ADIV · SGRS
APRIL 2025 / WWW.SGRS.BE

JAARVERSLAG 2024

56° 30' 0" N, 31° 43' 15" E

DEFENSIE

.be

OMSLAGFOTO: Munitiedepot in Toropets (RUS) na Oekraïense bombardementen.

De wereld verandert, maar onze missie blijft dezelfde.

INHOUD

GENERAAL-MAJOOR
STÉPHANE DUTRON
CHEF VAN DE ADIV

Quaero et Tego is ons motto; ons land, onze bedrijven en onze expats beschermen door middel van onze inlichtingen is onze primaire missie; de autoriteiten verstandig adviseren is onze plicht tegenover ons land, de samenleving en onze medeburgers.

VERANTWOORDELIJKE REDACTEUR

M. Van Hecke Bernard

Kwartier Koningin Elisabeth
Eversestraat 1, 1140 Evere

Beeldmateriaal : DG StratCom en personeel ADIV

Layout : ADIV-SGRS

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

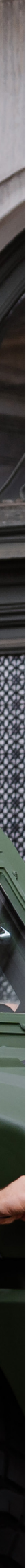
Generaal-majoor
Stéphane Dutron

DE KOMST VAN DE F-35

De komst van F-35 gevechtsvliegtuigen naar de Air- en Space Component stelt de Cyber Component voor een aantal technologische uitdagingen, met name op het gebied van de bescherming van wapensystemen.

ONZE BOODSCHAP

Uw toekomst. Onze missie.



Introductie

De wendbaarheid van de Dienst, een antwoord op de veranderingen in de veiligheidsomgeving

Ook 2024 zal niet het jaar zijn dat vrede in de wereld bracht, met voornamelijk twee grote conflicten met steeds zorgwekkender geopolitieke gevolgen. In februari 2025 is het alweer drie jaar geleden dat Rusland begon met zijn vernietigende invasie in Oekraïne. In het Nabije Oosten zal 2024 herinnerd worden vanwege de intensivering en geografische uitbreiding van het conflict tussen Israël en Hamas, dat opnieuw oplaaide na de tragische gebeurtenissen van 07 oktober 2023.

In Oekraïne was de frontlinie relatief stabiel, maar er is sprake van een langzame en gestage opmars van de Russische troepen, die gepaard gaat met kolossale verliezen, de toepassing van nieuwe doctrines voor het gebruik van middelen en, bovenal, de overgang naar een oorlogseconomie. Met logistieke steun van een aantal landen toonde Oekraïne zich weerbaar, zowel aan het front als in de diepte van zijn grondgebied, en slaagde het erin een symbolische en spectaculaire doorbraak te forceren in de regio Koersk, op Russisch grondgebied. Het zenden van Noord-Koreaanse troepen naar de regio zorgt voor een verdere internationalisering van het conflict en roept vooral vragen op over de langetermijngevolgen van deze nieuwe allianties en hun invloed op andere potentieel crisisgevoelige gebieden.

In het Nabije Oosten bombardeerde het Israëlische leger, naast interventies in Gaza en de westelijke Jordaanoever, intensief Hezbollah-stellingen in Zuid-Libanon, maar het sloeg ook toe in Syrië en Iran. De uitbreiding van de Tsahal-operaties wordt nauwlettend in de gaten gehouden door de Diensten, net als het verlies van invloed van Iran via zijn proxy's. De abrupte val van het Assad-regime in Syrië afgelopen december heeft een dosis onzekerheid toegevoegd en geleid tot een herschikking van de kaarten en de invloedssferen.

Mijn Dienst volgt de ontwikkelingen natuurlijk op de voet, en niet alleen in deze twee conflictgebieden. Onze analisten, ondersteund door onze vele middelen voor het verzamelen van gegevens, produceren diepgaande analyses waarin de feiten worden benadrukt, maar waarin ze vooral proberen trends te identificeren om zo goed mogelijk te anticiperen op mogelijke ontwikkelingen. We doen dit om onze militaire en politieke autoriteiten te adviseren en om van gedachten te wisselen met onze nationale en internationale partners, zonder het doel uit het oog te verliezen, namelijk het waarborgen van de veiligheid van onze staatsburgers en van onze nationale belangen.

De meeste regionale confrontaties hebben natuurlijk gevolgen in Europa en België. Dit heeft in het bijzonder geleid tot een zorgwekkende toename van antisemitisme en

radicalisering en, als gevolg daarvan, meer werk voor de inlichtingen- en veiligheidsdiensten. Het niveau van de dreiging, onder meer op het gebied van spionage en inmenging, is blijven stijgen, wat aanleiding geeft tot gerichte maatregelen om ons hiertegen te proberen verweren.

Mijn Dienst moest in een dergelijke context wendbaar zijn en mijn medewerkers hebben hun flexibiliteit en beschikbaarheid bewezen door zich met grote inzet aan te passen aan de wereldwijde veranderingen in de veiligheidsomgeving. Een van mijn prioriteiten voor mijn eerste jaar als hoofd van de Dienst werd dan ook verwezenlijkt.

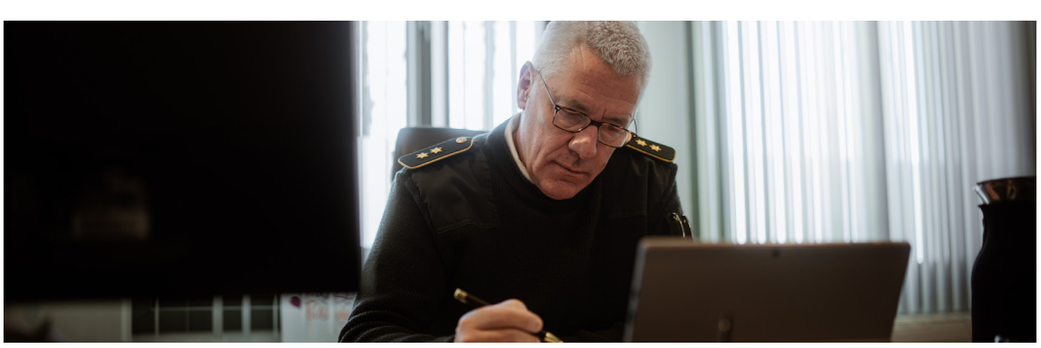
In dezelfde geest hebben we onze wervingsinspanningen voortgezet, zowel voor burgerpersoneel als voor militairen, met als doel een verdubbeling van ons personeelsbestand tegen 2040. Ik heb bijzondere aandacht besteed aan de ontwikkeling van de vormingsprogramma's en aan de begeleiding van onze nieuwe collega's. Ook in de toekomst zullen hiervoor aanzienlijke middelen worden uitgetrokken en hetzelfde geldt voor onze infrastructuur.

Tot slot zullen we de digitalisering van onze directies intensiveren en onszelf blijven uitrusten met geavanceerde capaciteiten om onze inlichtingenoperaties uit te voeren, zowel in de fysieke wereld als in cyberspace. In 2024 hebben we nieuwe projecten ontwikkeld met enkele van onze nationale partners zoals de Veiligheid van de Staat en de Federale Politie, terwijl ik persoonlijk heb gewerkt aan het versterken van onze banden met buitenlandse partners.

Veel leesplezier!

GENERAAL-MAJOOR

Stephane Outron



ADIV - SGRS / CYBER COMMAND

Cyber Command

Cyber Force Through Partnerships

2024 was een bijzonder druk jaar voor het Cyber Command. De eerste maand was daarop geen uitzondering.

In het kader van het Belgisch voorzitterschap van de Raad van de Europese Unie heeft er voor het eerst een gezamenlijke bijeenkomst plaatsgevonden van de cybercommandanten en -ambassadeurs van de lidstaten, in het zogenaamde "Egmont-formaat", met daarbovenop een nooit eerder geziene gemeenschappelijke verklaring die het belang van een cyberdefensiebeleid aantoont. Er staat enorm veel op het spel op het gebied van veiligheid in cyberspace en in de drie lagen ervan: fysiek, logisch en virtueel. Het versterken van cybersamenwerking op strategisch, operationeel en tactisch niveau is daarom essentieel. Eén van de concrete toepassingen van het Europese cyberdefensiebeleid was onze deelname aan de inzet van de Cyber Rapid Response Teams (CRRT) in Moldavië, waar deze multidisciplinaire teams uit verschillende Europese landen voluit hun rol hebben vervuld bij het veiligstellen van de Moldavische presidentsverkiezingen. Dit jaar zijn we trouwens voorzitter van het planningsmechanisme voor de implementatie van deze nieuwe Europese capaciteit.

Natuurlijk was het in België ook een verkiezingsjaar voor alle bestuursniveaus. We hebben meegewerkt aan de bescherming van de verkiezingen in juni en oktober met onze technische capaciteiten op het gebied van cyberverdediging en het opsporen van desinformatie afkomstig uit het buitenland. In de loop der jaren hebben we een toename gezien van dergelijke campagnes voor informatiemanipulatie en inmenging die steeds virulenter en geraffineerder worden. Ook al is ons land nog niet het slachtoffer geweest van massale desinformatiecampagnes zoals die tegen Frankrijk, Duitsland, de Baltische staten en bepaalde Centraal-Europese landen, het blijft een doelwit bij uitstek vanwege zijn geografische ligging in het hart van Europa en het aantal internationale instellingen die het huisvest.

In oktober was er ook een reeks cyberaanvallen gericht op een aantal websites van federale, gewestelijke en lokale overheden. Ten prooi aan zogenaamde "denial of service"-cyberaanvallen werden ze gedurende meerdere dagen door groepen hacktivisten met zo veel verzoeken overspoeld, dat ze sporadisch ontoegankelijk werden. De basisbeschermingsmaatregelen werkten over het algemeen goed en de gevolgen bleven beperkt. De modus operandi van deze groepen hacktivisten is om hun acties op zo'n manier bekend te maken dat andere actoren of individuen worden aangemoedigd om zich bij hen aan te sluiten, waardoor het verwoestende effect van het angstklimaat dat ze willen creëren, wordt vergroot. We moeten opmerken dat hoe minder ruchtbaarheid hun acties krijgen, hoe meer het gewenste effect vervaagt.

Gezien de geopolitieke situatie moeten we ook bijdragen aan de ontwikkeling van de verschillende plannen op het vlak van militaire defensie, nationale defensie, militaire mobiliteit ('enablement') en weerbaarheid waar de NAVO om vraagt. In deze context moeten we ook het hoofd bieden aan de hybride dreigingen die gegenereerd worden in cyberspace (elektromagnetische oorlogsvoering, cyberaanvallen, sabotage en desinformatie) tegen onze kritieke infrastructuren. Daarom hebben we het initiatief genomen om - voor het eerst in België - een Table Top Exercise (TTX) te organiseren met een aantal infrastructuurorganisaties die van cruciaal belang zijn voor militaire operaties en met deelname van het BOC en het NCCN als waarnemers.

Om al deze dreigingen aan te pakken, blijven we de Cyber Force binnen Defensie ontwikkelen, terwijl we de opdrachten van de ADIV in cyberspace versterken. De middelen die door de Strategische Visie en het STAR-plan in het leven zijn geroepen, worden geleidelijk aan geïmplementeerd. De ontwikkeling van de vaardigheden van ons menselijk kapitaal via innovatieve initiatieven, zoals de Cyber Defence Factory®, en via onze verschillende partnerschappen op internationaal en nationaal niveau, zoals met het Europees Ruimteagentschap (ESA), de Federale Gerechtelijke Politie, Agoria via het initiatief Cyber Made In Belgium en onze structurele partner in toegepast onderzoek, de Koninklijke Militaire School, werd voortgezet en verder verdiept. In iets meer dan twee jaar tijd, sinds de oprichting van het Cyber Command, hebben we ons menselijk kapitaal met 65% verhoogd, en we moeten dit opnieuw verdubbelen voor het einde van deze nieuwe legislatuur.

Ik blijf ervan overtuigd dat investeringen in ons menselijk kapitaal, innovatie en partnerschappen het juiste antwoord zijn op al deze dreigingen. Daarom zullen we ons, trouw aan ons motto Cyber Force Through Partnerships, blijven ontwikkelen ten dienste van de opdrachten van de ADIV, Defensie en het land.

GENERAAL-MAJOOR

Ondertekening van het aanvraagformulier voor een van onze partners (Eric Van Cangh van Agoria) om kandidaat-reservist te worden bij het Cyber Command

Een oorlogseconomie: **Voor hoelang?**

Na bijna drie jaar oorlog lijken de Russische objectieven met betrekking tot Oekraïne nauwelijks tot niet gewijzigd.

Hoewel Rusland regelmatig beweert dat het openstaat voor een staakt-het-vuren of vredesonderhandelingen, blijft het lange-termijndoel voor het Kremlin een volledige onderwerping van Oekraïne. Om dit te verwezenlijken is Rusland eind 2022 overgeschakeld naar een oorlogseconomie, waarbij de Russische staat enorme bedragen injecteert om onder meer wapens, brandstof, voedsel en kledij te vervaardigen.

De transitie naar een oorlogseconomie zorgde op korte termijn voor economische groei en een stijging van de lonen. Maar hoe langer deze situatie duurt, hoe groter de structurele schade voor de Russische economie zal zijn. Het is echter duidelijk dat voor het Kremlin de economie ondergeschikt is aan de geopolitieke ambities. Het Kremlin is er bovendien van overtuigd dat Oekraïne onvermijdelijk het onderspit zal delven in de huidige attritieoorlog als de Westerse economische en militaire steun afbrokkelt.

Hoewel er geen beslissende doorbraken waren langs het front, blijven zowel Rusland als Oekraïne bij hun standpunt dat een militaire overwinning nog steeds mogelijk is. Rusland doet dit door een gestaag offensief, verspreid over het hele front met een focus op de Donbas (Donetsk en Loehansk Oblasts). Ondanks de duidelijke vooruitgang in de richting van West-Oekraïne moet Rusland, net als bij Bakhmut en Avdiivka in 2022 en 2023, temporiseren door de gekende beperkingen zoals een gebrek aan zwaar militair materieel, personeel en munitie.

Defensieve aanpak

Oekraïne was na het minder succesvolle offensief in 2023 overgeschakeld naar een meer defensieve aanpak. Dit werd door zowel President Zelensky en Generaal Syrsky duidelijk gekaderd binnen een groter plan dat niet zou leiden tot een definitieve stagnatie van de gevechten. Hoewel die stagnatie, tot op vandaag, wel het geval is in het Zuiden van Oekraïne, slaagden de Oekraïnse strijdkrachten erin de zwakke Russische verdedigingslijnen langs de grens met de Kursk Oblast (Rusland) te doorbreken en hiermee de zwaktes van Rusland en zijn strijdkrachten bloot te leggen.

Deze operatie kaderde ook binnen de algemene strijd voor een Oostenlijke bufferzone tussen Oekraïne en Rusland en een poging om de Russische opmars in de Donbas te vertragen en eventueel te stoppen. Tijdens deze verschillende operaties blijft het gebrek aan Oekraïense strijdkrachten voor het grootste onevenwicht zorgen tussen de beide partijen. De nodige constante aanpassingen aan het mobiliseringsbeleid zorgen voor extra druk op het steeds meer gecontesteerde beleid van President Zelensky, op het evenwicht tussen militaire capaciteit en economische stabiliteit en als laatste, maar misschien wel meest doorslaggevende, op de eenheid van het Oekraïnse volk.

Luchtcampagnes

Naast de aanhoudende gevechten aan het front, richten beide partijen zich steeds meer op hun luchtcampagnes in een poging de tegenstander zo veel mogelijk te destabiliseren. Rusland richt zich voornamelijk op de Oekraïense energie-infrastructuur en op alles wat verband houdt met het Oekraïense defensieapparaat (onder andere de Westerse militaire steun) om de druk op de Oekraïense luchtafweersystemen te verhogen. Oekraïne blijft ondertussen Russisch grondgebied aanvallen en richt zich voornamelijk op militaire doelwitten (o.a. vliegvelden, munitiedepots en logistieke knooppunten) om maximaal druk uit te oefenen op de Russische operationele planning.

Hoewel Oekraïne kwantitatief in het nadeel is op het gebied van militair materieel ten opzichte van Rusland, woedt er een militair-industriële strijd tussen beide partijen op het vlak van de ontwikkeling en productie van wapensystemen die steeds innovatiever en ontwrichtender worden, zoals blijkt uit de verschillende drone-aanvallen in 2024.

Hoelang zal deze oorlogseconomie standhouden? De uitkomst van deze oorlog zal niet alleen afhangen van militaire overwinningen, maar ook van de veerkracht van Oekraïne en de internationale gemeenschap.

Elektromagnetische oorlogsvoering ten top gevoerd

Het Oekraïense conflict wordt gekenmerkt door de bijzonder doeltreffende en disruptieve inzet van ongebruikelijke, innovatieve en/of geïmproviseerde middelen.

Op alle terreinen heerst tussen de partijen een over het algemeen onbekende gevechtsvorm gebaseerd op het intensieve gebruik van het elektromagnetische spectrum: elektromagnetische oorlogsvoering (Electromagnetic Warfare).

Enerzijds wordt storing van telecommunicatie en elektromagnetische navigatiesystemen, waaronder satellietsystemen, veroorzaakt. Radarmiddelen worden gebruikt voor verdediging en aanval en communicatiemiddelen (waaronder mobiele telefoons) worden aangewend om de vijand te lokaliseren en aan te vallen. Het directe gevolg van deze radio-oorlog is een terugkeer naar basismiddelen, die sinds de Koude Oorlog vrijwel niet meer zijn gebruikt. Operaties worden uitgevoerd met behulp van kaarten, kompassen en bekabelde communicatiemiddelen die niet afhankelijk zijn van stroomvoorzieningen.

Aan de andere kant wordt er door de verschillende partijen intensief gebruikgemaakt van UAV's (Unmanned Aerial Vehicles). De trend naar middelgrote en grootschalige militaire systemen is voorbij. Die trend heeft plaatsgemaakt voor het gebruik van micro- en minidrones, commercieel of op maat gemaakt met onderdelen afkomstig van leveranciers overal ter wereld. Ze zijn op geïmproviseerde wijze uitgerust met een grote verscheidenheid aan nuttige ladingen zoals detectoren, stoorzenders, explosieven enz. Hun opdrachttype bestrijkt een breed spectrum van gevechten die te land, ter zee en in de lucht worden gevoerd. Deze UAV's zijn ontworpen om de telecommunicatie te onderscheppen en te bespioneren, om de vijand elektromagnetisch of visueel te lokaliseren en te identificeren en om doelen direct of indirect aan te vallen en fysiek te vernietigen.

Nieuwe uitdagingen voor analisten van satellietbeelden

In moderne oorlogsvoering is het nu een illusie om te denken dat een manoeuvre op de grond kan ontsnappen aan satelliettoezicht. Dit is een groot voordeel in termen van wereldwijde dekking en toegang tot informatie, maar ook een ontwikkeling die nieuwe uitdagingen met zich meebrengt.

Minder beperkende wetgeving, lagere lanceringskosten en de opkomst van technologieën zoals miniaturisatie en 3D-printen hebben de toegang tot de ruimte gedemocratiseerd voor zowel statelijke als niet-statelijke actoren. Dit leidt tot een exponentiële toename van het aantal observatiesatellieten met lage omloopbaan, waardoor over een paar jaar een quasi permanente dekking mogelijk wordt.

Gewapende conflicten

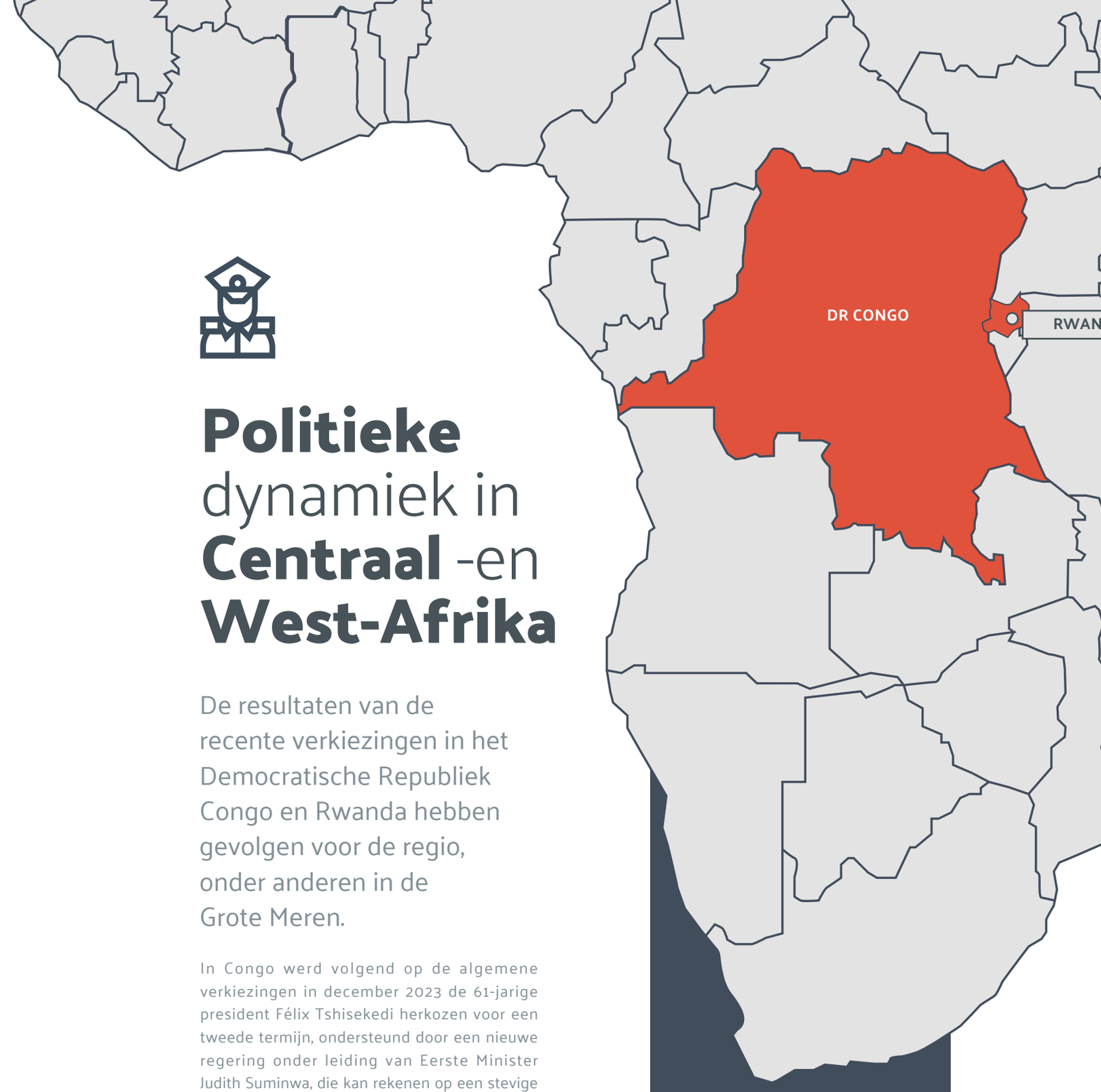
In de context van gewapende conflicten brengt de toenemende beschikbaarheid van satellietbeelden voor strategisch, operationeel en tactisch gebruik nieuwe uitdagingen met zich mee voor inlichtingen- en defensiediensten in de toekomst.

Het Russisch-Oekraïense conflict laat bijvoorbeeld zien dat de tegenover elkaar staande partijen kunnen profiteren van een nieuwe massa informatie en dat ontwijkende technieken, zoals optische lokmiddelen en digitale camouflage, steeds vaker worden gebruikt om te ontsnappen aan dit alomtegenwoordige toezicht.

De ruimte, een operationeel gebied

De ruimte is al lang een volwaardig operationeel gebied geworden en de hoeveelheid te analyseren beelden neemt voortdurend toe. Sinds het einde van de jaren 1990 heeft de ADIV zijn satellietbeeldvormingscapaciteiten ontwikkeld omdat sensoren essentieel zijn voor het bereiken van het informatieoverwicht. Gezien deze ontwikkelingen is het in de toekomst echter belangrijk om onze menselijke analysecapaciteiten, die op termijn zullen worden ondersteund door artificiële intelligentie, te versterken en om de synergieën met onze partners verder uit te bouwen.

Een betere wereldwijde dekking is een onbetwistbare troef, en de "Alliance Persistent Surveillance from Space" (APSS), ondertekend door 16 NAVO-landen waaronder België in 2023, illustreert dit collectieve bewustzijn. Het integreren van de overheids- en commerciële sensoren in een virtuele constellatie voor doeltreffende, gecoördineerde surveillance is onder andere noodzakelijk om onze inlichtingenoperaties te blijven uitvoeren.



Politieke dynamiek in **Centraal** -en **West-Afrika**

De resultaten van de recente verkiezingen in het Democratische Republiek Congo en Rwanda hebben gevolgen voor de regio, onder anderen in de Grote Meren.

In Congo werd volgend op de algemene verkiezingen in december 2023 de 61-jarige president Félix Tshisekedi herkozen voor een tweede termijn, ondersteund door een nieuwe regering onder leiding van Eerste Minister Judith Suminwa, die kan rekenen op een stevige parlementaire meerderheid. Als leider van de partij « Union pour la Démocratie et le Progrès Social » beloofde de president vijf jaar geleden om de corruptie uit te roeien, de economie op te bouwen, de ongelijkheid aan te pakken en de conflicten in het oosten op te lossen.

Rwanda kende eveneens een continuïteit in leiderschap volgend op de algemene verkiezingen van in juli 2024: president Paul Kagame van de partij FPR (Front Patriotique Rwandais) verzekerde zich van een nieuw mandaat.

Nieuwe mandaten voor Félix Tshisekedi in Congo en Paul Kagame in Rwanda

Kwetsbare stabiliteit in de Grote Meren

De relaties tussen Burundi en Rwanda kenden een dieptepunt door de ontplooiing van het Burundese leger in de Democratische Republiek Congo, evenals door een troepenopbouw aan en de sluiting van de gemeenschappelijke grenzen. Dat laatste gebeurde zonder veiligheids-incidenten.

De Regio van de Grote Meren wordt gekenmerkt door voortdurende instabiliteit, voornamelijk in het oosten van de Democratische Republiek Congo. In de provincie Noord-Kivu staan twee zaken tegenover elkaar: enerzijds de Congolese strijdkrachten, gewapende milities, particuliere militaire bedrijven en regionale en internationale partners. Anderzijds bevinden zich de M23-rebellen en het Rwandese leger. Ondanks bemiddelingspogingen op regionaal (Luanda, Angola) en internationaal niveau, die verdere escalatie voorlopig hebben weten te voorkomen, blijft de situatie ter plaatse uiterst kwetsbaar. Dit geldt niet alleen voor de veiligheid in de regio, maar ook voor de politieke dialoog, waaronder de pogingen tot toenadering tussen de twee presidenten van de Democratische Republiek Congo en Rwanda.

Nieuwe allianties en toenemende onveiligheid in de Sahel

In de Sahel-regio verdiepten de militaire junta's van Mali, Burkina Faso en Niger hun onderlinge relaties in een confederatie, in casu de Alliantie van Sahel Staten (AES). Hiermee namen ze aldus formeel afstand van de Economische Unie van West-Afrikaanse Staten (ECOWAS).

Terwijl de banden met Westerse landen steeds meer doorgeknipt werden en verzwakten, gingen zij nauwe banden aan met Rusland. In het kader van de grote, mondiale machtsstrijd engageerde die laatste zich ook op militair vlak in West-Afrika.

Ondanks deze nieuwe allianties blijft de veiligheid in de Sahel-regio verslechteren, waarbij terroristische activiteiten zich steeds verder uitbreiden naar het noorden van buurlanden zoals Benin, Togo, Nigeria, Ivoorkust en Ghana. In de juntageleide AES-staten blijft het risico op nieuwe staatsgrepen bovendien aanzienlijk.

Het Nabije en Midden-Oosten blijven opflakkeren

7 oktober 2023

Meer dan een jaar na de Hamas-aanval tegen Israël op 07 oktober 2023 blijft de oorlog in het Midden-Oosten aan intensiteit en vooral omvang winnen.

Na een voortdurende escalatie tussen Israël en Hezbollah, waarbij de rode lijnen aan beide kanten herhaaldelijk werden verlegd, lanceerde Tel Aviv vanaf september 2024 een reeks luchtaanvallen op Libanon. Israëlische troepen begonnen begin oktober met invallen in het zuiden van het land, waarmee de Israëlische grondoperaties in het land van de ceders van start gingen.

Deze aanvallen veroorzaakten niet alleen de uittocht van veel inwoners van Zuid-Libanon maar zorgden er ook voor dat veel Belgen die in Libanon woonden het land verlieten. Dankzij de met zowel menselijke als technische middelen verzamelde informatie hebben we een nauwkeurige en permanente inschatting van de veiligheid kunnen maken, in het bijzonder voor de bemanning die verantwoordelijk was voor de begeleide repatriëring van de Belgen.

As van de weerstand

Het aanhoudende conflict in het Midden-Oosten beperkt zich niet tot Gaza en Libanon. Het wordt met name gekenmerkt door de Israëlisch-Iraanse krachtmeting die heeft geleid tot de mobilisatie van een reeks spelers gegroepeerd onder de naam "As van de weerstand". Deze anti-Amerikaanse en anti-Israëlische alliantie bestaande uit Iran, Syrië, Hezbollah, de Houthi's, Hamas en Iraaks-Syrische sjiitische milities is alomtegenwoordig in het regionale veiligheidsvraagstuk.

De Houthi's onderscheidden zich al snel door het wereldwijde maritieme verkeer te bedreigen met hun operaties in de Rode Zee tegen Israëlische doelen of doelen die als bondgenoten van Israël werden geïdentificeerd. Ze hebben de doorvaart door de Bab el Mandeb-straat en het Suezkanaal, die van vitaal belang zijn voor de internationale handel, verstoord. België nam deel aan operaties om de vrijheid van scheepvaart in de regio te garanderen. Het Louise-Marie-fregat (LoMa) voerde een 121-daagse opdracht uit in de Rode Zee in het kader van Operatie ASPIDES en in de Straat van Hormuz als onderdeel van Operatie AGENOR. De ADIV heeft deze inlichtingenopdracht vanaf de voorbereidende fase en gedurende de hele operatie ondersteund.

Syrië en Irak

Na het conflict tussen Israël en Hamas en daarna Hezbollah, bevindt Syrië, dat onderdak biedt aan een reeks pro-Iraanse milities, zich in het oog van de storm en is het steeds vaker het doelwit van Israëlische aanvallen. Daarnaast zijn sinds oktober 2023 talrijke aanvallen met drones, raketten en ballistische missiles van korte dracht gericht geweest op de Amerikaanse basissen in Irak en Syrië. Als onderdeel van Operatie Inherent Resolve (OIR) voeren ze strijd tegen Islamitische Staat.

In Syrië profiteert Islamitische Staat van de destabilisering van de veiligheid door het aanhoudende conflict in Gaza en Zuid-Libanon. Hoewel de terroristische organisatie franchises heeft ontwikkeld op verschillende continenten - in het bijzonder Islamitische Staat Khorasan, die actief is in Afghanistan maar ook internationaal georiënteerd is - ligt het hart van Islamitische Staat nog steeds in Syrië en Irak. Enkele duizenden strijders zijn daar nog actief, terwijl enkele duizenden anderen gevangenzitten, vaak in handen van de Syrische Democratische Strijdkrachten.

Louise-Marie (LoMa) in de Rode Zee **121 dagen**

Rol van België en de ADIV

België heeft in het verleden al vrouwen en kinderen gerepatrieerd in het kader van operaties die zorgvuldig werden voorbereid met de ADIV, maar anderen worden nog steeds vastgehouden in Syrische kampen en gevangenissen. Er bestaat een reëel risico dat gevangenissen en kampen opnieuw het doelwit worden van leden van Islamitische Staat die strijders en sympathisanten willen bevrijden. Hoewel België niet langer met F-16's of Special Forces deelneemt aan Operatie Inherent Resolve, heeft ons land nog wel verschillende verbindingsofficieren binnen de operatie. De gegevens die via onze verschillende bronnen vanop het terrein binnenkomen, worden door onze specialisten geanalyseerd om nauwkeurige, prospectieve informatie te leveren. Deze inlichtingen worden gebruikt om onze politieke besluitvormers zo goed mogelijk te informeren over de ontwikkelingen op het terrein en de gevolgen daarvan voor de regionale en internationale veiligheid.

Veiligheidsmachtigingen en -verificaties: een alsmaar grotere werklast

Militaire veiligheid is niet alleen een kwestie van defensie-infrastructuur, maar ook van personeel en belangen van het land. Veiligheidsverificaties en veiligheidsmachtigingen worden verricht voor Defensie en de defensie-industrie, in samenwerking met verschillende partners zoals de Staatsveiligheid of de Federale Politie.

Sollicitanten, zowel burgers als militairen, degenen dus die nog niet bij Defensie werken, ondergaan een **veiligheidsverificatie** vooraleer ze eventueel hun machtiging bekomen als ze toegang nodig hebben tot geclassificeerde informatie.

Verificatie is ook noodzakelijk voor personen of bedrijven van buiten Defensie die regelmatig toegang moeten hebben tot kwartieren of installaties van Defensie. Voorbeelden hiervan zijn schoonmaakbedrijven en verschillende consultants die onder contract staan bij Defensie.

De verificatie houdt in dat de verschillende databanken van veiligheidspartners (lokale en federale politie, FOD Justitie, enz.) met elkaar worden vergeleken om na te gaan of de persoon, op positieve of negatieve wijze, bekend is bij hun diensten.

De ADIV behandelt ook verzoeken om veiligheids-verificaties van andere partners. Deze verzoeken hebben bijvoorbeeld betrekking op personeel van de luchthaven van Zaventem of regionale lucht-havens, van de haven van Antwerpen of van het FANC (Federaal Agentschap voor Nucleaire Controle).

300.000

veiligheidsverificaties worden er jaarlijks gemiddeld uitgevoerd

70%

stijging van het aantal aanvragen de afgelopen twee jaar

Een veiligheidsmachtiging is essentieel voor al het militaire en burgerpersoneel van Defensie dat tot geclassificeerde informatie toegang heeft. Ze bevestigt dat voor de nieuwe medewerker de nodige garanties van loyaliteit, discretie en integriteit vervuld worden. Met deze machtiging is er ook toegang tot een geclassificeerde zone of geclassificeerd computernetwerk.

Deze machtigingen zijn ook nodig voor privébedrijven (rechtspersonen) die een contract hebben met Defensie en die deze bevoorrechte toegang nodig hebben. Dit is bijvoorbeeld het geval voor de bedrijven die in de verschillende wapensystemen zoals CaMo (Gemotoriseerde capaciteit) van de Landcomponent, van de nieuwe fregatten van de Marine of van de jachtbommenwerper F-35 van de Lucht- en Ruimtecomponent werkzaam zijn.

Ze is **maximum 5 jaar** geldig en is gebaseerd op de resultaten van een veiligheidsonderzoek, waarvan de omvang en termijn onder andere van het gevraagde veiligheidsniveau (vertrouwelijk, geheim of zeer geheim), op basis van de “behoefte om te kennen”, afhangen. Met andere woorden, personen mogen alleen toegang krijgen tot informatie die strikt noodzakelijk is voor de uitvoering van hun taken.

De persoon die de aanvraag voor machtiging indient, moet ermee instemmen dat het veiligheidsonderzoek uitgevoerd wordt. Dit onderzoek heeft niet alleen betrekking op de aanvrager, maar ook op zijn of haar omgeving in de breedste zin van het woord (echtgeno(o)t(e), volwassen kinderen of huisgenoten).

De ADIV verstrekt ook veiligheidsmachtigingen voor andere bedrijven, zoals bedrijven die actief zijn in de lucht- en ruimtevaart (bv. SABCA of ASCO), die niet noodzakelijk een rechtstreekse band met Defensie hebben.

Veiligheidsonderzoeken nemen tijd in beslag om ze op een ernstige manier te kunnen voltooien. Dit kan worden verklaard door de persoonlijke omstandigheden van aanvragers: het aantal personen die samen een woning delen, een nieuwe partner, opeenvolgende verhuizingen zijn allemaal voorbeelden die de duur van onderzoek kunnen verlengen. Soms is er informatie nodig uit het buitenland of van buitenlandse diensten (grensarbeiders in het buitenland, internationale functies of opdrachten), wat ook enige tijd in beslag neemt.

15.000

veiligheidsonderzoeken per jaar gemiddeld, waarvan 9000 uitsluitend betrekking hebben op de industrie.

Meer dan
20.000

mensen van het departement, zowel burgers als militairen, zijn gemachtigd.

15.000

veiligheidsonderzoeken uitgevoerd in 2024, wat neerkomt op een toename van 33%. Dit komt door het aantal lopende projecten, met name de nieuwe wapensystemen van Defensie.

De **ADIV** als onmisbare schakel in de toekomst van de **Lucht -en Ruimtecomponent**

Het Belgische F-35 programma werd in 2024 mede door de ADIV sterk voorbereid. Om een efficiënte en gecentraliseerde aanpak te verzekeren, heeft de Directie Veiligheid het Special Access Program Central Office (SAPCO) opgericht. Deze cel is eindverantwoordelijke voor alle veiligheidsaspecten van het Belgische F-35 programma, waaronder militaire veiligheid, cyberveiligheid en counter-intelligence. In de toekomst zal deze afdeling ook de veiligheid van andere geavanceerde wapensystemen binnen Defensie opvolgen.

De topsnelheid bedraagt ongeveer

1900 km/h

Vooruitgang van het F-35 programma in 2024

Een belangrijke verwezenlijking was de opstelling en uitvoering van het « Construction Security Plan » voor de zwaarbeveiligde operationele gebouwen van het nieuwe F-35 complex op de vliegbasissen van Florennes en Kleine Brogel. Dankzij dit plan kan de veiligheid van de bouwwerkzaamheden worden gegarandeerd.

Ter voorbereiding op de ontvangst van het eerste F-35 vliegtuig in het najaar van 2025 werd de uitbouw en versterking van specifiek F-35 veiligheidspersoneel in Florennes zorgvuldig aangestuurd en begeleid door het SAPCO. Dit gebeurde in nauwe samenwerking met de betrokken diensten van de Luchtcomponent, en omvatte de wervings- en opleidingsprocessen voor gespecialiseerde veiligheidsteams. Deze teams van algemene veiligheidsexperts en cybersecurityspecialisten zullen verantwoordelijk zijn voor de bescherming van zowel de infrastructuur als de operaties rondom het F-35 toestel. Een specifiek opleidingsplan werd opgesteld en geïmplementeerd ter voorbereiding op de ontvangst en operationele inzet van de eerste vliegtuigen.

Eind 2024 werd de « Building Occupancy Date » voor het operationele gebouw van het F-35 complex te Florennes behaald. Deze belangrijke mijlpaal markeerde niet alleen de oplevering van het gebouw, maar ook de volledige operationele werking van alle veiligheidssystemen. Het vormt bovendien de basis voor een vlotte installatie van alle netwerken, informatiesystemen en flight simulators later dit jaar. Het SAPCO speelde hierin een cruciale rol door de coördinatie tussen de verschillende betrokken diensten binnen Defensie en private partners te waarborgen.

Een belangrijke stap in de infrastructuur

Daarnaast werd ook een « Design Review Process » voor de toekomstige ontplooibare infrastructuur voor F-35 operaties in het buitenland succesvol afgerond. Dit proces waarborgt de naleving van diverse veiligheidsvereisten voorafgaand aan de bouw. De Amerikaanse veiligheidsautoriteit heeft inmiddels toestemming verleend om over te gaan naar de uitvoeringsfase, waarmee een belangrijke stap vooruit is gezet in de realisatie van deze infrastructuur.

Strikte controle door de Verenigde Staten

Het Belgische F-35 programma wordt als een Special Access Program (SAP) nauwgezet gecontroleerd door de Verenigde Staten. Die toezichtmaatregelen zijn noodzakelijk om de hoogtechnologische eigenschappen van dit wapensysteem te waarborgen en te beschermen. De toegang tot informatie, faciliteiten en operationele procedures wordt strikt gereguleerd, zodat de integriteit en veiligheid van het programma gegarandeerd blijven.

In het najaar van 2024 voerde de Amerikaanse veiligheidsautoriteit bovendien een succesvolle inspectie uit van de F-35 faciliteit in het hoofdkwartier te Evere.

Het succes van het programma

Het SAPCO speelde doorheen het ganse jaar 2024 steeds een actieve rol in diverse werkgroepen en symposia, waarbij veiligheid altijd een centrale rol speelt. Deelname aan deze evenementen is essentieel voor het succes van het programma. Ze bieden de mogelijkheid om samen te werken met Europese en Amerikaanse partners, ervaringen uit te wisselen en expertise op te bouwen. Op die manier draagt de ADIV, en bij uitbreiding Defensie, bij aan de verdere ontwikkeling van het internationale F-35 programma en versterkt het de interoperabiliteit tussen alle F-35 partnerlanden.

Deze prestaties onderstrepen het onverminderde engagement van de ADIV om de hoogste veiligheidsnormen te hanteren binnen het F-35 programma en om de inzetbaarheid en bescherming van dit strategische wapensysteem maximaal te waarborgen.

Het beschermen van geclassificeerde systemen tegen TEMPEST-aanvallen

Elk CIWS (communicatie-, informatie- en wapensysteem) zendt een zekere mate van ongewenste straling uit. Deze straling kan informatie onthullen over de gegevens die het CIWS op dat moment verwerkt. Indien deze informatie geclassificeerd is en de straling onderschept en geanalyseerd wordt, kan dit leiden tot een ernstige inbreuk op de beveiliging. Met gebruik van antennes, hardware en software is het mogelijk om beelden en documenten op de schermen van het CIWS te reconstrueren zonder een rechtstreekse fysieke verbinding. TEMPEST richt zich op deze kwetsbaarheden en biedt tegenmaatregelen. Dagelijkse kost voor het Cyber Command van de ADIV.

De aard van TEMPEST-aanvallen

TEMPEST-aanvallen worden beschouwd als de “ideale” cyberaanval omdat ze geen fysieke toegang vereisen tot de geclassificeerde gegevens of het CIWS zelf. De gevoelige informatie wordt onbedoeld uitgezonden en het vastleggen ervan laat geen sporen na. TEMPEST-beveiligingsmaatregelen bestaan uit het evalueren van de mate waarin deze straling wordt verzwakt, ofwel door de structuur van het gebouw (zonering) of door de eigenschappen van het CIWS zelf (profilering).

TEMPEST-zonering: afscherming via het gebouwontwerp

TEMPEST-zonering meet hoe doeltreffend een gebouw deze straling kan blokkeren of verminderen. Factoren zoals de materialen die gebruikt werden bij de constructie, de aanwezigheid van ramen en de dikte van muren dragen allemaal bij tot deze verzwakking. Het doel is om een “inspecteerbare ruimte” te bepalen, een driedimensionale zone die een CIWS omsluit en binnen dewelke een poging tot TEMPEST-aanval onwaarschijnlijk is omdat deze gemakkelijk kan ontdekt of voorkomen worden door lokale veiligheidsmaatregelen. In de praktijk omvat zonering het plaatsen van een zender in de ruimte met het CIWS en een ontvanger op een strategisch punt waar straling opgevangen kan worden. De opgevangen gegevens worden dan geanalyseerd om te bepalen hoe goed het gebouw straling afschermt. Periodieke beoordelingen van de zonering zijn vereist wanneer een geclassificeerd CIWS pas geïnstalleerd is of wanneer de buitenkant van het gebouw verandert.

Uitdagingen bij de beoordeling van zonering

Een van de belangrijkste uitdagingen van TEMPEST-zonering is het bepalen van de gunstigste locatie voor een potentiële onderschepper. Weersomstandigheden kunnen deze metingen ook beïnvloeden, want regen of andere omgevingsfactoren kunnen de sterkte van het signaal tijdelijk veranderen. De beoordeling van zonering is van cruciaal belang op elke locatie waar geclassificeerde informatie gevaar kan lopen, waaronder militaire bases, internationale instellingen zoals de NAVO en de EU, en privébedrijven die nauw samenwerken met de defensiesector.

TEMPEST-profilering: de beoordeling van bescherming op systeemniveau

TEMPEST-profilering volgt een andere benadering door het ingebouwde vermogen van het CIWS om straling te beperken, te meten. Hiervoor wordt het systeem in een echovrije kamer geplaatst, een gecontroleerde omgeving die alle externe straling blokkeert, zodat alleen de emissies van het CIWS kunnen worden gemeten. De opgevangen gegevens worden dan geanalyseerd om het TEMPEST-niveau van het CIWS te bepalen, dat aangeeft hoe doeltreffend het zichzelf kan afschermen tegen het lekken van gevoelige informatie.

De combinatie van TEMPEST-zonering en -profilering is essentieel om het risico op een TEMPEST-aanval tot een minimum te beperken. Bijvoorbeeld, een CIWS met een lage interne bescherming tegen straling (slecht TEMPEST-niveau) moet in een sterk afgeschermd gebouw geplaatst worden (goede TEMPEST-zone). Omgekeerd is het geoorloofd om een systeem met een hoog TEMPEST-niveau op een locatie met een lagere afscherming te plaatsen omdat het eigen ontwerp stralingslekkage beperkt.

Het groeiende belang van TEMPEST-beveiliging

Verwacht wordt dat het belang van TEMPEST in de nabije toekomst aanzienlijk zal toenemen. Bijna elk militair systeem - van tanks en schepen tot luchtvaartuigen en wapensystemen - is afhankelijk van geavanceerde processors. Aangezien deze systemen steeds meer draadloze technologieën gebruiken, wordt het risico op TEMPEST-aanvallen nog groter. De snelle vooruitgang in elektronica, met steeds kleinere onderdelen en grotere verwerkingscapaciteit, vormt nog een extra uitdaging.

TEMPEST is niet alleen een zorg voor systeemontwerpers, maar ook voor eindgebruikers. Ontwerpers moeten vanaf het begin rekening houden met TEMPEST, terwijl gebruikers waakzaam moeten blijven en de beveiligingsprotocollen strikt moeten opvolgen om ervoor te zorgen dat gevoelige informatie beschermd blijft tegen afluisteren.

De **ADIV** en de **bescherming** van de **Belgische industrieën**

België, als strategische natie in het hart van Europa, heeft een gediversifieerde industriële sector die cruciaal is voor zijn economie en veiligheid. De bescherming van deze industrieën tegen de toenemende bedreigingen, zowel cyber-, economische als fysieke, is een nationale prioriteit geworden. Het Bureau voor de Industrie speelt een centrale rol in de bescherming van deze gevoelige sector en werkt nauw samen met de Nationale Veiligheidsoverheid (NVO) en andere nationale en internationale organisaties.

Het Bureau voor de Industrie is een sleutelentiteit in het economische en industriële beveiligingssysteem van België. Zijn belangrijkste missies zijn:

1 **Toezicht houden op de veiligheid van defensiegerelateerde bedrijven.**

Het bureau houdt toezicht op de veiligheids-machtigingen van een duizendtal bedrijven. Dat doet het niet alleen door controles uit te voeren maar ook door hen te adviseren over beschermingsmaatregelen, veiligheidsnormen en regelgeving.

2 **Sensibiliseren en informeren:**

De afdeling Industrie heeft een echte beheersing en expertise op het gebied van industriële veiligheid. Daarom informeert ze bedrijven over goede veiligheidspraktijken. Dit omvat bewustmaking van cyberveiligheid, de bescherming van geclassificeerde informatie en de beveiliging van gevoelige infrastructuren.

3 **Samenwerken met de Nationale Veiligheidsoverheid (NVO):**

Sinds 1 januari 2024 is de NVO een besluitvormend orgaan onder leiding van de Veiligheid van de Staat. In dit kader werken de Dienst voor de Industrie en de NVO samen om de veiligheidsnormen te harmoniseren die gelden voor Belgische bedrijven die actief zijn in strategische sectoren. Dit omvat strenge regels voor de bescherming van gevoelige informatie en het beheer van veiligheidsincidenten.

4 **Waarborgen van de rol van militaire DSA (Designated Security Authority):**

In de internationale context zijn relaties met NVO en/of buitenlandse DSA's belangrijk om transportplannen te kunnen uitwisselen, RFV's (Request For Visit) uit te wisselen, PSI's (Program Security Instructions) en SAL's (Security Aspect Letter) op te stellen en samen te werken in internationale werkgroepen.

5 **Coördineren van veiligheidsverificaties:**

Als onderdeel van een contract met Belgische Defensie moet elke persoon veiligheidscontroles aanvragen. Dit garandeert de bescherming van het personeel op militaire bases, de controle van informatie en de preventie van TESSOC-dreigingen «Terrorism Espionage Subversion Sabotage Organised Crime Cyber ».

Dankzij de versterkte samenwerking met de Nationale Veiligheidsoverheid in 2024 verhogen de NVO en de Dienst Industrie samen het beveiligingsniveau van geclassificeerde informatie, kritieke infrastructuren en risicopreventie voor de Belgische industrieën. In de toekomst zal deze samenwerking des te noodzakelijker zijn om zich aan te passen aan de technologische en geopolitieke ontwikkelingen en om een hoog beschermingsniveau voor de Belgische industrieën te behouden.

181
TOEGEKENDE BEDRIJFSMACHTIGINGEN

6
AUDITCONTROLES VAN POSTEN VOOR DEFENSIEATTACHÉS

25
VERSTERKINGEN BIJ VIP-EVENEMENTEN, WAARONDER 12 IN HET KADER VAN HET BELGISCH VOORZITTERSCHAP VAN DE EU

481
MILITAIRE VEILIGHEIDSINCIDENTEN

2
AUDITS VAN EENHEDEN IN OPERATIE

10
INSTALLATIES VAN ALARMEN, WAARONDER 8 IN HET BUITENLAND

Technologie aan de frontlinie

De bescherming van ons economisch en wetenschappelijk potentieel

In de wereldwijde machtsstrijd speelt technologie een cruciale rol. Er is een hectische race gaande om innovaties en geavanceerde technologieën en de winnaars daarvan hebben niet alleen economische maar ook strategische en militaire voordelen. Sommige grootmachten en kwaadwillende actoren hanteren al enkele jaren een "oogst nu, ontcijfer later"-strategie. Die heeft als doel grote hoeveelheden van zeer gevoelige versleutelde gegevens op te slaan die voorlopig ontoegankelijk zijn. Wanneer de kwantumtechnologie het dan mogelijk maakt, is het de bedoeling ze te ontcijferen.

Nieuwe veiligheidssystemen

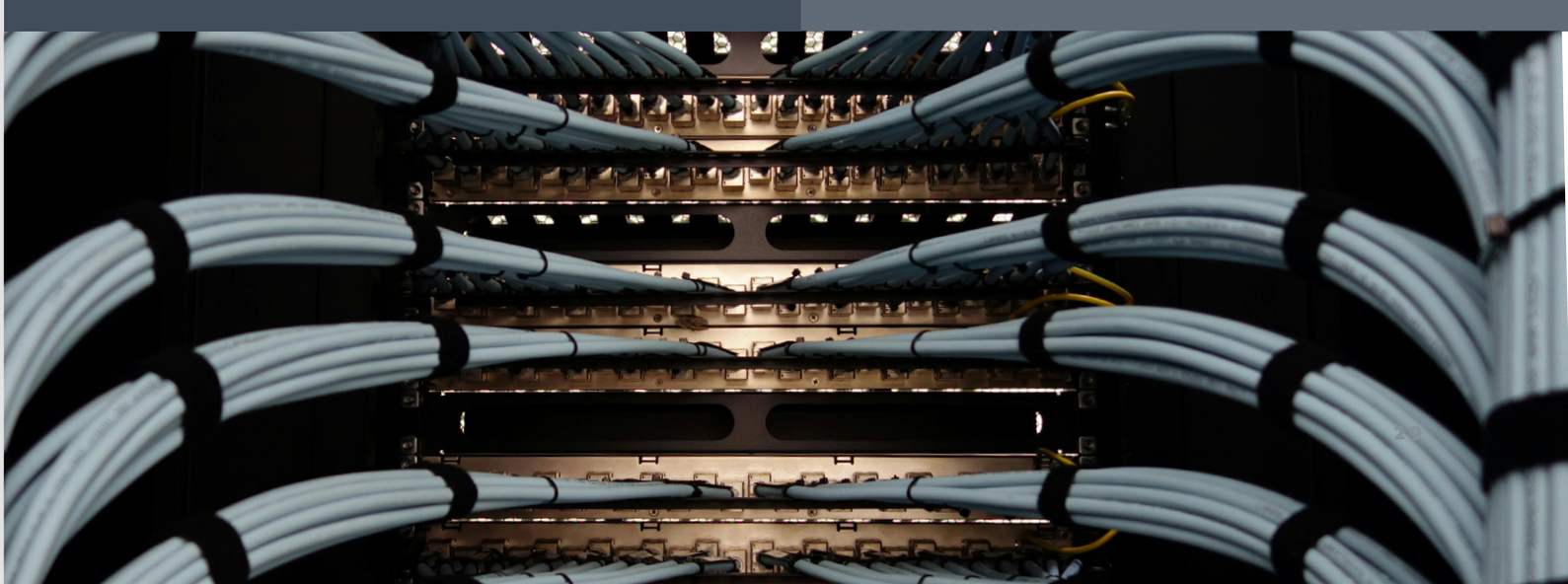
De grote westerse mogendheden worden zich geleidelijk aan bewust van het belang om hun economisch en wetenschappelijk potentieel te beschermen. Europa (in 2023) en de Verenigde Staten (in 2022) hebben regelgeving ingevoerd om de productie en innovatie op het gebied van halfgeleiders aan te moedigen, terwijl ze hun industrieën beschermen tegen de bedreiging van bepaalde vijandige staten. Europa heeft ook een systeem ingevoerd om Foreign Direct Investments (FDI) te filteren, die ook geïmplementeerd is in de Belgische wetgeving en waarvan we onlangs het eerste werkingsjaar hebben gevierd. De ADIV maakt integraal deel uit van dit filtersysteem en was de initiatiefnemer van enkele FDI-dossiers die onderworpen werden aan specifieke maatregelen (voorwaarden en garanties). In totaal werd deze screening uitgevoerd op een totaal investeringsbedrag van naar schatting 173.3 miljard euro, waarvan 2.06 miljard euro voor België.

Verder heeft ook de oorlog in Oekraïne aangetoond dat het belangrijk is om een technologisch voordeel te hebben op je tegenstander in een militair conflict. Oekraïne kan standhouden dankzij geavanceerde westerse apparatuur, ondanks zijn numerieke inferioriteit en geringe strategische diepte. Dit militaire voordeel werkt daarnaast ook afschrikkend omdat een vijandige staat tweemaal zal nadenken vooraleer hij een gewapend conflict zal beginnen indien hij denkt inferieur te zijn op het gebied van militaire technologie. Voorbeelden hiervan kunnen gezien worden in de hedendaagse spanningsgebieden zoals Taiwan.

Technologische ontwikkeling beschermd

Mede hierdoor zet België sterk in op technologische ontwikkeling via DEFRA-projecten (Defence-Related Research Action) en samenwerkingen tussen universiteiten en publieke en private sectoren. De ADIV is hierin voornamelijk betrokken bij de bescherming van deze defensie-industrieën en onderzoeksprojecten tegen spionage, inmenging en disruptie. De ADIV is er dan ook al in geslaagd om te voorkomen dat door vijandige naties gecontroleerde bedrijven deelnamen aan deze onderzoeksprojecten.

Het werk van de ADIV op dit niveau voorkomt niet alleen ongewenste technologieoverdracht, maar beschermt ook de reputatie van onze defensie-industrie en onderzoekscentra als betrouwbare partners die de veiligheid van hun onderzoek hoog in het vaandel hebben staan.



Information warfare: **een schot in de roos**

2024 was voor het departement Information Warfare van het Cyber Command het smeltpunt van verschillende eerder geïnitieerde werktrajecten, onder meer door de leidende rol in een Federale Interdepartementale Werkgroep die de opvolging verzekert van Foreign Information Manipulation and Interference (FIMI [1]).

De opvolging van mogelijke buitenlandse informatiemanipulatie en inmenging vond niet alleen plaats tijdens de verschillende verkiezingsmomenten, maar evenzeer vormde het Belgische EU Voorzitterschap een extra uitdaging.

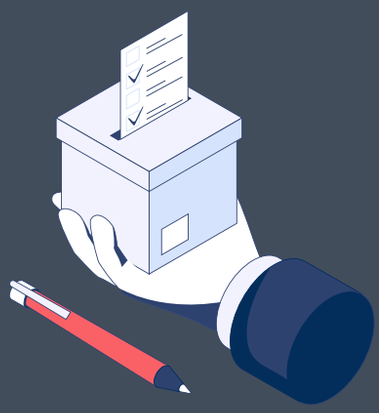
In aanloop naar beide gebeurtenissen, werden door de werkgroep procedures en bepaalde organismes in plaats gesteld zowel binnen de ADIV als op het Belgische Federaal niveau om op een gecoördineerde manier aan detectie, analyse en rapportering te kunnen doen. Een "Early Warning" systeem onder de noemer van een "Red Flag System" was hier een voorbeeld van.

Tijdens de beide verkiezingsdagen, op 9 juni met de Belgische Federale en Europese verkiezingen en op 13 oktober met de regionale verkiezingen, heeft onze dienst enkele FIMI-acties kunnen observeren. Echter, het Cyber Command benadrukt dat die in het niets vallen bij de reeds jarenlange actieve desinformatiecampagnes van bepaalde statelijke en/of niet-statelijke actoren en hun proxies richting een Belgisch, en bij uitbreiding een EU of Westers doelpubliek. In het Global Risk Report van het World Economic Forum begin januari 2024 werd namelijk een top 10 van de grootste bedreigingen op korte en langere termijn opgesomd waarbij mis- en desinformatie op de eerste plaats pronkten. Al sinds 2021 is men op Belgisch federaal vlak bewust van de nood aan een coherente opvolging van FIMI.

Zeker tijdens en na de invasie van Rusland in Oekraïne in februari 2022 kon onze Dienst een substantiële toename van digitale beïnvloedingsactiviteiten detecteren. Sindsdien hebben de snel evoluerende geopolitieke omstandigheden gezorgd voor een verdere substantiële uitbating en intensifiëring van FIMI-activiteiten naar een Westers en eveneens Belgisch doelpubliek. FIMI heeft in de afgelopen periode een voorname rol gespeeld in het kader van hybride dreigingen. De gebeurtenissen in het Midden-Oosten maar eveneens op bijvoorbeeld het Afrikaanse continent worden deze op een zodanige manier geïnstrumentaliseerd. Onder andere met economische en maatschappelijke gevolgen, niet alleen in de diverse internationale theaters, maar eveneens in onze eigen maatschappij.

[1] **Foreign Information Manipulation and Interference (FIMI)**

Trends in aanloop, tijdens en na de verkiezingen



Statelijke actoren

Het Russische desinformatie- en propaganda-ecosysteem kende een verdere intensifiëring op vlak van activiteiten. De gebeurtenissen in het Midden-Oosten vormden een bron van "exploitatie" om de perceptie zodanig te kneden dat die voor bijvoorbeeld een polarisatie binnen een Westers doelpubliek zorgden. Maar ook met betrekking tot de oorlog in Oekraïne werd de nodige creativiteit aan de dag gelegd om verdere verdeeldheid te zaaien binnen EU en/of NATO en de geallieerde steun voor Oekraïne te ondermijnen.

Binnen een Afrikaans informatielandschap lijken de Russische FIMI-activiteiten ook geen pauze te kennen. Integendeel, het verder inspelen en werken met lokale Afrikaanse influencers vergroot op een steeds uitdijende manier de invloed van Russische activiteiten in bijvoorbeeld de gemeenschappen van de Afrikaanse diaspora binnen een Westerse context.

Belgisch Informatie Landschap

De beloofde levering van F16-vliegtuigen door België aan Oekraïne net voor de Europese en federale verkiezingen had een verhoogde Russische FIMI-activiteit als gevolg. Net als de beloofde levering van drie Caesar kanonnen van net voor de Belgische lokale verkiezingen zorgden voor een nooit geziene DDoS-activiteit (Distributed denial-of-service), specifiek gericht tegen de Belgische infrastructuur. Echter, in de aanloop van de verkiezingen werd een substantiële toename van anti-migratienarratieven vastgesteld in combinatie met het versterken van een anti-establishment sentiment. Vooral tijdens de boerenprotesten in januari en februari 2024 zag men gecoördineerde niet-authentieke gebeurtenissen, maar eveneens binnen een "Gaza-context" was men getuige van diverse beïnvloedingsactiviteiten om de gemoederen verder te beroeren.

AI & Platformen

Het gebruik van Artificiële Intelligentie (AI) voor de creatie van memes, avatars, accounts… is een echte game changer geworden. Het snelle en eenvoudige gebruik vertaalt zich in een steeds grotere aanwezigheid van AI binnen FIMI.

We zien een verdere toename van desinformatie, propaganda en extremisme op socialemediaplatformen, met name op X. TikTok veroorzaakt ook bezorgdheid over de vaagheid van de gebruikte algoritmen en de verspreiding van Russische propaganda. De toegenomen polarisatie gaat ook gepaard met een toegenomen interesse van de kant van de veiligheidsdiensten. Telegram, dat sinds de COVID-periode meer aandacht heeft gekregen, lijkt een steeds breder publiek aan te spreken. Het blijft echter een verzamelplaats voor samenzweringstheoretici, anti-establishment verhalen enzovoort.

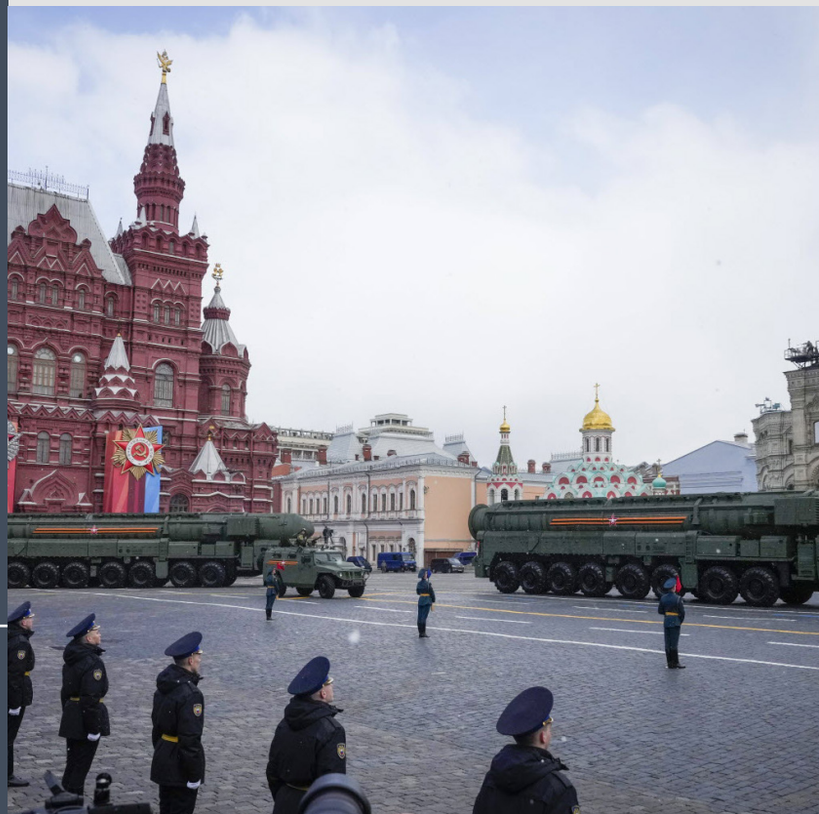
Proliferatie: **de gevaarlijke versnelling**

In 2024 kon de proliferatie van massavernietigingswapens en aanverwante technologieën, een trend die al merkbaar was in 2023, verder worden vastgesteld en kwam er zelfs een versnelling.

Rusland maakt nog steeds voortdurend gebruik van nucleaire dwang als onderdeel van zijn confrontatie met het Westen en om het verloop van het conflict in Oekraïne in zijn voordeel te beïnvloeden.

Deze dwang gaat gepaard met onverhulde intenties om strategische programma's op te starten of nieuw leven in te blazen. Maar ook met een wereldwijde versnelling in de proliferatie van strategische wapensystemen en aanverwante technologieën, die de neiging hebben om de nieuwe norm te stellen, die de historische architectuur van non-proliferatie van massavernietigingswapens aan het verdringen is.

De technologische en capaciteitenontwikkelingen van andere landen die zorgen baren, met name China, Noord-Korea en Iran op het gebied van massavernietigingswapens, en de proliferatie van aanverwante technologieën, ook in strijd met bestaande internationale normen, geven reden tot bezorgdheid. Deze dynamiek, tegen een achtergrond van toenemende spanningen in verschillende regio's van de wereld, dreigt de wapenwedloop te versnellen en het risico op misrekening te vergroten.



Een lanceersysteem voor de RS-24 Yars ballistische raket wordt tentoongesteld op het Rode Plein in Moskou.

Foto: Sipa/Ap/Alexander Zemlianichenko

België in het vizier

Geopolitieke spanningen en hun impact op België

Het huidige geopolitieke klimaat van internationale spanningen en conflicten waarin de samenleving steeds meer gemondialiseerd en gepolariseerd wordt, brengt tegelijk een aantal dreigingen met zich mee. De oorlog in Oekraïne en de houding van België in dat verband lokken reacties van Rusland tegenover ons land uit.

Zo is België opgenomen in een lijst van wat Rusland 'onvriendelijke landen' noemt. De nucleaire doctrine die Rusland hanteert, moet niet onmiddellijk tot grote onrust leiden, maar viseert ook België wel degelijk. De polarisering in de rest van de wereld bemoeilijkt onze relaties met Afrikaanse staten waar bijvoorbeeld militaire samenwerkingen zijn opgeschort of opgezegd. Deze dreigingen manifesteren zich op internationaal vlak onder meer in de vorm van gewapende conflicten en terrorisme.

De situatie in België kan niet los gezien worden van die internationale context. Dat betekent dat ook België te maken heeft met een aantal dreigingen die zeer divers van aard zijn. Enkele van die dreigingen zijn bovendien niet van elkaar los te koppelen. Steeds vaker maken tegenstanders gebruik van hybride tactieken om hun doel te bereiken en een strategisch voordeel te halen. Gebeurtenissen op het internationale vlak kunnen een trigger vormen voor het plegen van gewelddadige acties in eigen land door geradicaliseerde extremistische individuen of groeperingen. De positie van België als lid van en gastland voor Europese en NAVO-instellingen maken van ons land een aantrekkelijk doelwit voor spionage en inmengingsactiviteiten.

Het concept 'hybride oorlogvoering' houdt activiteiten in die onder de drempel van de klassieke benadering van oorlog blijven, maar die voor België een nadeel kunnen berokkenen. Dit jaar konden bijvoorbeeld cyberaanvallen zoals de DDOS-campagne tegen overheidsinstellingen, desinformatie gericht op o.a. extremistische groeperingen, spionage of sabotage vastgesteld worden.

Dreigingen voor Defensie

Defensie krijgt eveneens te maken met die dreigingen. Omdat het defensiepersoneel een afspiegeling is van de samenleving, kunnen ook medewerkers van Defensie gevoelig zijn voor extremistische ideologieën alsook voor buitenlandse beïnvloeding en inmenging. De geopolitieke spanningen leiden tot een verhoogde waakzaamheid voor sabotage van kritieke infrastructuren, zowel civiel als militair. Ten slotte vormt Defensie omwille van haar opdrachten een interessant doelwit voor spionageactiviteiten. Wat dat betreft, bracht 2024 de ADIV 'meer van hetzelfde'.

De rol van de ADIV bij het tegengaan van de genoemde dreigingen is meervoudig. Enerzijds heeft de ADIV een preventieve rol te spelen door zoveel mogelijk te sensibiliseren, anderzijds sporen onze medewerkers actief potentiële problemen op en nemen ze, indien nodig, de nodige maatregelen.

Onze partnerschappen, **van vitaal belang!**

De geglobaliseerde en geraffineerde aard van hedendaagse bedreigingen, zoals terrorisme, cyberaanvallen, desinformatiecampagnes en ontwrichtende technologieën, maken een gezamenlijke aanpak met partnerschappen noodzakelijk. Door middelen, deskundigheid, informatie en inlichtingen te bundelen, krijgen we betere dreigingsanalyses, betere operationele capaciteiten en een breder inzicht in de uitdagingen. Daardoor kunnen we beter anticiperen, voorkomen en reageren op nieuwe bedreigingen.

De ADIV heeft daarom zowel een bureau internationale relaties en sinds kort ook een bureau nationale relaties, die het contactpunt zijn voor officiële relaties en activiteiten met verschillende partners.

Sommige van deze partnerschappen zijn traditioneel en bijzonder vanwege hun inhoudelijke diepgang, zoals die met de Veiligheid van de Staat. Maar naast dergelijke traditionele veiligheidspartners is er een grotere behoefte aan minder gebruikelijke partnerschappen. De ADIV ziet zich namelijk geconfronteerd met een zeer dynamisch landschap van veiligheidsuitdagingen die vragen om innovatieve oplossingen, variërend van nieuwe militaire dreigingen tot snel opkomende cyber- en hybride technieken en tactieken.

De ADIV streeft ernaar om deze ontwikkelingen voor te blijven door gebruik te maken van geavanceerde technologie en een cultuur van voortdurende training en ontwikkeling te bevorderen. Partnerschappen zijn hierbij van bijzonder belang.

Een klein onderdeel van het samenwerkingsnetwerk van de ADIV en het Cyber Command

Het netwerk van de Dienst strekt zich uit over een breed scala aan partners en samenwerkingen. De ADIV en het Cyber Command werken nu bijvoorbeeld regelmatig samen met professoren aan een tiental universiteiten en hogescholen. Vaak gaat het om zeer gespecialiseerde onderwerpen, zoals toekomstgerichte technologieën of zeer specifieke kennisdomeinen, zoals cryptografie. Maar de ADIV deelt ook zijn eigen inlichtingenkennis met studenten, bijvoorbeeld aan de Universiteiten van Gent en Luik.

Regelmatig werkt de Dienst samen met zo'n twintig bedrijven, vaak maar niet uitsluitend in de defensie-industrie. Er wordt bijvoorbeeld samengewerkt met bedrijven die gespecialiseerd zijn in artificiële intelligentie of taaltechnologie.

EU en NAVO

Daarnaast zijn ook de EU en de NAVO multinationale organisaties met een eigen inlichtingenafdelingen en binnen die twee organisaties werken de inlichtingendiensten van de respectieve lidstaten samen binnen het EU- of NATO-raamwerk. De ADIV neemt actief deel aan deze samenwerking. Informatie en analyses worden er gedeeld. Experts nemen deel aan gespecialiseerde werkgroepen en stellen gemeenschappelijke dreigingsanalyses, evaluaties en mogelijke toekomstscenario's op. In het kader van het Belgische engagement voor nationale en internationale samenwerking en veiligheid draagt ADIV zo bij tot meer vrede.

Onze zusterdienst, onze « partner in crime » De ADIV en de VSSE samen sterker

De ADIV en de VSSE hebben al langer dan vandaag een nauwe samenwerking. Op het gebied van contraspionage bijvoorbeeld is deze coöperatie zeker niets nieuws, maar is het de afgelopen jaren wel bijzonder versterkt binnen een steeds formeler kader.

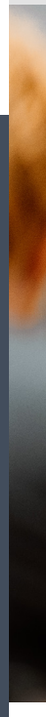
Naast de officiële samenwerkingsovereenkomst van 2004 werden twee gezamenlijke strategische plannen opgesteld in 2018 en 2022, namelijk het Nationaal Strategisch Inlichtingenplan (NSIP). Het doel hiervan was een groot aantal synergiën tussen de twee diensten te ontwikkelen.

Gemeenschappelijk platform

Beide diensten hebben intussen niet stilgezeten, want sinds april 2024 werd het gezamenlijk platform contra-extremisme, contra-terrorisme officieel op pootjes gezet. De zusterdiensten werkten sinds 2018 reeds samen voor het onderdeel contra-terrorisme, dit als gevolg van de aanslag op vraag van de parlementaire commissie. Dat deel boog zich vooral over het soennitisch geïnspireerd terrorisme. Een onderdeel contra-extremisme werd dit jaar bijgevoegd waardoor het platform momenteel een uitbreiding is geworden van de eerdere samenwerking waarbij men nu ook focust op zowel confessioneel als ideologisch terrorisme en extremisme, en dit ongeacht de herkomst of het doelwit van de dreiging militair of burger is.

De coördinator van het platform vertelt:

”De mix van beide inlichtingendiensten zorgt ervoor dat we onze capaciteiten kunnen cumuleren en makkelijker toegang hebben tot elkaars partners. We maken binnen ons platform geen onderscheid meer tussen militairen of burgers. Iedereen van het team is op de hoogte van alle dossiers, niets wordt geheimgehouden. Uiteindelijk werken we allemaal voor hetzelfde einddoel.”



Resultaten samenwerking

Deze gezamenlijke inspanningen met de Veiligheid van de Staat hebben niet alleen geleid tot een gemeenschappelijk platform, maar ook tot aanvullende verwezenlijkingen. Op het gebied van contra-spionage en contra-inmenging is er een toenemende samenwerking, inclusief gezamenlijke operaties. Beide diensten krijgen de mogelijkheid om gebruik te maken van elkaars informatiebronnen, volgens duidelijke en vastgelegde procedures, en verkrijgen wederzijdse toegang tot gegevens die bij de ander in bezit zijn. Daarnaast wordt er samengewerkt aan de ontwikkeling van digitaliseringsprojecten, met een sterke focus op het gebruik van gemeenschappelijke informatie- en communicatietechnologieën om de efficiëntie en effectiviteit van beide organisaties te verbeteren.

Deze samenwerking tussen de twee Belgische inlichtingendiensten versterkt hun complementariteit en garandeert een efficiënte en effectieve uitvoering van hun respectieve wettelijke opdrachten, met respect voor hun specifieke kenmerken, namelijk een militaire en extern gerichte dienst voor de ADIV.

Een gemeenschappelijke sensibiliseringssessie met de VSSE om parlementsleden bewust te maken van digitale risico's op 10 december 2024

Partnerschappen als kern van de **digitale Europese defensiestrategie**

Het Belgisch voorzitterschap van de Europese Unie in 2024 komt op een cruciaal moment voor de Europese veiligheid, met toenemende digitale dreigingen en geopolitieke uitdagingen. Cyberaanvallen en destabilisatie via digitale middelen zijn serieuze zorgen voor de EU en haar lidstaten.

Egmont-formaat

Tijdens het voorzitterschap bracht België cybercommandanten en cyberdiplomaten samen in het zogenoemde Egmont-formaat om dringende kwesties te bespreken. Dit platform dient om strategieën te ontwikkelen, informatie uit te wisselen en partnerschappen te versterken tussen lidstaten.

Een belangrijke boodschap tijdens de Egmont-bijeenkomsten was dat sterke samenwerkingen essentieel zijn om complexe cyberdreigingen het hoofd te bieden. Het benadrukt de noodzaak om nationale veiligheid in een bredere, Europese context te zien. Individuele lidstaten kunnen deze uitdagingen niet alleen aan, collectieve weerbaarheid is noodzakelijk.

Huidige dreigingen en partnerschappen

De digitale transformatie maakt Europa kwetsbaarder voor cyberaanvallen op kritieke infrastructuren zoals energievoorziening, financiële systemen en communicatienetwerken. Het Belgisch voorzitterschap erkent dat supranationale samenwerking cruciaal is. Initiatieven zoals de EU Cyber Diplomacy Toolbox helpen lidstaten om gecoördineerd te reageren op grootschalige cyberaanvallen.

Bilaterale en multilaterale samenwerkingen, zoals de EU Cybersecurity Act, die richtlijnen biedt voor het versterken van cyberweerbaarheid, en samenwerking met NAVO-landen, versterken de Europese cyberverdediging. Partnerschappen met strategische bondgenoten, zoals de VS en Canada, zijn eveneens essentieel, aangezien cyberdreigingen vaak grensoverschrijdend zijn. Platforms zoals de EU-US Trade and Technology Council bevorderen deze trans-Atlantische samenwerking.

De cyberambassadeur Pierre Gillon en toenmalig Minister van Defensie Ludivine Dedonder

Cyberverdediging

De EU-conferentie van cybercommandanten (CyberCo) biedt een forum voor hoge defensieambtenaren die door de EU zijn aangewezen als cybercommandanten op nationaal niveau in hun lidstaten en andere permanente leden. Het belangrijkste doel van de conferentie is het verbeteren van de samenwerking, de uitwisseling van relevante informatie en de coördinatie tussen de lidstaten. CyberCo wordt georganiseerd door elk voorzitterschap van de Raad van de EU, met de steun van het Europees Defensieagentschap (EDA) en de deelname van de Europese Dienst voor extern optreden (EDEO), met inbegrip van de Militaire Staf van de EU (EUMS). CyberCo biedt operationele richtsnoeren voor de uitvoering van het cyberverdedigingsbeleid van de EU, gevalideerd en goedgekeurd door de Raad van de EU.

Cyberdiplomatie

Cyberdiplomatie wint snel aan belang. Diplomatieke samenwerking is nodig om internationale normen en regels te ontwikkelen voor cybergedrag. Het Belgisch voorzitterschap heeft gepleit voor een nauwere samenwerking met de Verenigde Naties en andere organisaties om een internationaal normatief kader vast te stellen dat cyberaanvallen op kritieke infrastructuren veroordeelt.

Open Source Intelligence (r)evolutie

De oorlog in Oekraïne leidde tot hernieuwde focus op de OSINT-capaciteit (Open Source Intelligence). Mede dankzij het STAR-plan uit 2022 kwamen er versnelde investeringen voor de ADIV, onder andere door de nadruk op OSINT als cruciale inlichtingenbron in Oekraïne. Dit resulteerde in een capaciteitsuitbreiding binnen het Cyber Command van de ADIV en Defensie op vlak van personeel, materieel, technologie en verruiming van operationele capaciteit.

Van klassieke methoden naar OSINT 2.0 en OSINT 2.1

Hoewel OSINT al eeuwen bestaat, kreeg het dankzij internet en technologieën zoals machine learning een moderne dimensie, vaak "OSINT 2.0" genoemd. Hedendaags gebeurt een verwerking van grote hoeveelheden informatie op een efficiënter en accurater niveau. Open bronnen zoals kranten, rapporten, publieke toespraken en kaarten om inzichten te krijgen over de vijand en andere tegenstanders, zijn geen nieuwe inlichtingenmethodes. Onder andere sociale media, blogs, wetenschappelijke databases en nieuws-websites vormen nu ook essentiële databronnen. De integratie van deze technologieën heeft OSINT getransformeerd tot een onmisbare pijler binnen inlichtingenwerk naast disciplines zoals HUMINT (Human Intelligence) en SIGINT (Signal Intelligence).

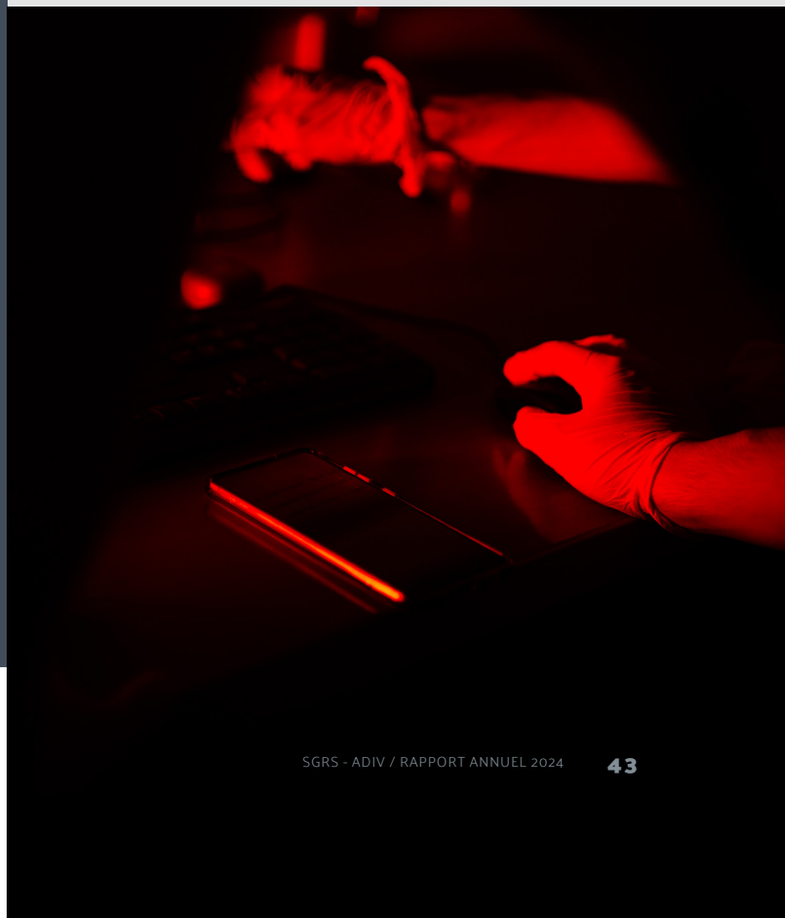
De oorlog bracht een heropleving van klassieke modus operandi, zoals desinformatie en fake news, die met behulp van moderne technieken massaal worden ingezet. Het Cyber Command van de ADIV volgt deze evolutie nauwgezet op en breidde daarom in 2024 het ontwikkelingstraject voor Information Warfare uit, gericht op het weerleggen, bevestigen en lokaliseren van content op sociale media. We groeien daarmee naar een OSINT 2.1. Deze capaciteit begon tactisch, bijvoorbeeld voor het analyseren en verwerken van socialemediaposts over Russische troepen-bewegingen in Oekraïne tot bruikbare tactische inlichtingen, maar wordt nu operationeel en strategisch ingezet.

Een nieuwe subdiscipline

In het afgelopen jaar heeft het Cyber Command van de ADIV een nieuwe subdiscipline binnen de DICU (Digital Influence Collection Unit) opgezet om operationele en strategische inlichtingen beter te ondersteunen, met een focus op onder andere Oekraïne. Dit omvatte de integratie van concepten, middelen, en personeelsplanning om tegen 2025 volledig operationeel te zijn.

Wat met de toekomstperspectieven?

De evolutie van OSINT benadrukt zijn groei en past zich voortdurend aan nieuwe technologieën en geopolitieke uitdagingen aan. Naar verwachting zal deze evolutie en toekomstige investeringen niet alleen bijdragen aan de veiligheid op het slagveld, maar ook aan het bredere strategische inzicht van regeringen in een steeds veranderende mondiale context.



China, kampioen van **online manipulatie met AI ?**

Statelijk actoren en cybercriminelen gebruiken Artificiële Intelligentie (AI) om verschillende fasen van een cyberaanval te automatiseren. Dit omvat het identificeren van kwetsbaarheden, het automatisch aanmaken van malware, het stelen of vernietigen van gegevens en het verstoren van de werking van systemen.

AI-systemen zoals WormGPT maken het mogelijk om snel kwaadaardige code te creëren en detectie te omzeilen. Tussen 2023 en2024 hebben bedrijven maatregelen genomen tegen AI-misbruik door statelijke actoren, die AI gebruiken voor hacking en manipulatie. Enkele van deze statelijke actoren gebruikten AI om kwetsbaarheden te vinden in bestaande software, hun eigen code te debuggen, kleine scripts te genereren en content te creëren gebruikt in (spear-) phishing campagnes.

Data, propaganda en beïnvloeding van publieke opinie met AI

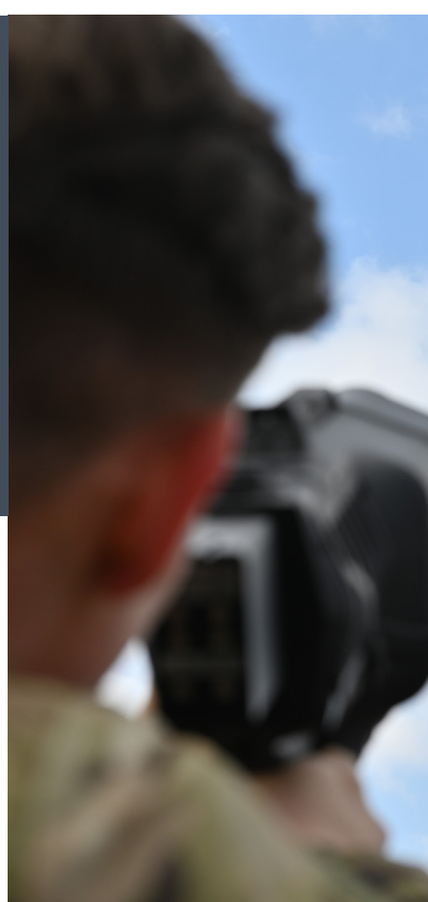
AI-systemen worden daarnaast ook gebruikt voor beïnvloedings- en propagandamateriaal, samen met het checken van data. Chinese apps zoals TikTok, CapCut, Temu en Shein verzamelen persoonlijke gegevens en leveren beeldmateriaal aan de Chinese overheid. Dit kan worden gebruikt om AI-systemen te trainen in hoe verschillende bevolkingsgroepen buiten China zich uitdrukken en hun emoties tonen.

Dit laat de Chinese overheid toe om getrainde AI-systemen in te zetten om doelgerichte video's te maken, bedoeld om publieke opinie buiten China te beïnvloeden. Er zijn namelijk reeds gevallen geïdentificeerd waar content werd gecreëerd om het stemmen tijdens (supra)nationale verkiezingen te beïnvloeden, zoals geobserveerd in Rwanda, India en overheen de EU tijdens de Europese verkiezingsperiode in Jun 2024.

Het Cyber Command van de ADIV volgt AI-ontwikkelingen nauwgezet op, werkt samen met nationale en private partners, en past verdediging en bewustzijn aan op basis van nieuwe inzichten en bedreigingen.

Drones, explosieven en elektronische oorlogsvoering: **de nieuwe veiligheidsuitdagingen**

Met het wijdverbreide gebruik van commerciële en op maat gemaakte micro- en minidrones inspireert de trend zelfs terroristische organisaties en veel commerciële spelers. Ze stellen nu voor om ze uit te rusten met nuttige ladingen die een veelheid aan opdrachten kunnen uitvoeren.



Gezien deze riskante trend heeft de NAVO enkele van haar analysegroepen gewijzigd. Daarom is het team van deskundigen dat zich bezighoudt met het tegengaan van op afstand bediende ontploffingstuigen in 2024 één niveau in de NAVO-hiërarchie opgeschoven. Het heeft ook de taak gekregen om kleine, onbemande, vanop afstand bestuurde systemen en ontploffingstuigen elektromagnetisch te bestrijden.

Binnen dit kader neemt een team van het Cyber Command, het Electromagnetic Warfare Center (EWC), deel aan NAVO-oefeningen en vergelijkend onderzoek in een multinationale context. Het is ook betrokken bij onderzoek in België naar de doeltreffendheid van de huidige Belgische militaire middelen in het tegengaan van deze dreigingen.

In 2024 nam het EWC deel aan de NAVO-oefening “Thor’s Hammer”, de grootste oefening voor elektronische oorlogsvoering tot nu toe. Hierdoor konden technologieën voor het tegengaan van geïmproviseerde ontploffingstuigen en kleine onbemande vanop afstand bestuurde systemen getest worden. Meer in het algemeen kunnen met dit soort oefeningen gecoördineerde antwoorden op hedendaagse elektronische dreigingen worden ontwikkeld, waarbij de nadruk ligt op interoperabiliteit.

Het EWC is regelmatig betrokken bij verschillende operaties van Defensie, zoals beveiligingsopdrachten van het luchtruim boven de Baltische staten, ter ondersteuning van F16-operaties (BAP 2024).

Defensie investeert momenteel en zal blijven investeren in een grote verscheidenheid aan nieuwe platformen met systemen voor elektromagnetische oorlogsvoering.

Classified Archives

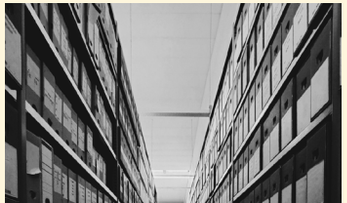
ADIV-SGRS NEWS

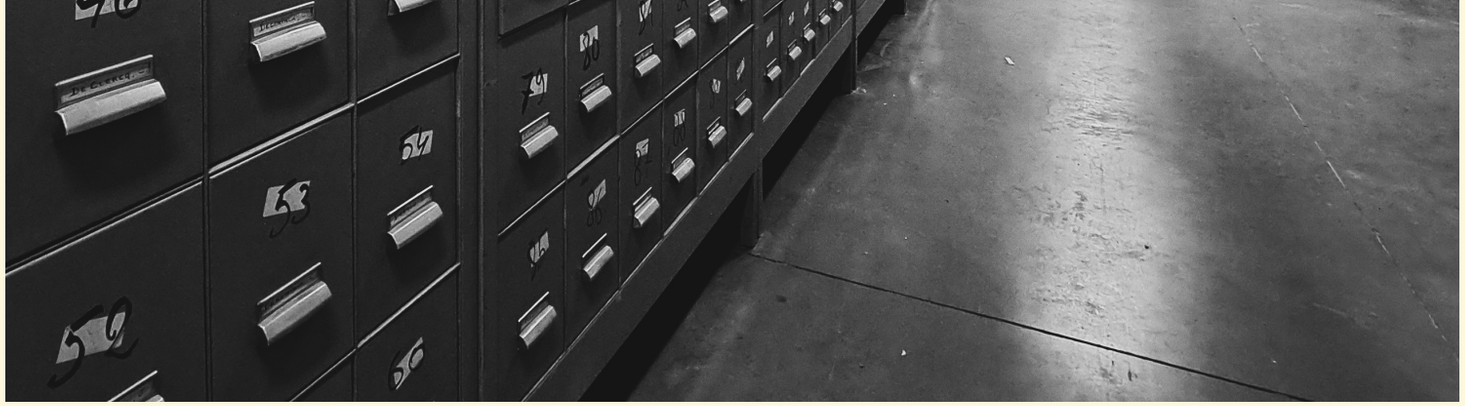
"The right of access cannot be without restrictions" (EU).

www.sgrs.be

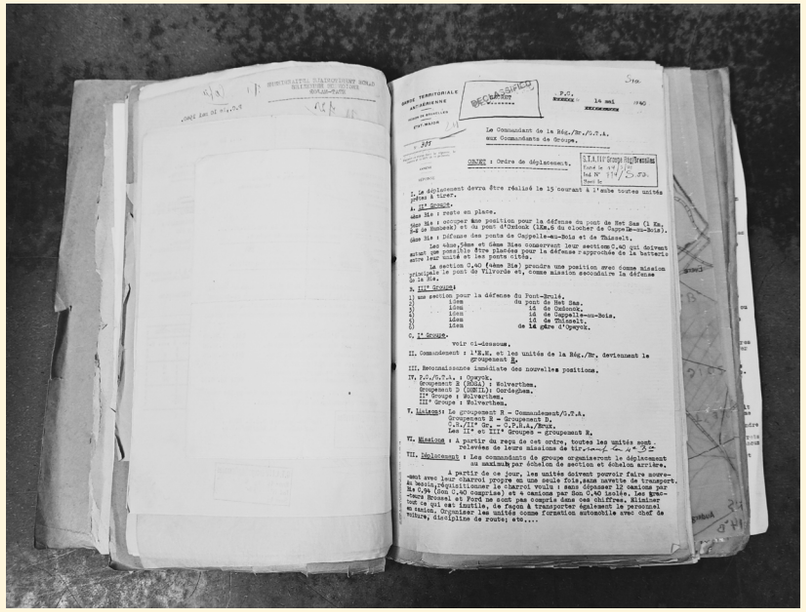
Reeds 200 meter aan archieven voor de "Campagne 1940-1945" geïnventariseerd

In het gigantische depot waar de Classified Archives van de ADIV zich bevinden, worden al jaren geclassificeerde en historische archieven bewaard die administratief en juridisch nut hebben voor Defensie. Er zijn militaire archieven opgemaakt tijdens de algemene mobilisatie in 1939, tijdens de 18-daagse veldtocht en tijdens de bezetting: de archieven "Campagne 1940-1945". Het archieffonds beslaat ongeveer 500 strekkende meter waarvan er ondertussen al een groot deel is geïnventariseerd.





Voor onderzoekers hebben de archieven van de "Campagne 1940-1945" een grote historische waarde en is het een schatkamer van informatie. Ondanks de leeftijd is een groot gedeelte van dit archief nog geclassificeerd. Desondanks komen er vragen tot declassificatie van deze documenten, zowel vanuit de politiek, als de publieke opinie en het Rijksarchief. Er bestaat echter ook een 'Regel van de derde partij' die stelt dat bij geclassificeerde documenten van andere landen en ieder andere instelling die geen deel uitmaakt van Defensie, eerst een toestemming moet worden gevraagd aan deze derde partij vooraleer een declassificatie gebeurt. Deze regel kan bijgevolg tot enige vertraging leiden.



Bij de gedetailleerde inventarisopstelling van het archief wordt gekeken naar de mogelijke gevoeligheden of problemen die declassificatie zouden kunnen verhinderen. De archivarissen van de Classified Archives zien geen probleem om de onderzochte documenten te declassificeren. Momenteel wordt daarom het archieffonds in delen gedeclassificeerd, op die manier kunnen onderzoekers reeds de gedeclassificeerde stukken inkijken. Eens dat de volledige declassificatie afgerond is, kan het overgebracht worden naar het Rijksarchief. Tot die tijd kunnen de onderzoekers het archief raadplegen in de leeszaal van CA.

De archiefstukken die reeds gedeclassificeerd zijn:

a. I° Legerkorps
b. II° Legerkorps
c. Lijsten Stalags en Oflags

Begeleiding en **ontwikkeling** : het tweevoudige engagement van de ADIV

Om hun integratie in de ADIV vlot te laten verlopen, werkt de dienst Human Ressources een vormingstraject voor nieuwkomers uit. Er worden generieke trainingen georganiseerd om de organisatie en haar werking voor te stellen aan alle nieuwe personeelsleden, inclusief militairen die intern zijn overgeplaatst. Afhankelijk van de juridische status van het personeel zal ook passende begeleiding worden aangeboden.

Een programma voor begeleiding en ontwikkeling

De ADIV zorgt ervoor dat militairen die op hun veiligheidsmachtiging wachten, kunnen deelnemen aan interne vormingen of vormingen binnen andere diensten (vorming van eerstehulpverlener, taalopleiding, enz.).

Naast de begeleiding van nieuwe militairen wordt er ook ondersteuning op maat geboden aan burgerpersoneel en reservisten. Enerzijds zullen de aangeworven burgers regelmatig in contact blijven met de ADIV voordat ze hun officiële functie opnemen. Anderzijds kunnen sommigen van hen worden opgenomen in een ander departement van Defensie in afwachting van het bekomen van de veiligheidsmachtiging die nodig is om in de sector van inlichtingen te werken. Voor reservisten is er ook personeel beschikbaar voor specifieke begeleiding, zoals het volgen van hun vormingstraject of hun administratief dossier.

Al deze initiatieven zullen de nieuwe medewerkers helpen om zo goed mogelijk te wennen aan hun nieuwe omgeving en ze zullen ook worden aangepast op basis van de feedback van de nieuwe medewerkers.

Getuigenis Margaux, 24

“ACOS IS had een tijdelijke functie geregeld in een andere eenheid om mijn start te versnellen. Nadien zou ik intern de overgang maken naar hun team.

Vandaag zijn beide departementen volop betrokken bij mijn onthaal en professionele ontwikkeling. Een handvol leidinggevenden van elke eenheid verbinden zich tot maandelijks overleg om te verzekeren dat iedereen op één lijn zit. Allemaal geven ze me de vrijheid om mijn eigen tempo te bepalen. Dit soort continuïteit, evenals het matchen van een persoon op basis van potentieel – en niet op basis van een functieomschrijving – is wat mijn keuze voor deze eenheid herbevestigd. Leuk weetje, ook mijn originele POC blijft bellen.”

Van integratie naar actie met een **innovatief** vormingstraject

Veertien militairen die de rangen van het Cyber Command kwamen vervoegen, hebben een aantal maanden een vormingstraject op maat gevolgd om de verschillende aspecten van hun toekomstige beroep te leren beheersen. Deze vorming werd georganiseerd tijdens de periode waarin ze wachtten op de goedkeuring van hun veiligheidsmachtiging en stelde hen in staat om zich efficiënt voor te bereiden alvorens zich bij hun respectieve teams aan te sluiten.

De vorming begon met een presentatie van de verschillende toegankelijke diensten, gevolgd door een speeddating-sessie waarop elke kandidaat zijn of haar voorkeuren kenbaar kon maken.

Gedurende 17 weken werden de toekomstige analisten vertrouwd gemaakt met de grondbeginselen van de inlichtingendienst en ontwikkelden ze innovatieve denkvaardigheden om hun doelen te bereiken.

Er werd ook een immersieve oefening van een dag gehouden in het « Cyber Sigint Missions Center », in de vorm van een War Game, om de functie te bepalen waarin elke kandidaat op basis van zijn of haar capaciteiten het beste tot zijn of haar recht zou komen.

Getuigenis Henri, 27

"De vorming was een uitstekende basis om in mijn nieuwe functie te starten en bereidde me voor om tijdens het werk te blijven leren. Ze combineerde zowel theoretische als praktische onderdelen, met name op het gebied van stressmanagement, en bood zeer bruikbare tips voor het omgaan met nieuwe en onverwachte situaties.

Voordat ik aan de vorming deelnam, had ik een aantal jaren ervaring opgedaan in Afrikaanse aangelegenheden, gevolgd door een carrièreswitch naar het leger. Het programma stelde me niet alleen in staat om mijn bestaande kennis toe te passen, maar hielp me ook om die op zinvolle manieren uit te breiden.

We kregen diepgaande training over verschillende onderwerpen, waaronder inlichtingen, cyberoperaties, management, stressmanagement en briefingtechnieken voor verschillende doelgroepen. Een van de meest waardevolle aspecten was het leren over de militaire cultuur, hoe structuren zijn georganiseerd, hoe efficiëntie wordt ervaren en zelfs praktische richtlijnen over gedrag, zoals hoe je jezelf moet presenteren op een militaire basis.

In het algemeen was de training een omslag, die me de tools en kennis gaf die ik nodig heb om uit te munten als analist."

The War Game: een innovatieve tool

Het spel is gebaseerd op een eenvoudig principe: de veldslagen van de Tweede Wereldoorlog nabootsen zodat deelnemers de rollen van bevelhebbers en sectiechefs kunnen aannemen. Op die manier bootsen ze de operationele structuur van de inlichtingencentra van het departement na. Elk centrum wordt geleid door een chef die kiest welke wapensystemen, zoals inzamelmiddelen, worden ontplooid. Hun opdracht is het achterhalen en verwerken van relevante informatie om vooraf bepaalde doelen te bereiken, zoals het in bezit nemen van een bepaald dorp of het uitschakelen van vijandelijke troepen.

« Deze simulatie helpt nieuwe analisten de praktische redeneervaardigheden te verwerven die essentieel zijn voor inlichtingenoperaties, door ze ervaring te laten opdoen met de besluitvormingsuitdagingen waarmee ze te maken zullen krijgen," legt M. uit, chef van het departement "Cyber Sigint Missions Center".

M. duidt op een van de belangrijkste voordelen van de War Game: « Het spel maakt heel snel duidelijk of de nieuwe analisten over de nodige creativiteit en proactiviteit beschikken. In de wereld van de inlichtingen is het vaak cruciaal om buiten de gebaande paden te treden om kostbare informatie te verzamelen. De wereld van de buitenlandse inlichtingen biedt veel mogelijkheden, maar alleen de meest creatieve geesten kunnen ze effectief benutten. »

Getuigenis Isaac, 25

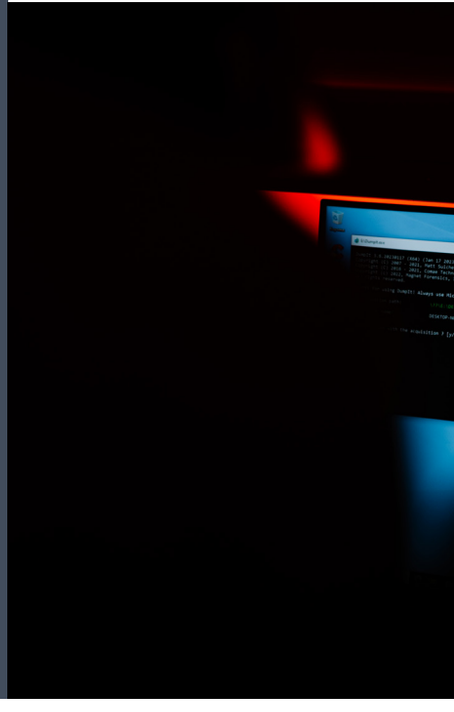
"De War Game was een ervaring van onschatbare waarde die me heeft geleerd hoe ik gefundeerde beslissingen moet nemen en de dynamiek van militaire operaties moet verbeelden. Het verscherpte mijn vermogen om situaties in te schatten, kansen te herkennen en gebruik te maken van wat er voor me ligt om een voordeel te behalen.

Een van de meest impactvolle lessen was het effectief leren werken binnen een team. De oefening benadrukte het belang van duidelijke communicatie, vooral bij het afwegen van verschillende meningen. We moesten samenwerken om prioriteiten te stellen en ons richten op de meest kritieke aspecten om maximale resultaten te behalen.

Over het geheel genomen heeft de War Game niet alleen mijn analytische vaardigheden verbeterd, maar ook mijn vaardigheden op het gebied van teamwork en communicatie - tools die essentieel zijn voor succes in elke missie."

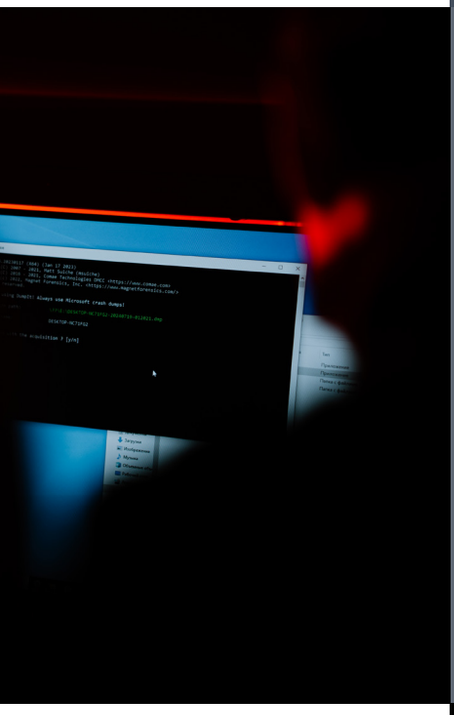
Sabrina, 28, agent screening

“Al drie jaar lang werk ik bij de ADIV, waarvan ongeveer een jaar als agent screening. Mijn job binnen de ADIV bestaat erin om veiligheidsverificaties uit te voeren voor, in eerste instantie, alle kandidaten die bij Defensie willen werken. In tweede instantie doen we dat ook voor de industrie die een contract voor Defensie hebben en voor onze partnerdiensten. Dat omvat het screenen van mensen die een risicovolle functie willen uitoefenen, zoals medewerkers van luchthavens of kerncentrales.”



Aarzel niet om onze website te bezoeken om onze artikelen en nieuwtjes binnen onze afdeling te ontdekken.
- www.sgrs.be

“Wij kijken vooral naar achtergrondinformatie uit database om te bepalen of deze mensen de nodige waarden en integriteit hebben om bijvoorbeeld een functie bij Defensie uit te oefenen. Drugsgebruik, slagen en verwondingen, diefstal etc. zijn bijvoorbeeld allemaal factoren die een belangrijke rol spelen om een beslissing te maken. We behandelen elk dossier individueel en elke casus wordt apart bekeken en behandeld zodat iedereen een gelijke kans krijgt.”



“Met ons team stonden we dit jaar voor de uitdaging om zo’n 300.000 screenings uit te voeren waardoor we vaak gelijktijdig 150 à 200 dossiers tegelijk verwerken. Dat overzicht bewaren is ook net het moeilijkste aan onze job. Aan de andere kant krijg ik een enorme voldoening uit mijn werk en heb ik echt een impact op de veiligheid van ons land en van Defensie. We dragen bij aan de veiligheid van ons land door ervoor te zorgen dat de mensen, voldoen aan de hoogste normen van integriteit.”

ADIV · SGRS

QUAERO ET TEGO

Cyber Force

Through Partnerships

WWW.SGRS.BE