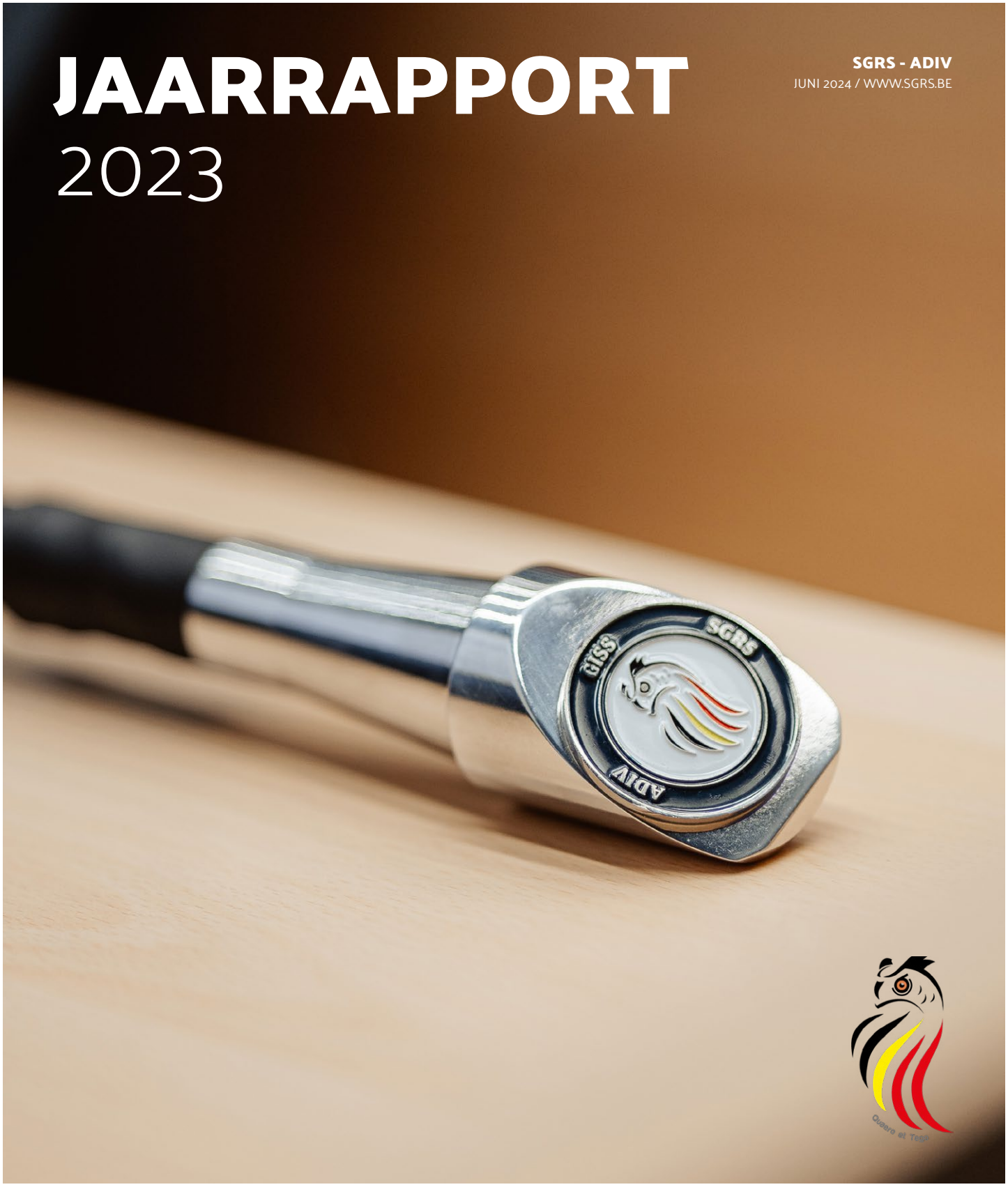
JAARRAPPORT
2023

SGRS - ADIV
JUNI 2024 / WWW.SGRS.BE



DEFENSIE

.be

De wereld verandert, maar onze missie blijft dezelfde

INHOUDSTAFEL

GENERAAL-MAJOOR
STÉPHANE DUTRON
CHEF VAN DE ADIV

Quaero et Tego is ons motto;

Het beschermen van ons land, onze bedrijven en onze expats door onze inlichtingen is onze primaire missie. Het adviseren van de autoriteiten is onze plicht tegenover ons land, onze samenleving en onze medeburgers.

VERANTWOORDELIJKE REDACTEUR

M. Van Hecke Bernard

Koningin Elisabethkwartier

Eversestraat 1, 1140 Evere

Foto's : DG StratCom en personeel ADIV

Lay-out: ADIV-SGRS

”Wij werken voor jou, voor ons ons land, voor vrede.”

Generaal-Majoor Stéphane Dutron

OVERNAME-OVERGAVE VAN DE RSM-STOK

Ajudant-majoor Frédéric Charlot, voormalig Korpsadjudant, heeft plaatsgemaakt voor de nieuwe Korpsadjudant Dolores Geeraert.

Introductie

Voor de inlichtingen- en veiligheidsdiensten was 2023 opnieuw een druk jaar op het vlak van de actualiteit.

De opeenvolgende staatsgrepen in West-Afrika, het weer oplaaien van het Israëlisch-Palestijns conflict, de voortdurende aanvalsoorlog van Rusland tegen Oekraïne en het conflict in het oosten van de Democratische Republiek Congo zijn maar enkele voorbeelden die we kunnen opnoemen.

Tijdens dezelfde periode bleven fenomenen, zoals extremisme, terrorisme, de georganiseerde misdaad, proliferatie en inmenging een structurele dreiging vormen voor het Europese continent. Zoals reeds aangegeven in het eerste verslag in 2022: de activiteiten op het gebied van spionage en buitenlandse inmenging hebben een niveau bereikt dat sinds de Koude Oorlog niet meer is voorgekomen. Deze tendens werd in 2023 helaas bevestigd. België, en Brussel in het bijzonder, als zetel van tal van internationale organisaties, blijven daarvan uiteraard niet gespaard.

Samenwerken voor een beter begrip

Om het hoofd te bieden aan die vele dreigingen, is samenwerking met de andere inlichtingen- en veiligheidsdiensten van essentieel belang, zowel op Belgisch als op internationaal vlak. Vooral de samenwerking met de Veiligheid van de Staat is van het grootste belang. In het kader van de invoering van het NSIP werd dit streven naar samenwerking concreet vertaald in de oprichting van platformen, die gemeenschappelijk zijn voor onze beide instellingen, voor de strijd tegen extremisme en terrorisme.

Tegelijkertijd wordt de digitalisering van mijn dienst voortgezet om de grondstof, waarmee wij werken, zo goed mogelijk te verwerken: de informatie. Wij moeten deze informatie beschermen, analyseren en in verband brengen met die van onze partners. Daartoe hebben wij moderne en beveiligde informaticamiddelen nodig, niet alleen voor het verzamelen ervan, maar ook voor de verwerking en verspreiding ervan.

De informatieoorlog, een realiteit

Het informatieterrein is overigens een nieuw slag- en beïnvloedingsveld geworden met de massale productie, door buitenlandse mogendheden, van leugenachtige content en/of content die verhalen promoot die tegen onze waarden ingaan. Het doel blijft hetzelfde, in België zowel als in de rest van de wereld: onze democratieën verzwakken door het vertrouwen in onze leiders

en onze instellingen te ondermijnen. Daartoe proberen deze mogendheden de publieke opinie te polariseren door gemeenschappen door middel van “fake news” tegen elkaar op te zetten. Wij hadden al toegezien op het verkiezingsproces in 2019 en wij schenken bijzondere aandacht aan de verkiezingen van juni 2024 met al onze partners op federaal niveau.

De modernisering van de ADIV voortzetten

Ik had het genoegen aan het hoofd te komen van de ADIV op 1 januari 2024. Ik wens mijn eer te betuigen voor het geweldige werk van mijn voorganger, viceadmiraal Wim Robberecht, die de functie van hoofd van de ADIV bijna drie jaar lang heeft bekleed. Hij heeft grondige veranderingen bewerkstelligd in onze organisatie en ik wens dezelfde koers aan te houden voor de transformatie en modernisering van onze dienst.

Ik ben mij ook bewust van een grote verantwoordelijkheid, want wij moeten onze ambities kunnen waarmaken in een wereld, waarin de traditionele geostrategische evenwichten ingrijpend veranderd zijn, waarin de veiligheidsuitdagingen veelsoortig zijn en waarin de crisissen elkaar opvolgen.

De maatschappelijke grondslag is de fundering van onze dienst. De ontwikkeling van onze communicatie, zoals dit tweede jaarverslag aantoont, is gericht op het versterken van deze band met de maatschappij en onze burgers, binnen de grenzen van transparantie die ons specifieke beroep ons oplegt.

Het is ook dankzij deze band dat wij verder gemotiveerd personeel zullen kunnen blijven rekruteren om onze tegenstanders te bestrijden, hier bij ons, in het buitenland of in cyberspace. Er zijn positieve signalen in die richting; zo hebben wij meer dan duizend kandidaten aangetrokken toen wij in 2023 40 vacatures van inspecteur hebben opengesteld.

Veel leesplezier!

GENERAAL-MAJOOR

Stephane Outron

VICE-ADMIRAAL
WIM ROBBERECHT

Chef van de ADIV van 2021 t.e.m. 2023

SGRS - ADIV / CYBER COMMAND

Cyber Command

Dag na dag wordt de ontwikkeling van het Cyber Command binnen de ADIV voortgezet alsook de introductie van een vijfde component binnen Defensie.

In onze steeds digitalere maatschappij is het van vitaal belang om de inlichtingen- en veiligheidscapaciteiten van de ADIV in cyberspace te versterken, maar ook om capaciteiten op het gebied van cyberdefensie, elektronische oorlogvoering en informatieoorlogvoering te ontwikkelen ter ondersteuning van alle componenten en heel Defensie.

Dit is zowel een menselijk als een technologisch avontuur. Menselijk, omdat we een groot aantal nieuwe medewerkers aanwerven uit verschillende achtergronden: Defensie, de academische wereld of onderzoek, of het verenigingsleven. We werven militairen, burgerpersoneel en reservisten aan. Het gaat zowel om STEM-profielen (Scientific, Technologic, Engineering, Mathematics) als om niet-STEM-profielen. Er zijn meer dan veertig functies in het Cyber Command. En we willen elk van deze profielen dezelfde kansen bieden om zich bij ons te ontwikkelen en door te groeien. Dit vergt niet alleen een enorme investering, maar ook een grote flexibiliteit. Maar ik ben ervan overtuigd dat deze diversiteit aan profielen en talenten deel uitmaakt van onze identiteit en de sleutel is tot ons succes.

Als onderdeel van deze “oorlog om talent” zetten we voornamelijk in op jonge mensen. In 2023 hebben we bijvoorbeeld de “Summer School” gelanceerd, de eerste cyberzomerschool voor studenten. Het is een onderdompeling van een week in militair milieu en achter de schermen van cyberdefensie, met onze experts en die van de Koninklijke Militaire School.

Tot nu toe zijn de wervingsresultaten zeer positief. Sinds de oprichting van het Cyber Command op 19 oktober 2022 is het aantal personeelsleden netto met meer dan 15% gestegen. Dit is een succes, aangezien de Belgische en internationale arbeidsmarkt bijzonder krap is op het vlak van cyberveiligheid.

Het is ook een technologisch avontuur, vooral met de opkomst van EDT’s (Emerging and Disruptive Technology) zoals artificiële intelligentie, soevereine cloudtoepassingen en post-kwantumcryptografie. Deze laatste technologieën bieden kansen, maar vormen ook krachtige dreigingen als ze worden misbruikt, met name in cyberspace.

Deze technologieën gaan een belangrijke rol spelen in de cryptografie, waardoor we de uitwisseling van extreem gevoelige informatie kunnen beveiligen of de communicatie- en commandosystemen kunnen beschermen die in de nieuwe wapensystemen van Defensie zijn geïntegreerd. Voorbeelden hiervan zijn het F-35 gevechtsvliegtuig, de nieuwe gemotoriseerde landcapaciteit en de toekomstige schepen van de marine.

We hebben een gecentraliseerd commando en een ambitieuze structuur binnen de ADIV ontwikkeld om ons in staat te stellen deze dreigingen het hoofd te bieden, ze op te sporen, erop te reageren en erop te anticiperen. Onze capaciteiten zullen verder versterkt worden binnen de inlichtingen- en veiligheidssfeer, omdat we daar intrinsiek mee verbonden zijn, of het nu gaat om ons wettelijk kader of de uitvoering van onze opdrachten.

Het avontuur gaat dus verder, en is eigenlijk nog maar net begonnen. Misschien met jou aan onze zijde?

GENERAL-MAJOOR

Michel Van Strythem

Ondertekening van een Memorandum of Understanding met de Koninklijke Militaire School over onderzoeks en ontwikkelingsprojecten.

Eerste bijeenkomst van cyberambassadeurs en Cyber Commanders tijdens het Belgische voorzitterschap van de Europese Unie.

De externe dreigingen van vandaag en morgen identificeren om ons er beter op voor te bereiden

De ADIV is de Belgische referentiedienst voor buitenlandse en defensie-inlichtingen.

In die hoedanigheid verschaft hij expertise in strategische en defensie-analyse aan zijn klanten, waarvan de voornaamste de Belgische regering en de minister van Defensie zijn.

Deze analyse stelt de ADIV in staat om, in het kader van de aan de ADIV toegekende bevoegdheden door de wet van 30 november 1998, dreigingen te identificeren die voortkomen uit ontwikkelingen buiten het Koninkrijk. Daartoe beschikt hij over een gediversifieerd netwerk voor het verzamelen van informatie. De ADIV ontwikkelt een versterkte samenwerking met bepaalde partners op het gebied van buitenlandse en defensie-inlichtingen, waaronder met name de FOD Buitenlandse Zaken.

De wereld in 2023

Twee conflicten, in Oost-Europa en het Midden-Oosten, hebben het nieuws in 2023 gedomineerd.

Op het militaire strijdtoneel in Oekraïne heeft het tegenoffensief in de zomer van 2023 geen enkele strategische wijziging van betekenis kunnen teweegbrengen. Het Oekraïense conflict is een uitputtingsoorlog geworden die waarschijnlijk zal voortduren.

In het Midden-Oosten heeft het weer oplaaien van het Israëlisch-Palestijnse conflict, door de gewelddadige reactie van Israël en de betrokkenheid van de Iraanse as via zijn proxy's, de regionale en internationale spanningen verhoogd. Dit heeft gevolgen gehad voor de maritieme veiligheid in de Rode Zee, met aanzienlijke economische repercussies.

Belangrijke geopolitieke ontwikkelingen

Deze twee conflicten zijn een weergave van de grote geopolitieke ontwikkelingen in de wereld. De "Rules-Based International Order", een systeem dat wordt gepromoot door de liberale democratieën en vooral wordt gesteund door de VN en de instellingen van Bretton Woods, wordt nu, steeds nadrukkelijker, ter discussie gesteld door revisionistische mogendheden zoals Rusland en Iran. . Het multilateralisme, de drijvende kracht achter de internationale betrekkingen van de afgelopen decennia, wordt ondermijnd. De westerse mogendheden wedijveren met hun geopolitieke rivalen om een verbond te sluiten met de grootmachten van het zogenaamde Globale Zuiden, die bonte verzameling van zuidelijke landen die onzeker zijn over hun strategische positie.

De concurrentie tussen de "grootmachten" is opnieuw een belangrijke kwestie in de internationale betrekkingen.

Hoewel deze twee conflicten, evenals de migratiekwestie, de aandacht van het westerse publiek en politici opeisen, mogen ze andere kwesties of gebieden in de wereld niet verdoezelen.

Het Afrikaanse continent worstelt met zijn economische ontwikkeling. Het blijft kampen met een sterke demografische druk, staatsgrepen en concurrentie tussen externe mogendheden. De landen van de Sahel en West-Afrika zijn bijzonder hard getroffen door deze golf van putschen, die tot veranderingen in bondgenootschappen heeft geleid. De veiligheidstoestand blijft er onzeker. Soedan wordt nog steeds verscheurd door een burgeroorlog. De regio van de Grote Meren in Afrika lijdt onder het conflict in het oosten van de Democratische Republiek Congo.

In Azië blijft de macht van India tegen een achtergrond van nationalisme toenemen, terwijl buurland Pakistan, dat over kernwapens beschikt, worstelt met een diepe economische crisis. China probeert de structurele groeivertraging onder controle te krijgen terwijl het zijn technologische en militaire ontwikkeling voortzet. De ontwikkeling en projectie van de Chinese macht leidt bovendien tot groeiende bezorgdheid in bepaalde buurlanden.

Een voortdurend veranderend slagveld

Gelijktijdig met deze crisissen vinden er structurele ontwikkelingen plaats die vandaag de dag moeilijk volledig te begrijpen zijn. Technologische ontwikkelingen, zoals artificiële intelligentie, en hun invloed op het voeren van gevechten, met name door het toegenomen gebruik van drones en cybermiddelen, betekenen dat we opnieuw moeten nadenken over hoe de wereld van morgen eruit zal zien om ons er beter op voor te bereiden. Ook de kwesties van toegang tot middelen en de energietransitie blijven essentieel.

De fragmentatie van de westerse samenlevingen door de opkomst van het extremisme, de aanhoudende terroristische dreiging en de groeiende macht van criminele groepen blijven een impact hebben op de veiligheidssituatie in België. Ook de dreigingen van spionage, beïnvloeding en sabotage, die het gevolg zijn van de terugkeer van de concurrentie tussen de grootmachten, zullen een blijvende impact hebben op ons veiligheidslandschap.

Terugkeer van concurrentie tussen “grootmachten”

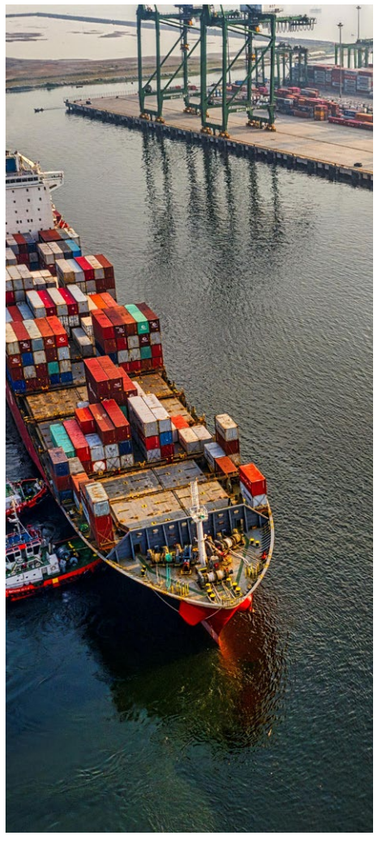
Het uiteenvallen van de Sovjet-Unie in 1991 luidde een periode in van quasi-hegemonie voor de Verenigde Staten. De globalisering van de economie en de verspreiding van de liberale democratie gaven aanleiding tot concepten zoals Francis Fukuyama’s ‘Het einde van de geschiedenis’.

Terwijl het eerste decennium van de 21e eeuw in het teken stond van de strijd tegen het terrorisme, is de concurrentie tussen de grootmachten geleidelijk weer het belangrijkste kenmerk van de internationale betrekkingen geworden. De liberale democratieën worden geconfronteerd met autoritaire en revisionistische mogendheden die zowel de westerse macht als de wereldorde en haar instellingen ter discussie stellen.

Een spel van invloed en concurrentie

De groeiende macht van China op alle fronten verstoort de gevestigde evenwichten. In het spel van invloed en internationale concurrentie heeft China een wereldwijd project gelanceerd om “nieuwe zijderoutes” te creëren, bedoeld om de land- en zeeverbindingen tussen het land en tientallen Aziatische, Afrikaanse en Europese landen te verbeteren. En dit door middel van economische investeringen in, onder andere, infrastructuur, diplomatieke betrekkingen, militaire steun en de projectie van ‘soft power’.

Rusland heeft met zijn beleid van gewapende agressie in Oekraïne een grote breuk veroorzaakt met de westerse liberale democratieën. Om zijn isolement tegen te gaan, probeert het sindsdien zijn invloed in de wereld te vergroten. Het manipuleert in zijn voordeel bewegingen die de westerse overheersing afwijzen, vooral in Afrika, door het initiatief te nemen in militaire en veiligheidssamenwerking. Op diplomatiek vlak wenst Rusland zijn



visie van een multipolaire wereldorde te ontwikkelen en zoekt daartoe bondgenoten in internationale fora.

Een kwestie van middelen

China en Rusland hebben een basis van overeenkomst gevonden in hun pogingen om de overheersing van de liberale democratieën tegen te gaan. Zo kondigden de staatshoofden van Rusland en China vlak voor de Russische invasie in Oekraïne een ”onbeperkt partnerschap” aan. Aanvankelijk bevond China, dat in zijn internationale betrekkingen de beginselen van territoriale integriteit en soevereiniteit verdedigt, zich in een ongemakkelijke positie door de internationale sancties tegen Rusland af te wijzen. Het heeft de Russische economie overeind gehouden door grondstoffen te leveren en een alternatief te bieden voor internationale monetaire uitwisselingen die beperkt worden door de sancties. Toch wil China de perceptie van neutraliteit behouden en zichzelf presenteren als een verantwoordelijke internationale speler.

Voor China dient de oorlog in Oekraïne niet alleen als oefenterrein voor een mogelijke toekomstige invasie van Taiwan. Hij verschuift ook het machtsevenwicht tussen China en Rusland in het voordeel van China. Rusland is afhankelijk geworden van China om zijn militaire industrie draaiende te houden. Bovendien, nu Moskou al zijn aandacht richt op het conflict in Oekraïne, kan China zijn invloedssfeer uitbreiden ten koste van Rusland, bijvoorbeeld in Centraal-Azië of het noordpoolgebied.

Een spel van communicerende vaten

Dit spel van grootmachten gaat veel verder dan alleen de Amerikaanse, Chinese en Russische mogendheden.

Zo blijft het Midden-Oosten gekenmerkt door rivaliteit tussen de Iraanse as en de traditionele mogendheden van de Golfstaten. Bij deze eerste breuklijn komen de spanningen tussen de mogendheden die dicht bij de politieke islam staan en de soennitische mogendheden die de

Moslimbroederschap als een bedreiging voor hun stabiliteit zien. (Egypte, Saoedi-Arabië, Verenigde Arabische Emiraten).

In Zuid-Azië is India al enkele jaren een volwaardige speler in de globalisering, met een sterke groei en de grootste bevolking ter wereld. Zijn aartsrivaal Pakistan maakt een diepe economische en politieke crisis door.

De internationale orde en het multilateralisme ter discussie gesteld

De internationale orde gebaseerd op de Rules Based International Order is het systeem dat is opgebouwd door de liberale democratieën, geleid door de Verenigde Staten. Dit systeem steunt voornamelijk op diverse internationale en regionale instellingen, waaronder de VN en de instellingen van Bretton Woods. Het is gebaseerd op internationale normen die soms wettelijk bindend zijn, soms meer traditioneel en gebaseerd op codes van goed gedrag. Het bestrijkt de gebieden economie, politiek, veiligheid en grondrechten.

Deze internationale orde wordt nu aan het wankelen gebracht. De Russische aanvalsoorlog in Oekraïne en de annexatie van de Krim die eraan voorafging, zijn flagrante schendingen van het Handvest van de Verenigde Naties. Staten zoals China en bepaalde landen van het Globale Zuiden stellen het gebruik van het rechtskader dat is ontwikkeld om de grondrechten te bevorderen, ter discussie.

Empowerment van het Globale Zuiden en teruggang van democratieën

De westerse mogendheden wedijveren momenteel met hun rivalen de BRICS (Brazilië, Rusland, India, China en Zuid-Afrika) in het grote beïnvloedingsspel in de landen van het zogenaamde Globale Zuiden.

Dit concept, dat weliswaar slecht gedefinieerd is, verwijst naar deze bonte verzameling van niet-westerse landen die min of meer de volgende ambities delen: een grotere economische ontwikkeling bereiken, meer respect krijgen van de oude mogendheden en meer inspraak krijgen in het wereldtoneel. Sommige van deze naties uiten hun onbehagen of verwerpen zelfs de concepten die in het Westen zijn ontwikkeld met betrekking tot grondrechten en individuele vrijheden.

Steeds meer staten van dit zogenaamde “Globale Zuiden” geven nu blijk van een groeiende autonomie in hun positionering in de concurrentie tussen de grootmachten, waarbij ze soms kiezen voor de Westerse mogendheden, soms voor de BRICS, afhankelijk van wat zij als hun belangen beschouwen.

Het is nuttig staatsgrepen, militaire putschen en andere machtsveranderingen te beschouwen als onderdeel van een grotere wereldwijde beweging op het stuk van de afkalving van de invloed van liberale westerse democratieën op verschillende landen van het Globale Zuiden, in het bijzonder in de context van de grote machtsstrijd tussen de Verenigde Staten van Amerika en autoritaire regimes zoals Rusland en China.

Netwerken

Enkele voorbeelden van desinformatie die circuleren op sociale netwerken.

Wereldwijde informatieoorlog is overal

Statelijke actoren zoals Rusland en China gebruiken informatieoorlogvoering om hun strategische langetermijndoelen te bereiken. Ze maken gebruik van de reeds bestaande kloof binnen bepaalde sociale groepen en spelen in op actuele gebeurtenissen om de polarisatie te vergroten en mensen te overtuigen. Ze zetten in op beïnvloedingsactiviteiten, zowel ten aanzien van hun eigen nationale publiek als ten aanzien van het externe en internationale publiek, elk met hun eigen accenten.

Deze activiteiten hebben over het algemeen tot doel de percepties en overtuigingen te veranderen, helpen samenzweringstheorieën in onze samenlevingen aan te wakkeren, en in het kader van de actuele conflicten, westerse regeringen in diskrediet te brengen en wantrouwen tussen bondgenoten te zaaien.

Bij wijze van voorbeeld: China stelt het conflict in Oekraïne voor als het resultaat van westerse inmenging en vindt in Rusland een bondgenoot om de bestaande wereldorde te wijzigen. China versterkt de Russische retoriek en desinformatie in Afrika, Latijns-Amerika en onder zijn bondgenoten in het Midden-Oosten, die vaak economisch afhankelijk zijn, om Rusland diplomatiek te steunen. China heeft daarmee de westerse inspanningen om Rusland te isoleren en af te snijden van de wereldeconomie ernstig verzwakt.

Deze beïnvloedingsstrategieën zijn niet beperkt tot het buitenlandse publiek, maar strekken zich ook uit tot heel Europa. Ze hebben langetermijneffecten en zullen in de toekomst een uitdaging vormen voor onze autoriteiten

> **ONZE DIENST IS WERELDWIJD ACTIEF**

Via zijn inlichtingen adviseert de ADIV politieke en militaire leiders zodat ze onafhankelijk en autonoom de beste keuzes kunnen maken om België en zijn burgers zo goed mogelijk te beschermen. Daartoe opereert onze dienst overal ter wereld waar onze belangen dat vereisen, ter ondersteuning van militaire operaties maar ook ten dienste van onze inwoners, onze politici en onze veiligheidspartners, zowel nationaal als internationaal.

HET BELANG VAN ONZE DEFENSIEATTACHÉS

Voor een goede kennis van de internationale omgeving is er ook een netwerk van defensieattachés nodig. In nauwe samenwerking met Buitenlandse Zaken, de lokale autoriteiten en de partnerlegers verzorgen ze de liaison met de ADIV.

1 Militair adviseur bij de Belgische vertegenwoordiging van de OVSE en defensieattaché voor Oostenrijk, Slowakije en Slovenië.

"Als defensieattaché neem ik in de drie landen deel aan bilaterale activiteiten die tot doel hebben de Belgische Defensie te promoten. De grote uitdaging bestaat erin de passende aanpak voor elk land te bepalen. Het lidmaatschap van de NAVO of van de EU, de neutraliteit van Oostenrijk en het politieke klimaat zijn stuk voor stuk factoren die in aanmerking worden genomen. Zich informeren over de actualiteit van die landen en netwerken zijn dus dagdagelijks aan de orde. Dit uitgebreide takenpakket kan een ware uitdaging vormen, maar dat maakt dit werk naar mijn mening ook aantrekkelijk."

2 Defensieattaché in Polen, ook geaccrediteerd voor Estland, Letland en Litouwen.

"Ik ben werkzaam in een regio waarvan het geostrategische belang niet meer hoeft te worden aangetoond. Al die landen hebben een grens met Wit-Rusland en/of Rusland en de recente ontwikkelingen hebben grote gevolgen voor het veiligheids- en defensieaspect, met onder meer de versterking van de aanwezigheid van de NAVO en de hulp aan Oekraïne.

Polen vervult een essentiële rol bij de steun aan Oekraïne, of het nu om de levering van materieel of om de vorming van Oekraïense militairen in het kader van de Europese missie EUMAM UKR gaat. De drie Baltische staten vervullen eveneens een sleutelrol bij de verdediging van de NAVO en ons land werkt daaraan actief mee in de drie dimensies, de land-, de lucht- en de maritieme dimensie.

Zowel voor de hulp aan Oekraïne als voor de collectieve verdediging vervul ik een rol als facilitator en coördinator met het gastland om het goede verloop van de missie mogelijk te maken.

3 Defensieattaché in Jordanië, ook geaccrediteerd voor Irak.

"Dialoog is één van de sleutels van de bilaterale samenwerking tussen Jordanië en België. Ons team, dat verankerd is in het Midden-Oosten, beschikt over een uitgebreid netwerk waarmee het informatie kan inwinnen voor onze beide landen, en dit onder andere op het gebied van inlichtingen en veiligheid. De ontwikkeling van deze expertise met betrekking tot de regio is enkel mogelijk door een aanwezigheid in de zone en directe contacten.

Binnen de ambassade beteken ik een meerwaarde als militair adviseur van de ambassadeur door mijn specifieke militaire ervaring te delen met de diplomaten, bijvoorbeeld in het geval van de planning van een evacuatie van landgenoten van een buurland bij een crisis. Het is een boeiende functie met vele aspecten, die militaire diplomatie, bilaterale samenwerking en operationaliteit combineert."

4 Defensieattaché in Rusland, ook geaccrediteerd voor Armenië.

"De sancties die tegen Rusland werden getroffen, hebben er onder andere toe geleid dat alle EU-lidstaten op de lijst van "niet-bevriende landen van Rusland" zijn terechtgekomen. Bilaterale betrekkingen zijn momenteel dan ook beperkter. Toch vormt het feit dat men persoonlijk aanwezig is in het grootste land ter wereld, waarvan de hoofdstad zich op slechts 2.500 km van Brussel bevindt en dat dagelijks voorpaginanieuws vormt in de westerse media, een grote meerwaarde. In crisistijd is het immers onontbeerlijk om de gebeurtenissen zo waarheidsgetrouw mogelijk en in hun specifieke context te kunnen observeren, en aldus de Belgische autoriteiten te helpen om een klare kijk te krijgen op de situatie."

5 Defensieattaché in Marokko, ook geaccrediteerd in Senegal en Kaapverdië.

"Mijn mandaat in de landen van accreditering is drieledig. Eerst en vooral is het noodzakelijk kennis te verwerven over de situatie in de regio waarvoor men is aangewezen, een lokaal netwerk op te bouwen en te onderhouden, teneinde opportuniteiten gemakkelijker te herkennen.

Bovendien bestaat mijn werk erin jaarlijks bilaterale activiteiten met de plaatselijke strijdkrachten te bepalen en de verwezenlijking ervan op te volgen. Meer en meer neemt de Belgische defensie-industrie contact met mij op, opdat ik ze zou helpen toegang te krijgen tot de lokale strijdkrachten.

Ten slotte is er nog de adviesfunctie. In mijn functie moet ik in staat zijn de strategische tendensen te bepalen, maar ook klaarstaan om de Defensiestaf te informeren als reactie op een incident of bij een knelpunt in een bepaald dossier."

Hybride oorlogvoering in Oekraïne: waar stopt dit?

De Russische aanvalsoorlog tegen Oekraïne is veranderd in een uitputtingsoorlog tussen de strijdende partijen

Aan Russische zijde streeft het Poetin-regime ernaar, hoewel het sedert februari 2022 onderworpen is aan spanningen van politieke en economische aard, om koste wat kost aan de macht te blijven en blijft het vrij stabiel. Het jaar 2023 werd gekenmerkt door de actie die in juni werd uitgevoerd door de leider van de huurlingen van de Wagnergroep, Jevgeni Prigozjin, maar iedere poging tot een volksopstand werd verijdeld door het gebruik van repressie en desinformatie.

Aan Oekraïense zijde blijft het leiderschap van president Zelensky vooralsnog onbetwist, ook al beginnen de eerste barsten zichtbaar te worden. Zijn charisma en zijn rol die symbool staat voor het verzet, leveren hem onmiskenbaar het respect op binnen de maatschappij en de Oekraïense instellingen, ondanks zijn grote afhankelijkheid van (politieke, economische en militaire) steun van buitenaf. De door zijn strijdkrachten vastgestelde maximalistische doelstellingen werden niet behaald na de mislukking van het tegenoffensief in de zomer van 2023. In deze moeilijke context loopt het Oekraïense leiderschap het risico dat zijn legitimiteit en stabiliteit worden bedreigd.

Aan het militair front blijft de strategische situatie relatief ongewijzigd. In 2023 heeft Rusland zijn posities over de hele frontlijn dermate verstevigd, dat het offensieve operaties kan uitvoeren, zonder evenwel in staat te zijn een echte militaire doorbraak te forceren. Na de mislukking van het Oekraïense tegenoffensief heroverde Rusland het initiatief op het terrein. In zijn propaganda wordt de situatie door middel van desinformatiecampagnes voorgesteld als een totale mislukking van Oekraïne en, bij uitbreiding, van het Westen.

Na meer dan twee jaar oorlog worden Oekraïne en Rusland nog steeds geconfronteerd met dezelfde militaire uitdagingen: massale rekrutering en mobilisaties van een deel van de bevolking, gebrek aan zware uitrusting en aan munitie. De beide partijen zijn verder niet in staat om hun militaire successen samen te voegen of te exploiteren. Er wordt gevreesd voor een voortdurende uitputtingsoorlog met aanvallen in de diepte en rampzalige gevolgen voor de bevolking aan beide kanten. Deze uitputtingsoorlog breidt zich ook uit naar de defensie-industrie, die van cruciaal belang is voor de continuïteit van de operaties.

BATTLE GROUP

Sinds juli 2023,

neemt de Belgische Defensie deel aan de Battle Group ingezet in Roemenië onder Frans bevel, met als doel aanwezigheid van de NAVO op de oostelijke flank te versterken.

INFORMATIE OVER DE ROL VAN DE ADIV

Ter directe ondersteuning van de verschillende detachementen van Defensie in de Baltische staten en Roemenië levert de ADIV, zowel in België als ter plaatse, bijstand op het vlak van inlichtingen, contra-inmenging en veiligheid.

Vanuit strategisch oogpunt speelt de ADIV bovendien een actieve rol om de regering en zijn partners in de inlichtingen- en veiligheidsgemeenschap op de hoogte te houden van de ontwikkelingen in het conflict in Oekraïne, in het bijzonder door het opstellen van analyserapporten over zowel de politieke als de militaire aspecten. De expertise van de ADIV vergroot het begrip van de Belgische politieke en militaire besluitvormers met betrekking tot de vele facetten van het conflict.

Belgische UAV-drones die voornamelijk gebruikt worden voor verkenningsmissies.

Op weg naar een droneoorlog

Het gebruik van drones, of Unmanned Aerial Systems (UAS), is lange tijd in handen gebleven van conventionele strijdkrachten, hoewel sommige terroristische groeperingen al enkele jaren kleine commerciële drones gebruiken voor propagandadoeleinden of lichte kinetische aanvallen. Hoewel het gebruik van militaire drones snel toenam, was het nog niet op brede schaal ingevoerd.

De invasie van Rusland in Oekraïne bracht daar snel verandering in, aangezien beide partijen de technologische ontwikkelingen op dit gebied en het gebruik ervan hebben opgevoerd. Militaire drones voor verkenningsvluchten of kinetische opdrachten; gerichte aanvallen met “kamikaze-” of “One-way Attack”-drones; met industrieel geproduceerde of geïmproviseerde drones; gebruik van kleine “First-Person View” commerciële drones met kleine en middelgrote springladingen om voertuigen of personeel te raken; Unmanned Surface Vessels (USV) om vijandelijke vloten te vernietigen, … Het gebruik van drones op het Oekraïense strijdtoneel is gevarieerd en uitgebreid. Na meer dan twee jaar conflict zijn deze nieuwe gevechtsmiddelen de drijvende kracht geworden achter een groot aantal fabrikanten over de hele wereld en beginnen ze geëxporteerd te worden naar andere operatiegebieden.

Deze ontwikkelingen en de democratisering van bepaalde systemen hebben veel opkomende landen, vooral in Afrika en het Midden-Oosten, overtuigd om militaire gevechts-UAS (UCAV) aan te schaffen om rebellen of terroristische groeperingen op hun grondgebied te bestrijden. Landen als Turkije, China en Iran, die behoren tot de belangrijkste fabrikanten van UCAV’s, exporteren op grote schaal naar deze landen, zonder zich veel zorgen te maken over internationale sancties of wettelijke of ethische aspecten.

De Jemenitische Houthi’s, met steun van Iran, maken eveneens massaal gebruik van drones, zowel lucht- als zeedrones, die het maritieme verkeer in de Golf van Aden en de Rode Zee bedreigen.

In het kader van de lopende herinvestering in zijn strijdkrachten zal België bij het voeren van gevechten rekening moeten houden met deze belangrijke ontwikkeling.

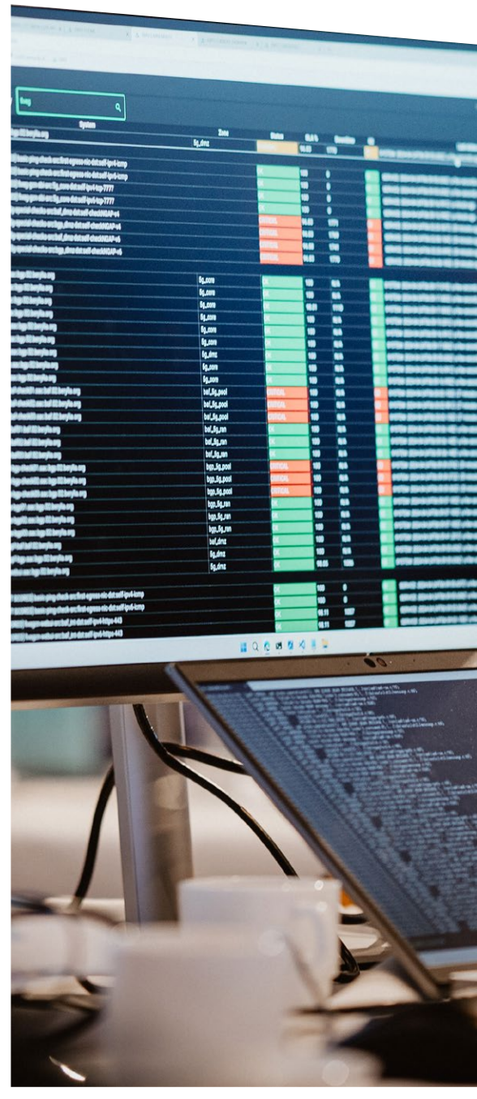
Het Europese ”COURAGEOUS” project heeft als doel een gestandaardiseerde testmethode te ontwikkelen voor anti-drone systemen

Hybride aanvallen op kritieke infrastructuur

In 2023 lanceerde Rusland een grootschalige campagne tegen kritieke Oekraïense infrastructuur. Deze campagne was met name gericht op het elektriciteitsopwekkings- en distributienetwerk, waarbij gebruik werd gemaakt van intensieve en steeds terugkerende bombardementen (kruisraketten, hypersonische raketten, drones, enz.) en cyberaanvallen.

Zo heeft een cyberactor die gelinkt is aan de Russische militaire inlichtingendienst (GRU) zijn destructieve cyberoperaties gericht op kritieke infrastructuren, zoals elektriciteitscentrales, operatoren van netwerken en telecommunicatieoperatoren. Russische cyberspionageoperaties hebben trouwens getracht de contraspionage-inspanningen en de onderzoeken naar oorlogsmisdaden te verhinderen.

Er is een duidelijke trend waarneembaar: de Russische cyberactoren viseren herhaaldelijk dezelfde organisaties, voeren aanhoudende aanvallen uit op de Oekraïense media, en proberen de, nochtans verbeterde, Oekraïense detectie- en herstelcapaciteiten te omzeilen, dankzij een snellere exfiltratie van gegevens.



GETUIGENIS

“Ik heb in 2023 op drie continenten gewerkt.”

Matthew, 36 jaar

In de praktijk is de ADIV altijd rechtstreeks of onrechtstreeks betrokken bij alle operaties van Defensie. Jaarlijks worden ze op een rijtje gezet en vertaald in operatieplannen. Dat gebeurt op het land, in zee, in de lucht en in het cybernetisch domein. Maar hoe ziet een werkdag in het leven van een officier van ADIV in het buitenland eruit en waarmee wordt hij dagelijks geconfronteerd?

“Mijn naam is Matthew en ik werk in de ontplooibare teams van ADIV. Met mijn klein team vertrek ik voor langere tijd naar het buitenland en opereer ik op plaatsen waar ook detachementen van Defensie aanwezig zijn.

Waarin bestaat mijn werk daar dag in dag uit? Ik heb regelmatige contacten met de plaatselijke veiligheidsdiensten en met anders partners. ‘s Avonds zet ik die gesprekken om in een rapport, dat zowel wordt verstuurd naar het hoofdkwartier in Brussel als naar de Belgische troepen die in mijn regio zijn ingezet. Vervolgens bereid ik nauwgezet mijn gesprekken voor de volgende dag voor. Op die manier houd ik de vinger aan de pols en help ik de wijzigingen in de situatie op te sporen. Zodoende kan ik de Belgische troepen op de hoogte houden en meewerken aan hun bescherming.

Mijn werk is zeer gevarieerd en boeiend. Vorig jaar heb ik op drie verschillende continenten gewerkt: Afrika, Europa en het Midden-Oosten. Zelfs al verandert de aard van het werk niet op de verschillende continenten, toch moet ik mij telkens aanpassen aan de plaatselijke omstandigheden en aan de cultuur van de plaatselijke partners.”

Israëlisch-Palestijns conflict: weerklank over de grenzen heen

De terroristische aanslag van Hamas op 7 oktober 2023 heeft een reeks gebeurtenissen in gang gezet waarvan de uitkomst nog onbekend is. De militaire operaties, gewapende incidenten en protesten worden steeds talrijker, zowel in de regio als op internationaal vlak.

Eén land, vier conflicten

Sinds het uitbreken van het conflict nemen de spanningen aan de Israëlische grenzen almaar toe, waardoor een steeds complexere situatie met talrijke facetten is ontstaan.

In Gaza bevindt de bevolking zich tussen twee vuren. De Israëlische operaties in reactie op de aanval van 7 oktober 2023 zijn gericht op het uitschakelen of verzwakken van het militaire potentieel van Hamas, maar veroorzaken een diepe humanitaire crisis met een hoge tol aan mensenlevens en enorme verwoestingen.

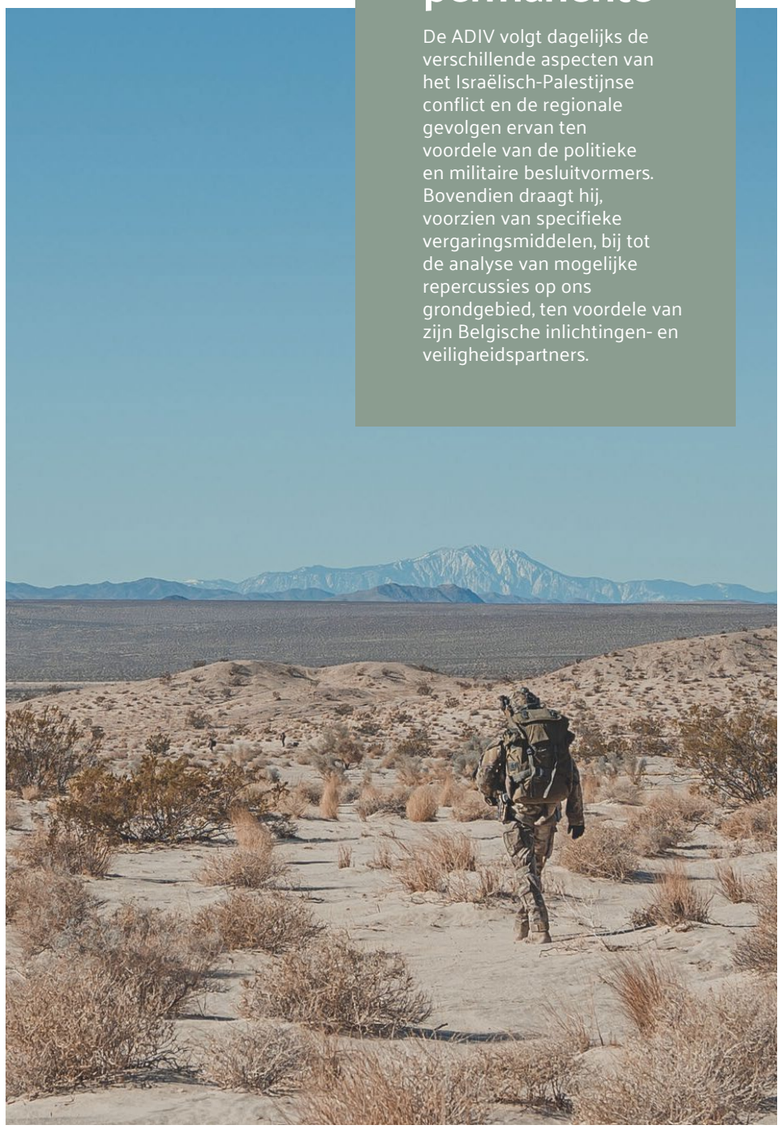
Op de Westelijke Jordaanoever blijft de temperatuur stijgen. Het komt steeds vaker tot gewelddadige confrontaties tussen de Palestijnse bevolking enerzijds en de Israëlische troepen en kolonisten anderzijds.

In het noorden van Israël wordt de Hebreeuwse staat aan de grens met Libanon geconfronteerd met het risico op een open conflict met Hezbollah. Sinds 7 oktober is het aantal incidenten en wederzijdse bombardementen toegenomen.

Binnen Israël zelf vormt de groeiende polarisatie die de Israëlische bevolking en haar politici verdeelt, een vierde dimensie van het conflict..

Veille permanente

De ADIV volgt dagelijks de verschillende aspecten van het Israëlisch-Palestijnse conflict en de regionale gevolgen ervan ten voordele van de politieke en militaire besluitvormers. Bovendien draagt hij, voorzien van specifieke vergaringsmiddelen, bij tot de analyse van mogelijke repercussies op ons grondgebied, ten voordele van zijn Belgische inlichtingen- en veiligheidspartners.



Een dodelijk spel van proxy's

De ADIV merkt op dat Iran niet alleen achter de schermen betrokken is, maar ook via zijn indrukwekkende netwerk van milities en proxy's in de regio.

In Libanon vormen de militaire capaciteiten van Hezbollah een directe dreiging voor Israël. Hoewel Hezbollah na 7 oktober 2023 militaire operaties van beperkte omvang uitvoerde tegen Israël, wat leidde tot tegenaanvallen door Israëlische troepen, is een groot conflict tot nu toe vermeden, maar dreigt het nog steeds.

In Syrië toont de aanwezigheid van pro-Iraanse sjiitische milities en elementen van de Iraanse Revolutionaire Garde aan hoe complex de situatie daar is. Deze troepen, die het Syrische regime in staat hebben gesteld om zijn gezag over grote delen van zijn grondgebied te herstellen, hebben zich daar blijvend gevestigd. Israëlische troepen voeren regelmatig luchtaanvallen uit op deze milities en Iraanse elementen, vooral in het oosten van het land en langs de demarcatielijnen met de Golanhoogte. Hoewel de Syrische president officieel een standpunt heeft ingenomen ten gunste van de Palestijnen, is er geen concrete actie ondernomen.

In Irak vormen de pro-Iraanse sjiitische milities die zijn verenigd in het "Islamitisch Verzet in Irak" een bedreiging voor zowel de stabiliteit in Irak als voor de internationale coalitietroepen. In oktober 2023 lanceerden deze milities een reeks aanvallen op Amerikaanse basissen in Irak en Syrië en ook op een Amerikaanse basis in Jordanië. De Verenigde Staten hebben gereageerd met aanvallen tegen pro-Iraanse milities in Irak en in Syrië, maar zonder rechtstreeks in botsing te komen met Iran. Op politiek vlak hebben de pro-Iraanse actoren het incident aangegrepen om hun eis tot terugtrekking van de Amerikaanse troepen uit het gebied te herhalen. Een stemming in het parlement is in die zin op niets uitgelopen, maar de onderhandelingen met de VS gaan nog verder.

In Jemen heeft de Houthi-beweging, die het noorden van het land en de hoofdstad controleert, een reeks acties in de regio ondernomen die een directe bedreiging vormen voor de vrijheid van scheepvaart in de Rode Zee. Ze hebben rechtstreekse aanvallen op Israël uitgevoerd. Ze hebben ook offensieve acties uitgevoerd in de Rode Zee en de Golf van Aden met als doel commerciële schepen met banden met Israël aan te vallen. Sedert november 2023 werden meer dan zestig aanvallen geregistreerd, waarbij hoofdzakelijk raketten en zowel lucht- als zeedrones werden gebruikt. De VS en het Verenigd Koninkrijk hebben aanvallen uitgevoerd met als doelwit de militaire capaciteiten van de Houthi's op Jemenitisch grondgebied, waardoor de beweging haar acties uitbreidde tot Amerikaanse en Britse koopvaardijschepen. Een coalitie onder leiding van de Verenigde Staten heeft geleid tot de inzet van verschillende militaire schepen in de Rode Zee.

Bescherming van het maritiem verkeer

In februari 2024 heeft de Europese Unie officieel een bijkomende operatie gelanceerd, ASPIDES, die louter defensief van aard is en tot doel heeft het maritieme verkeer te beschermen. Het fregat Louise-Marie is de Belgische bijdrage aan zowel ASPIDES als de operatie European Maritime Awareness in the Strait of Hormuz (EMASoH), die sinds 2020 aan de gang is. Deze twee multinationale opdrachten beogen het behoud van de vrijheid van scheepvaart in respectievelijk de Rode Zee en de Straat van Hormuz. De ADIV levert bijstand op het vlak van inlichtingen en veiligheid in het kader van deze inzet.

Een conflict dat gevolgen heeft voor de westerse democratieën

De polemieken rond mogelijke oorlogsmisdaden leiden tot spanningen binnen de westerse democratieën zelf. Deze interne spanningen in de westerse democratieën en de polemieken rond oorlogsmisdaden betekenen dat Israël het risico loopt steeds meer geïsoleerd te raken.

Netwerk van milities, proxy's, maar ook hacktivisten

Voor Iran blijft Israël een belangrijk cyberdoelwit. Destructieve cyberaanvallen, soms verhuld als ransomware, gaan regelmatig door. Het Iraanse regime voert regelmatig cyberaanvallen uit tegen leden van de oppositie en Iraanse dissidenten, zowel in Iran als in Europa.

De oorlog tussen Israël en Hamas toont aan dat de hacktivisten bij een nieuw conflict op korte termijn gemobiliseerd kunnen worden en, op verzoek van of met de samenwerking van de inlichtingendiensten, verstorende of vernietigende operaties kunnen proberen uit te voeren. In het conflict tussen Israël en Hamas zijn het niet alleen de regeringsdiensten en de kritieke infrastructuren die geviseerd werden, maar ook de alarmsystemen in geval van een raketaanval.

GETUIGENIS

Rachel, 42, is een "agent handler"

In haar dagelijks werk staat ze in contact met "menselijke bronnen". In 2023 voerde ze een operatie uit in het Midden-Oosten om mensen te rekruteren die inlichtingen konden verschaffen.

"Ik ontmoette een Afrikaanse bron, een zeer fijngevoelige vrouw die ik in een derde land heb leren kennen. Ze wist niet dat ik voor de ADIV werkte, maar tijdens onze ontmoeting deelde ze wat gevoelige informatie met me die voor ons van belang zou kunnen zijn.

De moeilijkheid van mijn werk ligt dus in het feit dat ik enerzijds heel flexibel en anderzijds heel discreet moet kunnen handelen. Tijdens zulke interacties zoek ik altijd naar motivaties die deze mensen ertoe zouden kunnen leiden om ons concreter te helpen, zoals een financiële motivatie, maar meestal gaat het om een eerder ideologische motivatie.

Dit werk geeft me enorm veel voldoening, vooral als ik dankzij mijn inspanningen essentiële informatie kan verzamelen in het groter belang van ons land."

AFRIKA

staatsgrepen, inmengingen en strategische herschikking

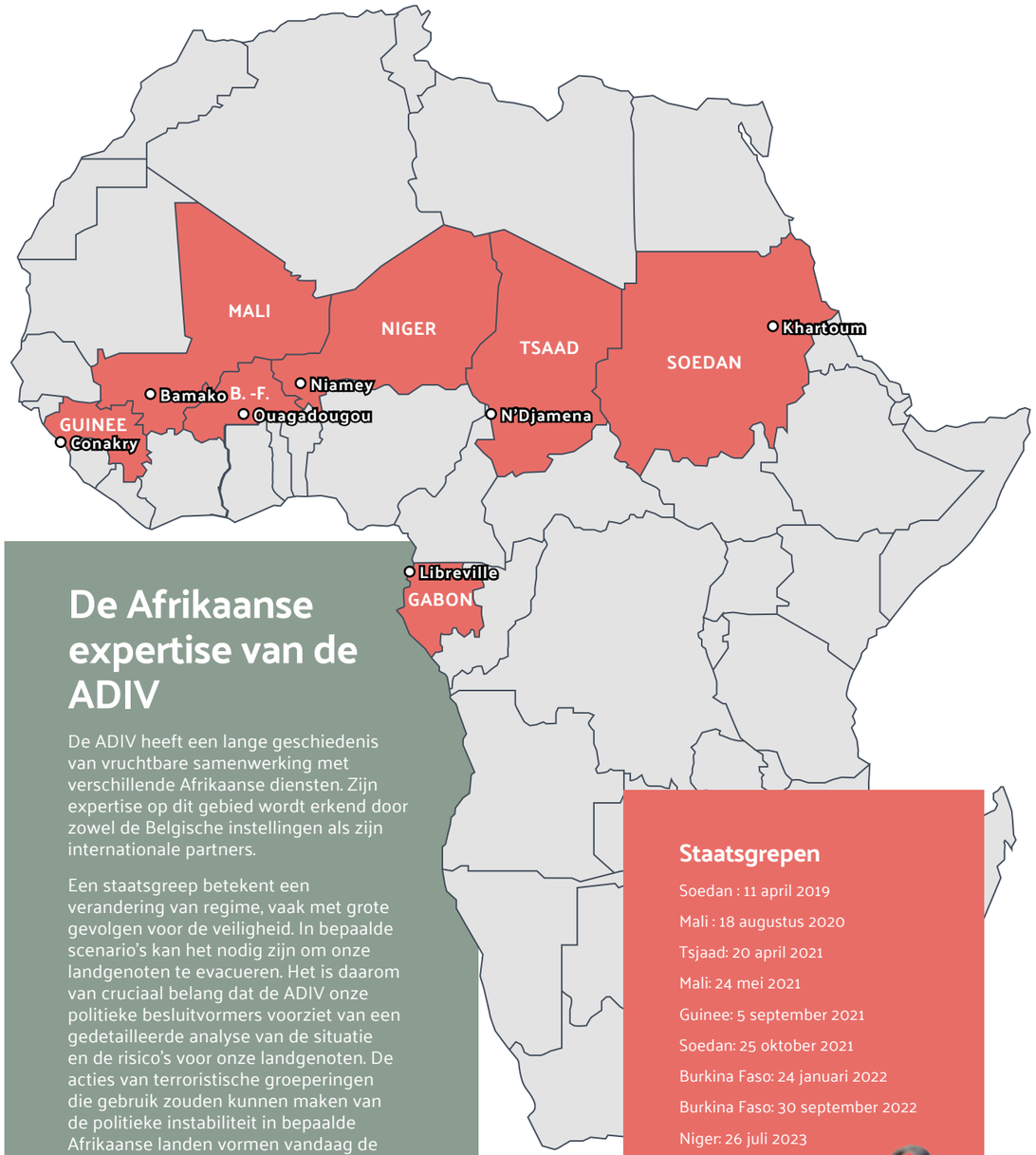
Terwijl de Israëlisch-Palestijnse en Russisch-Oekraïense conflicten de krantenkoppen domineren, vinden er in Afrika ontwikkelingen plaats die op de lange termijn een even grote impact kunnen hebben. De ADIV moet er al zijn aandacht en expertise aan besteden om zijn klanten erover te informeren.

Toename van het aantal staatsgrepen

Militaire staatsgrepen zijn de voorbije jaren weer een verontrustend kenmerk geworden van het Afrikaanse politieke landschap. De voorbije drie jaar heeft Afrika niet minder dan acht dergelijke staatsgrepen gekend, onder andere in Tsjaad, Guinee, Mali, Burkina Faso en, in 2023, in Niger en Gabon.

De hoofdoorzaak is het onvermogen van bepaalde regeringen om een antwoord te bieden op de sociaaleconomische en veiligheidsuitdagingen waarmee een deel van de bevolking wordt geconfronteerd en dit gepercipieerde falen van de gezagsfunctie leidt tot putschistische acties. Dit kan aanleiding geven tot twee fenomenen: ten eerste kan de ene putsch de andere verbergen als de levenskwaliteit op korte termijn niet verbetert. Ten tweede hebben putschisten de neiging om vrij snel een transitie aan te kondigen, die vervolgens op de lange baan wordt geschoven.

Hoewel de Afrikaanse Unie (AU) en de regionale organisaties, zoals de Economische Gemeenschap van West-Afrikaanse Staten (ECOWAS) de staatsgrepen veroordeeld hebben, waren hun politieke beslissingen en hun economische sancties tot nu toe veeleer inefficiënt. Hun gebrek aan capaciteiten en hun vaak incoherente strijd tegen staatsgrepen en andere anticonstitutionele regeringswissels blijven zorgwekkend.



De Afrikaanse expertise van de ADIV

De ADIV heeft een lange geschiedenis van vruchtbare samenwerking met verschillende Afrikaanse diensten. Zijn expertise op dit gebied wordt erkend door zowel de Belgische instellingen als zijn internationale partners.

Een staatsgreep betekent een verandering van regime, vaak met grote gevolgen voor de veiligheid. In bepaalde scenario's kan het nodig zijn om onze landgenoten te evacueren. Het is daarom van cruciaal belang dat de ADIV onze politieke besluitvormers voorziet van een gedetailleerde analyse van de situatie en de risico's voor onze landgenoten. De acties van terroristische groeperingen die gebruik zouden kunnen maken van de politieke instabiliteit in bepaalde Afrikaanse landen vormen vandaag de dag nog steeds een gevaar voor Europa.

Ten slotte levert de ADIV de traditionele inlichtingen- en veiligheidsondersteuning voor Belgische militaire ontplooiingen in Afrika.

Staatsgrepen

Soedan : 11 april 2019
Mali : 18 augustus 2020
Tsjaad: 20 april 2021
Mali: 24 mei 2021
Guinee: 5 september 2021
Soedan: 25 oktober 2021
Burkina Faso: 24 januari 2022
Burkina Faso: 30 september 2022
Niger: 26 juli 2023
Gabon: 30 augustus 2023

Oorlog ook in Afrika

Niet alleen in Oekraïne woedt een interstatelijke oorlog. Ook op het Afrikaanse continent zijn Rwanda en de Democratische Republiek Congo verwikkeld in een quasio-orlog tussen staten. Toegegeven, dit gebeurt gedeeltelijk onder de dekmantel van suppletietroepen die aanwezig zijn in Oost-Congo en gemanipuleerd worden ten voordele van een van de strijdende partijen, naar het voorbeeld van de M23-rebellen.

Andere Afrikaanse landen worden getroffen door gewapende opstanden of burgerconflicten. Met name in Soedan brak in april 2023 een oorlog uit tussen twee grote groepen van het militaire en veiligheidsapparaat: de strijdkrachten en de Rapid Support Forces. Deze twee partijen genieten ook hun eigen externe steun.

Strategische herschikking

In 2023 onderging het Afrikaanse continent belangrijke veranderingen, waaruit blijkt dat er een strategische herschikking aan de gang is in verschillende Afrikaanse staten. Deze staten keren zich af van hun traditionele partners, vooral de westerse, ten gunste van andere spelers.

Na het uiteenvallen van de gezamenlijke G5-troepenmacht in de Sahel nemen we dan ook een geleidelijke terugtrekking van de internationale aanwezigheid in de regio waar. MINUSMA heeft zich in december 2023 teruggetrokken uit Mali en de Franse militaire aanwezigheid in de Sahel is eveneens significant teruggeschroefd.

In Centraal- en Oost-Afrika is de internationale aanwezigheid ook verminderd: in de Democratische Republiek Congo bereiden de Verenigde Naties het einde van MONUSCO voor, terwijl de Afrikaanse Unie in Somalië het vertrek van ATMIS tegen eind december op stapel heeft gezet.

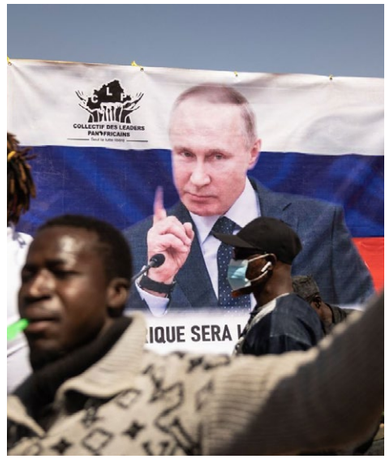
China en Rusland hebben hun invloed opgevoerd in het “Globale Zuiden”, en dit in uiteenlopende domeinen. De twee staten hebben echter verschillende benaderingen voor het aanknopen van geprivilegieerde betrekkingen met bepaalde Afrikaanse staten. Rusland geeft de voorkeur aan samenwerking op militair en veiligheidsgebied, terwijl China zijn samenwerking vooral in de economische sector opzet. Andere landen, zoals Turkije, Iran en de Golfstaten, mengen zich ook in het grote Afrikaanse spel en vergroten eveneens hun betrokkenheid in bepaalde Afrikaanse gebieden.

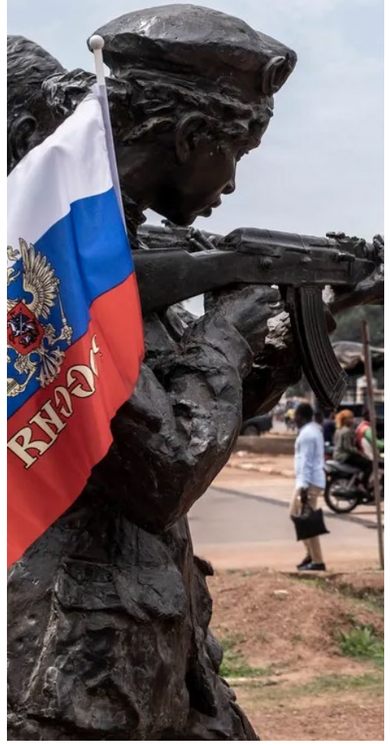
Het resultaat van deze strategische herschikking is een omwenteling in het landschap van buitenlandse inmenging op het Afrikaanse continent.

MINUSMA: multidimensionale geïntegreerde stabilisatieopdracht van de Verenigde Naties in Mali

MONUSCO: stabilisatieopdracht van de Verenigde Naties in de Democratische Republiek Congo

ATMIS: African Union Transition Mission in Somalia





© AFP

Rusland breidt zijn invloedssfeer uit naar Afrika

Moskou heeft de Afrikaanse landen in het vizier. Rusland, dat meer en meer inzet op antiwesterse desinformatie, het gebruik van Russische huurlingen en, meer algemeen, op de verzwakking van de democratische instellingen, streeft ernaar nauwere betrekkingen aan te knopen met een hele reeks Afrikaanse staten.

Het maakt specifiek gebruik van het discours, volgens hetwelk de westerse landen de Afrikaanse bevolkingen blijven uitbuiten en dringt het zogenaamde Russische “antikolonialistische” model op. Hoewel de economische impact van Rusland in Afrika onbeduidend is ten opzichte van die van het Westen of van China, is Rusland er - in het bijzonder in het onstabiele Sahelgebied - in geslaagd nauwere banden aan te knopen met een bepaald aantal landen, deels dankzij de ontplooiing van huurlingen (Africa Corps - voorheen Wagner).

Inmiddels zijn er na de staatsgreep in Guinee, Mali, Burkina Faso, Niger, Soedan en de Centraal-Afrikaanse Republiek al verschillende pro-Russische regeringen aan de macht. In de praktijk doet dit een min of meer aan elkaar grenzend gebied van autocratische regimes ontstaan en brengt dit, behalve sterke antiwesterse gevoelens in die landen, ook onveiligheid en illegale migratiestromen teweeg.

Buiten het Sahelgebied is de invloed van Rusland, hoewel beperkter, geenszins verwaarloosbaar. Ook daar zijn er verschillende Afrikaanse regeringen, zoals die van Zuid-Afrika, die ervoor kiezen om de banden met Moskou aan te halen ondanks de Russische invasie van Oekraïne. Dat kan deels verklaard worden door de ontevredenheid veroorzaakt door het gebrek aan vertegenwoordiging en gewicht in de internationale instellingen, maar ook door pragmatische economische overwegingen.

ONZE REALISATIES IN 2023

Kwaliteitsproducten voor onze partners

De kwaliteit van verschillende analyseproducten van de ADIV werd geprezen door de NAVO-instellingen, zoals blijkt uit het feit dat deze producten zijn opgenomen in de leesportefeuilles die worden aanbevolen aan de leden van de organisatie. Het aanprijzen van de producten van de ADIV benadrukt de erkenning door internationale instanties van de deskundigheid op de gebieden waarin de dienst actief is.

Nauwere samenwerking met de academische wereld

Er werd een Memorandum of Understanding ondertekend met de Koninklijke Militaire School (KMS), ons 'bruggenhoofd' met Belgische en buitenlandse civiele universiteiten. Deze overeenkomst dekt verschillende gebieden van cyberspace, waaronder 5G en cryptografie, en draagt bij tot de ondersteuning van talrijke langlopende onderzoeks- en ontwikkelingsprojecten, ten voordele van zowel Defensie als de burgermaatschappij.

Meer inspanningen om het bewustzijn te vergroten

Of het nu gaat om beschermingsmaatregelen tegen spionagerisico's, nieuwe veiligheidsrichtlijnen of cyberveiligheidsmaatregelen, de ADIV heeft zich gericht op de bewustmaking van al het Defensiepersoneel om de veiligheid van de organisatie te vergroten. Deze bewustmakingsacties zijn onderdeel van informatie- en communicatiecampagnes binnen de ADIV.

Het Belgisch expertisecentrum voor cryptografie is geboren

In samenwerking met de KMS werd de structuur ervan bepaald en werden er middelen aan toegewezen. Uiteindelijk zal dit expertisecentrum, geïnspireerd op het Franse model, technische expertise produceren ten voordele van zijn federale en internationale partners.

Cyberveiligheidsexpertise ter ondersteuning van onze federale partners

Het Cyber Command van de ADIV, expert op het vlak van cyberaudit en -controle, is aangesteld door de Nationale Veiligheidsraad om het nieuwe federale geclassificeerde BSC-systeem (Belgian Secure Communication) goed te keuren, dat in de toekomst door alle Federale Overheidsdiensten zal worden gebruikt.

Nauwere samenwerking met het NGI

Door de ondertekening van een samenwerkingsovereenkomst met het NGI in 2023 kunnen synergieën worden gemaximaliseerd, in het bijzonder door de overdracht van personeel aan te moedigen, en kan het NGI als expertisecentrum structureel geassocieerd worden met de geostrategie van Defensie.

Militaire veiligheidsnormen bijwerken

De militaire veiligheidsnormen werden bijgewerkt en geoptimaliseerd met het oog op de verbetering van de veiligheidscultuur van Defensie, overeenkomstig de aanbevelingen van het Comité I en het actieplan dat is opgesteld naar aanleiding van de "zaak-Jürgen Conings".

Gezamenlijk platform met de VSSE CECT

De ADIV en de VSSE werkten gedurende heel 2023 samen, wat leidde tot de oprichting van een gezamenlijk platform om extremisme en terrorisme te bestrijden, zowel religieus als ideologisch.

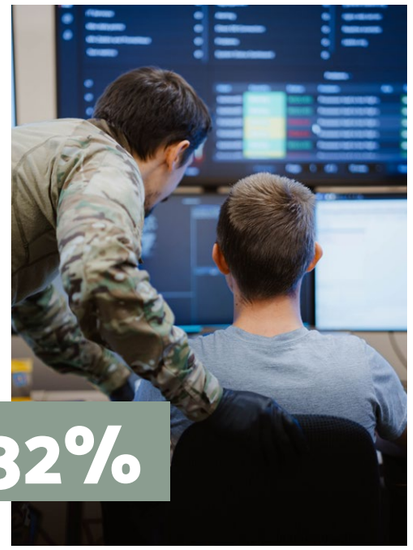
IF5 : Sterke betrokkenheid bij de bescherming van personeel en geclassificeerde informatie. Behendigheid en permanente evaluatiecommissie.

Eerste editie van de Cyber Summer School

Deze zomercursus, die in 2023 voor het eerst werd aangeboden door het Cyber Command van de ADIV, is niet alleen bedoeld om jongeren inzicht te geven in de uitdagingen van vandaag en morgen op het vlak van cyberdefensie maar ook om nieuw talent aan te trekken. De ADIV blijft investeren in menselijk kapitaal.

FACTS & FIGURES

6% meer personeel



32%

BURGERS BIJ DE ADIV

160

MEER DAN 160 RESERVISTEN IN DIENST VAN DE ADIV

652

"PAPERS" GEPRODUCEERD EN GEVALIDEERD DOOR DE DIRECTIE INLICHTINGEN: ANALYSEDOCUMENTEN GEDEELD MET ONZE KLANTEN/PARTNERS

7226

"REQUESTS FOR INFORMATION" AANGEVRAAGD DOOR ONZE PARTNERS EN VERWERKT DOOR DE ADIV

236

AANTAL BIM'S (UITZONDERLIJKE ONDERZOEKSMETHODEN)

5483

BEHANDELDE VEILIGHEIDSVERIFICATIES

AANTAL SATELLIETBEELDEN/ AANTAL KAARTEN GEMAAKT VOOR OPERATIES:

15560
beelden gemaakt, waarvan 3154 geproduceerd

747
geografische ondersteuningsaanvragen

5
topografische opdrachten uitgevoerd

Deel II

Het dreigingsniveau beoordelen om er bescherming tegen te bieden

Grensoverschrijdende conflicten geven vorm aan de wereld van morgen en bepalen de dreigingen waaraan ons land het hoofd moet kunnen bieden.

We zien nu al een hoog spionagedreigingsniveau; een toename van pogingen tot beïnvloeding en inmenging, evenals cyberaanvallen op Belgische en Europese instellingen en bedrijven. Het is onze taak om te voorkomen dat machten buiten onze samenleving bepaalde verdeeldheid zaaiende kwesties, zoals de oorlog in Oekraïne of het Nabije Oosten, uitbuiten om ons democratische model te ontwrichten.

De dreigingen op het vlak van desinformatie en beïnvloedings-operaties

Beïnvloedingsoperaties nemen toe, er is steeds meer verscheidenheid in de gebruikte kanalen en hun impact op gedragingen wordt steeds beter waarneembaar. Voorbeelden hiervan zijn de onrust rond EVRAS, de verschillende boerenbetogingen en de rellen na de "zaak-Nahel" in Frankrijk, die allemaal een tastbaar en gewelddadig stempel hebben gedrukt op onze samenleving.

Aan de vooravond van onder andere de Belgische en Europese verkiezingen maken deze gebeurtenissen dat onze autoriteiten in de hoogste staat van paraatheid verkeren met het oog op pogingen tot beïnvloeding door vijandige statelijke actoren zoals Rusland, China en Iran.

Sinds Twitter X werd, zien we een toename van "coordinated inauthentic behaviour". Het gebruik van Telegram, het favoriete kanaal van pro-Russische actoren, neemt toe in België dat 12% van de gebruikers van het platform levert. De antivax- en COVID-samenzweringsgroepen zijn bovendien nog steeds actief terwijl er zich andere groepen ontwikkeld hebben rond nieuwe thema's zoals klimaat, energie en immigratie. Recente gebeurtenissen hebben duidelijk aangetoond dat de grens tussen de virtuele en de echte wereld steeds vager wordt en kan leiden tot fysiek geweld. In verband met onze opdrachten moeten deze beïnvloedings- en desinformatiepogingen absoluut van nabij worden gevolgd.

In 2023 nam de ADIV de leiding over van de SIMII, een werkgroep bestaande uit de belangrijkste spelers op het gebied van veiligheid. Het doel van deze samenwerking is het ontwikkelen van een uniforme en globale aanpak van Foreign Information Manipulation and Interference (FIMI), in het bijzonder in verband met de verkiezingen van 2024.

2023

Door het afgelopen jaar,

Het afgelopen jaar heeft SIMII[1] talrijke multilaterale bijeenkomsten georganiseerd, waardoor informatie kan worden uitgewisseld tussen de verschillende belanghebbenden, en er is een waarschuwingssysteem ontwikkeld om eventuele buitenlandse beïnvloedingsactiviteiten in een vroeg stadium op te sporen. Dit project zal in de toekomst worden ontwikkeld en versterkt aangezien pogingen tot desinformatie voortdurend worden gemonitord.

Samenzwerin-gen op Telegram

De inspanningen op het vlak van beïnvloeding en het ecosysteem voor desinformatie van Rusland om het nationale en Europese publiek te bereiken, richten zich hoofdzakelijk op Telegram, het kanaal bij uitstek om pro-Kremlin-narratieven te verspreiden en samenzweringstheorieën te voeden. Rusland maakt handig gebruik van iedere gebeurtenis die de publieke opinie kan polariseren en het vertrouwen van de burgers ten aanzien van hun regeringen en instellingen kan verzwakken.

[1]SGRS Interdepartmental Information Manipulation and Interference

De spionagedreiging neemt toe

Spionage wordt in de Belgische wet gedefinieerd als het opzoeken of het verstrekken van niet voor het publiek toegankelijke informatie en het onderhouden van geheime verstandhoudingen die deze handelingen kunnen voorbereiden of vergemakkelijken.

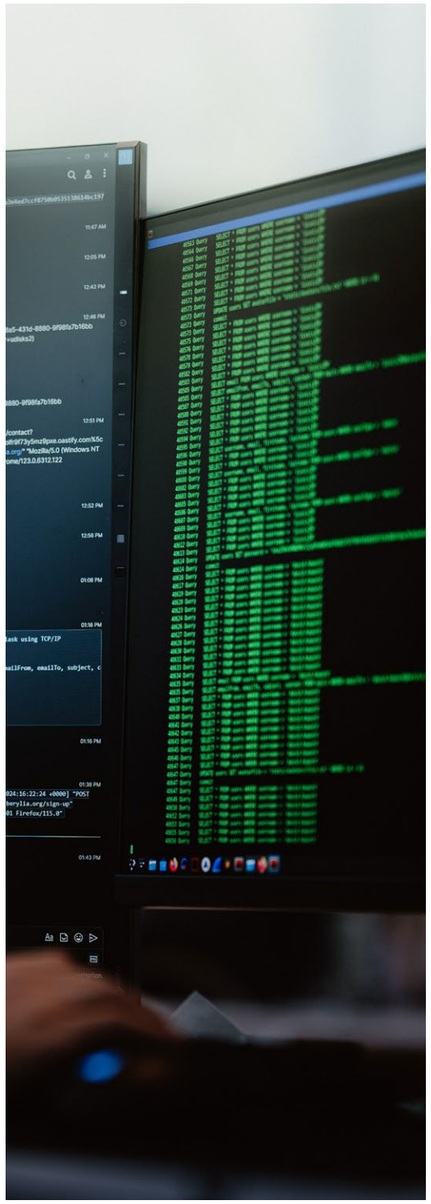
Voor de ADIV heeft dit betrekking op alle informatie die een buitenstaander met kwade bedoelingen kan helpen om de uitvoering van defensieopdrachten te belemmeren, en dus niet alleen geheime of vertrouwelijke informatie in de strikte zin van de wet.

Als gastland van verschillende internationale organisaties zoals de NAVO en de EU is België een belangrijk doelwit, en de ADIV is medeverantwoordelijk voor hun bescherming. De ADIV is van mening dat de huidige geopolitieke context tot uiting komt in het zeer hoge spionagedreigingsniveau waarmee onze instellingen geconfronteerd worden op het gebied van spionage en inmenging. Deze trend zal zich in 2024 voortzetten.

Gedurende 2023 voerde de ADIV verschillende inlichtingenonderzoeken uit op het gebied van contraspionage en contra-inmenging. Waar nodig nam de ADIV maatregelen om de bestaande dreiging te neutraliseren, in samenwerking met of ter ondersteuning van zijn Directie Veiligheid, de Algemene Directie Human Resources van Defensie en zijn Belgische partners (Veiligheid van de Staat, Openbaar Ministerie).

Hoewel de ADIV een grotere verscheidenheid in de gebruikte spionagetechnieken vaststelt, wat deels het gevolg is van technologische ontwikkelingen, blijft het traditionele gebruik van menselijk contact als informatiebron een wijdverspreide methode. In 2023 werden verschillende pogingen tot spionage geïdentificeerd en doorkruist.

Er werd in die periode dan ook speciale aandacht besteed aan de bewustmaking van het personeel met betrekking tot de technieken die worden gebruikt door buitenlandse inlichtingenagenten en hoe we ons hiertegen kunnen beschermen. In 2023 werd een grootschalige interne bewustmakingscampagne opgezet. In de toekomst zullen preventiemiddelen worden ontwikkeld en ter beschikking worden gesteld van al het Defensiepersoneel.



Spionage, ook in de activiteiten van cyberspace

Naast de diefstal van bedrijfsgeheimen en intellectuele eigendom nemen de spionageactiviteiten door Chinese cyberactoren toe, waarbij vooral de instellingen van de Europese Unie en de regeringsinstanties van de Europese landen en de NAVO het doelwit vormen. Een van hun doelen is om de standpunten van de Europese landen over Taiwan en de Europese initiatieven gericht op het verminderen van de risico's verbonden aan de economische afhankelijkheid ten opzichte van China te achterhalen.

Deze actoren maken gebruik van steeds complexere netwerkstructuren om de onvoldoende beveiligde infrastructuren van particulieren en bedrijven te hacken of zogenaamde zero-day-kwetsbaarheden uit te buiten.

Belgische overheidsinstanties, waaronder Defensie, zijn ook reeds het slachtoffer geworden van Chinese cyberspionage. Deze aanvallen beperkten zich echter tot spionagedoeleinden en verschaften geen blijvende toegang tot de gegevens van de getroffen instellingen.

Naast de cyberactoren die gelinkt zijn aan de Chinese inlichtingendiensten, vormen ook de Chinese publieke en private bedrijven een potentiële cyberdreiging. De Chinese National Intelligence Law staat Chinese inlichtingendiensten immers toe om van Chinese bedrijven en burgers waar ook ter wereld te eisen dat ze te allen tijde meewerken. Chinese hardware- en softwareoplossingen die gebruikt worden in de telecommunicatie- en transportsector vormen daarom een potentiële cyberspionagedreiging, nu en in de toekomst, ook in België.

De ADIV heeft de plicht om de nodige capaciteiten te ontwikkelen om de Belgische belangen te beschermen. Samen met zijn partners zoals het Centrum voor Cybersecurity België (CCB), het Nationaal Crisiscentrum (NCCN) en de FOD Justitie levert het Cyber Command van de ADIV een actieve bijdrage aan de nationale cyberweerbaarheid. Het ondersteunt regelmatig de gezamenlijke inspanningen door technisch advies te geven en beschikt over geavanceerde defensieve capaciteiten.

Cyberdreigingen: België en zijn bondgenoten worden het slachtoffer van pro-Russische hacktivisten

In de context van het Russisch-Oekraïens conflict hebben de Russische cyberspionageoperaties die uitgevoerd worden door een cyberactor verbonden aan de Russische buitenlandse inlichtingendienst (SVR), vooral de diplomatieke instellingen van de lidstaten van de Europese Unie en van de NAVO geviseerd. Deze operaties hebben geleid tot een toename van de frequentie van de aanvallen en tot de voortdurende ontplooiing van nieuwe kwaadaardige software die tot doel heeft de ingezette detectietools te dwarsbomen. Bovendien is het binnendringen in Microsoft Cloud-oplossingen, vanwege het toenemende gebruik ervan door regeringsinstanties en bedrijven, een belangrijk doel geworden voor deze cyberactor.

Tegelijkertijd hebben pro-Russische hacktivisten zogenaamde 'Distributed Denial of Service'-aanvallen (DDoS) uitgevoerd in nagenoeg alle NAVO-lidstaten. Door de websites te overladen door het sturen van talrijke query's of kwaadaardige gegevens, beletten zij de goede werking ervan. België is ook het slachtoffer geweest van verschillende van die aanvallen, met name op regerings-, haven- en luchtverkeersleidingssites. Over het algemeen hebben die cyberaanvallen echter maar een beperkte impact gehad. De hacktivisten hebben veeleer de daarop betrekking hebbende media-aandacht benut om de Russische desinformatiecampagnes te voeden.

Uit verschillende informatiebronnen blijkt dat Rusland doorgaat met het ontwikkelen van zijn cybersabotagecapaciteiten en het uitvoeren van operaties in cyberspace, in het bijzonder om kritieke infrastructuren aan te tasten.

GETUIGENIS

"Cyberdefensie is vooral een kwestie van preventie en detectie.", Gilda, 40 jaar

België ondergaat bijna maandelijks verstorende aanvallen van pro-Russische 'hacktivisten' die de internetsites van verschillende regeringsdiensten viseren. Bovendien trachten de cybereenheden van de verschillende Russische inlichtingendiensten voortdurend de zwakheden van de software te benutten of de toegang van de gebruikers tot systemen te verkrijgen via phishing en andere technieken. De intrusiepogingen nemen voortdurend toe, ongeacht of het publieke of privéstructuren betreft.

De opdracht van het Cyber Command van de ADIV als transversale capaciteit, is het beschermen van de netwerken en wapensystemen die door Defensie worden gebruikt. Gilda, analiste CSOC (Cyber Security Operations Centre) staat op de eerste rij van de cyberdefensie.

"Als data analyst bestaat mijn rol erin om gegevens met een preventief, maar ook reactief doel te analyseren. Met mijn team bewaken we de netwerken en ICT-infrastructuren van Defensie, genereren we waarschuwingssystemen om abnormale activiteiten op te sporen en wanneer we zulke activiteiten opsporen, bepalen we de acties en maatregelen die moeten worden genomen om een optimale veiligheid te garanderen.

Mijn leitmotiv daarbij is bij te dragen tot de bescherming van ons land en zijn bevolking. Vandaag lijkt mij dat in het kader van mijn functies meer dan ooit waar te zijn. Dag in dag uit reageer ik op zwakke plekken in de veiligheid die wel degelijk reëel zijn en onderneem ik concrete actie voor onze veiligheid, en dus de veiligheid van ons land."

Proliferatiedreiging

Op het gebied van proliferatie was er in 2023 een groeiende trend in de overdracht van gevoelige technologieën tussen staten en aan niet-statelijke proxy's, waaronder geavanceerde tactische en strategische lanceersystemen die worden gebruikt in Oekraïne en het Midden-Oosten. De toename in proliferatie, ondanks de gevestigde internationale normen, en het toegenomen gebruik van nucleaire dwang door Rusland als onderdeel van de confrontatie met het Westen (in het bijzonder door de terugtrekking uit verschillende strategische wapenverminderingsverdragen zoals New START - Strategic Armament Reduction Treaty of CTBT - Comprehensive Test Ban Treaty), versnellen de erosie van de architectuur van non-proliferatie van massavernietigingswapens.

De achteruitgang van de non-proliferatiearchitectuur en de versnelde concurrentie tussen grootmachten leiden tot een wapenwedloop, ook op strategische gebieden, en een verhoogd risico op escalatie en misrekening. De ontwikkeling van ballistische en nucleaire programma's door een aantal gevoelige landen (waaronder - maar niet beperkt tot - China, Iran en Noord-Korea) en de moeilijkheden die internationale instellingen ondervinden bij het beheren van deze vooruitgang zijn ook een toenemende bron van bezorgdheid.

EU2024BE

Vergadering van de Cyber Commanders

Internationale betrekkingen in cyberspace

Interactie met nationale, internationale en multinationale organisaties blijft een van onze prioriteiten. Deze interacties stellen ons niet alleen in staat om ons te profileren als een betrouwbare internationale partner, maar ook om de ontwikkelingen op het gebied van governance en cyberveiligheid te volgen, nieuwe initiatieven te ondersteunen en mogelijke kansen voor samenwerking of synergieën te zoeken.

Regelmatig vinden er vergaderingen plaats met onze collega's van het Centrum voor Cybersecurity België, de Permanente Vertegenwoordiging van België bij de NAVO en de Europese Unie, en de FOD Buitenlandse Zaken, zodat we effectiever kunnen samenwerken om de uitdagingen van vandaag en morgen aan te gaan.

In 2023 is een speciale inspanning geleverd om nationale strategieën en processen af te stemmen op het nieuwe beleid en de governance op het gebied van cyberveiligheid zoals gedefinieerd door de NAVO en de EU. Dit is van vitaal belang om een harmonieuze samenwerking te garanderen en de technische interoperabiliteit van onze landen in stand te houden. In maart 2023 werd het Cyber Command bovendien een volwaardig lid van de "Cyber Rapid Response Teams" (CRRT), een project dat is opgezet om lidstaten in staat te stellen elkaar te helpen een hoger niveau van cyberweerbaarheid te bereiken en collectief te reageren op cyberincidenten.

Deel III

De dreigingen trotseren en bijdragen aan nationale weerbaarheid

De ADIV anticipeert op technologische ontwikkelingen, houdt zijn expertise op peil en draagt samen met zijn partners bij aan de binnenlandse veiligheid.

Om onze veiligheid te waarborgen en bij te dragen aan nationale weerbaarheid, moeten we niet alleen onze expertise op een groot aantal gebieden op peil houden, maar ook anticiperen op technologische en maatschappelijke ontwikkelingen in de komende jaren. Door middel van partnerschappen past onze organisatie zich in al haar ontwikkelingslijnen aan en versterkt ze voortdurend haar vermogen om de haar toevertrouwde opdrachten te vervullen.

In geval van een nationale of internationale crisis kan er een beroep worden gedaan op de ADIV om expertise of technische ondersteuning te bieden. Voorop blijven lopen op het gebied van technologie en de laatste trends is daarom meer dan een strategische beslissing, het is een noodzaak. Dit wordt bereikt door middel van partnerschappen met de inlichtingendiensten, de industrie, de academische wereld en verenigingen. Optimalisatie en innovatie zijn hier de sleutelwoorden.

Gemeenschappelijke platforms in de strijd tegen extremisme en terrorisme

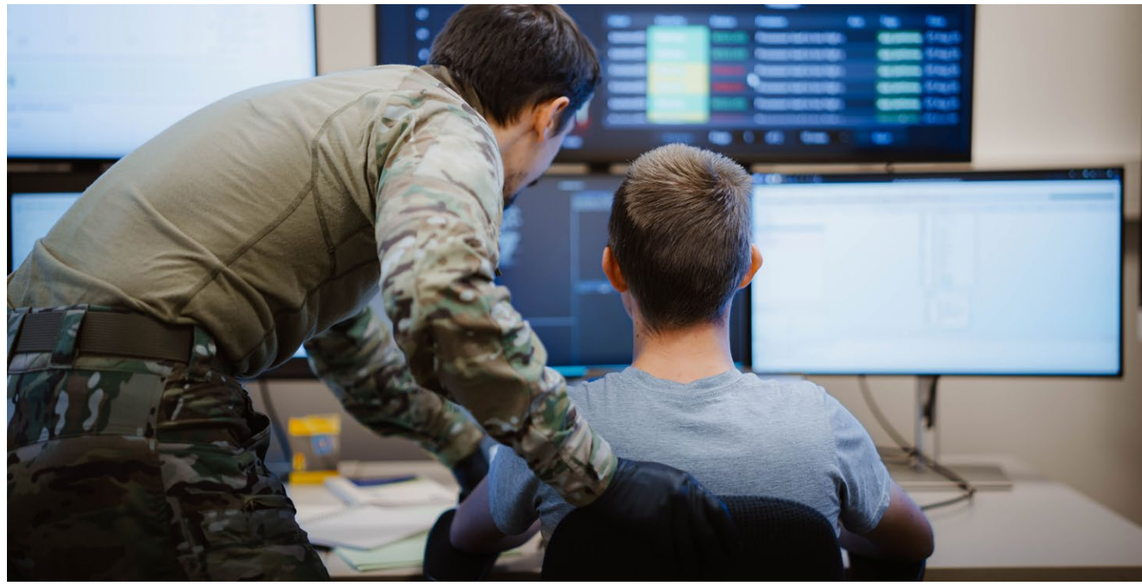
In 2018 bereikten de ADIV en de Veiligheid van de Staat overeenstemming over het "nationaal strategisch inlichtingenplan" (NSIP), een ambitieus plan voor een versterkte structurele samenwerking om de gemeenschappelijke dreigingen die onder hun bevoegdheid vallen beter te bestrijden. Sinds 2022 bevindt het zich in een tweede fase, die wordt gekenmerkt door een versterking van de samenwerkingsgebieden en synergieën. Het is de bedoeling dat elke dienst op intelligente wijze gebruikmaakt van de comparatieve voordelen van de andere, in het bijzonder op het gebied van expertise en specifieke middelen om informatie te vergaren, en ook dat de inspanningen in de strijd tegen bepaalde specifieke dreigingen gebundeld worden.

Begin 2024 is het gezamenlijk platform ter bestrijding van extremisme en terrorisme, zowel religieus als ideologisch (rechts- en links-extremisme), in werking getreden. Het personeel van de ADIV en de VSSE werkt nu samen in één entiteit, waardoor de uitwisseling van informatie en de inzet van beschikbaar personeel worden geoptimaliseerd. Dit is een belangrijke uitbreiding van een reeds bestaand gezamenlijk platform dat sinds 2018 operationeel is. Dit laatste, dat beperkt was tot de strijd tegen religieus terrorisme, heeft tot veel vooruitgang geleid.

De recente terroristische aanslagen in Europa en België hebben de noodzaak aangetoond van een nauwere samenwerking tussen onze verschillende inlichtingendiensten. Deze synergie moet een maximale uitwisseling van informatie, het bundelen van middelen en een gezamenlijke beoordeling voor onze partners mogelijk maken. Naast andere maatregelen zullen gemengde teams van ADIV- en VSSE-personeel worden opgezet.

Op lange termijn zal deze samenwerking ook betrekking hebben op andere soorten dreigingen, in het bijzonder spionage en inmenging, volgens procedures die specifiek zijn voor elke dreiging. Door informatie beter te delen en te coördineren zouden spionnen die op ons grondgebied opereren of die tegen onze nationale belangen werken, gemakkelijker en doeltreffender moeten worden ontmaskerd.

Naast deze vooruitgang omvat het NSIP ook ICT- en opleidingsaspecten. De geleidelijke implementatie weerspiegelt de wens van beide diensten om steeds nauwer samen te werken, in een geest van wederzijds respect en vertrouwen, in overeenstemming met de leuze van ons land "eendracht maakt macht".



Militaire veiligheid verzekeren, nationale veiligheid versterken

Naar aanleiding van de zaak ”Jurgen Conings” in 2021 is een reeks maatregelen vastgelegd in een actieplan om de veiligheidscultuur bij Defensie te verbeteren.

Na de zaak “Jurgen Conings” in 2021 is een reeks maatregelen vastgelegd in een actieplan om de veiligheidscultuur bij Defensie te verbeteren. In het jaar 2023 werden er een aantal maatregelen geïmplementeerd en geconcretiseerd, in het bijzonder de actualisering van de militaire veiligheidsnormen van Defensie door een ADIV-werkgroep.

Spionage, subversie en sabotage, maar ook terrorisme en georganiseerde misdaad zijn realiteiten waar de hele organisatie behendig mee om moet kunnen gaan. De implementatie van deze nieuwe normen die gebaseerd zijn op potentiële risico’s, rekening houdend met technologische ontwikkelingen en nieuwe wetgeving, is een belangrijke stap in het waarborgen van de veiligheid van Defensie. Evenals die van haar industriële en institutionele partners, zowel nationaal als internationaal. Bij incidenten worden de te ondernemen acties bepaald om de paraatheid zo snel mogelijk te herstellen.

Er zijn aanzienlijke inspanningen geleverd op een aantal gebieden, zoals bewustmaking op alle commandoniveaus, opleiding, toezicht op veiligheidsmachtigingen en meer controle op wapens en munitie.

Het doel van al deze maatregelen is het garanderen van een zekere striktheid, maar ook het bieden van de flexibiliteit die Defensie nodig heeft om zich aan te passen aan de voortdurend veranderende veiligheidsomgeving, en meer samenwerking tussen de verschillende bevoegde autoriteiten.

Concreet

1. Invoering van het concept ”Security by Design”, ook wat cyberveiligheid betreft, bij het ontwerpen van de infrastructuur van Defensie.
2. Versterking van de uitwisseling tussen de eenheden, de Algemene Dienst Inlichting en Veiligheid (ADIV) en de Algemene Directie Human Resources (DGHR).
3. Bewustmaking, opleiding en versterkte controle op alle commandoniveaus.
4. Controle van de betrouwbaarheid van Defensiemedewerkers vanaf het moment dat ze worden aangeworven en gedurende hun hele loopbaan.
5. Oprichting van een orgaan voor permanente evaluatie dat aanpassingen kan uitvoeren in het licht van bijvoorbeeld technologische of contextuele ontwikkelingen.

GETUIGENIS

”Ik wilde me concentreren op een job met sterke waarden.” Jean, 30 jaar

Bij Defensie zijn alle huidige en toekomstige communicatie- en wapensystemen gebaseerd op het gebruik van cryptografische sleutels. Hun operabiliteit en bewegingsvrijheid hangen hier rechtstreeks van af. Jean, 30, IT-ingenieur gespecialiseerd in cyberbeveiliging, is momenteel verantwoordelijk voor de Audit en Accreditatie van systemen. Na voor verschillende multinationals te hebben gewerkt, kwam hij bij het Cyber Command terecht.

”Ik wilde me concentreren op een job met sterke waarden. Dus ik voelde me vanzelf aangetrokken tot Defensie. Hier voel ik me onderdeel van een team en werken we samen om een gemeenschappelijk doel te bereiken. Op dagelijkse basis bestaat mijn rol uit het goedkeuren van wapensystemen of het waarborgen van hun veiligheidsniveau. Het gaat over zowat alles, van netwerkinfrastructuur tot systemen gekoppeld aan de F-35, de nieuwe gemotoriseerde capaciteit (CaMo) en het Belgisch-Nederlandse mijnenjagerprogramma.”

Een officier van de KMS voor het défilé van 21 juli.

Mijn job is heel gevarieerd. Morgen ben ik in de Koninklijke Militaire School (KMS) voor een opleiding, daarna ga ik naar de kazerne van Peutie om een inspectie te doen en de week daarna ga ik naar Straatsburg om steun te bieden aan het Eurokorps … Er is een diversiteit aan acties en taken waardoor het werk interessant blijft, ook al blijft mijn functie hetzelfde.

In feite heeft het Cyber Command van de ADIV gewoon de middelen beschikbaar gesteld om zijn ambities waar te maken. Er is een politieke wil die direct wordt omgezet in actie en dat bevalt me.”

Jean en zijn team zullen ook betrokken worden bij het ontwerp van het toekomstige Hoofdkwartier in Evere, waar ze eveneens verantwoordelijk zullen zijn voor de controle van domotica, veiligheidsnormen voor elektromagnetische emissies en vele andere systemen.

Het momentum van technologische verandering aangrijpen

Cyberspace is een van de krachtigste vectoren geworden voor het verspreiden van dreigingen. Pogingen om defensiesystemen binnen te dringen en de explosieve toename van cyberaanvallen op zowel publieke als privéstructuren, in het bijzonder in de context van de aanvalsoorlog van Rusland tegen Oekraïne, nemen voortdurend toe. Het kunnen reageren op deze dreigingen in de verschillende gebieden van cyberspace is een van de fundamentele taken van het Cyber Command.

Het Cyber Command van de ADIV heeft 140 miljoen euro toegewezen gekregen om zijn capaciteiten te ontwikkelen als onderdeel van het STAR-plan, dat ook de uitvoering van de DIRS (Defence, Industry and Research Strategy) omvat om zich te richten op de ontwikkeling van een sterke en technologisch geavanceerde Defensie-industrie.

Op het gebied van cyberdefensie is samenwerking met de industrie, nationale onderzoekscentra en de academische wereld een conditio sine qua non voor de ontwikkeling van nieuwe technologieën. Het Cyber Command, toekomstige Defensiecomponent en nog steeds verbonden aan het inlichtingenmilieu, moet op korte en lange termijn de kennis en middelen kunnen garanderen die nodig zijn om te reageren op huidige en toekomstige hightechdreigingen.

In deze context werd op 26 juni 2023 een structurele samenwerkingsovereenkomst ondertekend met de Koninklijke Militaire School, waarbij deze laatste werd aangewezen als bevoorrechte partner in cyberonderzoeks- en -ontwikkelingsprojecten. De overeenkomst ondersteunt talloze langlopende onderzoeks- en ontwikkelingsprojecten ten voordele van Defensie en de burgermaatschappij. Naast deze samenwerking zijn er uitwisselingen met andere universitaire instellingen zoals de KU Leuven, de Universiteit Gent en HOWEST.

Er wordt ook intensief samengewerkt met de industrie via Cyber Made in Belgium for Defence (CMIB4Def), een gezamenlijk initiatief van AGORIA, de federatie van technologiebedrijven, en het Cyber Command. De samenwerking is gebaseerd op de vaststelling dat het verbeteren van onze cyberdefensie en onze collectieve weerbaarheid noodzakelijkerwijs nauwere banden tussen Defensie en de industrie vereist. De discussies en werkzaamheden binnen CMIB4Def hebben betrekking op onderwerpen als ondersteuning van operationele Defensiecapaciteiten, versterking van de toeleveringsketen voor cyberdefensie en de ontwikkeling van cybercompetenties.

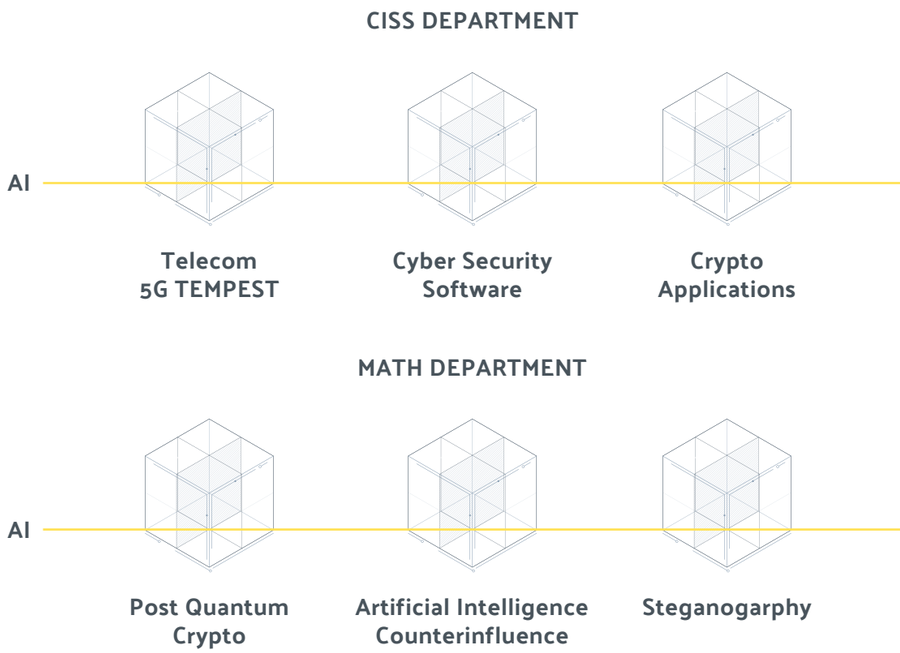
Partnerschap met AGORIA, de federatie van technologiebedrijven.

ESA

Sinds mei 2023 werkt het Cyber Command ook samen met het Europees Ruimtevaartagentschap aan de ontwikkeling van hun opleidingscentrum, het European Space Security & Education Centre (ESEC) in Redu. Deze structurele samenwerking is gericht op het bevorderen van uitwisselingen tussen de twee partijen, onder meer inzake onderzoek en ontwikkeling op het gebied van kwantumtechnologieën.

ONZE ZES ONDERZOEKSGEBIEDEN

Een voorbeeld: de beschikbaarheid van een 5G-netwerk garanderen in geval van een crisis



Het Cyber Command is betrokken bij talloze projecten in samenwerking met de academische en industriële wereld en bereidt zich voortdurend voor op de toekomst. Een van de belangrijkste gebieden voor het ontwikkelen van onze nationale cyberweerbaarheid is de bescherming van kritieke netwerken en infrastructuren.

Het doel van een project dat voortvloeit uit het Memorandum of Understanding met de Koninklijke Militaire School is om, in samenwerking met Orange België, het gebruik van een 5G-installatie te bestuderen om 'kritieke' netwerken op Belgische Defensiebasissen te ondersteunen. Deze netwerken moeten immers permanente ondersteuning kunnen bieden voor operaties of logistieke en technische ondersteuning in het kader van de noodplannen. Het is daarom belangrijk dat Defensie analyseert welk type 5G-infrastructuur geschikt is voor deze behoefte op het gebied van informatiebeveiliging (vertrouwelijkheid, integriteit en beschikbaarheid) en communicatie (integratie met onze bestaande netwerken, specifieke diensten enz.).

Bovendien ontving het consortium met Orange België voor de uitvoering van zijn studie subsidies voor zowel experimentele ontwikkeling als onderzoeksinfrastructuur, onder meer door te reageren op een oproep voor subsidies gelanceerd door de FOD Economie. Alles bij elkaar zal het mogelijk zijn om kritieke oplossingen te testen en te integreren en een volledige evaluatie van de cyberveiligheid en het 5G-plan uit te voeren.

Deel IV

Ons menselijk kapitaal ontwikkelen

Onze agenten en medewerkers zijn de grootste troef van de ADIV. De diversiteit aan beroepen binnen onze dienst en de technologische ontwikkelingen maken het essentieel om te blijven investeren in ons menselijk kapitaal en om meer open te staan voor de burgermaatschappij.

In een snel veranderende arbeidsmarkt die wordt gekenmerkt door een tekort aan geschoolde arbeidskrachten, een groeiende strijd om talent en voortdurende veranderingen in de technologiesector, wil de ADIV afstand nemen van de paradigma's van het zogenaamde 'traditionele' aanwervingsbeleid. Er wordt gekeken naar nieuwe manieren om talent te ondersteunen, in samenwerking met de academische wereld, verenigingen en de industrie. Als het gaat om collectieve veiligheid en defensie zijn, zowel voor bedrijven als voor de publieke sector, de afwegingen die moeten worden gemaakt en de uitdagingen die voor ons liggen, inderdaad aanzienlijk.

De professionele wereld van cyberdefensie blijft bijzonder veeleisend en competitief. En bepaalde transversale competenties zijn soms onvoldoende ontwikkeld bij degenen die de arbeidsmarkt betreden. In deze context kan elke vorm van striktheid in wervings- en selectieprocedures schadelijk zijn.

In 2023 zijn er een aantal initiatieven gelanceerd om de toegankelijkheid te verbeteren, de wervingsprocedures te stroomlijnen en natuurlijk een opleidingstraject aan te bieden dat beter aansluit bij de verwachtingen van alle belanghebbenden.

BEZOEK

Cyber Command

In januari 2024 kreeg het Cyber Command van de ADIV een bezoek van de Chef Defensie, Admiraal Hofman.

Spelers die arbeidsbemiddeling en beroepsopleiding bieden, zijn zich sterk bewust van hun maatschappelijke toegevoegde waarde bij het (weer) aan het werk krijgen van jonge “NEETs” (Not in Education, Employment or Training) en proberen zichzelf nu te promoten als echte wervingspartners. Hun benadering is om werkzoekenden niet alleen op te leiden om aan praktische eisen te voldoen, maar ook om zo effectief mogelijk tegemoet te komen aan de verwachtingen en behoeften van toekomstige werkgevers. De ADIV is van plan deze initiatieven volledig te ondersteunen. Als partner van Molengeek en BeCode en door de krachten te bundelen met deze talentaanbieders biedt de dienst kandidaten de kans om op een flexibelere manier aan de slag te gaan in de cyberdefensie en om meer bij te leren tijdens hun beroepsleven. Deze inspanning moet in 2024 worden voortgezet met onder andere de opening van civiele kantoren in de A6K-kantoren te Charleroi.

Een van de initiatieven om de rekrutering en opleiding van toekomstige cyberdefensie-experts te bevorderen, zowel nu als in de toekomst, is de deelname van de ADIV aan de onderzoeks- en innovatiegroep Cyber Made in Belgium for Talents, geïnitieerd door Agoria Een ander initiatief is de aanwending van ADIV zijn communicatie- en toenaderingsinspanningen voor de organisatie van gerichte evenementen. De ADIV wil daarnaast ook zijn reserve meer in lijn brengen met de bedrijfswereld.

[1]A6K

A6K is een uniek en stimulerend ecosysteem in het hart van Europa dat industrieleiders, opkomende start-ups, universiteiten, institutionele spelers en onderzoekscentra op één locatie samenbrengt om innovatie op het gebied van engineering te stimuleren.

Cyber Command onderhoudt nauwe contacten met non-profitorganisaties zoals BeCode om cyberexperts te werven in het kader van Rosetta-contracten.

Een ”win-win-winformule” op korte en lange termijn voor iedereen, van werkzoekenden, jong en minder jong talent, tot professionals en industrieën in de cyberbeveiligingssector. In de toekomst wil de ADIV een echt “waardevoorstel” doen waarbij iedereen als winnaar uit de bus komt, steeds met het oog op het bijdragen aan de nationale weerbaarheid.

Naar een nieuw concept voor de reserve?

Het versterken en promoten van de reserve is een manier om banden te smeden met het publiek, een echt ”waardevoorstel” te doen aan professionals en bij te dragen aan de nationale cyberweerbaarheid.

Reservist worden

geeft je de kans om bij het leger te gaan en je land te dienen, maar ook om je kennis te delen, ideeën uit te wisselen met andere professionals en je expertise te ontwikkelen door bij te dragen aan innovatieve projecten.

Bij de ADIV hebben reservisten bijvoorbeeld de mogelijkheid om opleidingen te volgen, deel te nemen aan trainingen zoals “Locked Shields”, de belangrijkste grootschalige cyberdefensieoefening die wordt georganiseerd door het Cooperative Cyber Defence Centre of Excellence (CCDCOE) van de NAVO. Door concrete projecten en mogelijkheden voor ”vorming en bijscholing” van cyberbeveiligingsprofessionals aan te bieden, wil de ADIV beter tegemoetkomen aan de behoeften van bedrijven, professionals en Defensie.

Vanuit dit oogpunt is de reserve een win-win-win-situatie voor bedrijven, professionals en Defensie. Het zal de kennis en expertise van elke partij vergroten, de mobiliteit van cyberbeveiligingsdeskundigen bevorderen en de samenwerking tussen de industrie en de cyberdefensiegemeenschap stimuleren.

Het is ook een middel om de nationale cyberweerbaarheid te versterken. In het geval van een nationale crisis blijft het Cyber Command een essentiële schakel, maar door deze samenwerking met bedrijven en hun professionals te ontwikkelen, kunnen zij ook op hun eigen niveau actie ondernemen. De eerste linie van cyberdefensie blijft de gebruiker, dat wil zeggen de burger, en het vergroten van zijn of haar bewustzijn draagt ongetwijfeld bij aan de veiligheid van onze natie als geheel. De reserve ontwikkelen betekent onze bescherming vergroten door een breder netwerk te ontwikkelen, zowel met de professional als met zijn of haar bedrijf.

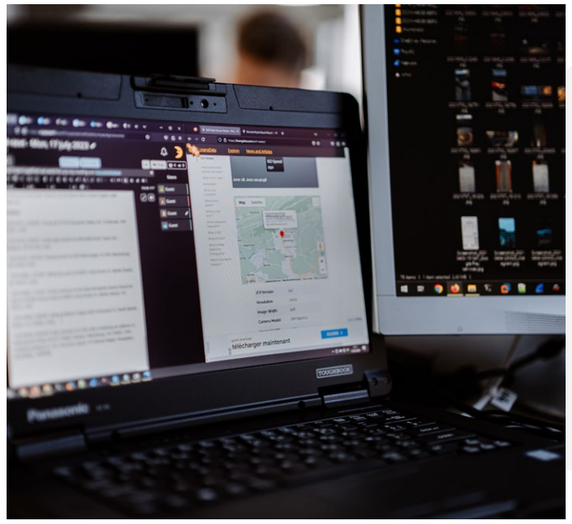
Eerste editie van de “Cyber Summer School” en de “Cyber Discovery Day”

Jong talent de kans geven om het DNA van hun toekomstige werkgever te ontdekken en meer inzicht te krijgen in de uitdagingen van cyberdefensie is zeker een van de wegen die moeten worden verkend om de uitdagingen van de arbeidsmarkt aan te gaan.

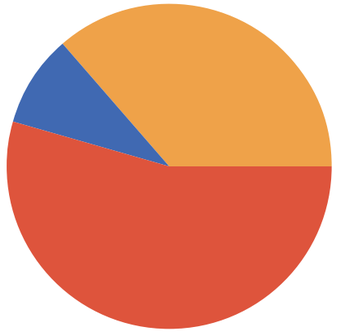
Als onderdeel van dit streven naar openheid organiseerde het Cyber Command in de zomer van 2023 zijn eerste “Cyber Summer School”, gevolgd door een miniversie ervan, de “Cyber Discovery Day”. Deze twee nieuwe initiatieven nodigden studenten en jonge professionals uit om op een meer diepgaande, menselijke en originele manier achter de schermen van het Cyber Command en zijn opdrachten te kijken.

Na een uitgebreide selectieprocedure werden ongeveer twintig kandidaten gekozen om deel te nemen aan het “Cyber Summer School”-programma, een zomerstage in een militaire omgeving. Ze werden vijf dagen lang ontvangen op de Koninklijke Militaire School en kregen de kans om de cultuur en capaciteiten van het Cyber Command van binnenuit te ontdekken door middel van praktische workshops en ludieke activiteiten. Deelnemers kregen de kans om een forensische analyse van smartphones uit te voeren, het hacken van een computernetwerk te ontleden en technieken te leren voor het zoeken naar informatie op het dark web.

SGRS - ADIV / DEEL IV



Heel erg bedankt voor een heerlijke week die we niet snel zullen vergeten.” Als we de reacties van de deelnemers mogen geloven, was het evenement dit jaar een groot succes. Het initiatief, dat doelgericht is en het imago van het Cyber Command weerspiegelt, heeft duidelijk veel nieuwe rekruten aangetrokken, aangezien bijna een kwart van hen zich al bij onze dienst heeft aangesloten, hetzij als reservist of als voltijds werknemer.



ZOU JE NA DE CYBER SUMMER SCHOOL GENEIGD ZIJN OM BIJ HET CYBER COMMAND TE GAAN WERKEN?

- MILITAIR (BLAUW)
- BURGER (ROOD)
- RESERVE (ORANJE)
- NEEN (GROEN)

WWW.SGRS.BE