in te lichten.[67]

Het opzet van dit deel van de inlichtingenopdracht, aangeduid als de inlichtingensteun aan militaire operaties, bestaat in het beschermen van de troepen en in het ondersteunen van de eigenlijke operaties[68] via het verzamelen en verwerken van gegevens over vreemde mogendheden, vijandige of potentieel vijandige (elementen van) reguliere strijdkrachten, irregulier strijdende partijen en over gebieden en omstandigheden waarin wordt opgetreden of in de toekomst mogelijk moet worden opgetreden.[69]

(c) het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op de activiteiten van buitenlandse inlichtingendiensten op Belgisch grondgebied.[70]

De ADIV is, net zoals overigens de Veiligheid van de Staat (VSSE), belast met het toezichthouden op de diverse soorten activiteiten van buitenlandse inlichtingendiensten op Belgisch grondgebied. De wetgever verplicht beide diensten om ter zake een samenwerkingsakkoord af te sluiten op grond van richtlijnen van de Nationale Veiligheidsraad (NVR).[71] In het Nationaal Strategisch Inlichtingenplan (NSIP) van 2022 werd, op gezamenlijk voorstel van de VSSE en de ADIV, door de NVR beslist dat acties van buitenlandse inlichtingendiensten tegen de Belgische belangen op transversale wijze zal worden benaderd, ongeacht de oorsprong van de dreiging (militair of burgerlijk) of het

---

66 Art. 11, §1, 1°, tweede onderdeel, en §2, 1° tot 4° W.I&V.

67 Art. 11, §1, 1°, eerste onderdeel W.I&V.

68 *Parl. St.* Kamer 2015-2016, nr. 54-2043/001, 8, pp. 31 tot 33.

69 Afgeleid van de NAVO-definitie van het begrip 'intelligence', zijnde: *"The product resulting from the processing of information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. The term is also applied to the activity which results in the product and to the organisations engaged in such activity."* AAP-6 (ed. 2009) "NATO Glossary of Terms and Definitions".

70 Art. 11, §1, 5° W.I&V.

71 Art. 20, §4 W.I&V.

doelwit (militair of burgerlijk).[72]

6.2.2. Veiligheidsopdrachten, inclusief cybersecurity

56. De ADIV is door de wetgever ook belast met meerdere **veiligheidsopdrachten, inclusief cybersecurity**:

(a) de handhaving van de militaire veiligheid:

- de veiligheid van het personeel, de installaties, wapens en wapensystemen, munitie, uitrusting, plannen, geschriften, documenten, informatica- en verbindingssystemen of andere voorwerpen van Defensie;[73]
- de veiligheidssteun aan militaire operaties.[74]

Van belang in dit kader is het van de ADIV afkomstige Reglement IF5 "Onderrichting van de Militaire Veiligheid" van 26 september 2023. Dit reglement omvat alle richtlijnen rond de militaire veiligheid binnen het ministerie van Landsverdediging, inclusief de richtlijnen m.b.t. cyber/information security.

(b) de bescherming van het militaire geheim:

- het handhaven van het geheim dat verbonden is met de militaire installaties, wapens en wapensystemen, munitie, uitrusting, plannen, geschriften, documenten of andere voorwerpen, de militaire inlichtingen en verbindingen, alsook de informatica- en verbindingssystemen van of beheert door het ministerie van Landsverdediging.[75]

Het verslag aan de Koning bij het KB Structuur Defensie stelt dat Cybercommando een rol te vervullen heeft binnen het *"verlenen van de nodige accreditaties en uitvoeren van controlebezoeken om het geheim te beschermen van de militaire informatica- en communicatiesystemen of deze die de Minister van Defensie beheert overeenkomstig het artikel 11, § 1, 3°, van dezelfde wet"*.[76]

---

72 Nationaal Strategisch Inlichtingenplan 2022 (VERTROUWELIJK Wet 11.12.1998), toelating tot declassificatie.

73 Art. 11, §1, 2°, eerste onderdeel W.I&V.

74 Art. 11, §1, 2°, eerste onderdeel W.I&V, vgl. art. 21, 1° KB Structuur Defensie (*a contrario*).

75 Art. 11, §1, 3° W.I&V. De toevoeging van "de wapensystemen" gebeurt *ad analogiam* met art. 11, §1, 2°, eerste onderdeel W.I&V.

76 Het Comité stelt vast dat het verslag aan de Koning bij het KB van 30 juni 2025, vreemd genoeg, niet in het Staatsblad werd gepubliceerd. Betrokken tekst werd evenwel integraal aan het Comité overgemaakt alsook veelvuldig geciteerd in het antwoord van de ADIV op de door het Comité gestelde vragen (zie: nota van ADIV gericht aan Comité R/I nr. 25-00159405 van 1 oktober 2025).

(c) het optreden als de bevoegde veiligheidsoverheid voor wat betreft defensie, middels:

- het afleveren van veiligheidsmachtigingen en van goedkeuringen van fysieke installaties, communicatie- en informatiesystemen en cryptografische producten, alsook het uitvoeren van controles en inspecties[77];
- het verstrekken van veiligheidsadviezen voor (kandidaat-) personeelsleden van het ministerie van Landsverdediging.[78]

Het Cybercommando heeft wettelijk geen bevoegdheden binnen de eigenlijke aflevering van vernoemde machtigingen, goedkeuringen of adviezen. Het kan wel worden ingeschakeld binnen de hieraan voorafgaande onderzoeken of verificaties alsook binnen het uitvoeren van voorafgaande of navolgende controles of inspecties.

(d) het uitvoeren van veiligheidsscreenings:

- veiligheidsonderzoeken, voorafgaand aan de beoordeling over de aflevering van een veiligheidsmachtiging[79]);
- veiligheidsverificaties, voorafgaand aan de verstrekking van een veiligheidsadvies (bv. voor kandidaat-militairen).[80]

6.2.3. Specifieke cyberopdrachten

57. Tot slot is de ADIV, naast de uitvoering van bovenstaande inlichtingen- en veiligheidsopdrachten in cyberspace (cyberintelligence en cybersecurity), belast met **specifieke cyberopdrachten**:

(a) het neutraliseren, binnen de zorg voor het behoud van de militaire veiligheid, van een cyberaanval op wapensystemen, militaire informatica- en verbindingssystemen of systemen die de minister van Landsverdediging beheert en er de daders van identificeren, onverminderd het recht onmiddellijk met een eigen cyberaanval te reageren overeenkomstig de bepalingen van het internationaal recht.[81]

Het verslag aan de Koning bij het KB Structuur Defensie stelt expliciet dat Cybercommando een rol te vervullen heeft binnen *'de identificatie, de verstoring, de neutralisatie van en in laatste instantie de tegenaanval tegen de cyberdreiging, om de bescherming van de informaticanetwerken en de wapensystemen die de Minister van Defensie beheert te verzekeren alsook andere netwerken in het kader van een nationale cybersecurity crisis, overeenkomstig de artikelen 11, § 1, 2°, 2°/1 en 44/1 van dezelfde wet*'. Uit het recente

77 Artt. 1*bis*, 14°, c), en 1*quinquies*, tweede lid WCV.

78 Art. 40 ev. WCV.

79 Art. 11, §1, 4° W.I&V *juncto* artt. 1*bis*, 9° en 10°, en art. 18, eerste lid WCV.

80 Art. 11, §1 6° W.I&V *juncto* artt. 23° en 24°, en art. 32, §1, 2° WCV.

81 Art. 11, §1, 2°, tweede onderdeel W.I&V.

karakter van het betrokken KB – waarin zowel het Cybercommando als de Cybermacht juridisch worden opgericht – kan afgeleid worden dat de minister van Defensie deze toewijzing specifiek aan het Cybercommando toewijst.

Deze opdracht kadert zowel binnen de veiligheidsopdracht (m.n. het neutraliseren van een cyberaanval) als binnen de inlichtingenopdracht (m.n. het identificeren van de daders van de cyberaanval). De wetgever heeft het noodzakelijk gevonden om de ADIV het recht te geven om op een cyberaanval een tegenaanval uit te voeren met als oogmerk het zorgen voor het behoud van de militaire veiligheid.[82] Zoals de wettelijke term zelf aangeeft, betreft het een "tegen"-aanval. De aard van tegenaanval brengt met zich mee dat de door de ADIV uitgevoerde cyberactie punctueel en reactief is alsook temporeel begrensd wat betreft het aanvangsmoment van de tegenactie. Als tegenaanval betreft het ook een activiteit die de verderzetting is van het neutraliseren van de initiële aanval en het identificeren van de dader ervan. De bevoegdheid tot tegenaanval is duidelijk een *corollarium* van de inlichtingen- en veiligheidsactiviteiten van de ADIV in cyberspace. Vanuit het oogpunt van de offensieve cybermogelijkheden van Defensie betreft de mogelijkheid tot tegenaanval overigens slechts een beperkt aspect. De eigenlijke offensieve cyberopdrachten en -bevoegdheden behoren bovendien niet de ADIV toe, maar de Cybermacht (*infra*).

(b) het neutraliseren, in het kader van een nationale cybersecurity crisis, van een cyberaanval op informatica- en verbindingssystemen niet beheerd door de minister van Landsverdediging en er de daders van identificeren, onverminderd het recht onmiddellijk met een eigen cyberaanval te reageren overeenkomstig de bepalingen van het internationaal recht.[83]

Een nationale cybersecurity-crisis is elke cybersecurity-gebeurtenis die wegens haar aard of gevolgen: (1) de vitale belangen van het land of de essentiële behoeften van de bevolking bedreigt (m.n. de openbare veiligheid, rust en gezondheid; het wetenschappelijk en economische potentieel van het land; de nationale soevereiniteit en de instellingen opgericht bij de Grondwet en de wetten; en de integriteit van het nationaal grondgebied[84]), (2) een dringende besluitvorming vereist en (3) de gecoördineerde inzet van verscheidene departementen en organismen vergt.[85] De activiteiten van de ADIV – en dus ook van het Cybercommando - binnen dit kader moeten aanzien worden als steun van Defensie aan de Natie.[86]

82 Deze bevoegdheid werd toegekend via art. 4 BIM-Wet van 4 februari 2010.

83 Art. 11, §1, 2°/1 W.I&V.

84 *Parl. St.* Kamer 2021-2022, nr. 55-2706/001, 13.

85 Art. 11, §2, 5° W.I&V.

86 *Parl. St.* Kamer 2021-2022, nr. 55-2706/001, pp. 11 en 14.

6.2.4. (Onderzoeks-)bevoegdheden

58. De ADIV heeft een ruim gamma aan **(onderzoeks)bevoegdheden** ter beschikking om haar opdrachten uit te voeren. Naast algemene onderzoeksbevoegdheden (de zgn. gewone, specifieke en uitzonderlijke inlichtingenmethoden), die overeenstemmen met deze van de VSSE, heeft de wetgever de ADIV ook specifieke bevoegdheden toegekend om welbepaalde informatie in te winnen. Zo kan de ADIV, in het kader van de uitvoering van zijn opdrachten, elke vorm van communicatie uitgezonden of ontvangen in het buitenland opsporen, onderscheppen, afluisteren en er kennis van nemen alsook opnemen (art. 44 W.I&V). Ook beschikt de ADIV over de mogelijkheid om een informaticasysteem dat zich in het buitenland bevindt binnen te dringen (art. 44/1 W.I&V) en om beelden in het buitenland op te nemen (art. 44/2 W.I&V).[87] In de praktijk worden deze ook wel de *speciale* methoden voor het verzamelen van gegevens genoemd.

59. Zoals eerder gesteld, doet dit geheel het Comité besluiten dat het cyberinlichtingenwerk verricht door de aan de Krijgsmacht toegewezen cybercapaciteit, de cyberveiligheid van het ministerie van Landsverdediging en de operationele uitvoering van bepaalde cyberoperaties niet kunnen plaatsvinden zonder het wettelijke kader van de ADIV.[88]

60. Dit wettelijk kader zorgt er tegelijkertijd voor dat er ernstige wettelijke beperkingen zijn aan welke opdrachten en bevoegdheden de regering reglementair aan de Cybermacht kan toewijzen. Een toewijzing die volgens het Comité wel noodzakelijk is. De onduidelijkheid in afbakening tussen de opdrachten van het Cybercommando en de Cybermacht, en de verwarring die hieruit voortvloeit, creëert onduidelijkheid over de afbakening van het gezag en de bijhorende verantwoordelijkheden van de minister van Defensie en de Chef Defensie als betrokken gezagsoverheden.

61. Ook zou een reglementaire bepaling dienen te verduidelijken welke instructies de Onderstafchef paraatstelling en operaties (ACOS R&O) kan toevertrouwen aan de Cybermacht. Krachtens artikel 15, 3° van het KB Structuur Defensie heeft de ACOS Ops immers het operationeel commando over de eenheden van de strijdkrachten, en dus ook over de Cybermacht. Dit betekent dat "*een operationele inzet van capaciteiten voor de uitvoering van opdrachten van de strijdkrachten gebeurt onder leiding van het stafdepartement Readiness & Operations en in wezen ook de Cyber Force Commander op dat moment geen rechtstreeks hiërarchisch gezag meer uitoefent. Hetzelfde geldt voor alle*

---

87 Deze drie onderzoeksbevoegdheden kunnen niet ingezet worden binnen een veiligheids-onderzoek.

88 In het bijzonder gaat het dan over wettelijke opdrachten van de ADIV (art. 11 W.I&V), de gewone en bijzondere inlichtingenmethoden (artt. 14 tot 18/17 W.I&V), de SIGINT-bevoegdheden (art. 44 tot 44/2 W.I&V) en de bevoegdheid inzake de doorgifte van inlichtingen (art. 19 W.I&V en de Classificatiewet). Voor wat betreft de operationele uitvoering van bepaalde cyberoperaties gaat het over de specifieke cyberopdrachten die wettelijk werden toegewezen aan de ADIV (art. 11, §§2° en 2°/1 W.&IV).

andere capaciteiten van de strijdkrachten (land, air & marine).”[89]

6.3. CYBERMACHT-OPDRACHTEN

62. Conform artikel 38 van het KB Structuur Defensie ”[zijn] [d]e commandanten van de machten […]” – en dus ook van de Cybermacht – ”specifiek verantwoordelijk voor de paraatstelling van hun respectieve capaciteiten, met het personeel, het materieel, de infrastructuur en de trainingsmiddelen die hun worden toegekend. Ze zijn verder ook verantwoordelijk voor de aanwending van hun respectieve capaciteiten, waarin de hun toegewezen intermachtencapaciteiten worden opgenomen, en dat ter ondersteuning van de paraatstelling van de Krijgsmacht.”

63. Het Comité stelt vast dat, net zoals dit het geval is bij de andere strijdkrachten, het KB Structuur Defensie noch de Wet Aanwending en Paraatstelling Defensie of zijn uitvoeringsbesluit een concrete opsomming bevat van de specifieke opdrachten van de Cybermacht. Enerzijds is dit begrijpelijk. Vernoemde wet en uitvoeringsbesluit bevatten reeds, in algemene termen, de diverse vormen van operationele inzet, hulpverlening en militaire bijstand, alsook de voorbereidingsactiviteiten met het oog op de aanwending van de Krijgsmacht. Verder is het ook de verantwoordelijkheid van de commandanten van de betrokken machten – en dus ook van de Cybercommandant – om dit verder uit te werken. Ad hoc en concreet wordt dit ook nader ingevuld onder leiding van het Stafdepartement paraatstelling en operaties. Zoals gezegd, beschikt de betrokken onderstafchef immers, voor het voeren van militaire operaties, over het operationeel commando over de eenheden van de machten[90]; en zodoende ook over de Cybermacht.

64. De Cybercommandant geeft o.m. volgende verdere invulling: «La Force Cyber s’inscrit dans la continuité de l’unité Cyber Command par le déploiement de cyber-combattants au sein des autres Forces. Ils allieront l’expertise cyber à la connaissance du métier et à la connaissance opérationnelle spécifique à chaque Force bénéficiant de l’appui cyber. Progressivement, les capacités opérationnelles terrestre, aérienne, marine et médicale seront renforcées pour assurer la protection, la défense, le renseignement et le combat dans le cyberspace selon les spécificités individuelles de ces Forces et services.».[91]

---

89 Nota van ADIV gericht aan Comité R/I nr. 25-00159405 van 1 oktober 2025, p. 15.

90 Art. 15, 3° KB Structuur Defensie.

91 Generaal-majoor Ciparisse, «Grille de lecture de la menace cybernétique à travers la mise en place de la Force Cyber belge», Wetenschap en technologie, 23 september 2025. *”De Cyber Force is een voortzetting van de Cyber Command-eenheid door de inzet van cyberstrijders binnen de andere strijdkrachten. Zij zullen cyberexpertise combineren met professionele kennis en operationele kennis die specifiek is voor elke strijdmacht die cyberondersteuning ontvangt. Geleidelijk aan zullen de operationele capaciteiten op land, in de lucht, op zee en in de medische sector worden versterkt om*

65. Tegelijkertijd kan niet om de vaststelling heen dat deze verdere invulling niet afdoende is, temeer omdat de Cybermacht niet volledig gelijkgesteld mag worden met de andere machten/strijdkrachten. De Cybermacht is de enige macht waarbij zijn commandant tevens de commandant is van een uitvoeringsorgaan van een ander onderdeel van de Krijgsmacht. In het licht van een duidelijke afbakening van de verantwoordelijkheden van de Chef ADIV (rechtstreeks gezag over het Cybercommando) en de Chef Defensie (rechtstreeks gezag over de Cybermacht) dringt een duidelijke reglementaire taakomschrijving van de Cybermacht zich op (i.c. in het KB Structuur Defensie). Het Comité herinnert er in dit kader aan dat ook de Onderstafchef inlichtingen en veiligheid een duidelijke taakomschrijving in het betrokken KB kreeg net omdat de Chef ADIV tevens de hoedanigheid van Onderstafchef inlichtingen en veiligheid heeft en indachtig de mogelijk taakverwarring tussen ADIV en ACOS IS voor wat betreft de inlichtingen- en veiligheidssteun aan militaire operaties (art. 21, 1° KB Structuur Defensie). Niet in het minst noodzaken de verantwoordelijkheden van de Chef Defensie en van de minister van Defensie een duidelijke taakafbakening tussen beide.

66. Voor de toepassing van de personeelsstatuten, voor de werving en om redenen van vertegenwoordiging in bepaalde organen behoort elk militair personeelslid, naar gelang het geval, tot de Landmacht, de Luchtmacht, de Marine, de Medische dienst of tot het burgerpersoneel.[92] Elk militair personeelslid wordt aldus verbonden met een bepaalde macht. Voor de werking van vernoemde regelingen bestaat evenwel geen categorie Cybermacht. Een dergelijke keuze is legaal en legitiem, maar heeft logischerwijs eveneens gevolgen voor de positie en de organisatie van de Cybermacht binnen Defensie.

67. Hoewel het KB Structuur Defensie geen specifieke taakomschrijving van de Cybermacht omvat, bevat het wel de diverse bevoegdheden waarmee de Cybercommandant, als commandant van een strijdkracht, wordt belast en die generiek zijn voor alle commandanten op strategisch niveau binnen de Krijgsmacht.[93]

68. Binnen zijn bevoegdheidsdomein van Cybermacht is de Cybercommandant zodoende belast met volgende generieke taken:

    - raadgever van de Chef Defensie; daartoe bezorgen zij hem gegevens en informatie die hem toelaten een coherent defensiebeleid voor te stellen aan de minister van Defensie;
    - het ontwikkelen, in het kader van het vastgelegde beleid, van de planning, de programmering ten behoeve van de paraatstelling en de algemene

---

bescherming, verdediging, inlichtingen en gevechten in cyberspace te waarborgen, afgestemd op de specifieke kenmerken van deze strijdkrachten en diensten." (vrije vertaling).

92 *Cf*. art. 1, derde lid KB Structuur Defensie.

93 Hiermee worden generieke bevoegdheden bedoeld die toegewezen zijn aan de Vicechef Defensie, de directeur Intermachtenstaf, de onderstafchefs, de directeurs-generaal, de andere commandanten van de machten en de inspecteur-generaal.

functioneringsrichtlijnen voor de Krijgsmacht, in samenspraak met de onderstafchefs, directeurs-generaal, commandanten van de andere machten en inspecteur-generaal.[94]

- het ondersteunen van de directeur Intermachtenstaf, onderstafchefs, directeurs-generaal, commandanten van de andere machten en de inspecteur-generaal bij het beheer van de kwaliteit en de risico's specifiek voor hun bevoegdheidsdomeinen;
- het afleggen van verantwoording aan de Chef Defensie over de maturiteit van zijn kwaliteits- en risicobeheersysteem specifiek voor zijn bevoegdheidsdomeinen in overeenstemming met het beleid en de doelstellingen van Defensie;
- het verstrekken aan de Vice-chef Defensie, de directeur Intermachtenstaf, de onderstafchefs, directeurs-generaal, de commandanten van de andere machten en de inspecteur-generaal van de gegevens en informatie die toelaten hun respectieve bevoegdheden uit te oefenen[95];
- het verzekeren van de productie, de verzameling en de uitbating van controle- en evaluatie-informatie met betrekking tot de processen en de beheersingsobjectieven[96] die tot zijn bevoegdheidsdomein behoren;
- het opstellen van de ontwerpakkoorden die tot zijn respectieve bevoegdheidsdomeinen behoren en het waken over de naleving van enerzijds de akkoorden die ten behoeve van of voor rekening van het departement zijn gesloten en anderzijds de door België geratificeerde internationale akkoorden.[97]

69. Binnen Cybermacht heeft de Cybercommandant volgende generieke taken:

- het uitvoeren van het beleid van de directeur Intermachtenstaf, de onderstafchefs, de directeurs-generaal, de commandanten van andere machten en de inspecteur-generaal, dat op zijn dienst van toepassing is;
- het integreren van het kwaliteits- en risicobeheer in de cyclus van planning, beheer en in de interne werking, voor al het beleid van toepassing op zijn dienst, overeenkomstig het beleid en de doelstellingen van het departement;
- het verzekeren van de productie, de verzameling en de uitbating van controle- en evaluatie-informatie ten aanzien van zijn dienst;

---

94 De onderstafchef inlichtingen en veiligheid doet dit na overleg met de directeur Intermachtenstaf, net zoals de onderstafchef paraatstelling en operaties, de onderstafchef transformatie, de directeur-generaal human resources, de directeur-generaal material resources en de andere commandanten van de machten.

95 Deze bepaling creëert een meldingsplicht in hoofde van ACOS IS ten aanzien van bepaalde commandanten binnen de Krijgsmacht, zelfs voor wat betreft informatie verwerkt in het kader van de inlichtingenopdrachten van de ADIV (*cf*. art. 10, §1, 5° KB Structuur Defensie *juncto* art. 10, 11 en 13, §1 W.I&V.

96 Zoals bedoeld in het KB van 15 mei 2022 betreffende de organisatiebeheersing binnen sommige diensten van de federale uitvoerende macht (*BS* 17 juni 2022).

97 Art. 10, §1 KB Structuur Defensie.

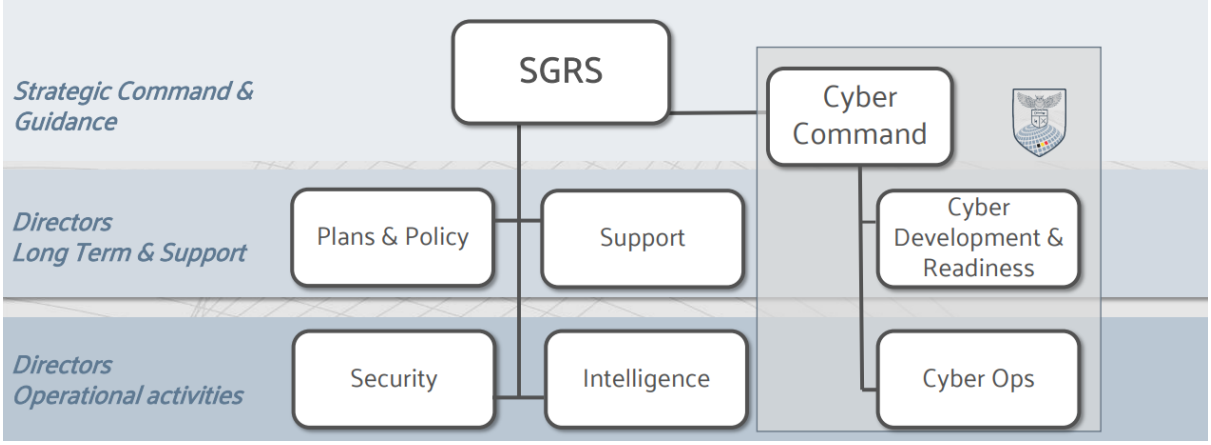
- het formuleren van adviezen en aanbevelingen over behoeften en toegekende middelen voor de uitvoering van zijn opdracht;
- het dragen van verantwoordelijkheid voor de personeels-, materiële en budgettaire middelen die aan hem zijn toegekend.[98]

70. Tot slot. Op de vraag van het Comité aan de ADIV wie er beslist in het geval van conflict bij het beheer van de beschikbare cybercapaciteit ten behoeve van, enerzijds, de opdrachten van ADIV en, anderzijds, van de opdrachten van de Cybermacht, antwoordde de dienst dat *"[i]n de praktijk […] alle middelen op dit moment [toebehoren] aan de ADIV, dus is het […] hoofd van de ADIV die beslist over de prioriteiten. Het doel is om de bestaande interne processen binnen Defensie te verfijnen die bepalen hoe capaciteiten worden geïmplementeerd in dienst van de ADIV en/of de Cyber Force en op welke criteria de prioriteiten moeten worden gebaseerd."*. Het Comité juicht dergelijke richtlijnen onverkort toe. Dit vermindert evenwel niets aan de nood om een reglementair kader te hebben die de taakomschrijving van de Cybermacht verduidelijkt, en die nodig is om te bepalen hoe de betrokken capaciteiten naar concrete activiteiten en taken verdeeld kunnen worden.

98 Art. 10, §2 KB Structuur Defensie.

7.
INTERNE ORGANISATIE VAN DE CYBEREENHEID

71. Het Cyber Command (CyCom) is in zijn geheel geïntegreerd binnen de Algemene Dienst Inlichting en Veiligheid (ADIV). Het overzicht van de structuur van het CyCom is gebaseerd op vijf briefings die het Vast Comité I op zijn vraag ontving van medewerkers van het CyCom in de maanden mei en juni 2025, evenals op een geclassificeerd document dat dateert van juni 2025.

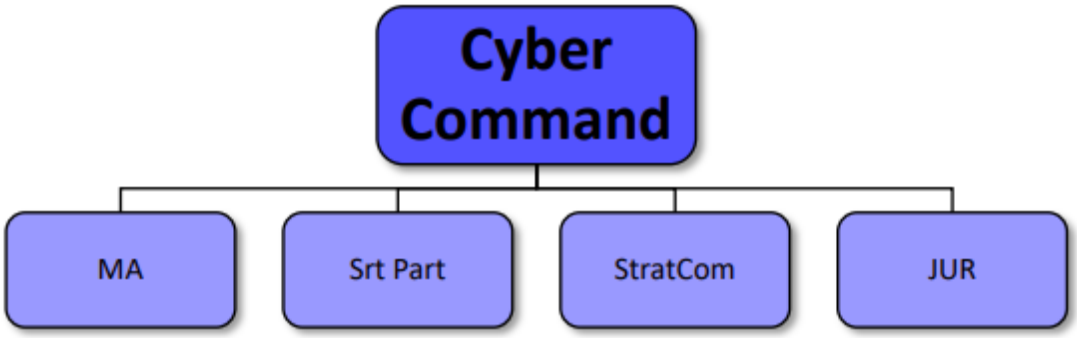


7.1. DE DIRECTIE INTELLIGENCE VAN DE ADIV

72. Binnen de structuur van het Cyber Command bevinden zich een aantal collecte- en analyseorganen. Deze collecteorganen geven uitvoering aan de informatiebehoeften van externe partners zoals de VSSE, maar uiteraard ook van andere onderdelen van de ADIV. Binnen de ADIV is het vooral vanuit de Directie Intelligence, dat deze informatiebehoeften worden geformuleerd, in de vorm van *Intelligence Collection Plans* (ICP).

7.2. HET COMMANDO VAN HET CYCOM

73. Het Commando van Cyber wordt uitgeoefend door de Cyber Commander (CyC). Hij wordt bij de uitoefening van zijn opdrachten bijgestaan door een Deputy (DCOM – cumulpost – Director Cyber Operations) en een Chief of Staff (COS - cumulpost – Director Cyber Development & Readiness). De ondersteuning van het Commando bestaat uit een militair assistent (MA), een particulier secretariaat (Part Srt), een juridische sectie (JUR) en een sectie Strategische communicatie (StratCom).[99]



7.2.1. De Commandant van het Cyber Command (CyC)

74. De Cyber Commander is verantwoordelijk voor de uitvoering van de opdrachten van de ADIV in de cyberspace. Hij is ook de commander van de Cybermacht (Cyber Force).

7.2.2. De Military Assistant

75. De Military Assistant (MA) staat de CyC bij, door het uitvoeren van synthesetaken en het bieden van zowel praktische als inhoudelijke ondersteuning. De MA ondersteunt de besluitname op het Commandoniveau.

7.2.3. Secretariaat (SrtPart)

76. Het Secretariaat beheert de IN/OUT-correspondentie van de CyC en kent een officieel nummer toe in Enhanced Document Tracker (EDT) voor de dienstnota's.

---

99 Deze paragraaf werd overgenomen uit de VERTROUWELIJK geclassificeerde nota '*Structuur 2.1 en bevoegdheden binnen de ADIV*'. Op verzoek van het Comité R/I ging de ADIV akkoord met de declassificatie hiervan.

7.2.4. StratCom

77. De sectie StratCom is verantwoordelijk, in nauwe coördinatie met de cel StratCom van het Algemeen Commando van de ADIV, voor het uitwerken van een cyber-gerichte communicatiestrategie, zowel intern als extern, met als doel enerzijds de informatiestromen te bevorderen en anderzijds het imago van de dienst te verbeteren.

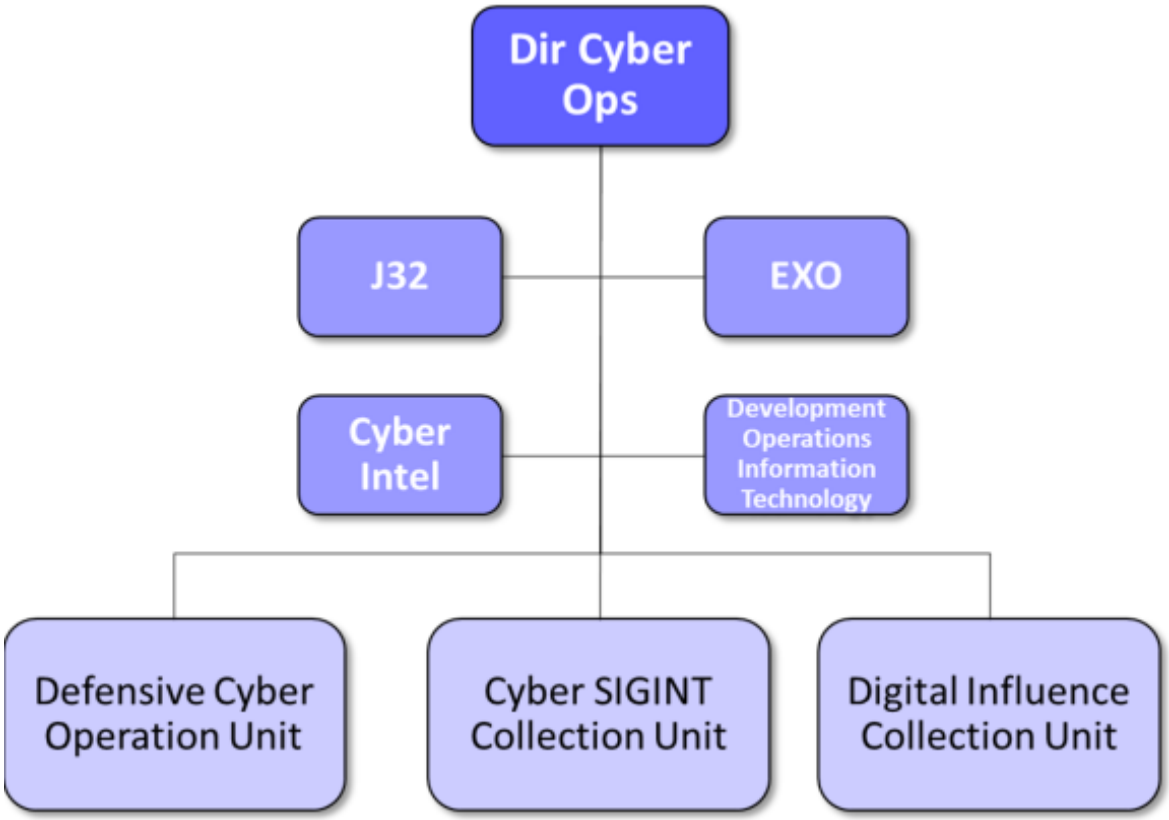
78. Zij is eveneens verantwoordelijk voor de organisatie van cyberevenementen (rekrutering, public relations…). Ten slotte is zij het centrale aanspreekpunt voor de coördinatie en de behandeling van alle verzoeken afkomstig van de pers en van alle parlementaire vragen met betrekking tot het cyberdomein, in nauwe coördinatie met de cel StratCom van het Algemeen Commando van de ADIV.

7.2.5. JUR (Cyber)

79. De sectie JUR Cyber is binnen het Cyber Command de adviseur voor alle zaken met juridische aspecten in cyberspace en dit met betrekking tot inlichtingen, veiligheid, cyber en de bescherming van persoonsgegevens voor het Cyber Command. Deze sectie vervult dezelfde taken (analyse van de wetgeving, juridische adviezen, controle van de wettelijke conformiteit, enz.) als de juridische cel van het Algemeen Commando van de ADIV, maar dan specifiek binnen het domein van de cyberspace. Bij de uitvoering van haar taken wordt samengewerkt met deze juridische cel van het Algemeen Commando en indien nodig met de DG JUR.

7.2.6. Directie Cyber Operations (CyOps)

80. De Directie Cyber Operations (CyOps) is in cyberspace verantwoordelijk voor het beschermen, verdedigen, verzamelen en neutraliseren, en voor het reageren, in bepaalde gevallen, met een aanval. Zij voert vier soorten opdrachten uit: Cybersecurity Operations, Defensive Cyber Operations, Cyber ISR (Intelligence, Surveillance, Reconnaissance) Operations en Offensive Cyber Operations.



7.2.6.1. J32

81. J32 is een stafdienst die een combinatie vormt van de functies “inlichtingen en veiligheid” (J2) en “operaties” (J3).

7.2.6.2. Cyber(space) Intelligence (Cyber Intel)

82. Dit platform houdt zich bezig met het opvolgen en analyseren van kwaadaardige cyberactiviteiten die gericht zijn tegen Belgische belangen, afkomstig van statelijke actoren of door staten gesteunde groepen.

7.2.6.3. Development Operations Information Technology (DO IT)

83. Deze sectie voorziet de Dir Cy Ops van een beveiligde IT-infrastructuur. Zij beheert onder andere de specifieke IT-apparatuur en de interne netwerken die nodig zijn voor het uitvoeren van cyberoperaties.

7.2.6.4. Defensive Cyber Operations Unit (DCOU)

84. Deze eenheid is verantwoordelijk voor het beschermen en het verdedigen van de militaire netwerken en wapensystemen.

7.2.6.5. Cyber-SIGINT Collection Unit (CSCU)

85. Deze eenheid is verantwoordelijk voor alle collecteoperaties in de fysieke en logische lagen van de cyberspace.

7.2.6.6. Digital Influence Collection Unit (DICU)

86. Deze eenheid is verantwoordelijk voor het verzamelen van gegevens uit open bronnen en sociale media (OSINT & SOCMINT) en voor de analyse van beïnvloedingsactiviteiten en informatieoorlogsvoering. De eenheid levert een bijdrage aan de opdrachten "Collect " en "Defend", en doet dit binnen de "sociale" laag van de cyberspace.

7.2.7. Directie Cyber Development & Readiness (Cy D&R)

87. Deze Directie is verantwoordelijk voor de ontwikkeling van de cybercapaciteiten van het Cyber Command en de Cyber Macht.

7.2.7.1. Innovation

88. Deze sectie sensibiliseert industriële en academische partners om onderzoek en ontwikkeling op het gebied van Cyber te stimuleren.

7.2.7.2. Support CyJ1/CyJ2/CyJ4/CyJ8

89. CyJ1 voert structurele HR-analyses uit voor de cybercapaciteit van de Belgische Defensie en organiseert examens en opvolging van de rekrutering via Werkenvoor.be, E-Gov, enz. Ze vervult de rol van aanspreekpunt tussen CyCom en de ADIV J1 voor de klassieke rekruteringskanalen en tussen CyCom (en de ADIV) en de DGHR voor de specifieke ICT-rekruteringskanalen (bijv. E-Gov), beheert het administratief secretariaat en de DAES-functie van het CyCom, met uitzondering van de afdelingen DICU, CSCU en DCOU, die over een eigen DAES beschikken. Ten slotte houdt de afdeling CyJ1 zich bezig met aspecten van *cultural management* (met name de *Own Way of Working*).

90. CyJ2 vervult de rol van aanspreekpunt tussen het Cyber Command en de ADIV J2 en neemt de taken van veiligheidsofficier op zich voor de systemen en de infrastructuur van CyCom.

91. CyJ4 beheert het materieel van het CyCom in nauwe coördinatie met Dir Sp/J4.

92. CyJ8 adviseert de CyC over het gebruik van de aan het CyCom toegewezen budgetten. Zij stelt een begrotingsplan op en stelt prioriteiten overeenkomstig de beschikbare middelen. De dienst evalueert de evolutie van de budgetten, in nauwe coördinatie met de ADIV J8. Zij coördineert voor het personeel van CyCom met ACOS Ops&Trg alle geldelijke aspecten van de zendingen. Zij is verantwoordelijk voor de behandeling van de dossiers inzake lokale aankopen en treedt op als leidend ambtenaar voor meerdere contracten die specifiek aan het CyCom zijn toegewezen. Zij staat in voor het beheer van het Contractbureau (BCU) van

het CyCom.

93. CyICS staat in voor de organisatiebeheersing, in directe ondersteuning aan Dir P&P/ICS.

94. CyIM organiseert de informatiestromen binnen het CyCom.

7.2.7.3. External relations

95. Deze sectie onderhoudt de contacten met de partners en neemt deel aan nationale, EU- en NAVO-werkgroepen, enz. met betrekking tot het domein cyberspace, en dit in nauwe coördinatie met Dir P&P/REL/RELINT en RELNAT.

7.2.7.4. Education & Training

96. Deze sectie is verantwoordelijk voor de organisatie van de vorming en training van de cyberspace-troepen, door opleidingsnormen vast te stellen voor alle cyberpersoneel, de opvolging van opleidingscontracten te verzekeren en de opleidingen te evalueren in nauwe coördinatie met de ADIV J7. Zij organiseert en coördineert cyberspace-oefeningen en –evenementen, evenals interne en externe opleidingen. Zij is verantwoordelijk voor de Awareness-opleiding (JICCS) en het bijbehorende Awareness-dossier. Ten slotte biedt zij ondersteuning aan activiteiten in het kader van de rekrutering.

7.2.7.5. TRADOC

97. Deze sectie zorgt voor de ontwikkeling van de Cyberspace Doctrine, evenals de ontwikkeling en opvolging van de structurele cyberspaceprogramma's voor CyCom en de gehele Defensie, in nauwe coördinatie met de machten en in direct contact met Dir P&P/Plans van de ADIV.

8.
AANBEVELINGEN

Het Comité is van oordeel dat de keuze om één militaire cybercapaciteit zowel te belasten met inlichtingen- en veiligheidsopdrachten in cyberspace als met de cyberopdrachten verbonden met de hoedanigheid van strijdkracht, om zowel operationele als personeels- en beheersmatige redenen, sterk te verdedigen valt.

Het Comité wenst ter zake wel volgende aanbevelingen te formuleren:

TOEC.2025.317/01

Het Comité beveelt aan om, net zoals bij het stafdepartement inlichtingen en veiligheid, de specifieke opdrachten van de Cybermacht, dus de cybereenheid handelend als strijdkracht, in het KB van 30 juni 2025 tot bepaling van de algemene structuur van het Ministerie van Landsverdediging en van de bevoegdheden van bepaalde autoriteiten, nader te omschrijven. Meer bepaald, beveelt het Comité aan dat de regering, via koninklijk besluit, op concrete wijze de vormen van operationele inzet van de Cybermacht, en desgevallend de vormen van hulpverlening en militaire bijstand, vastlegt.

Het Comité herinnert eraan dat de Cybermacht geenszins belast kan worden, reglementair of operationeel, met het verrichten van inlichtingenactiviteiten zoals bedoeld in artikel 11 W.I&V noch met de uitvoering van de in deze bepaling en in de Classificatiewet omschreven veiligheidsopdrachten. Het Comité brengt hierbij ook onder de aandacht dat activiteiten die onder de wettelijke draagwijdte vallen van de handhaving van de militaire veiligheid (art. 11, §1, 2° W.I&V) of van de bescherming van het militaire geheim (art. 11, §1, 3°) niet aan de Cybermacht toegewezen kunnen worden (m.n. reglementair via een koninklijk besluit of operationeel via een instructie van de onderstafchef paraatstelling en operaties).

TOEC.2025.317/02

Binnen de ADIV bestaat de gewoonte om een tweewekelijkse commandomeeting te organiseren tussen de Chef ADIV, de adjunct-chef, de hoofdcommissaris en adjunct-hoofdcommissaris, de Cybercommandant alsook de directeurs van alle directies. Deze commandomeeting doet *de facto* dienst als het directiecomité van de ADIV. Het Comité beveelt aan om deze meeting juridisch, in een koninklijk of ministerieel besluit, te bestendigen.[100] Een dergelijke, reglementair ingerichte commandomeeting zou een goede gewoonte juridisch bevestigen en bestendigen. Daarnaast zou het tevens een verplichting creëren in hoofde van

[100] Ter vergelijking: het directiecomité van de VSSE, en diens samenstelling, werd bij KB vastgelegd (art. 4 KB van 5 december 2006 betreffende het algemeen bestuur van de Veiligheid van de Staat).

de Chef ADIV en de Cybercommandant om formeel overleg te plegen en om zodoende het Cybercommando verder in te kapselen binnen de ADIV.

TOEC.2025.317/03

Het Nationaal Strategisch Inlichtingenplan van 2022 voorziet in een versterkte samenwerking op cybervlak tussen de VSSE en de ADIV. Deze stelt dat in het licht van de toename van de voorziene middelen de ADIV ondersteuning biedt aan zijn nationale partners, die zich onder meer vertaalt in het gebruik van vergarings- en analysecapaciteiten van de ADIV ten gunste van de VSSE.

Tijdens zijn toezichtonderzoek heeft het Comité elementen ontvangen die erop wijzen dat de VSSE vooralsnog weinig gebruik zou maken van de cybercapaciteiten van de ADIV. Het Comité benadrukt dat ze dit niet verder heeft onderzocht, en dus betrokken informatie kan bevestigen noch ontkrachten. Het maakte ook niet de scope uit van dit toezichtonderzoek (cf. 1.3. Doelstelling van het onderzoek). Desondanks is het Comité van oordeel dat de ADIV een kwantitatieve en kwalitatieve evaluatie moet maken van de door de eenheid geleverde diensten en producten aan andere instanties, en dit zowel klanten die behoren tot Defensie alsook extern eraan. Gelet op de verwachting van de regering zoals blijkt uit het Nationaal Strategisch Inlichtingenplan dient een verhoogde aandacht te geschieden wat betreft de geleverde diensten en producten aan de VSSE.

TOEC.2025.317/04

De actuele geopolitieke situatie noodzaakt tot een verhoogde aandacht voor de militaire cybercapaciteit van ons land. De beheersmatige en juridische inrichting van het Cybercommando en de Cybermacht vormen hierbij een noodzakelijke eerste stap. Het Comité beveelt aan dat de regering en Defensie afdoende aandacht besteden aan de noodzakelijke middelen van de cybercapaciteit om te kunnen voldoen aan de vele verwachtingen van de politieke en militaire overheden ten aanzien van deze eenheid. Het Comité adviseert hierbij om het budget van vergelijkbare cybereenheden in de lidstaten van de NATO als referentie te hanteren. Indien vanuit dit referentiepunt de middelen van de cybereenheid als onvoldoende kunnen beoordeeld worden, adviseert het Comité om het budget van de Cybereenheid hieraan aan te passen.

TOEC.2025.317/05

Tijdens het toezichtonderzoek deelde de ADIV mee dat het een studie ging uitvoeren om na te gaan of de Inlichtingenwet gewijzigd moet worden voor wat betreft de specifieke cyberopdrachten van de ADIV en, in het bijzonder, de zogenaamde 'tegenaanval'-bevoegdheid. Er dient in hoofde van de ADIV en de Cybereenheid te worden bestudeerd of deze bevoegdheid niet dient te worden geschrapt als bevoegdheid van de ADIV (Cybercommando) en deze te laten overhevelen naar de Cybermacht? Het Comité is van oordeel dat, hoewel *prima facie* dit logisch lijkt, dit geenszins het geval is. Zoals eerder verduidelijkt, is de bevoegdheid om een tegenaanval uit te voeren na een cyberaanval, onlosmakelijk verbonden met de inlichtingen- en veiligheidsopdrachten van de ADIV.

Daarenboven zou een dergelijk wettelijke overheveling naar de Cybermacht maar mogelijk zijn wanneer Cybermacht als entiteit bij wet wordt ingericht. Het Comité ziet geen reden waarom de Cybermacht bij wet zou worden georganiseerd wanneer de andere strijdkrachten, zoals grondwettelijk voorzien voor wat betreft de organisatie van de Krijgsmacht, bij koninklijk besluit worden ingericht.

Overigens herinnert het Comité eraan dat recentelijk door de regering de keuze werd genomen om deze bevoegdheid te verbinden met het Cybercommando (zie het verslag aan de Koning bij het KB Structuur Defensie van 30 juni 2025 waar '*de identificatie, de verstoring, de neutralisatie van en in laatste instantie de tegenaanval tegen de cyberdreiging, om de bescherming van de informaticanetwerken en de wapensystemen die de Minister van Defensie beheert te verzekeren alsook andere netwerken in het kader van een nationale cybersecurity crisis, overeenkomstig de artikelen 11, § 1, 2°, 2°/1 en 44/1 van dezelfde wet*' specifiek werd geplaatst onder de opdrachten van het Cybercommando).

TOEC.2025.317/06

Het Comité stelt vast dat de regering heeft besloten om de Cybermacht als aparte strijdkracht in te richten. Tegelijkertijd dient het vast te stellen dat elk militair personeelslid, voor diverse redenen, verbonden wordt met een bepaalde macht en de oprichting van de Cybermacht zich hierin niet vertaalt. Elke militair behoort, voor de toepassing van deze regeling, tot de Landmacht, de Luchtmacht, de Marine, de Medische dienst of tot het burgerpersoneel. Het Comité beveelt aan na te gaan of en zo ja in welke mate er een categorie Cybermacht toegevoegd kan worden voor de werking van vernoemde regelingen.

TOEC.2025.317/07

Het Comité is bevoegd om ambtshalve een toezichtonderzoek te openen naar de Cybereenheid handelend als Cybermacht. In het verlengde hiervan beveelt het Comité aan om de Kamercommissie Opvolging Militaire Missies, die belast is met het parlementair toezicht op de operationele aspecten van de Krijgsmacht en dus ook op de activiteiten van de militaire cybercapaciteit binnen een militaire operatie, wettelijk bevoegd te maken om het Vast Comité I te belasten met een toezichtonderzoek naar de cybercapaciteit handelend als Cybermacht. Binnen het federaal parlement beschikken nu reeds de Begeleidingscommissie en een parlementaire onderzoekscommissie over de bevoegdheid om het Vast Comité I met een toezichtonderzoek te belasten.

AFKORTINGEN

ACOS IS	Assistant Chief of Staff Intelligence and Security
ACOS R&O	ACOS Readiness & Ops - Onderstafchef paraatstelling en operaties
ADIV	Algemene Dienst inlichting en Veiligheid van de Krijgsmacht
AJP	Allied Joint Publication
AJP-2	Allied Joint Doctrine for Intelligence, Counterintelligence and Security
BIM-Wet	Wet van 4 februari 2010 betreffende de methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten
C	Chef ADIV
CCB	Centrum voor Cybersecurity België
CCIV	Cybersecurity van het Coördinatiecomité voor Inlichtingen en Veiligheid
CFP	Cyber Force Protection
CHOD	Chief of Defense (Chef Defensie)
COS	Chief of Staff
Comdo	Algemeen Commando
CSMC	Cyber SIGINT Mission Centers
CSCU	Cyber SIGINT Collection Unit
CSOC	Cyber Security Operations Center
CTS-B	Cosmic Top Secret Bohemian
CyC	Commandant Cyber Command
CyCom	Cyber Command
Cyber Intel	Cyber(space) Intelligence
DCOM	Adjunct Chef ADIV
DCOU	Defence Cyber Operation Unit
DICU	Digital Influence Collection Unit
Dir Cy D&R	Directie Cyber Development & Readiness
Dir Cy Ops	Directie Cyber Operations
Dir P&P	Directie Plans & Policy
Dir Rens	Directie Inlichtingen
Dir S	Directie Veiligheid
Dir Sp	Directie Steun
DO IT	Development Operations Information Technology
EDT	Enhanced Document Tracker
EU CDCC	European Union Cyber Defence Coordination Centre
JCDRFU	Joint Cyberspace Defense Resilience Force Unit
JUR	Juridische sectie
HCC	Hoofdcommissaris
HCC Adj.	Adjunct Hoofdcommissaris
J32	Sectie Operationele Coördinatie
KMS	Koninklijke Militaire School
LtGen	Luitenant-generaal
MA	Military Assistant

NCCB	National Cybersecurity Council Belgium
NCCN	Nationaal Crisiscentrum
NEO	Non-Combatant Evacuation Operation
NSIP	Nationaal Strategisch Inlichtingenplan
NVO	Nationale Veiligheidsoverheid
NVR	Nationale Veiligheidsraad
Part Srt	Particulier secretariaat
StratCom	Strategische Communicatie
TTP's	Tactics, Techniques and Procedures
VSSE	Veiligheid van de Staat
WCV	Wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, de veiligheidsadviezen en de publiek gereguleerde dienst
W.I&V	Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten
W.Toezicht	Wet van 18 juli 1991 tot regeling van het toezicht op de politie- en inlichtingendiensten en op het coördinatieorgaan voor de dreigingsanalyse