JAARVERSLAG 2022

Service Général du Renseignement et de la Sécurité
ADIV - SGRS
Algemene Dienst Inlichting en Veiligheid

Quaero et tego

Decodering
van Belgische militaire Inlichting, Veiligheid en Cyberdefensie

DEFENSIE
LA DÉFENSE

.be

ADIV

Algemene Dienst
Inlichting en
Veiligheid

INHOUDSTAFEL

Verantwoordelijke uitgever : Viceadmiraal Wim Robberecht
Kwartier Koningin Elisabeth – Eversestraat 1 in 1140 Evere

Fotografie: Patrick Bouillon, DG StratCom en personeel ADIV
Ontwerp: 2SeeDesign

Viceadmiraal Wim Robberecht © Patrick Bouillon

DE WERELD VERANDERT, MAAR ONZE MISSIE BLIJFT DEZELFDE

Quaero et Tego is ons motto; ons land, onze bedrijven en onze expats **beschermen** dankzij onze **Inlichtingen** en onze knowhow is onze primaire missie; de autoriteiten zorgvuldig **met raad bijstaan** is onze plicht tegenover ons land, de maatschappij en onze medeburgers.

Zonder meer zal 2022 in het geheugen van de ADIV als het jaar van verandering gegrift staan.

Op 19 oktober laatstleden heeft de ADIV een nieuwe structuur in het leven geroepen met als voornaamste bedoeling een beter inzicht te krijgen in de huidige en toekomstige uitdagingen op het gebied van Inlichtingen, Veiligheid en Cyberspace. Het doel van onze dienst blijft ongewijzigd: ons land en onze medeburgers in binnen- en buitenland beschermen tegen alle vormen van mogelijke en denkbare bedreigingen, maar ook onze autoriteiten, partners en industrieën het best mogelijke advies verstrekken.

Deze aanpassing was noodzakelijk geworden door de huidige ingrijpende veranderingen in de wereld en in België.

Het is voor iedereen die betrokken is bij Inlichtingen, Veiligheid of Informatieverwerking in het algemeen duidelijk dat de wereld van vandaag fundamenteel verschilt van die van het begin van de XXI eeuw. De mechanismen die nog maar 22 jaar geleden in gebruik waren, zijn al achterhaald in het licht van de huidige bedreigingen. Onze wereld is digitaal geworden - in alle lagen van de samenleving - en vereist dat we steeds meer informatie verwerken aan een almaar toenemende snelheid.

De wereld mag dan veranderen, informatie blijft de essentiële grondstof voor de werking van de Inlichtingen- en Veiligheidsdiensten.

WIJ WERKEN VOOR U, VOOR ONS LAND EN VOOR DE VREDE

Tegelijkertijd krabbelt de wereld op uit de wereldwijde pandemie, likt haar wonden en ontdekt de gevolgen van een nieuwe maatschappelijke realiteit. Er hebben zich ingrijpende veranderingen voorgedaan die hun weerslag hebben op ons gedrag en onze gewoonten in bijna alle facetten van ons leven en onze samenleving.

Het was daarom absoluut noodzakelijk dat de ADIV de juiste lessen trok uit deze veranderingen en zich in zijn bevoegdheden aanpaste. Door deze veranderingen ontstaan weer nieuwe bedreigingen die voor grote ongerustheid bij de bevolking zorgen. Een toenemend onveiligheidsgevoel door de opmars van extremen en toenemende fraude tegen internetgebruikers in cyberspace zijn enkele voorbeelden die voor ongerustheid zorgen.

Ieder van ons moet zich ervan bewust zijn dat de bedreigingen de veranderende cyclus van de wereld volgen en zich voortdurend aanpassen aan de nieuwe omstandigheden van ons dagelijks leven. Het gevoel van latente instabiliteit en de indruk van onomkeerbare achteruitgang van de Belgische samenleving bieden ideale omstandigheden voor kwaadwillenden om hun speelveld uit te breiden en deze situatie uit te buiten, vooral omdat manipulatie en desinformatie gemeengoed zijn geworden. Als Dienst helpen wij onze burgers over deze bedreigingen te informeren en met de hulp van onze partners proberen wij de gevolgen van deze plagen uit te roeien of tot een minimum te beperken.

Op het moment dat we dit schrijven, stellen wij vast dat de activiteiten op het gebied van spionage en buitenlandse inmenging een niveau hebben bereikt dat sinds de Koude Oorlog niet meer is voorgekomen. De belangrijkste bedreigingen voor de nationale veiligheid zijn, naast deze inmenging, gewelddadig extremisme, terrorisme en malafide cyberactiviteiten. Bovendien keerde de oorlog terug naar de grenzen van Europa. Er zijn ook andere, verder weg gelegen conflicten die invloed hebben op ons samenlevingsmodel. Het is duidelijk dat het tempo van de bedreigingen almaar toeneemt en dat de gevolgen ervan onze bevolking direct of indirect treffen. Uiteindelijk vormen deze bedreigingen een rechtstreeks gevaar voor ons democratisch bestel.

Als chef ben ik bijzonder trots op mijn personeel, zowel militairen als burgers. Vaak werken zij onvermoeibaar en onder soms zeer moeilijke omstandigheden in de schaduw om ervoor te zorgen dat ons land zo goed mogelijk wordt beschermd tegen bedreigingen ten aanzien van de nationale veiligheid, onze burgers - zowel hier als in het buitenland - en de kwetsbare en kritische sectoren van de Belgische economie.

Samen met onze nationale partners en veiligheidsactoren zijn wij de ogen en oren van onze natie. We zoeken naar wat onze tegenstanders geheim willen houden. Wij opereren waar ze zich schuilhouden, meestal in de schaduw en met maximale discretie. Wij doen onderzoek naar vijandige mogendheden om te anticiperen op nieuwe bedreigingen en we waken over de veiligheid van onze geheimen, militaire operaties en kennis.

Wij adviseren onze politieke en militaire leiders zodat zij onafhankelijk en soeverein de beste keuzes kunnen maken om ons land en zijn burgers zo goed mogelijk te beschermen. Wij opereren overal ter wereld waar onze belangen dat vereisen. Want vandaag zijn de bedreigingen voor onze samenleving nog complexer, onvoorspelbaarder en veelvuldiger geworden.

Wij zijn actief op vele gebieden zoals het ondersteunen van militaire operaties, cyberveiligheid, de strijd tegen spionage en inmenging, terrorisme, alle vormen van extremisme, bescherming van onze onderdanen, de strijd tegen de verspreiding van massavernietigingswapens, tegen sektarische of criminele organisaties, alsook op het gebied van de bescherming van het economisch en wetenschappelijk potentieel en van vitale infrastructuren.

Wij werken voor u, voor ons land en voor de vrede.

GEBOORTE VAN HET CYBER COMMAND

CYBERSPACE IS EEN NIEUW STRIJDTONEEL GEWORDEN

Op 19 oktober 2022 hebben wij het Cyber Command officieel boven de doopvont gehouden tijdens een inauguratie in aanwezigheid van heel wat partners en journalisten.

Het Cyber Command is dus een realiteit geworden, niet alleen binnen de militaire gemeenschap, de inlichtingen- en veiligheidsgemeenschap, maar ook ten aanzien van het maatschappelijke middenveld, de academische wereld en het bedrijfsleven.

En volgens de politieke richtsnoeren van onze minister van Defensie zal Cyber Command een almaar belangrijkere maatschappelijke rol gaan spelen, niet enkel binnen de bestuurlijke microkosmos van de cyberveiligheid, maar ook ten aanzien van de samenleving als geheel. De verwerving van «dubbele» capaciteiten strookt met de wens om ons zowel in een militaire als burgerlijke omgeving in te zetten.

GMJ Van Strythem

Dit Cyber Command heeft groeipotentieel, maar blijft wel lid van de familie van veiligheid en inlichtingen waarmee het niet enkel de opdrachten, maar ook het wettelijk kader deelt. Om Cyber Command te kunnen laten groeien, is voldoende personeel natuurlijk onze eerste zorg. Het ontbreekt ons niet aan troeven, of het nu gaat om onze opleidingstrajecten, onze militaire specificiteit of de diversiteit van onze opdrachten. Maar om potentiële kandidaten aan te trekken, moeten we een evenwicht vinden tussen open communicatie en het respecteren van onze veiligheidseisen.

Naast communicatie bepaalt onze capaciteit om partnerschappen op lange termijn aan te gaan met niet enkel onze operationele partners maar ook de actoren uit het maatschappelijk middenveld het succes van Cyber Command. Deze partnerschappen vormen de kern van ons project en ze krijgen vorm samen met het bedrijfsleven, de academische wereld en de onderzoekswereld, en niet te vergeten de wereld van het verenigingsleven en opleidingen.

Deze partnerschappen zijn om verschillende redenen van strategisch belang. Ten eerste zullen zij ons in staat stellen de nodige expertise in stand te houden en te ontwikkelen om het hoofd te bieden aan almaar gesofisticeerdere bedreigingen in een voortdurend veranderende omgeving. Maar zij zullen ons ook in staat stellen te anticiperen op onze toekomstige behoeften, aangezien het van essentieel belang is een langetermijnvisie uit te werken die is afgestemd op de maatschappij van morgen. Ten slotte bieden ze aanwervingsmogelijkheden doordat ze onmisbare banden vormen met het verenigingsleven in milieus die niet vertrouwd zijn met Defensie.

Met grote trots zal ik mijzelf en de competenties van mijn personeel blijven inzetten in het belang van de ontwikkeling van Cyber Command tot een nieuwe Cyber Component bij Defensie. De uitdaging is groot, zowel qua personeel als qua huidige en toekomstige opdrachten. Maar ik ben ervan overtuigd dat we over genoeg troeven beschikken om ze allen samen het hoofd te bieden.

PARTNER-SCHAPPEN

COMMUNICATIE

DE ADIV IN DE SCHOOT VAN DEFENSIE

Viceadmiraal Wim Robberecht
Chef van ADIV

De Algemene Dienst Inlichting en Veiligheid maakt deel uit van de Belgische Defensie. Het is de Belgische referentiedienst voor **buitenlandse** en **defensie-inlichtingen**. De meeste leden zijn militairen, hoewel er steeds meer burgers in de gelederen zijn.

Gezien de militaire aanhorigheid worden er bepaalde kenmerkende functies in uitgeoefend met de benaming van korpsoverste, korpsadjudant en korpskorporaal.

Hun functies zijn voornamelijk gericht op de interne regeling van de dienst, de tucht en het welzijn van het personeel als geheel.

De korpsadjudant en de korpskorporaal zijn ook verantwoordelijk voor de organisatie en uitvoering van militaire tradities en officiële bezoeken binnen de organisatie.

Adjudant-majoor Frédéric Charlot,
Korpsadjudant

Eerste-Korporaal-chef Bruno Wilmart,
Korpskorporaal

De traditionele militaire feestdagen zijn :

07 April
Veteranendag

21 Juli
Nationale feestdag

11 November
Wapenstilstand

15 November
Koningsdag

© SFRS

OPDRACHT

QUAERO ET TEGO
IK ZOEK EN IK BESCHERM

De ADIV is de Belgische militaire inlichtingen- en veiligheidsdienst.

Hij heeft als opdracht het opzoeken, analyseren en behandelen van elke **inlichting** die betrekking heeft op om het even welke activiteit die de integriteit van het nationaal grondgebied of de bevolking, de militaire verdedigingsplannen, het militair gerelateerd wetenschappelijk en economisch potentieel, de opdrachten van de strijdkrachten en de veiligheid van de Belgische onderdanen in het buitenland zou kunnen bedreigen en van elke inlichting in verband met de activiteiten van buitenlandse inlichtingendiensten op Belgisch grondgebied.

Hij handhaaft de militaire **veiligheid** van het personeel van Defensie en van militaire installaties, wapens, munitie, documenten en computersystemen, en beschermt de daarmee verbonden geheimhouding.

De ADIV is verantwoordelijk voor het uitvoeren van veiligheidsonderzoeken en -verificaties en het afgeven van veiligheidsmachtigingen, -adviezen en -attesten.

In het kader van de uitoefening van zijn opdrachten verstrekt de ADIV inlichtingen aan politieke en militaire autoriteiten in een nationale en internationale context om hen bij te staan in hun besluitvorming.

VISIE

WETEN EN LATEN WETEN

De ADIV draagt bij tot de bescherming van de belangen van de Natie, Defensie en de bevolking dankzij een **geïntegreerde benadering** van de veiligheid die de dimensies Inlichtingen, Contra-Inmenging, Veiligheid en Cyber met elkaar verbindt, zowel op het nationale grondgebied als in het buitenland.

Het is de Belgische referentiedienst voor **buitenlandse inlichtingen** en **defensie-inlichtingen.**

Hij draagt samen met zijn nationale partners bij tot de handhaving en versterking van de **binnenlandse veiligheid.**

WAARDEN

ONZE 10 GEBODEN

1. Wij zoeken en vinden wat anderen over het hoofd zien
2. Wij hebben vertrouwen in onszelf en in elkaar
3. Wij hebben de juiste mensen op de juiste plaats
4. Wij zijn verenigd
5. Wij werken onophoudelijk en op een slimme manier
6. Wij verstrekken de juiste informatie, aan de juiste persoon, op de juiste manier en op het juiste moment
7. Wij werpen de blik vooruit
8. Wij onderhouden uitstekende relaties
9. Wij vatten de cultuur van inlichtingen
10. Wij werken in de schaduw

Kathleen Van Acker

ONZE GESCHIEDENIS

Na de onafhankelijkheid van België in 1830 was een van de eerste acties van de voorlopige regering het oprichten van een leger. Aangezien dit leger geen departement had dat verantwoordelijk was voor het verzamelen van informatie en het analyseren van inlichtingen, werd in 1831 voor dit doel de «Militaire Politie van het Departement van Oorlog» opgericht. Dit nieuwe korps werkte op onregelmatige basis met informanten onder toezicht van officieren en was voornamelijk verantwoordelijk voor het opsporen en bewaken van orangisten en republikeinse elementen binnen het leger.

Bij Koninklijk Besluit van 26 juni 1910 werd een Generale Staf van het Leger opgericht. Deze laatste bestond uit vier bureaus, waaronder de 2e sectie belast met inlichtingen.

Begin 1911 richtte de 2e Sectie «Inlichtingen» een bewakings- en inlichtingendienst op aan de grenzen, waarin 300 plaatselijke rijkswachters, douaniers en boswachters werden aangesteld.

Op 1 april 1915 werd de Belgische militaire Veiligheid opgericht. Haar belangrijkste taak was het verijdelen van de spionageactiviteiten van de vijand. Daartoe beschikte de Dienst over uitgebreide bevoegdheden, waaronder de verwijdering en internering van delinquenten en personen die verdacht werden van collaboratie en spionage, de bevoegdheid tot (lichaams)fouillering, doorzoeking en inbeslagname van wapens en de bevoegdheid om subversieve bijeenkomsten te verhinderen en privé-correspondentie te onderscheppen.

Na de wapenstilstand was de Dienst ook verantwoordelijk voor de veiligheid van de Belgische troepen die deelnamen aan de bezetting van het Ruhrgebied.

In 1929 werd de Dienst ontbonden wegens een schandaal met betrekking tot de vervalsing van militaire plannen tegen Duitsland. Toen deze militaire plannen in handen van de Nederlandse pers vielen, veroorzaakten ze een internationaal schandaal, «De Utrechtse Documentenvervalsing» genaamd.

In 1937 zal de Dienst in het grootste geheim uit de as herrijzen om de groeiende Duitse spionage het hoofd te bieden.

Na de Belgische Achttiendaagse Veldtocht in 1940 wil de Belgische regering in ballingschap in Londen de banden met het bezette land zo snel mogelijk herstellen. Twee Belgische inlichtingendiensten bestonden naast elkaar en werkten elk vanuit Londen. Door een

gebrek aan duidelijkheid over de door de regering aan de twee diensten toegewezen bevoegdheden brak een bevoegdheids-geschil uit, dat niet alleen schadelijke gevolgen had voor de relatie tussen de twee diensten, maar ook voor de samenwerking met de Britse inlichtingendiensten. Het probleem bleef bestaan tot oktober 1942, toen een akkoord dat de bevoegdheden van de twee diensten vastlegde, werd ondertekend door de nieuwe ministers van Landsverdediging en Justitie.

Na de Tweede Wereldoorlog wordt naast de Militaire inlichtingendienst een specifieke dienst opgericht, genaamd «Service de Documentation de Renseignement et d'Action VIII» (SDRA VIII). Zijn belangrijkste bestaansreden was, in geval van een conflict, de Belgische regering naar een veilige plaats te evacueren en de contacten met het vaderland te onderhouden. Binnen dit kader verzamelde de SDRA VIII inlichtingen en bereidde zich voor op ontsnapping-sopdrachten, waaronder de exfiltratie van neergehaalde piloten of van door de vijand ontdekte agenten. De Dienst trainde zich ook in sabotage van militaire doelen, organiseerde een structuur om weerstand te bieden aan de tegenstander en was betrokken bij contra-in-formatie.

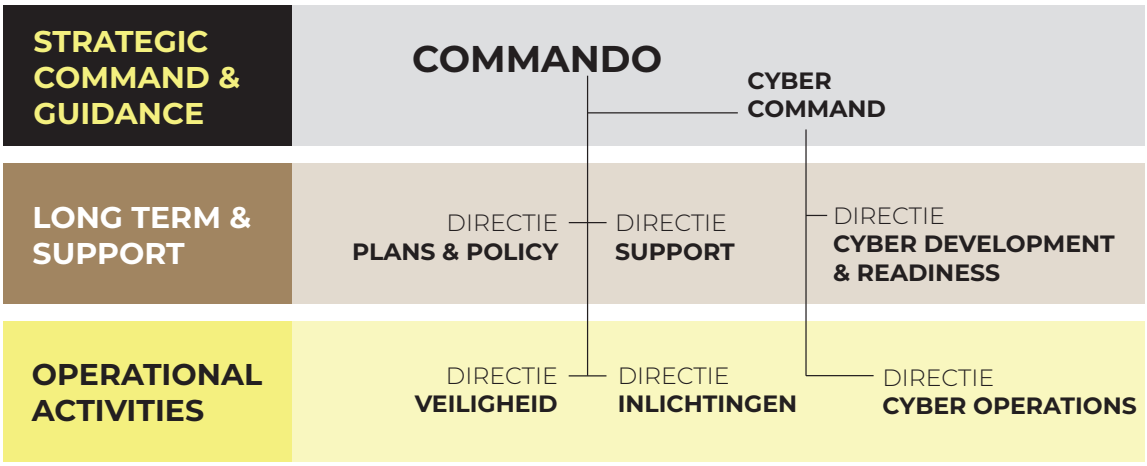
Op 3 augustus 1990 moest premier Giulio Andreotti, na een parlementair onderzoek naar terrorisme in Italië, het bestaan van het Italiaanse «Stay-behind»-netwerk erkennen. Dit laatste was een onderdeel van operatie "Gladio", die heel Europa bestreek en bestond uit de oprichting door elk Europees land van een «Stay-behind» netwerk met als doel weerstand te bieden aan de vijand op nationaal grondgebied.

De toenmalige Belgische minister van Defensie, de heer Guy Coëme, moest toen uitleg verschaffen over deze netwerken op een internationale bijeenkomst die eind oktober 1990 in Brussel werd gehouden. Dezelfde dag

ontbood de minister de chef van de militaire inlichtingendienst en de chef van SDRA VIII om nadere informatie te bekomen.

Terwijl niemand vóór november 1990 ooit van Gladio had gehoord en het Belgische «Stay-behind»-netwerk volledig onafhankelijk opereerde, kwam SDRA VIII in het oog van een mediastorm en werd het voorwerp van complottheorieën die het Belgische geheime netwerk in verband brachten met de bloedige aanslagen die in de jaren tachtig in België waren gepleegd, met name via de dossiers van de Bende van Nijvel of de Cellules Communistes Combattantes. Op 20 december 1990 besloot de regering het ondergrondse netwerk op te heffen en een parlementair onderzoek in te stellen. Het verband met mogelijke terroristische aanslagen is nooit bewezen en de identiteit van de agenten is nooit bekendgemaakt.

ONZE STRUCTUUR



DE BELANGRIJKSTE WET DIE ONS REGEERT

De opdrachten van de ADIV staan beschreven in artikel 11 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten. Voor de goede uitvoering van deze opdrachten heeft de wetgever in de wet verschillende "methoden voor het verzamelen van gegevens" opgenomen. De verschillende methoden voor inzameling zijn onderworpen aan specifieke voorwaarden en juridisch toezicht, om de vereisten van nationale veiligheid in evenwicht te brengen met de beginselen en waarden van een democratische rechtsstaat.

Bij het gebruik van deze methoden besteden de operationele verantwoordelijken van de ADIV veel aandacht aan de naleving van de wettelijke voorschriften.

Het ontstaan van nieuwe bedreigingen en de ontwikkeling van nieuwe technologieën brengen altijd een restrisico van (onbedoeld) onrechtmatig handelen met zich mee. Onafhankelijk toezicht op dit restrisico en op de dagelijkse acties van de ADIV wordt voor, tijdens en na deze acties gegarandeerd door het Vast Comité van Toezicht op de inlichtingen- en veiligheids-diensten en de bestuurlijke Commissie die belast is met het toezicht op de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten.

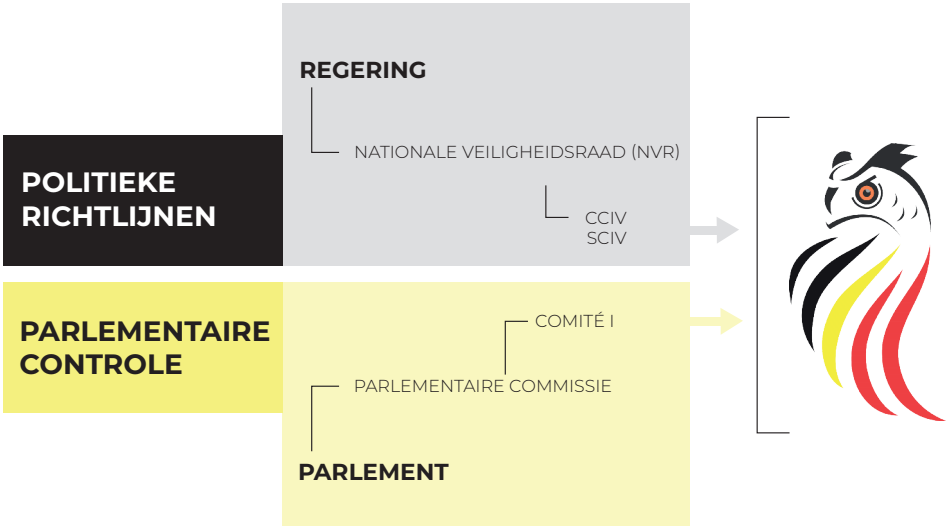
Gedeeltelijk op basis van de aanbevelingen van de parlementaire onderzoekscommissie "Terroristische aanslagen van 22 maart 2016" werden door de wetgever in 2022 wijzigingen aangebracht aan de wet van 30 november 1998. Voor de agenten van de inlichtingen- en veiligheidsdiensten zijn er regelingen getroffen opdat ze in de virtuele en de reële wereld kunnen infiltreren en werden de mogelijkheden om strafbare feiten te plegen uitgebreid, dit weliswaar met de bijbehorende toezichtsmaatregelen. Voorts wordt, wat de menselijke bronnen betreft, de mogelijkheid geboden om strafbare feiten te plegen, maar onder zeer strikte voorwaarden. Tot slot, en meer specifiek voor de ADIV, is een extra bevoegdheid toegevoegd in geval van een nationale cyberveiligheidscrisis.

De implementatie van deze nieuwe wettelijke bevoegdheden en de aanbevelingen van het Vast Comité van Toezicht naar aanleiding van de zaak «Jürgen Conings» worden als een prioriteit beschouwd, hoewel de dagelijkse operationele werkzaamheden van de ADIV worden voortgezet.

In de loop van 2022 werden de eerste initiatieven ontplooid om voorstellen voor te bereiden tot wijziging van de wet betreffende classificatie en veiligheidsmachtigingen, -attesten en -adviezen (wet van 11 december 1998) en de wet betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (wet van 30 juli 2018).

ONZE ENGAGEMENTEN

Politiek engagement :



De Nationale Veiligheidsraad bepaalt het algemeen inlichtingen- en veiligheidsbeleid, staat in voor de coördinatie ervan en bepaalt de prioriteiten van de inlichtingen- en veiligheidsdiensten. De Raad is ook bevoegd voor de coördinatie van de strijd tegen de financiering van het terrorisme en de verspreiding van massavernietigingswapens. De Raad bepaalt bovendien het beleid inzake de bescherming van gevoelige informatie. Hij wordt voorgezeten door de Eerste Minister en omvat de ministers van Justitie, Defensie, Binnenlandse Zaken en Buitenlandse Zaken. En ook de vicepremiers die deze bevoegdheden niet in hun portefeuille hebben.

Leden van de regering die geen deel uitmaken van de Raad, kunnen door de Eerste Minister worden uitgenodigd om eraan deel te nemen voor de behandeling van dossiers die hen in het bijzonder aangaan. Wanneer de agenda hun aanwezigheid vereist, worden ook uitgenodigd:

De chef van de Algemene Dienst Inlichting en Veiligheid,
De administrateur-generaal van de Veiligheid van de Staat,
De commissaris-generaal van de Federale Politie,
De directeur van het Coördinatieorgaan voor de dreigingsanalyse,
De voorzitter van het Directiecomité van de Federale Overheidsdienst Binnenlandse Zaken,
Een vertegenwoordiger van het College van procureurs-generaal,
De federale procureur.

Het Coördinatiecomité voor Inlichtingen en Veiligheid (CCIV) is samengesteld uit de leidinggevenden van de autoriteiten en diensten die betrokken zijn bij het inlichtingen- en veiligheidsbeleid. Het ontwikkelt strategische voorstellen, ziet toe op de implementatie van de door de Nationale Veiligheidsraad vastgestelde prioriteiten en staat in voor een efficiënte samenwerking en informatie-uitwisseling tussen diensten en autoriteiten.

Het Strategisch Comité Inlichtingen en Veiligheid (SCIV) is verantwoordelijk voor zowel de voorbereiding als de uitvoering van het beleid en bestaat uit vertegenwoordigers van de leden van de Nationale Veiligheidsraad en de voorzitter van het Coördinatiecomité. Het secretariaat van het Strategisch Comité wordt verzorgd door de FOD Kanselarij van de Eerste Minister.

Het toezicht :

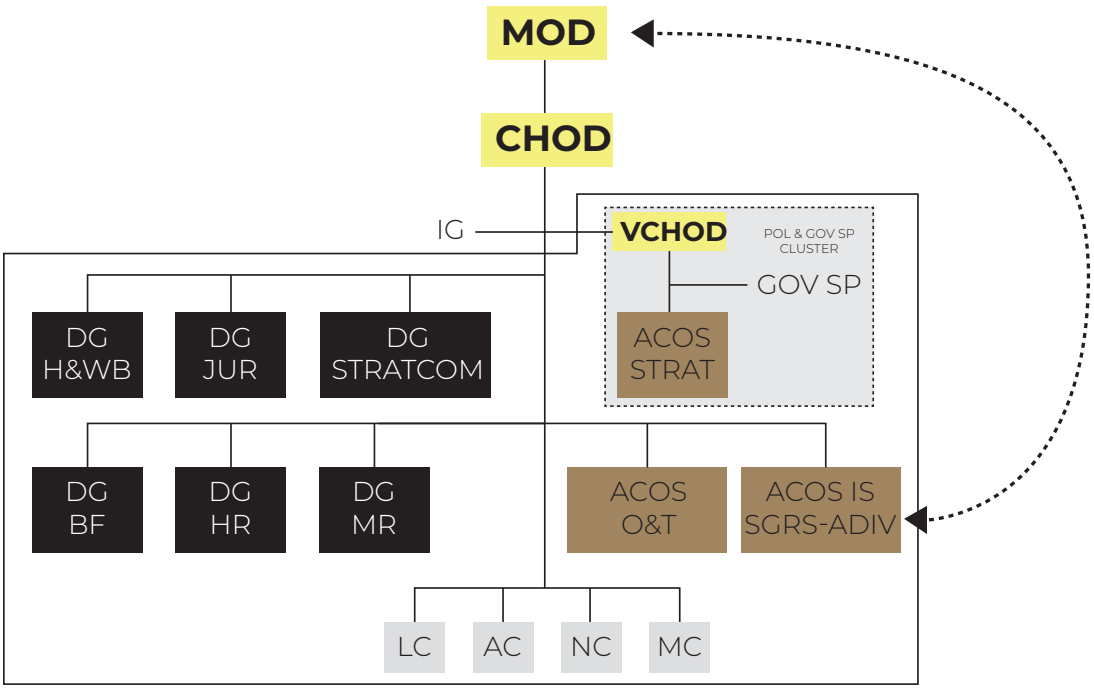
Het Vast Comité I is verantwoordelijk voor het toezicht op de activiteiten en de werking van de Veiligheid van de Staat en de Algemene Dienst Inlichting en Veiligheid. Het toezicht heeft zowel betrekking op de legitimiteit (toezicht op de naleving van de wetten die de materie regelen) als de efficiëntie en de coördinatie van de inlichtingendiensten (onderlinge afstemming van hun werking).

De parlementaire commissies en het parlement kunnen tijdens hun respectieve zittingen niet alleen ministers om uitleg vragen en/of specifieke vragen stellen, maar ook verzoeken om een of meer leden van een inlichtingen- en veiligheidsdienst op te roepen. Wanneer echter het ondervragen en oproepen van een persoon geïntegreerd deel uitmaakt van de democratische controle, kan om redenen van classificering van de inhoud van de antwoorden een zitting achter gesloten deuren worden gevraagd.

Militair engagement :

De geschiedenis van de ADIV houdt verband met militaire operaties. Ook vandaag is een belangrijk deel van zijn werk bestemd voor de Belgische Defensie en in het bijzonder voor militaire operaties. Deze band met defensie blijkt duidelijk uit het feit dat zijn personeel, infrastructuur en budget door militaire algemene directies worden beheerd. Dat is ook de reden waarom de ADIV hiërarchisch gezien afhangt van de chef defensie onder de naam ACOS IS (departement van Defensie Intelligence Service).

De afgelopen jaren zijn de werkzaamheden van de ADIV uitgebreid en ze overlappen nu ook specifiek civiel-militaire gebieden zoals de strijd tegen terrorisme of extremisme. Dat is de reden waarom de ADIV rechtstreeks van de minister van Defensie afhangt.



DIRECTIE INLICHTINGEN

De Directie Inlichtingen levert hoogwaardige analyses op basis van verschillende soorten informatie en bronnen om onze Regering en onze partners te adviseren.

De Directie Inlichtingen is, enerzijds, verantwoordelijk voor de verzameling en exploitatie van informatie en, anderzijds, voor de omzetting daarvan in de vorm van inlichtingen. De informatie wordt verzameld door agenten of door specifieke technische apparatuur die tot de Inzamelingspijler behoort. Vervolgens wordt ze naar de analisten van de Exploitatiepijler overgemaakt om er verwerkt te worden. Er zijn, afhankelijk van het gewenste eindproduct, verschillende soorten benaderingen van informatieverwerking. De analist kan, naar keuze, meer de nadruk leggen op de militaire, politieke, economische, sociale of veiligheidsas. De rijkdom van ons inlichtingenwerk zit hem net in de mogelijkheid om verschillende eindverslagen te kunnen afleveren in functie van de behoeften van de aanvrager.

De Inzamelingspijler

De Inzamelingspijler van de Directie Inlichtingen bestaat uit een aantal verschillende diensten die informatie verzamelen via agenten op het terrein, technici die specifieke apparatuur gebruiken, of beide. Deze diensten worden in het jargon “inzamelingsdiensten” genoemd.

Wanneer we in de inlichtingentaal spreken over een «menselijke bron» of «contact», bedoelen we een persoon die informatie verstrekt. Die persoon kan zich bevinden ofwel in het buitenland, in een militair operationeel gebied of in een doelland, ofwel op nationaal grondgebied. De Dienst die verantwoordelijk is voor de nationale bronnen en contacten komt ook tussen in de onderzoeken naar een T.E.S.S.O.C. bedreiging. Deze zogenaamde

ONZE DIRECTIE INLICHTINGEN IS DE EERSTE EN LAATSTE VERDEDIGING VOOR DE CHAOS

onderzoeken van contra-inmenging houden verband met een dreiging op het gebied van terrorisme, links- en rechts-extremisme, spionage, sabotage, subversie en georganiseerde criminaliteit (“Organised Crime”) gericht tegen de belangen van het land en Defensie in het bijzonder.

De term «apparatuur» verwijst naar elektromagnetische signalen zoals telefoontaps of geografische informatie zoals satellietbeelden. Het gaat ook om informatie uit zogenaamde «open bronnen» zoals de geschreven pers, radio of televisie en alle informatie die op het internet beschikbaar is.

De evolutie van inlichtingen vereist tegenwoordig een hergroepering van menselijke en materiële middelen om de prestaties te verbeteren. Bij een fysieke achtervolgingsoperatie worden bijvoorbeeld een of meer agenten op het terrein en verschillende passende technische middelen ingezet om elke situatie het hoofd te bieden of elke door de bewaakte persoon getroffen tegenmaatregel te verijdelen.

> **De Inzamelingspijler heeft ook een dienst die fungeert als in- en uitgang voor de gehele informatiestroom van de NAVO om de militaire samenwerking tussen de bondgenoten te waarborgen.**

De Exploitatiepijler

De Exploitatiepijler van de Directie Inlichtingen bestaat uit verschillende platformen die per geografisch gebied of per thema zijn georganiseerd en die uiteindelijk tot doel hebben inlichtingenproducten over verschillende onderwerpen te leveren. Bijvoorbeeld over dreigingen voor een militaire operatie in het buitenland, extremisme in een bepaalde regio, de politieke situatie in Oekraïne of over onderwerpen in verband met een prognose over bijvoorbeeld de veiligheid in Oost-Congo.

De platformen bestaan uit analisten die gespecialiseerd zijn in spionage, enerzijds, en contra-inmenging, anderzijds. De belangrijkste betrokken geografische gebieden zijn Europa, Afrika, Azië en het Midden-Oosten. De belangrijkste thema's zijn terrorisme, extremisme, spionage, sabotage, subversie en georganiseerde criminaliteit (T.E.S.S.OC.).

> **Om de kwaliteit van de eindproducten te waarborgen, beschikt de Exploitatiepijler over een dienst «Quality control».**

Het Coördinatiecentrum

De Directie Inlichtingen beschikt over een Coördinatiecentrum dat bestaat uit vertegenwoordigers van de Inzamelings- en Exploitatiepijlers en van de Directie Cyber Operations.

Het Coördinatiecentrum verspreidt alle inkomende informatie of verzoeken naar de betrokken personen en alle uitgaande informatie of verzoeken naar de juiste klanten of partnerdiensten.

Het centrum beschikt ook over een dienst voor beheer van de inzameling die de inzamelingsinspanningen afstemt op de analysebehoeften en de contra-inmengingsinspanningen tussen de platformen, enerzijds, en het personeel dat in België op het terrein werkt, anderzijds, coördineert.

Met het oog op de naleving van de wet beschikt het coördinatiecentrum over een dienst die alle verzoeken voor het gebruik van specifieke en uitzonderlijke methoden voorlegt aan de bestuurlijke Commissie die belast is met het toezicht op de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten. Met deze machtiging kan de ADIV bijvoorbeeld telefoontaps uitvoeren of afluisterapparatuur installeren.

DIRECTIE VEILIGHEID

De Directie Veiligheid is verantwoordelijk voor de handhaving van de militaire en industriële veiligheid. Deze bevoegdheid heeft betrekking op het personeel, de installaties, de wapensystemen, de uitrusting en de operaties van Defensie, zowel in België als in het buitenland. Ze is ook verantwoordelijk voor de bescherming van geclassificeerde informatie van Defensie en de handhaving van de geheimhouding, tot de archivering toe. Ze voert veiligheidsonderzoeken uit voor medewerkers van Defensie en aanverwante industrieën.

ALLES BEGINT EN EINDIGT MET ONZE DIRECTIE VEILIGHEID

Militaire en industriële veiligheid

Dit departement is verantwoordelijk voor de handhaving van de militaire en industriële veiligheid van heel Defensie en van de industrie gekoppeld aan Defensie.

Ten eerste heeft zij een regulerende rol ten aanzien van heel Defensie en civiele bedrijven die diensten of wapensystemen leveren.

De veiligheidsagenten adviseren de eenheden van defensie of de bedrijven over de manier waarop deze richtlijnen correct kunnen toegepast worden. Aangekondigde inspecties of onaangekondigde controlebezoeken behoren ook tot de taken van de agenten. Als het misgaat, voeren ze onderzoeken uit naar de veiligheidsincidenten of helpen ze de politiediensten.

Ten slotte beschikt deze dienst over specialisten in het opsporen van spionage-apparatuur om onze eigen installaties tegen afluisteren te beschermen.

Dienst voor veiligheidsonderzoek

Deze dienst voert onderzoeken uit in overeenstemming met de wet betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen (wet betreffende de classificatie 11 dec. '98). Deze wet regelt de bescherming van de geheimhouding die nodig is om de nationale veiligheid, de militaire defensieplannen en de fundamentele belangen van ons land veilig te stellen. Ongemachtigd of oneigenlijk gebruik van geclassificeerde informatie en wapensystemen kan niet alleen Defensie, maar het hele land schade berokkenen.

Daarom worden alle toekomstige personeelsleden van Defensie, zowel burgers als militairen, tijdens het aanwervingsproces onderworpen aan een antecedentenonderzoek om hun integriteit en betrouwbaarheid te beoordelen. Bovendien komt het overgrote deel van het personeel tijdens de uitoefening van zijn functie in onze organisatie in contact met geclassificeerde informatie, procedures en wapensystemen. Daartoe moeten deze personeelsleden beschikken over een veiligheidsmachtiging van het vereiste niveau: vertrouwelijk, geclassificeerd of geheim. De diepgang van het onderzoek hangt af van het niveau en de uitgeoefende functie. Voor deze onderzoeken doen de veiligheidsonderzoekers een beroep op de medewerking van onder meer politiediensten, rechterlijke macht, het Rijksregister, de fiscale autoriteiten en zelfs buitenlandse partnerdiensten. Een veiligheidsmachtiging wordt alleen verleend als de kandidaat blijk geeft van voldoende integriteit, loyaliteit en discretie. Een onderzoek van de omgeving van de aanvrager, een digitale controle of een gesprek met de aanvrager behoren tot de mogelijke onderzoeksmethoden om deze drie criteria te controleren. Wanneer een weigering van een veiligheidsmachtiging wordt meegedeeld, heeft de aanvrager de mogelijkheid om tegen deze beslissing in beroep te gaan bij de Beroepscommissie van veiligheidsmachtigingen.

De geclassificeerde archieven

Deze dienst is het geheugen van Defensie voor alle geclassificeerde informatie die is gearchiveerd. De dienst bewaart en beheert alle geclassificeerde archieven en ook de historische archieven van Defensie zolang deze administratief van nut zijn. Bewaring vindt plaats in zowel fysieke als digitale vorm. Alle inkomende archieven worden zodanig geïnventariseerd, bewaard en opgeslagen dat ze gemakkelijk kunnen worden benut. De geclassificeerde archieven worden regelmatig door de verschillende diensten van de ADIV als databank geraadpleegd. Op onze dienst wordt beroep gedaan voor wetenschappelijk historisch onderzoek, parlementaire onderzoeken, vragen van families van oorlogsgevangenen of gerechtelijke onderzoeken. Ter gelegenheid van belangrijke verjaardagen van eenheden van Defensie, stellen onze archieven ons in staat om zich een bepaald boek of een brochure te herinneren. Wanneer het administratieve nut van het bewaren van de archieven bij het ministerie van Defensie vervalt, worden zij gedeclassificeerd en vervolgens overgebracht naar het Rijksarchief.

REGULATIE
CONTROLE
GEHEUGEN

CYBER COMMAND

De Belgische Cyber Command bouwt aan een Cyber Force via partnerschappen om te beschermen, te verdedigen, te verzamelen en te vechten in cyberspace en de elektromagnetische omgeving.

ONZE CYBERDEFENSIE IS DE EERSTE EN LAATSTE VIRTUELE GRENS VAN HET STRIJDTONEEL

Binnen de cyberspace- en elektromagnetische omgeving is Cyber Command verantwoordelijk voor het leiden van de inlichtingen- en veiligheidsopdrachten van de ADIV, het waarborgen van de manoeuvreerruimte van Defensie en het genereren van militaire effecten ter ondersteuning van deze operaties.

Cyber Command zorgt voor de exploitatie van cyberspace ten behoeve van de gehele natie, alsook van de ADIV en Defensie. Het speelt een sleutelrol in de nationale veerkracht en neemt een centrale plaats in de cyberarchitectuur van ons land in en is een betrouwbare internationale partner en een nationale referentie op het gebied van cryptografie. Cyber Command ontwikkelt zijn innovatieproces en nieuwe militaire capaciteiten. Het implementeert deze capaciteiten op de fysieke, logische en virtuele lagen van de cyber- en elektromagnetische ruimte. Het onderhoudt een bevoorrechte relatie met de industrie, de academische wereld en het verenigingsleven. Zijn echte kracht ligt in zijn menselijk kapitaal.

Om zijn opdrachten te realiseren, voert Cyber Command vier verschillende taken uit:

- Ten eerste ondersteunt het zijn zusteronderdelen en andere departementen van Defensie door een samenhangend en geïntegreerd instrumentarium voor cybercapaciteiten te ontwikkelen.
- Ten tweede staat het in voor de ontwikkeling van de gespecialiseerde cybercapaciteiten van de ADIV.
- Ten derde voert het veiligheids- en inlichtingenoperaties uit in cyberspace en de elektromagnetische omgeving (Protect, Defend, Collect and Fight).
- Ten vierde beschikt het over gespecialiseerde capaciteiten in het kader van hulp aan de natie en nationale cybercrisissituaties.

> Cyber Command beschikt over bevoegdheden van een 5e component (land, marine, lucht, medisch en cyber) binnen Defensie en die van een directie binnen de ADIV. Afhankelijk van zijn opdracht valt hij onder twee verschillende juridische kaders: de organieke wet op de inlichtingen- en veiligheidsdiensten of het juridische kader voor de inzet van de Belgische strijdkrachten.

CYBER COMMAND IS GEORGANISEERD ROND TWEE DIRECTIES :

De Directie «Cyber Operations» bestaat uit vier ondergeschikte primaire eenheden.

- Allereerst de Eenheid van defensieve cyberoperaties (EDC) die verantwoordelijk is voor de bescherming en verdediging van de Belgische militaire netwerken en wapensystemen. Deze eenheid keurt onze communicatie-, informatie- en wapensystemen goed, voert evaluaties van de kwetsbaarheid uit en herbergt het Centrum voor cryptografische uitmuntendheid van de Strijdkrachten. Ze voert analyses van malware uit, bewaakt de netwerken van Defensie vanuit zijn Cyber Security Operations Centre (CSOC) en staat klaar om onze netwerken te verdedigen tegen buitenlandse of kwaadwillende actoren.
- Ten tweede is de Cyber-SIGINT Collection Unit (CSCU) verantwoordelijk voor alle intrusieve en niet-intrusieve inzamelingsoperaties en het genereren van militaire effecten in cyberspace en de elektromagnetische omgeving.
- Ten derde is de Digital Influence Collection Unit (DICU) verantwoordelijk voor het verzamelen van gegevens uit open bronnen en sociale media (OSINT en SOCMINT). Ze is ook verantwoordelijk voor invloedsanalyse en vijandelijke operaties van informatieoorlog.
- Ten slotte voert het Cyber(space) Threat Intelligence platform inlichtingenanalyses uit over schadelijke cyberactiviteiten tegen Belgische militaire belangen.

De Directie «Cyber Development & Readiness» is verantwoordelijk voor de ontwikkeling van cyberdefensiecapaciteiten ter ondersteuning van de ADIV en de strijdkrachten.

Ze richt zich daarom op het opzetten van partnerschappen met de academische wereld, de industrie en het maatschappelijk middenveld om innovatie op het gebied van cyberdefensie te stimuleren. Ze is ook verantwoordelijk voor de opleiding en training van het personeel, de vaststelling van een doctrinaire basis voor de cyberoperaties en de ontwikkeling van een civiele cyberreservemacht. Tot slot maakt ook de verbinding met structurele partners en internationale organisaties deel uit van haar takenpakket.

DIRECTIE «PLANS & POLICY»

1. Planning in alle verantwoordelijkheidsdomeinen van de ADIV, zowel wat betreft inlichtingen, veiligheid, cyber en werking (personeel, materieel, infrastructuur, begroting enz.),

2. Omkadering, coördinatie en ontwikkeling van synergieën met de nationale en internationale partners van de Dienst,

3. Het opzetten van een beheersingssysteem voor de organisatie.

PLANNING, SAMENWERKING, SYNCHRONISATIE EN EVALUATIE ZIJN DE DAGELIJKSE UITDAGINGEN VAN ONZE DIRECTIE «PLANS & POLICY»

De sectie « Plans »

Deze sectie is verantwoordelijk voor de planning in alle verantwoordelijkheidsdomeinen van de ADIV. Ze is verantwoordelijk voor het opstellen, in samenwerking met alle andere directies, van de verschillende plannen van de Dienst, zoals het op 19 oktober 2022 geïmplementeerde herstructureringsplan, het stuurplan met de prioriteiten van de ADIV, het nationaal strategisch inlichtingenplan, een crisisbeheersplan enz.

Deze sectie is ook verantwoordelijk voor de documentatie van alle door de Dienst ondertekende overeenkomsten en, wat belangrijker is, voor de documentatie van alle ADIV-processen. Ze ziet ook toe op de NAVO-doctrine met betrekking tot inlichtingen, veiligheid en cyber.

Stuurplan (SPADIV)

Eind 2021 heeft de ADIV zijn stuurplan voor het jaar 2022 vastgesteld met als doel te bepalen welke taken prioritair moeten worden uitgevoerd in het licht van de beschikbare middelen. In de loop van 2022 heeft de ADIV zijn stuurplan voor de jaren 2023 tot 2027 opgesteld. Met dit plan wordt beoogd de ADIV-capaciteit te verbeteren om de toekomstige ontwikkelingen op het gebied van bedreigingen en risico's beter te doorgronden.

Het bestaat uit drie complementaire delen:

- Het **«OPERATIONELE»** deel bepaalt de op korte en middellange termijn geplande activiteiten, met inachtneming van het juridisch kader, de internationale verbintenissen en de hogere richtlijnen. Bij de evolutie van deze activiteiten wordt rekening gehouden met de verwachte komst van extra middelen.
- In het deel **«MIDDELEN»** wordt een overzicht gegeven van de middelen die de Dienst nodig zal hebben en hoe deze in de loop van de tijd zullen evolueren.
- Het deel **«WERKING»** is gericht op het uitzetten van de krachtlijnen van de belangrijkste projecten voor het verbeteren en handhaven van de operationaliteit van de ADIV.

Het evenwicht tussen middelen en taken is de drijvende kracht achter deze planning.

De sectie «Relaties»

Deze sectie heeft tot taak alle bestaande synergieën tussen de ADIV en nationale en internationale partners te inventariseren en na te gaan welke partnerschappen verder moeten worden ontwikkeld. Ze bepaalt de richtsnoeren voor synergieën en de regels die in aanwezigheid van de partners moeten worden nageleefd. Ze is het in- en uitgangspunt voor alle contacten met buitenlandse inlichtingendiensten. Ze zorgt ook voor verbindingsofficieren bij onze nationale partners.

De sectie «Middelen en capaciteiten»

Deze sectie is verantwoordelijk voor de planning van ondersteunende taken binnen de ADIV. Dit omvat niet alleen de planning op het gebied van personeels-, materieel- en infrastructuurbeheer, maar ook de ontwikkeling van een digitaliseringsproject dat vooral tot doel heeft het werk van de analisten en de documentatie te verbeteren door bepaalde processen te automatiseren.

De sectie «Interne controle»

Deze sectie heeft tot doel een doeltreffend beheersingssysteem voor de organisatie te implementeren. Het betreft een systeem van goede beheerspraktijken om ervoor te zorgen dat de doelstellingen worden bereikt via de cyclus "Plan Do Check Act". Bijzondere aandacht wordt besteed aan proces- en risicobeheer. Deze sectie is verantwoordelijk voor het bepalen, in samenwerking met de verschillende directeurs, van de strategische en operationele doelstellingen van de ADIV. Ze geeft ook gevolg aan de aanbevelingen van onze toezichthoudende organen. Ten slotte trekt ze lessen uit de resultaten van een crisis en stelt ze een jaarverslag op.

> Naast deze secties is er een **projectofficier cultuur**, die tot doel heeft de organisatiecultuur, de veiligheidscultuur en de inlichtingencultuur te bevorderen. Het doel is het personeel te verenigen rond gemeenschappelijke waarden en gedragingen en een gevoel van verbondenheid met de ADIV te ontwikkelen.

DIRECTIE SUPPORT

De belangrijkste taak van de Directie Support van de ADIV is advies en ondersteuning te verlenen aan de chef van de ADIV en alle directies van de ADIV op het gebied van personeel, veiligheid, materieel, infrastructuur, vorming, training en begroting. De Directie Support is ook verantwoordelijk voor het toezien op de Defensieattachés via het **Defence Attaché Office** (DAO).

ADVIES, ONDERSTEUNING EN MIDDELENBEHEER ZIJN DE ESSENTIËLE DIENSTEN DIE ONZE DIRECTIE SUPPORT LEVERT OM DE STRATEGIE EN AMBITIES VAN DE DIENST TE WAARBORGEN

DE DIRECTIE SUPPORT IS VERDEELD IN ZES SECTIES, DIE ELK VERANTWOORDELIJK ZIJN VOOR SPECIFIEKE GEBIEDEN :

Personeelsbeheer

Deze sectie adviseert de commandant over alle aangelegenheden betreffende het personeel van de ADIV. Ze houdt het personeelsbestand bij, plant en zorgt voor de aanstelling van het personeel in het kader van de verschillende mutatieplannen of de ondersteuning van operaties van de ADIV. Ze coördineert en implementeert ook de verschillende richtlijnen van Defensie op dit gebied.

Ze is bovendien verantwoordelijk voor het beheer van het reservepersoneel van de ADIV.

Veiligheid

Deze sectie is verantwoordelijk voor de veiligheidsproblemen binnen de ADIV. Dit domein omvat de bescherming van personen, installaties, uitrusting en informatie van de ADIV.

Ze treedt op als veiligheidsofficier in de zin van de wet in het kader van de veiligheidsmachtigingen voor alle personeelsleden van de ADIV. Ze houdt een lijst van veiligheidsincidenten bij, voert de onderzoeken uit en stelt zo nodig corrigerende maatregelen voor.

Beheer van materieel en infrastructuur

Op het gebied van materieel is deze sectie verantwoordelijk voor de bevoorrading, verwijdering en het beheer van al het materieel van de ADIV, met uitzondering van zendapparatuur, computerapparatuur en cryptoapparatuur. Ze is verantwoordelijk voor het coördineren en bekendmaken van de behoefte-uitdrukking voor dit materieel met de beheerders van het Directoraat-generaal Material Resources. Deze sectie beheert ook alle voertuigen en transportaanvragen van de ADIV.

Ten slotte is ze verantwoordelijk voor het onderhoud van de infrastructuur die door de diensten van de ADIV wordt gebruikt, met de steun van de kazernering van het kwartier.

Beheer van communicatie- en informatiesystemen

Deze sectie adviseert de Chef van ADIV over de informatiesystemen en het informatiebeheer binnen de ADIV. Ze geeft een opportuniteitsadvies over de behoefte aan zendapparatuur, computerapparatuur en cryptoapparatuur. Ze biedt logistieke en technische ondersteuning voor de interne ADIV-netwerken en implementeert de door de functionele autoriteiten vastgestelde rechten en toegangen. Ze zorgt voor de ondersteuning van het Information Management binnen de eenheid.

Vorming en training

Deze dienst analyseert de behoeften en het vormings- en trainingsaanbod voor alle ADIV-medewerkers, zowel intern als extern. De dienst coördineert en zorgt voor vormings- en trainingsperiodes. Ten slotte worden de vormingen geëvalueerd en wordt het aanbod ontwikkeld in functie van de evolutie van de behoeften.

Budgetbeheer

Deze sectie adviseert de Chef van ADIV over het gebruik van de aan de ADIV toegewezen budgetten. Ze stelt een begrotingsplan op en stelt prioriteiten overeenkomstig de beschikbare middelen. Met het onderdepartement Operaties & Training coördineert ze alle geldelijke aspecten van de zendingen voor het personeel. Deze dienst zorgt ook voor de financiële ondersteuning en de boekhouding van de Belgische Defensieattachés in het buitenland. Ten slotte is de dienst verantwoordelijk voor het beheer van visa en dienstpaspoorten.

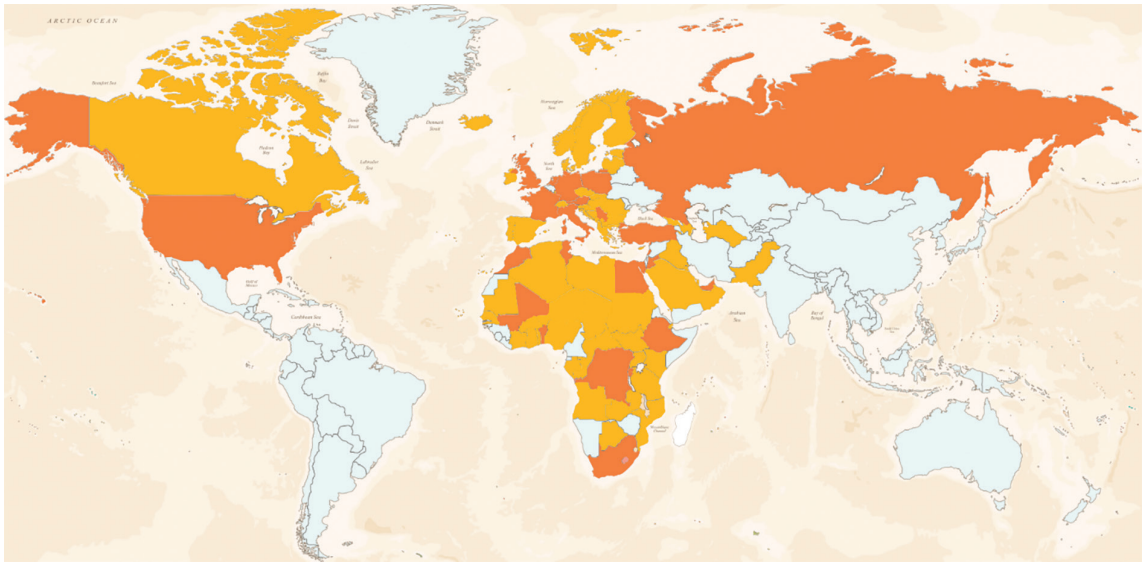
ONZE DIENST DEFENSIEATTACHÉS

De Dienst Defensieattachés is verantwoordelijk voor de contacten met Belgische en buitenlandse Defensieattachés, alsook met Belgische militaire adviseurs en veiligheidsattachés in het buitenland.

Deze dienst is belast met de toepassing van de selectieprocedure voor Belgische Defensieattachés, militaire adviseurs, veiligheidsattachés en hun Belgische assistenten die in het buitenland worden aangesteld. De dienst stelt hun specifieke vormingsprogramma vast. De dienst fungeert ook als tussenpersoon bij de verschillende secties van de Directie Support van de ADIV op logistiek, financieel en administratief gebied. In coördinatie met verschillende andere diensten van de ADIV organiseert deze dienst de evaluaties van alle posten volgens een specifiek tijdschema.

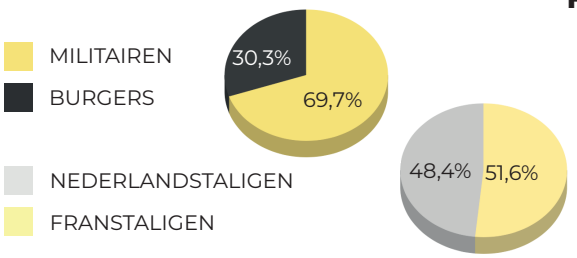
De Dienst Defensieattachés heeft ook de leiding over de bij België geaccrediteerde buitenlandse Defensieattachés en is betrokken bij de afronding van het accreditatieproces op Belgisch grondgebied. De dienst die verantwoordelijk is voor de buitenlandse Defensieattachés is het bureau dat werd aangewezen als enig contactpunt voor Defensie. Het centraliseert alle correspondentie (verzoeken om inlichtingen, bezoekaanvragen, verzoeken om een onderhoud, uitnodigingen, het aanbieden van cursussen enz.) van de voor België geaccrediteerde buitenlandse Defensieattachés. Elk jaar stelt de dienst die verantwoordelijk is voor de buitenlandse Defensieattachés een activiteitenprogramma op ten behoeve van de buitenlandse Defensieattachés, waaronder bezoeken aan Defensie-eenheden en aan de Belgische defensie-industrie. Ook is er jaarlijks een informatiesessie gepland die wordt voorgezeten door de Chef Defensie.

De onderstaande kaart geeft een overzicht van alle landen waar Belgische Defensieattachés op post zijn (oranje) en de landen waarvoor zij geaccrediteerd zijn (oranje en geel).



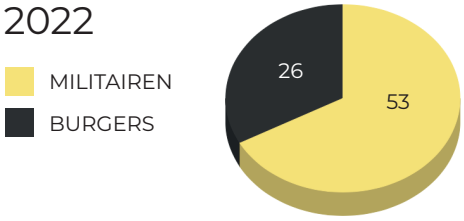
ONZE CIJFERS

PERSONEEL



AANTAL AANGEWORVEN PERSONEN (PERSONEELSGROEI)

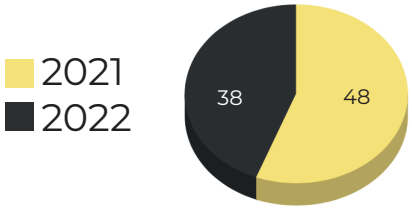
2022



IMPACT IN DE MEDIA

AANTAL KEREN VERMELD IN NATIONALE GEDRUKTE MEDIA	**219**
AANTAL KEREN VERMELD IN NATIONALE ELEKTRONISCHE MEDIA	**294**
CUMULATIEVE UREN ZENDTIJD OP NATIONALE TELEVISIE EN RADIO	**27H**

AANTAL ONDERWERPEN BETREFFENDE PARLEMENTAIRE VRAGEN



AANTAL «PAPERS»

	2021	2022
Informatieverzoeken van onze klanten en partners	5350	6982
	30,50% evolutie in % ten opzichte van 2021	
Hoeveelheid input	65323	69748
	6,77% evolutie in % ten opzichte van 2021	
Hoeveelheid ouput		
Verzoeken om informatie aan partners (nationaal en internationaal)	60	320
	433,33% evolutie in % ten opzichte van 2021	
Antaal ADIV-producties	486	591
	21,60% evolutie in % ten opzichte van 2021	

AANWERVING

Menselijk kapitaal, onze grootste troef:

IT-werving is nauw verbonden met de digitale transformatie van onze samenlevingen. Meer bepaald op het gebied van cyberveiligheid en cyberdefensie gaat de kwantitatieve en kwalitatieve evolutie van de behoeften aan menselijk kapitaal hand in hand met de snelle en ontwrichtende evolutie van de risico's en bedreigingen op het vlak van cyberveiligheid. In de context van wat we gewoonlijk collectieve verdediging noemen, draait alles om de cyberweerbaarheid van onze staat in rechtstreeks verband met onze wervingscapaciteit.

Protect-Defend-Collect-Fight... & recruit with agility:

Het Cyber Command omvat al niet minder dan 40 beroepen, "STEM" (Science, Technology, Engineering and Mathematics) en «niet-STEM», die verband houden met zijn vier activiteitendomeinen. De doelstelling om onze soevereiniteit in cyberspace te doen gelden resulteert dus duidelijk in gestage wervingsdoelstellingen voor de komende tien jaar en daarna. De bezinning over de beroepen van de toekomst is al begonnen.

Defensie is nooit zomaar een job, het is altijd een MISSIE... met een grote maatschappelijke meerwaarde:

In termen van aantrekkingskracht, tussen een overvloed aan Cyber-IT-vacatures uit andere sectoren, kan het Cyber Command rekenen op een ongewone positionering met betrekking tot de specificiteit van de Krijgsmacht en de opdrachten die exclusief voorbehouden zijn aan onze Defensie. Als werkgever investeert Defensie massaal in opleiding en het voortdurend op peil houden van de vaardigheden van haar medewerkers, zowel burgers als militairen.

INNOVEREN IN MENSELIJK KAPITAAL: EEN GROTE UITDAGING EN EEN GROTE KANS

Verkennende en innovatieve projecten:

Het gebrek aan geschikte competentieprofielen op de arbeidsmarkt is berucht. Sommige essentiële competenties om aan de behoeften van morgen te voldoen, zijn op onze scholen nog steeds niet verheven tot het niveau van transversale competenties. Bovendien is het duidelijk dat noch onze directe concurrenten op de arbeidsmarkt, noch onze zelfverklaarde tegenstanders in cyberspace last hebben van bepaalde bureaucratische rompslomp bij hun eigen inspanningen om mensen aan te trekken en in dienst te nemen. Het Cyber Command is niet bedoeld om een talentenoorlog te beginnen. Maar veeleer om talrijke belanghebbenden te verenigen rond een gemeenschappelijk maatschappelijk project: elke cybervaardige burger in staat stellen zijn tijd en talent ten dienste te stellen van een nieuw soort reserve. Hiervoor zijn «junior»-profielen, niet noodzakelijkerwijs afgestudeerd, maar vol talent, en gecertificeerd door externe instanties, een interessante optie. In die zin heeft het Cyber Command in de verenigingssector een reeks partnerschappen ontwikkeld met vzw's zoals «Molengeek» of «BeCode».

ONZE SAMENWERKING MET DE VEILIGHEID VAN DE STAAT: HET NATIONAAL STRATEGISCH INLICHTINGENPLAN

In 2018 hebben de Veiligheid van de Staat en de ADIV nauw samengewerkt en bepaalde taken of capaciteiten gedeeld. Zo hebben medewerkers van beide diensten zich verenigd in een gemeenschappelijk platform voor terrorismebestrijding. Ook de controleteams werden samengevoegd. Andere synergieën zijn versterkt, in het bijzonder bij het beheer van de menselijke bronnen. Dit werd geformaliseerd in een nationaal strategisch inlichtingenplan (NSIP 2018).

In 2022 hebben de twee diensten besloten nog verder te gaan in hun samenwerking.

VIER GEBIEDEN ZIJN ALS PRIORITAIR AANGEMERKT:

1. De strijd tegen extremisme en terrorisme

2. De strijd tegen spionage en inmenging

3. Cyberinlichtingen

4. De onderlinge koppeling van de ICT-omgevingen (Information and Communication Technologies).

De twee inlichtingen- en veiligheidsdiensten hebben elk hun eigen opdrachten en specifieke capaciteiten, maar zij vullen elkaar aan. Het delen van gegevens, het uitwisselen van kennis, het harmoniseren van processen, het bundelen van taken of het centraliseren van middelen zijn manieren om de efficiëntie van beide diensten te vergroten en zo bij te dragen tot de nationale veiligheid.

De strijd tegen terrorisme en extremisme

In overeenstemming met de oprichting van het gezamenlijke platform voor terrorismebestrijding zullen de Veiligheid van de Staat en de ADIV ook hun taken en middelen bundelen om extremisme te bestrijden. Daartoe zal het bestaande platform voor terrorismebestrijding worden omgevormd tot een gemeenschappelijk platform voor de bestrijding van confessioneel extremisme en terrorisme en zal een tweede platform voor de bestrijding van ideologisch extremisme en terrorisme worden opgericht.

De strijd tegen spionage en inmenging

Om spionage en inmenging te bestrijden zal de samenwerking de vorm aannemen van «Houses» waarin de verschillende dreigingen van landen of entiteiten samen prioriteit krijgen. De taken worden zo optimaal mogelijk verdeeld en voor de behandeling van bepaalde dossiers kunnen gemengde teams worden gevormd.

Cyberinlichtingen

Cyber Intelligence heeft tot doel informatie te verzamelen over bedreigingen in cyberspace en deze te analyseren voor inlichtingendoeleinden. Informatie verzamelen in cyberspace kan op verschillende intrusieve of niet-intrusieve manieren. De ADIV ontwikkelt een aanzienlijke cybercapaciteit via zijn Cyber Command. De samenwerking op dit gebied is erop gericht de Veiligheid van de Staat te laten genieten van de capaciteiten van de ADIV door ze te koppelen aan de specifieke niches die binnen de Veiligheid van de Staat zijn ontwikkeld.

De koppeling van ICT-omgevingen

Om de samenwerking en uitwisseling tussen beide inlichtingen- en veiligheidsdiensten structureel te ondersteunen, is een diepgaande koppeling van de ICT-omgevingen van beide diensten onontbeerlijk. Daartoe moeten de respectieve ICT-ontwikkelingen op elkaar worden afgestemd. Dit zal onder meer een snelle en efficiënte uitwisseling van geclassificeerde informatie, de harmonisatie, waar nodig, van IT-processen en het gebruik van gemeenschappelijke tools mogelijk maken.

Ook andere synergieën worden versterkt, in het bijzonder op het gebied van vorming en training.

De Veiligheid van de Staat en de ADIV stellen alles in het werk om de verschillende synergieën die in het nationaal strategisch inlichtingenplan 2022 zijn voorzien, tot stand te brengen.

ONZE PARTNERS

DEFENSIE
VEILIGHEID VAN DE STAAT
POLITIE
DOUANE
FOD ECONOMIE
FOD BUITENLAND ZAKEN
NATIONAAL CRISIS CENTRUM
CFI
MP/OM
OCAD
EUROPA
NAVO
CCB
COMITÉ I
FOD JUSTITIE

De ADIV maakt deel uit van verschillende gemeenschappen:

- De inlichtingengemeenschap, zowel op nationaal niveau met de Veiligheid van de Staat en het OCAD, als op internationaal niveau met de buitenlandse inlichtingendiensten.
- De veiligheidsgemeenschap, waardoor de ADIV nauwe banden onderhoudt met de geïntegreerde politie, het openbaar ministerie, de douane, het CCB, het crisiscentrum ... De ADIV is lid van de Nationale Veiligheidsoverheid.
- Internationale organisaties, waarvan de belangrijkste de Europese Unie en de NAVO zijn.
- Als hoofdzakelijk extern gerichte dienst onderhoudt de ADIV nauwe betrekkingen met de FOD Buitenlandse Zaken.

Vanwege zijn brede scala aan bevoegdheden onderhoudt de ADIV ook banden met tal van andere Belgische instellingen, te veel om op te noemen: Dienst Vreemdelingenzaken, CGVS, CFI, IACSSO en FANC...

Het is voor een inlichtingendienst essentieel om vertrouwensrelaties met zijn partners te onderhouden en informatie uit te wisselen. Ook de synergieën met de federale politie moeten worden versterkt, in het bijzonder op het gebied van opleiding en Cyber. De ADIV heeft een nieuwe verbindingsofficier aangesteld om deze contacten en de verdere samenwerking met Buitenlandse Zaken te vergemakkelijken.

Het **Centrum voor Cybersecurity België (CCB)** coördineert de uitvoering van de nationale cyberveiligheidsstrategie waarvan de ADIV en in het bijzonder zijn Cyber Command een actieve partner is. Wij leveren het CCB niet alleen technische hulp bij het reageren op incidenten, maar ook expertise op het gebied van malwareanalyse en diepgaande analyses van cyberdreigingen van statelijke actoren dankzij onze unieke inlichtingenpositie.

Op internationaal niveau werkt de ADIV samen met de Veiligheid van de Staat aan een actualisering van de door de Nationale Veiligheidsraad goedgekeurde richtlijn over de betrekkingen met buitenlandse inlichtingendiensten.

ONZE RETROSPECTIEVE VAN DE MEDIA IN 2022

Januari - Februari - Maart:

- Het stuurplan van de ADIV voor het jaar 2022 wordt goedgekeurd door de minister van Defensie.
- Op 10 februari wordt door de Kamer de wet goedgekeurd die extra veiligheidsmaatregelen invoert voor de verstrekking van mobiele 5G-diensten. De wet schrijft voor dat mobiele operatoren die 5G-componenten willen gebruiken, vooraf toestemming moeten krijgen. Die toestemming zal komen van een groep bestaande uit de premier en de ministers van Telecommunicatie, Defensie, Justitie, Binnenlandse en Buitenlandse Zaken. Om het risicoprofiel van de provider te bepalen, zullen de ministers zich baseren op een advies van de inlichtingen- en veiligheidsdiensten en het BIPT (de telecomregulator).
- De ADIV wordt in het kernkabinet gehoord over de oorlog in Oekraïne.
- De inval van Rusland in Oekraïne gaat gepaard met een golf van Russische cyberoperaties, zowel in Oekraïne als daarbuiten. Onder leiding van het centrum voor computerbeveiliging zijn op nationaal niveau verschillende initiatieven genomen en is overleg gepleegd met vertegenwoordigers van de Directie Cyber. Onze teams waren verantwoordelijk voor het toezicht op verdachte cyberactiviteiten in nauwe samenwerking met de NAVO en andere internationale partners.
- De ADIV waarschuwt het Defensiepersoneel om extra waakzaam te zijn voor incidenten die verband kunnen houden met de Russische inval in Oekraïne.
- België zet 21 Russische diplomaten uit.
- De minister van Defensie legt in de commissie Landsverdediging achter gesloten deuren een plan ter verbetering van de werking van ADIV (Stuurplan 22) voor.
- Op 30 maart verschijnt een interview van de minister van Defensie en viceadmiraal Wim Robberecht in De Standaard en La Libre over het stuurplan.

April - Mei - Juni:

- Op 7 april verschijnen in de Nederlandstalige pers beschuldigingen over de aankoop en het gebruik door de ADIV van wifirouters van Huawei. Deze poging tot desinformatie wordt door viceadmiraal Wim Robberecht in verschillende interviews ontkend.
- Het kabinet van de minister van Justitie zou graag zien dat in de bepalingen inzake overheidsopdrachten de mogelijkheid wordt opgenomen om een offerteaanvraag te weigeren indien er gevaar voor spionage bestaat.
- Op 29 mei verschijnt in De Tijd en L'Echo een interview met viceadmiraal Wim Robberecht over de structurele evolutie van de ADIV.
- Minister van Justitie Vincent Van Quickenborne en minister van Defensie Ludivine Dedonder dienen in het parlement een wetsontwerp in om de Belgische inlichtingendiensten meer armslag te geven.
- Er verschijnen artikels op de eerste verjaardag van de «Jürgen Conings»-crisis.
- De verschillende regeringen van ons land sluiten een samenwerkingsovereenkomst binnen het Raadgevend comité. Het gaat om een screeningsmechanisme voor buitenlandse investeringen in sectoren die van belang zijn voor de openbare orde en veiligheid of van strategisch belang zijn.
- Operatie Cerberus is een succes. België heeft 16 kinderen van jihadisten en zes moeders met de Belgische nationaliteit gerepatrieerd uit een door Koerden gecontroleerd kamp in het noordoosten van Syrië met een Defensievliegtuig.
- De commissie Economie van de Kamer keurt in tweede lezing de nieuwe versie van de wet inzake dataretentie goed, die telecomoperatoren verplicht de metadata van hun klanten te bewaren.
- De ADIV neemt zijn nieuwe "Mission Statement" aan: missie, visie en waarden.
- De regering dient met spoed een wetsontwerp in bij het parlement over vijf verdragen inzake wederzijdse rechtshulp.

Juli - Augustus - September:

- De wet tot wijziging van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten wordt aangenomen.
- ADIV en VSSE ondertekenen een nieuwe samenwerkingsovereenkomst: het nationaal strategisch inlichtingenplan 2.0 (NSIP22).
- Op een persconferentie van Buitenlandse Zaken wordt de cyberaanval op Defensie toegeschreven aan Chinese actoren. In de eerste helft van 2022 werden inspanningen geleverd om alle aangevallen systemen weer operationeel te maken en alle malware te verwijderen. Er werd een verslag over de afhandeling van het incident vergezeld van een inlichtingenverslag met technische bevindingen verstrekt.
- Het Defensiepersoneel (burgers en militairen) zal om de vijf jaar gescreend worden.
- Volgens een rapport van het OCAD worden in België ongeveer 500 jihadstrijders prioritair gevolgd.
- In september wordt de wet tot invoering van een algemene regeling betreffende het declassificeren van geclassificeerde documenten in het Belgisch Staatsblad gepubliceerd. Deze wet zorgt ervoor dat geclassificeerde documenten niet langer voor onbepaalde tijd geclassificeerd kunnen blijven. De wet bepaalt dat de regering van oorsprong na een periode van 20 jaar (voor vertrouwelijke documenten), 30 jaar (voor geheime documenten) of 50 jaar (voor zeer geheime documenten) moet beslissen of een geclassificeerd document kan worden gedeclassificeerd. Indien de overheid van oorsprong van oordeel is dat het op dat ogenblik niet kan worden gedeclassificeerd, moet dit grondig worden gemotiveerd. Een document kan nooit langer dan 100 jaar geclassificeerd blijven. Daarna vervalt de classificatie automatisch.
- Er zijn berichten dat na een onderzoek van de ADIV een Belgische militair uit zijn functie is ontheven vanwege zijn sterke sympathieën voor het rechts-extremisme.

Oktober - November - December:

- De nieuwe ADIV-structuur wordt uitgevoerd.
- De inhuldiging van het Cyber Command vindt plaats in Evere in aanwezigheid van de minister van Defensie: het zal zorgen voor de exploitatie van cyberspace ten behoeve van de hele natie, Defensie en de ADIV. De ambitie van het Cyber Command is een nationale referentie te worden op het gebied van cryptografie en een centrale positie in te nemen in het federale ecosysteem voor cyberbeveiliging. Dankzij zijn netwerk van partners in de economische, academische en verenigingswereld zal het zorgen voor de groei van de toekomstige vijfde component.
- De Chinees Yanjun Xu wordt in de Verenigde Staten veroordeeld tot 20 jaar gevangenisstraf wegens bedrijfsspionage.
- De investeringen van China in de havens van Antwerpen en Zeebrugge houden een risico in van inmenging of beïnvloeding van onze besluitvorming, aldus de minister van Justitie in de commissie Justitie van de Kamer.
- Het stuurplan voor de jaren 2023 tot en met 2027 (SP ADIV 23-27) is voltooid.
- Uit het kerstinterview van Belga met viceadmiraal Wim Robberecht blijkt dat er over het algemeen meer naar de ADIV geluisterd wordt door politici.
- De puzzel van de ADIV wordt onthuld. Dit spel is bedoeld om de belangstelling te wekken van het grote publiek voor de inlichtingenwereld.

ONZE VOORUITZICHTEN VANDAAG OP DE BEDREIGINGEN VAN MORGEN

Door de Directie Inlichtingen en per thema :

Terrorisme

Het aantal incidenten, die door de aard van hun motivatie als religieus-terroristische aanslagen kunnen worden aangemerkt, zal in 2023 naar verwachting stabiel zijn ten opzichte van 2022.

In 2022 werden verschillende hooggeplaatste leden van de twee belangrijkste internationale jihadistische bewegingen, Al Qaida en Islamitische Staat, uitgeschakeld. In tegenstelling tot wat in het verleden is waargenomen, hebben de twee organisaties niet gecommuniceerd over de aanstelling van opvolgers. Voorts is er momenteel geen bevestigde informatie over de reactivering van een structuur voor de organisatie van externe operaties gericht op westerse landen en/of België binnen deze twee bewegingen. Hoewel de capaciteit momenteel waarschijnlijk ontbreekt, blijft de terroristische opzet van deze groepen echter bestaan. Bovendien kunnen opportuniteitsaanslagen en/of -eisen niet worden uitgesloten, evenals de daad van een op zichzelf geradicaliseerde persoon. Een aanslag door een eenling is trouwens het meest waarschijnlijke scenario.

Extremisme

De dreiging van niet-religieus extremisme zal in 2023 naar verwachting niet afnemen.

De economische crisis, nog verergerd door de energiecrisis en de oorlog in Oekraïne, zal worden gekenmerkt door een aanhoudende hoge inflatie die de koopkracht zal blijven drukken, in het bijzonder voor de meest kwetsbare groepen. Deze crisis zal dus het ontstaan van protestbewegingen in de hand werken, waarvan extremistische groeperingen, zowel links als rechts, gebruik zullen proberen te maken. De aanhoudende migratiedruk op Europa zal de extreemrechtse propaganda blijven voeden. Door de structurele fragmentatie van het politieke toneel in veel westerse democratieën en de polarisatie die door het gebruik van sociale netwerken wordt bevorderd, zullen extremistische groepen en individuen aantrekkelijk blijven. Het ontstaan van nieuwe vormen van extremisme die slechts in geringe mate voldoen aan de criteria voor links- en rechts-extremisme, maar gekenmerkt worden door het aanhangen van complottheorieën, zal zich waarschijnlijk voortzetten. Het ontstaan van een nieuwe gezondheidscrisis zou in dit verband een katalysator zijn.

Proliferatie

In het algemeen blijft de architectuur van de non-proliferatie van massavernietigingswapens eroderen.

Deze tendens ondermijnt de internationale betrekkingen, bevordert de wapenwedloop en vergroot daardoor het risico van escalatie en misrekening. Vanuit dit oogpunt is Rusland de belangrijkste en meest directe bedreiging voor de Euro-Atlantische vrede, vooral in de huidige context van zijn invasie in Oekraïne. In het Midden-Oosten vormt het gedrag van Iran (ballistische en nucleaire ontwikkelingen, inmenging) een groot potentieel voor destabilisatie in een regio die van groot belang is voor de wereldeconomie. Het Syrische regime, met Russische steun, blijft een uitdaging voor de chemische ontwapening. In Azië blijven de conflicterende betrekkingen tussen de kernmachten Pakistan en India, de opkomst van China en de nucleaire ontwikkelingen in Noord-Korea een bron van zorg. In het Westen blijft de terroristische CBRN-dreiging bestaan.

Door de Directie Inlichtingen en per land :

Rusland

Verschillende uitzettingen leidden tot een tijdelijke vermindering van de Russische inlichtingencapaciteit op Belgisch grondgebied. Niet alleen de uitzetting van 21 Russische diplomaten verbonden aan de Russische ambassade in België en het consulaat in Antwerpen op 29 maart, maar ook die op 5 april van 19 Russische diplomaten van de Russische missie bij de EU. Het verslechterde beeld van Rusland in de Belgische samenleving als gevolg van de oorlog versterkt deze tendens.
De Russische inlichtingendiensten zullen zich echter aan de veranderende situatie aanpassen om aan hun inlichtingenbehoeften te voldoen.

China

Met de derde ambtstermijn van XI Jinping zijn de inlichtingenbehoeften van de Chinese Communistische Partij (CCP) steeds meer op het buitenland gericht. Voor het eerst maakt een hoofd van de inlichtingendienst deel uit van het Politburo, wat zal leiden tot meer middelen voor de inlichtingendiensten. Deze zijn bedoeld om inlichtingen te verschaffen die China in staat stellen technologisch zelfvoorzienend te worden, zich te positioneren in conflicten met het Westen en de economische belangen van China wereldwijd veilig te stellen.

Met het verzamelen van inlichtingen en de invloed op de EU en de NAVO zal het belang van België in het Chinese inlichtingenwerk alleen maar toenemen.

Afrikaanse landen

De komende parlementsverkiezingen in de RDC en Rwanda moeten de wil van de verschillende Afrikaanse autoriteiten versterken om door te gaan met activiteiten ter ondersteuning van hun nationale belangen. De inval van Rusland in Oekraïne zal waarschijnlijk ook gevolgen hebben voor het Afrikaanse continent in 2023. Revisionistische staten zoals China of Rusland kunnen trachten Afrikaanse proxies te gebruiken als instrumenten om een voordelige, zelfs dominante positie ten opzichte van politieke, militaire of economische rivalen te verwerven of te consolideren. Dergelijke spanningen kunnen gevolgen hebben in België of voor de Belgische belangen en bevolking in Afrika.

De ADIV zal daarom de internationale ontwikkelingen en de mogelijke gevolgen voor de activiteiten van de Afrikaanse inlichtingendiensten blijven volgen.

Door de Directie Cyber Operations :

Algemeen

Cyberdreigingsactoren zijn steeds meer geïnteresseerd in aanvallen op de IT-toeleveringsketen en aanvallen op aanbieders van cloud- en IT-diensten.

Dankzij dergelijke aanvallen kunnen deze actoren voet aan de grond krijgen in de entiteiten die zij als doelwit kiezen. De verstoring van satellietcommunicatie zal op korte tot middellange termijn waarschijnlijk een steeds belangrijkere trend worden. De verstoring van glasvezelkabels kwam in 2022 in het nieuws en het is waarschijnlijk dat dergelijke cyber-fysieke aanvallen op korte tot middellange termijn zullen toenemen.

Rusland

Op korte termijn zal de Russische militaire inlichtingendienst GRU fors in beslag genomen worden door Oekraïne, terwijl de Russische buitenlandse inlichtingendienst SVR regeringen, ngo's en denktanks blijft aanvallen met nieuwe malware. Economische sancties die de toegang van Rusland tot technologie beperken, kunnen leiden tot een toename van economische cyberspionage.
Na in de eerste helft van 2022 ontwrichtende aanvallen tegen Oekraïne te hebben uitgevoerd met maar liefst 9 gegevenswissers, bleven GRU-gelieerde actoren Oekraïne in de tweede helft van 2022 aanvallen met nieuwe malware voor het

wissen van gegevens.

In 2022 werden nieuwe soorten Russische malware ontdekt die gericht zijn op industriële besturingssystemen en operationele technologieën. Een Russische aanval op het elektriciteitsnet in Oekraïne kan de stroomvoorziening verstoren. Russische statelijke actoren hebben ook cyberverkenningen uitgevoerd tegen kritieke infrastructuur in westerse landen. Analisten maken zich zorgen over een mogelijke aanval op westerse kritieke infrastructuur als de oorlog in Oekraïne zich uitbreidt tot buiten het Oekraïense toneel.

Pro-Russische hacktivisten hebben een toenemend aantal verstorende cyberaanvallen uitgevoerd tegen bijna alle NAVO-landen (en daarbuiten), vaak als reactie op acties van deze landen die Rusland als bedreigend ervaart. De Baltische staten werden naar verluidt het hardst getroffen door de hacktivisten, waardoor Rusland cyber- en desinformatieoperaties kon uitvoeren. Deze verstorende cyberaanvallen zullen in 2023 doorgaan en zijn vaak een Russische reactie op een krachtig politiek statement of de levering van militair materieel aan Oekraïne.

Cybercriminaliteit in de vorm van ransomwareaanvallen wordt sinds de tweede helft van 2022 steeds vaker gebruikt als geopolitiek wapen, niet alleen tegen Oekraïense entiteiten maar ook tegen regeringsdiensten van NAVO-leden (bv. Montenegro).

Ransomwareaanvallen bieden Rusland niet alleen de mogelijkheid aannemelijke ontkenning te claimen, maar stellen het ook in staat vernietigende aanvallen tegen NAVO-leden uit te voeren, terwijl het onder de drempel van artikel 5 blijft. Daarom denken wij dat deze trend om ransomware als geopolitiek wapen te gebruiken, zal aanhouden.

China

Cyber targeting zal waarschijnlijk economische en militaire belangen blijven dienen, met bijzondere aandacht voor landen die een belangrijke rol spelen in China's "Belt and Road"-initiatieven en in China's strategische doelstellingen in de Zuid-Chinese Zee. De verstorende aanvallen van Chinese hacktivisten op Taiwan tijdens het bezoek van mevrouw Nancy PELOSI aan Taipei in augustus 22 zullen waarschijnlijk worden herhaald indien China het optreden van andere landen ten aanzien van Taiwan als strijdig met China's «één-China-beginsel» beschouwt.

Rest van de wereld

Verstorende cyberoperaties tegen de regeringsdiensten van een NAVO-partner (Albanië) zijn toegeschreven aan Iran, hetgeen doet vermoeden dat Iran zich in de toekomst minder terughoudend zal opstellen bij het aanvallen van EU/NAVO-doelen. Een in Irak gevestigde Iraanse proxygroep heeft twee keer Oekraïense doelwitten aangevallen, wat kan wijzen op een toenemende samenwerking tussen Iran en Rusland op het gebied van cyberoperaties.

Hoewel sommige offensieve cyberactoren uit de privésector, zoals de Israëlische groep NSO (Pegasus), door verschillende regeringen onder de loep worden genomen, blijkt uit persberichten dat de handel in cyberhuurlingen een hoge vlucht neemt. Met hun «surveillance as a service»-aanbod kunnen hun klanten de netwerken, computers en smartphones van hun doelwitten (vaak dissidenten, journalisten, mensenrechtenactivisten) binnendringen.

Een trend om in de gaten te houden is de samenwerking van offensieve cyberactoren uit de privésector met militaire privébedrijven (bv. de Wagner-groep).

WIJ DOEN HET WERK

Wij zijn de ogen en oren van onze natie. We zoeken naar wat onze vijanden geheim willen houden. Wij treden op waar onze tegenstanders zich schuilhouden, altijd in de schaduw en met maximale discretie. We winnen inlichtingen in over onze tegenstanders om te anticiperen op nieuwe bedreigingen en de veiligheid van onze militaire geheimen en technologische kennis te waarborgen.

Wij adviseren onze politieke en militaire leiders zodat zij onafhankelijk en soeverein de beste keuzes kunnen maken om ons land en zijn burgers zo goed mogelijk te beschermen. We opereren overal ter wereld waar onze belangen dat vereisen. Vandaag zijn de bedreigingen voor onze samenleving immers nog complexer, onvoorspelbaarder en veelvuldiger.

We zijn aanwezig ter ondersteuning van militaire operaties, in de strijd voor cyberveiligheid en tegen spionage en inmenging, tegen terrorisme, tegen extremisme, tegen de verspreiding van massavernietigingswapens. Laten we daarnaast de strijd tegen sektarische of criminele organisaties en op wetenschappelijk en economisch gebied, zoals de bescherming van bedrijven en vitale infrastructuren, niet vergeten.

BEKNOPT LEXICON

ADIV : Algemene Dienst Inlichting en Veiligheid

VSSE : Veiligheid van de Staat

OCAD : Coördinatieorgaan voor de dreigingsanalyse

GRU : Russische militaire inlichtingendienst

SVR : Russische buitenlandse inlichtingendienst

NAVO : Noord-Atlantische Verdragsorganisatie

EU : Europese Unie

Ngo : niet-gouvernementele organisatie

CBRN : chemische, biologische, radiologische en nucleaire agentia of materialen

NSIP : Nationaal strategisch inlichtingenplan

SPADIV : Stuurplan ADIV

CGVS : Commissariaat-generaal voor de Vluchtelingen en de Staatlozen

FANC : Federaal Agentschap voor Nucleaire Controle

CFI : Cel voor Financiële Informatieverwerking

IACSSO : Informatie- en adviescentrum inzake schadelijke sektarische organisaties

CCB : Centrum voor Cybersecurity België

DAO : Defence Attaché Office

EDC : Eenheid van defensieve cyberoperaties

CSOC : Cyber Security Operations Centre

CSCU : Cyber-SIGINT Collection Unit

DICU : Digital Influence Collection Unit

OSINT : verzamelen van gegevens uit open bronnen en sociale media

T.E.S.S.OC : Terrorisme - Spionage - Subversie - Sabotage – Georganiseerde misdaad