ADIV - SGRS
APRIL 2026 / WWW.SGRS.BE

JAARVERSLAG 2025

QUAERO ET TEGO

DEFENSIE

.be

OMSLAG : De Ariane 6-raket, ontwikkeld door het Europees Ruimteagentschap

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 middel van onze inlichtingen is onze belangrijkste missie; het geven van deskundig advies aan de autoriteiten is onze plicht jegens ons land, de samenleving en onze medeburgers.

VERANTWOORDELIJK REDACTEUR

M. Van Hecke Bernard

Koninging Elisabeth Kwartier
Eversestraat 1 in 1140 Evere

Foto's : DG StratCom en personeel ADIV

Lay-out : Quentin Moonen

Door ADIV-SGRS

“Wij zetten ons in voor u, voor ons land en voor de vrede.”

Generaal-majoor
Stéphane Dutron

P. 36

DE AANKOMST VAN DE EERSTE F-35

Op 13 oktober 2025 werd een historische mijlpaal bereikt met de aankomst van de eerste F-35A Lightning II-gevechtsvliegtuigen op de luchtmachtbasis van Florennes.

ONZE BOODSCHAP

Uw toekomst. Onze missie.

Inleiding

In ons beroep, waarbij we vaak in de schaduw werken, bestaan er geen makkelijke of rustige jaren

We zijn inmiddels toe aan de vierde editie van ons jaarverslag. Deze publicatie verschijnt in een wereld die ingrijpende veranderingen ondergaat, en de geopolitieke chaos heeft zwaar gewogen op de inlichtingendiensten. De afgelopen maanden waren immers getuige van ingrijpende gebeurtenissen die het grote publiek hebben laten zien hoe groot de omvang is van veranderingen die vaak al veel eerder in gang waren gezet. De strijd tussen grootmachten, de terugval van het multilateralisme en de druk op de internationale orde liggen ten grondslag aan veel instabielere internationale betrekkingen, waarin nationale belangen vaak voorrang krijgen boven alle andere overwegingen. Een onzekere wereld met een steeds lagere drempel voor interstatelijk geweld, zelfs in gebieden die tot nu toe als relatief stabiel werden beschouwd. In deze context wordt een inlichtingendienst als de onze des te belangrijker: dankzij onze inspanningen op het gebied van informatieverzameling en -analyse hebben we talrijke conflictsituaties kunnen kruisvergelijken, interpreteren en in hun context plaatsen, waardoor we besluitvormers het inzicht hebben geboden dat onmisbaar is voor het nemen van beslissingen en het ondernemen van actie, ten behoeve van onze nationale belangen. We hebben alleen gehandeld of met de steun van onze partners, afhankelijk van de omstandigheden en de beschikbare middelen.

In 2025 was de oorlog tussen Oekraïne en Rusland nog steeds aan de gang en bleef Rusland bescheiden terreinwinst boeken in de Donbas-regio, ondanks een oorlogseconomie die op volle toeren draaide. De uitgaven voor defensie en binnenlandse veiligheid maakten meer dan 43 % van de officiële overheidsuitgaven uit. De internationale sancties en de Oekraïense aanvallen op kritieke installaties in Rusland sorteren echter langzaam maar zeker effect. Ten koste van verschrikkelijke menselijke verliezen en met de steun van bondgenoten die hen blijven bevoorraden, hebben de legers van Poetin slechts weinig terrein gewonnen op een slagveld dat technologisch voortdurend verandert, waardoor bepaalde eerdere tactische concepten ter discussie worden gesteld. De veerkracht van de Oekraïners neemt niet af, ondanks de aanhoudende aanvallen op kritieke installaties en steden op Oekraïens grondgebied.

In het Midden-Oosten vreesde men voor een algemene escalatie in de regio toen Israël in juni luchtaanvallen uitvoerde op Iraanse nucleaire installaties. De Iraanse vergeldingsaanvallen waren namelijk niet alleen op Israël gericht; er werden onder meer ballistische raketten afgevuurd op de Amerikaanse basis Al-Udeid in Qatar. In Gaza en op de Westelijke Jordaanoever blijft de situatie onduidelijk, de kwetsbaarheid van de instellingen in Libanon en Syrië is – ondanks de geleverde inspanningen – relatief zorgwekkend, terwijl de uitkomst van de parlementsverkiezingen van november in Irak ons meer duidelijkheid over de toekomst moet geven. De toegang tot de Rode Zee blijft uiteraard een voortdurend aandachtspunt, evenals de aanwezigheid van de Islamitische Staat en zijn bondgenoten, die zouden kunnen proberen zich duurzaam in de regio te vestigen.

In Afrika werd het begin van het jaar 2025 gekenmerkt door de opmars van de rebellenmilities van de M23 in het gebied van de Grote Meren in het oosten van Congo. De inname van Goma en Bukavu leidde tot een humanitaire ramp en tot het eenzijdige besluit van de

Rwandese autoriteiten om alle diplomatieke banden met ons land te verbreken. Onze dienst werd gevraagd om te helpen bij de evacuatie van onze ambassade binnen een uiterst kort tijdsbestek en ik wil mijn waardering uitspreken voor de professionaliteit en de kalmte van ons personeel en dat van de FOD Buitenlandse Zaken. Ondanks diplomatieke akkoorden duurt het conflict ter plaatse voort en de inname van Uvira in december was een nieuwe klap in het gezicht voor sommige strijdende partijen, maar ook voor de onderhandelende landen en een deel van de internationale gemeenschap.

In het westen van het Afrikaanse continent zetten verschillende terroristische groeperingen die banden hebben met Al-Qaida en, in mindere mate, met Islamitische Staat, hun opmars in de Sahel voort. Deze groeperingen breiden hun grondgebied uit in Mali, Burkina Faso, Niger, het noorden van Benin en het noordwesten van Nigeria. Op het moment van schrijven vormen ze nog steeds een bedreiging voor verschillende hoofdsteden in de Sahel (Bamako, Ouagadougou en Niamey).

We blijven de ontwikkeling van de internationale situatie en de gevolgen daarvan voor België op de voet volgen, samen met onze analisten, maar ook in nauwe samenwerking met het diplomatieke netwerk, via onze militaire attachés en onze talrijke internationale contacten.

In België zetten we onze inspanningen in de strijd tegen radicalisme en extremisme gezamenlijk voort met de Staatsveiligheid (VSSE), onze belangrijkste partner op het gebied van inlichtingen en veiligheid, waarmee we de synergieën in de loop der jaren steeds verder versterken. Pogingen tot inmenging of spionage zijn eveneens een bron van voortdurende bezorgdheid, met name binnen de wetenschappelijke en onderzoekswereld die verband houdt met Defensie. Onze dienst neemt actief deel aan de versterking van de federale interdepartementale samenwerking in de strijd tegen deze verschijnselen.

Ten slotte worden hybride pogingen tot destabilisatie door vijandige staatsactoren, via cyber-aanvallen, desinformatie, inbreuken op het luchtruim van de NAVO of pogingen tot sabotage, met de nodige aandacht gevolgd. Hoewel sommigen geneigd zijn de talrijke dronevluchten boven onze kazernes, civiele luchthavens of kritieke infrastructuur aan Rusland toe te schrijven, is er op dit moment geen concreet bewijs om deze hypothese te bevestigen.

In ons werk achter de schermen is er geen enkel jaar dat gemakkelijk of rustig is. Integendeel, de geopolitieke spanningen en de hybride dreiging in België zijn groter dan ooit en dwingen ons om extra aandacht te besteden aan de veiligheid van het personeel en de militaire infrastructuur, maar ook om onze nationale belangen te beschermen.

Maar de intensivering en diversificatie van de dreigingen vragen jaar na jaar meer flexibiliteit en veerkracht van ons. Dat betekent dat we onszelf voortdurend opnieuw moeten uitvinden, zowel wat betreft onze opleidingen, onze procedures als ons materieel, en daarom blijft de wendbaarheid van de Dienst mijn prioriteit.

We moeten meer middelen inzetten voor technologie en de verwerking van de steeds grotere hoeveelheden gegevens, om de processen te versnellen.

We moeten anticiperen op de dreigingen en ons, samen met al onze nationale en internationale partners, inzetten om Defensie te ondersteunen, onze besluitvormers te informeren en ons land, zijn bevolking, zijn waarden en zijn instellingen te beschermen. We moeten een antwoord geven op de vraag: “Quid Belgica? ”

Namens het personeel van de ADIV wens ik u veel leesplezier!

GENERAAL-MAJOOR

Stephane Lutron

ADIV - SGRS / CYBER FORCE

Inleiding

Er is een netwerk nodig om een netwerk te verdedigen

Het was mij een grote eer om in september 2025, na ettelijke jaren als directeur operaties te hebben gewerkt aan de zijde van luitenant-generaal Michel Van Strythem, de functie van commandant van de Cybermacht op te nemen.

Mijn prioriteit is de ontwikkeling van dit nieuwe krijgsmachtdeel, zodat het zijn opdrachten in steun van de ADIV en de andere krijgsmachtdelen van Defensie zo goed mogelijk kan vervullen. Onze verscheidenheid aan functies, profielen en statuten is niet enkel een troef, maar verschaft ons ook het voordeel dat wij snel kunnen evolueren binnen Defensie en ons netwerk van externe partners. Wij blijven dag na dag groeien, maar om die groei te kunnen ondersteunen, moeten wij ook onze inspanningen voortzetten op het vlak van rekrutering.

In dit verband is de inplaatsstelling van de Cyberreserve, de "Joint Cyber Defence Resilience Force Unit", van kapitaal belang. Meer dan ooit hebben wij mannen en vrouwen nodig met de meest uiteenlopende achtergronden, uit het bedrijfsleven of de academische wereld, om deze kennis- en expertiseoverdracht tussen de civiele en militaire wereld permanent mogelijk te maken, teneinde de weerbaarheid van Defensie te waarborgen en aan de weerbaarheid van ons land mee te werken.

Met hetzelfde doel voor ogen hebben wij onze "Cyber Defence Factories" opgezet, ontmoetings- en onderzoekscentra in het hart van de lokale cyberbeveiligingsecosystemen. Na de site van de innovatiecluster in Charleroi hebben wij in 2025 een nieuwe locatie geopend op de campus van de Hogeschool Howest in Brugge. Vandaag werken ongeveer 30 studenten nauw samen aan cyberveiligheidsprojecten met de ondernemingen uit de sector en koesteren wij ambities voor de toekomst.

Een van de markante nieuwsfeiten van dit jaar 2025 is uiteraard de toename van het aantal waarnemingen van ongeïdentificeerde drones boven verschillende kazernes, nationale of regionale luchthavens en kritieke infrastructuren.

België was uiteraard niet het enige land dat met dit fenomeen geconfronteerd werd, maar deze operaties werden duidelijk op grote schaal gepland en gecoördineerd. Dit fenomeen moet in de ruimere context van hybride oorlogsvoering worden gezien, waarbij deze drones slechts een van de vele middelen zijn: schendingen van het luchtruim en van de maritieme ruimte, desinformatiecampagnes, enz.

Een van de bijzonderheden van deze hybride oorlog is de bijzonder interessante kosten-batenverhouding. Drones zijn niet duur, maar hebben een aanzienlijke media- en psychologische impact

doordat ze een gevoel van onveiligheid teweegbrengen. Om nog maar te zwijgen van de economische gevolgen van de sluitingen van het luchtruim en de verlamming van de luchthavens.

De kwestie van de drones vestigt de aandacht op de noodzaak om onze detectie- en beveiligingsmiddelen op het vlak van elektronische oorlogsvoering te ontwikkelen. Het elektromagnetische spectrum is een nieuw strijdtoneel geworden en dat is bijzonder waar in Oekraïne, waar drones toelaten om een beslissend tactisch voordeel op de vijand te verwerven.

Om die reden ontwikkelen wij het JEWSC (Joint Electronic Warfare Support Center), dat belast is met de programmering van de elektromagnetische databases die in alle huidige en toekomstige wapensystemen moeten worden geladen. Het zal ook toelaten om een hele reeks parameters te analyseren die tijdens de operaties worden geregistreerd.

Het is mijn overtuiging dat wij enkel samen met al onze (privé- en publieke) partners het hoofd kunnen bieden aan al die dreigingen, die versterkt worden door het gebruik van disruptieve technologieën, zoals artificiële intelligentie.

In dat verband is de aanwijzing van een verbindingsofficier bij de gefedereerde entiteiten uitstekend nieuws, wat ook de lopende projecten zal vergemakkelijken. Wij breiden de initiatieven met de Gewesten uit, onder meer met de “cyber week” van het Agence du numérique. Wij zetten onze samenwerking voort met ESA (Europees Ruimteagentschap) en met IDELUX (intercommunale van de provincie Luxemburg), waar wij operatoren van de Luchtmacht trainen om in een simulator in realtime een hele reeks cyberincidenten het hoofd te bieden.

Meer dan ooit is er een netwerk nodig om een netwerk te verdedigen!

GENERAAL-MAJOOR

Pierre Cipariße

Commando-wissel bij de Cyber Force op 19 september 2025

Nabije Oosten : **de vrees voor een brandhaard**

Net als 2024 werd 2025 gekenmerkt door het conflict tussen Israël en Hamas, een conflict dat zich verder ontwikkeld heeft in 2025 en waarbij tal van landen in de regio, rechtstreeks of onrechtstreeks, betrokken raakten, wat de vrees voor een regionaal gewapend conflict deed rijzen.

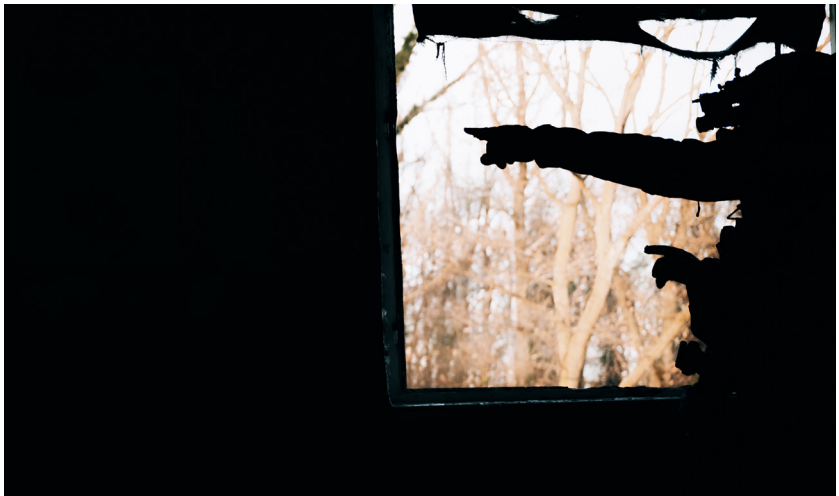
De vrees voor een regionale escalatie bereikte zijn hoogtepunt op 13 juni 2025, de dag waarop Israël begon met de operatie “Rising Lion”, met als doel de vernietiging van de Iraanse nucleaire installaties en van de infrastructuur en het militaire commando.

Na de Amerikaanse operatie “Midnight Hammer” op 21 juni 2025, die tot doel had de Iraanse nucleaire installaties in Fordow, Natanz en Isfahan te neutraliseren, is er op 23 juni een tegenreactie van Iran gekomen. Iran heeft een salvo ballistische raketten afgevuurd op de Amerikaanse basis van Al-Udeid in Qatar. Een staakt-het-vuren tussen Israël en Iran op 24 juni heeft uiteindelijk een nieuwe escalatie van de confrontatie vermeden, die inmiddels de “Twaalfdaagse Oorlog” wordt genoemd.

Verzwakking van Iran

Iran heeft zeer zware verliezen geleden. Niet alleen werd het Iraanse militaire potentieel geraakt, maar bovendien kreeg de militaire leiding zware klappen te verduren. De passiviteit van verschillende actoren van de “As van Verzet” (beschouwd als het geheel gevormd door de proxy’s van Iran, zoals de Palestijnse Hamas, de Libanese Hezbollah en ook de pro-Iraanse milities in Irak) was de bevestiging van de verzwakking van de projectiekracht van Iran. De Houthi’s vormen een uitzondering op de regel. De Jemenitische beweging is er meermaals in geslaagd Israël te bedreigen.

Het Iraanse regime lijdt ook onder een interne instabiliteit, die verergerd wordt door de recente crisissen. Dat leidde tot een golf van betogingen die einde 2025 op gang kwam.



Gevolgen voor Libanon en Syrië

De instabiliteit die is ontstaan door het conflict tussen Israël en Hamas had ook in 2025 verdere gevolgen voor Libanon. Ondanks het akkoord over een staakt-het-vuren dat eind 2024 werd ondertekend, bleven er Israëlische operaties tegen Hezbollah doorgaan in het zuiden van Libanon en sporadisch in andere regio's, zoals in Beiroet of in de Bekavallei. De aankondiging van een ontwapeningsproces begin september 2025 lijkt in de richting van een stabilisering van de situatie in Libanon te gaan, maar Hezbollah blijft politiek en sociaal belangrijk. De keuze voor een gedwongen ontwapening brengt dus risico's met zich mee in dit land, dat gekenmerkt wordt door het naast elkaar bestaan van talrijke gemeenschappen.

Syrië blijft een gebied waar regionale actoren hun belangen proberen te verdedigen. De toestand blijft er precair. Ondanks een officieel beleid van democratisering en inclusiviteit is de kwestie van de minderheden nog steeds een bron van spanningen. Bovendien maakt de terreurbeweging Islamitische Staat ook gebruik van de instabiliteit van het land om zijn activiteiten weer te ontplooien.

Irak: interne politieke conflicten

Irak daarentegen heeft verder te kampen met interne politieke conflicten: conflicten tussen de verschillende etnisch-sektarische groeperingen; relaties met de Autonome Regio Koerdistan (waaronder de economische problematieken, onder meer in verband met de olie-inkomsten); invloed van de pro-Iraanse milities, enz. Vanwege deze interne uitdagingen heeft het land geprobeerd zich afzijdig te houden van het Israëlisch-Iraanse conflict, een allesbehalve vanzelfsprekende poging, gelet op de aanwezigheid van tal van milities die aan de kant van Iran staan. De Iraakse verkiezingen, waarvan de grote opkomst verbazing heeft gewekt, zijn vlot verlopen. Het resultaat van de verkiezingen heeft de traditionele politieke elite opnieuw aan de macht gebracht. Na de verkiezing van de voorzitter van het parlement op 29 december 2025 zijn de onderhandelingen aan de gang voor de vorming van een regering.

Heel wat staten in de regio doen hun uiterste best om de verspreiding van de instabiliteit naar hun grondgebied zo veel mogelijk te voorkomen. De Iraanse en Israëlische aanvallen tegen Qatar in 2025 tonen aan dat verschillende staten, waaronder de Golfstaten, zich in het centrum van de regionale dynamiek bevinden, ondanks alle pogingen om niet meegesleurd te worden in het conflict.

Na meer dan twee jaar oorlog lijkt het conflict tussen Israël en Hamas, dat gevolgen had voor de hele regio, zich te ontwikkelen in de richting van onderhandelingen, na het op 30 september 2025 door president Trump aangekondigde akkoord over een staakt-het-vuren. De situatie blijft echter zeer broos wegens tal van interne en externe factoren.

Conflict tussen Rusland en Oekraïne : droneoorlog en geopolitieke onzekerheid

De Russische regering voorzag voor het jaar 2025 een recordbedrag voor de oorlog tegen Oekraïne.

Militaire uitgaven en interne veiligheid bedroegen meer dan 43% van de officiële staatsuitgaven. Dit geeft aan dat de oorlog de absolute prioriteit bleef voor het Kremlin, ondanks hoge verliezen aan het front, toenemende problemen voor de Russische economie en stelselmatige tekorten in de begroting.

De twijfelende houding van Amerikaans president Donald Trump tegenover Rusland en zijn wisselende standpunten over de oorlog en onderhandelingen hebben binnen het Westerse kamp geleid tot enerzijds hoge politieke druk en verwachtingen en anderzijds onzekerheid en verdeeldheid over de juiste aanpak. Desalniettemin weigerde de Russische president Poetin enige vorm van compromis en hield hij vast aan zijn maximale eisen ondanks de sterke toename van de Amerikaanse druk op Oekraïne om concessies te doen en de relatief voordelige voorstellen aan Rusland.

De evolutie van drone-aanvallen

De evolutie naar het gebruik van meer geavanceerde en massale drone-aanvallen heeft zich in 2025 voortgezet. De inzet van verkennings- en aanvalsdrones maakte grootschalige grondaanvallen zonder zware verliezen onmogelijk, terwijl traditionele verdedigingslinies werden vervangen door verspreide en gedecentraliseerde troepen en materieel. De continue aanwezigheid van drones zorgde voor een permanente dreiging voor zowel militairen als de overblijvende burgers nabij de frontlinie.

Bescheiden Russische doorbraak

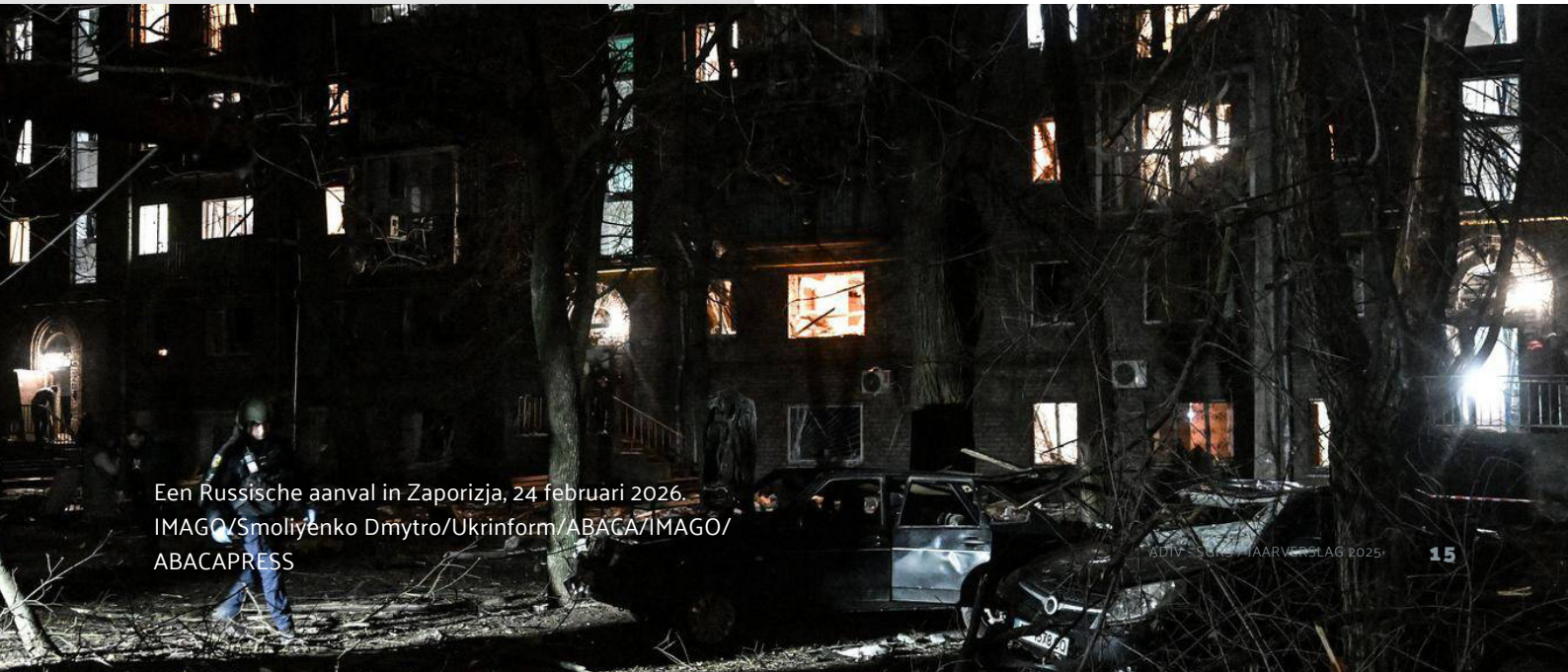
Rusland won langzaam maar gestaag terrein, wel ten koste van enorm hoge verliezen aan voornamelijk militair personeel. De Russische opmars was vooral geconcentreerd in delen van de Donbas en de Zaporizja regio, waar het met verhoogde inzet en intensief gebruik van drone-eenheden terrein probeerde te winnen.

Oekraïne van zijn kant had duidelijk problemen met personeelstekorten. Hoewel de Russische terreinwinsten in 2025 substantiëler waren dan in voorgaande periodes, was Oekraïne echter nog steeds in staat om stevig weerwerk te leveren en zijn tactiek van het ruilen van grondgebied voor hoge Russische verliezen toe te passen.

Luchtcampagnes

Naast de aanhoudende gevechten aan het front, richtten beide partijen zich steeds meer op luchtcampagnes om de tegenstander zo veel mogelijk te destabiliseren. Rusland richtte zich vooral op de Oekraïense energie-infrastructuur in de hoop de Oekraïense bevolking te demoraliseren en letterlijk in de kou te zetten. Ondanks de nijpende humanitaire situatie in sommige steden, leken deze aanvallen voorlopig weinig tastbaar effect te hebben op het moreel van de bevolking.

Oekraïne bleef ondertussen Russische raffinaderijen en de petroleum-infrastructuur maar ook de Russische olie-exportcapaciteit (inclusief schaduwvloot) bestoken. Deze succesvolle campagne trof naar schatting al meer dan 20% van de totale Russische raffinagecapaciteit en zorgde voor disrupties in de olie-export. Hoewel de directe impact voor de situatie aan het front hiervan beperkt is, zetten deze aanvallen Rusland wel verder onder druk.



Een Russische aanval in Zaporizja, 24 februari 2026.
IMAGO/Smoliyenko Dmytro/Ukrinform/ABACA/IMAGO/ABACAPRESS

Afrika : ontwikkelingen in het gebied van de **Grote Meren**

Het jaar 2025 kende een dramatische start in de regio van de Grote Meren, en met name in het oosten van de Democratische Republiek Congo, met de inname van de provinciehoofdsteden Goma in januari en Bukavu in februari door de door Rwanda gesteunde rebellen van de Alliance Fleuve Congo (AFC)/Mouvement du 23 mars (M23).

Ondanks de urgentie blijven humanitaire corridors een theoretisch concept.

De inname betekende ook dat de internationale luchthaven van Goma onbruikbaar werd voor het sturen van humanitaire hulp, en dit tot nader order. Ondanks de hoge nood, blijven humanitaire corridors een theoretisch concept.

De gebeurtenissen in Oost-Congo zorgden voor nervositeit in Kinshasa en leidden tot de bestorming van de Belgische ambassade eind januari 2025.

Een ander gevolg van de gebeurtenissen in Oost-Congo voor ons land was de beslissing van de Rwandese autoriteiten om de diplomatieke banden met België te verbreken. Via (veelal Rwandese) sociale media-accounts werd desinformatie over de militaire aanwezigheid van België in Congo verspreid.

Vredesproces

Een nieuwe dynamiek in het vredesproces leidde tot een formeel akkoord tussen Congo en Rwanda, ondertekend in Washington, DC, op 27 juni 2025, en herbevestigd door de presidenten van beide landen op 4 december 2025. Parallelle gesprekken tussen de regering in Kinshasa en de AFC/M23 rebellen werden opgestart in Doha, in de hoop dat deze leiden tot een permanent staakt-het-vuren. Ondanks deze diplomatieke inspanningen blijft de situatie op het terrein in Oost-Congo fragiel. Een mogelijke regionale escalatie van het conflict blijft eveneens een bezorgdheid, gezien de militaire aanwezigheid van zowel Burundi als Oeganda in Oost-Congo.

De Sahel: toename van religieus terrorisme

Religieus-geïnspireerd terrorisme blijft de meest acute dreiging voor West-Afrika. Rond het Tsjaadmeer controleert Islamic State West Africa Province (ISWAP) een gebied dat driemaal zo groot is als België. Het is de belangrijkste IS-groep ter wereld na de nederlagen van IS elders. ISWAP probeert een brug te maken naar het grensgebied tussen Mali en Niger, waar Islamic State Sahel Province (ISSP) opereert. Het aan al-Qaeda gelieerde Jama'at Nusrat al-Islam wa al-Muslimin (JNIM) is echter de dominante terreurgroep in de Sahel. De groepering is volop zijn territorium aan het uitbreiden in Mali en Burkina Faso, Noord-Benin en Noordwest Nigeria. De groepering is verantwoordelijk voor de blokkade rond de Malinese hoofdstad Bamako.

In de Sahellanden zien we een stelselmatige achteruitgang in democratie en vrijheden, gekoppeld aan een antiwesters narratief. Dit is in het bijzonder het geval voor de drie junta's die de Confederatie van Sahellanden (AES) vormen, in casu Mali, Burkina Faso en Niger waar Rusland (en China) een serieuze voet aan de grond krijgt. Rusland kiest evenwel voor de uitbating van minerale rijkdommen en een ondersteuning van de regimes, en niet voor een effectieve bijdrage in de strijd tegen terrorisme. De terroristische groeperingen drijven de drie AES junta's steeds meer in het nauw.

Global Outreach Intelligence : een toegenomen mondiale concurrentie

Het bureau Global Outreach Intelligence (GOI) van de ADIV analyseert de supranationale fenomenen die de regionale kaders overstijgen.

In 2025 wordt de internationale context gekenmerkt door een ingrijpende transformatie: de internationale betrekkingen, die lange tijd gebaseerd waren op een evenwicht tussen coöperatie en concurrentie, verschuiven naar een logica van algemene concurrentie, soms zelfs tot confrontatie.

Fragmentering van de wereldorde

De grote mogendheden wedijveren met elkaar op verschillende gebieden - technologie, energie, zeldzame metalen, strategische allianties - waardoor de fragmentering van de wereldorde vergroot. De conflicten in Oekraïne en in de Gazastrook ondermijnen de westerse geloofwaardigheid, terwijl het Globale Zuiden zijn wil om de internationale orde te “ontwesteren” te kennen geeft.

De alternatieve fora in opmars

Deze beweging uit zich in de versterking van alternatieve fora, zoals de BRICS+ en de Shanghai-samenwerkings-organisatie (SSO), waarvan de uitbreidingen en mediatisering hun aantrekkelijkheid illustreren. Hoewel ze allesbehalve een homogeen blok vormen, betwisten deze actoren de liberale orde en eisen ze een multipolair systeem.

China: centrale speler in een nieuw evenwicht

Als pijler van beide organisaties vergroot China zijn invloed door een alternatief voor de wereldorde voor te stellen. Deze dynamiek intensiveert de strategische concurrentie tussen de Verenigde Staten, China en Rusland en doet het gewicht van de autoritaire regimes toenemen. De staten van het Zuiden worden strijdtonelen voor invloed en proxyoorlogen.

Instabiliteit en hybride dreigingen

De rivaliteit blijft niet beperkt tot de economie of de politiek: ze is ook identitair en normatief, waarbij elke mogendheid ernaar streeft haar regels en beschavingsmodel op te leggen. Deze systemische transitie leidt tot instabiliteit, terug-kerende crisissen en spanningen op energiegebied, terwijl de grens tussen oorlog en vrede vervaagt. De hybride dreigingen tegen de westerse landen worden erdoor versterkt.

De **hybride dreiging** in het hart van onze samenlevingen

De Russische hybride dreiging vormt vandaag nog steeds een van de meest complexe uitdagingen voor de Europese veiligheid. Deze dreiging beperkt zich niet tot het slagveld, maar combineert militaire en niet-militaire middelen om westerse samenlevingen te verzwakken, politieke cohesie te ondermijnen en internationale hulpstromen richting Oekraïne en andere kwetsbare regio's te verstoren.

Ook België, als NAVO-lid en logistiek doorvoerland, werd nog steeds volop geconfronteerd met cyberaanvallen, spionagepogingen, sabotage, desinformatie en maritieme verkenningen langs kritieke infrastructuur.

Naast onze diplomatieke en logistieke knooppuntpositie zijn ook de recente investeringen in de modernisering van onze Defensie van belang voor de tegenpartij. Enerzijds betekent dit een versterking van de collectieve afschrikking op de oostflank van Europa ten opzichte van Rusland, anderzijds biedt de modernisering van Defensie een opportuniteit voor Rusland om spionageactiviteiten te voeren betreffende onze technologische capaciteiten, logistieke processen en onze industriële partnerschappen.

« Insider threat »

De bescherming van onze belangen vereist strikte toegangsbeperkingen tot gevoelige installaties, documentatie en informatiestromen. De voorbije jaren werden we geconfronteerd met verschillende incidenten waarbij onder meer individuen zich ongeoorloofde toegang trachten te verschaffen tot de installaties van Defensie. En ook verschillende spionageactiviteiten zoals spotting en drone overvluchten van gevoelige installaties.

Deze bedreigingen komen niet enkel van buiten onze organisatie. De insider threat is mogelijks de gevaarlijkste dreiging waar we in het heden met geconfronteerd worden. In eerste instantie worden onze militairen benaderd door derde partijen met het oog op het ongeoorloofd bekomen van informatie. Anderzijds vormt het gebrek aan security awareness en het laks omspringen met de opgelegde restricties door onze personeelsleden de grootste zwakte in ons veiligheidsdispositief.

De adviezen van Militaire Veiligheid beogen niet alleen het opleggen en controleren van restricties, maar ook het beperken van aansprakelijkheid bij veiligheidsincidenten. Uiteindelijk is veiligheid een collectieve verantwoordelijkheid, waarbij het professionalisme van elk personeelslid, militair of burger, de belangrijkste bouwsteen vormt.

Een **nieuwe impuls** voor de **Europese defensie**-industrie ?

In maart 2025 heeft de EU “ReArm Europe” aangekondigd, een grootschalig investeringsplan van 800 miljard euro om de Europese defensie-industrie een nieuwe impuls te geven. België blijft niet achter, met een verhoging van de defensiebegroting en tal van federale en regionale initiatieven voor de financiering van militaire onderzoeks- en ontwikkelingsprojecten.

Bescherming van de defensie-industrie

De ADIV komt in actie bij de bescherming van deze defensie-industrieën en van deze onderzoeksprojecten tegen spionage, inmenging en disruptie. De ADIV heeft al kunnen voorkomen dat bedrijven, die onder controle staan van vijandige naties, toegang krijgen tot deze onderzoeksprogramma’s en is van mening dat deze projecten nog steeds een zekere belangstelling zullen wekken bij inlichtingenofficieren van allerlei slag. Dankzij het werk van de ADIV op dat gebied kan niet alleen de ongewenste overdracht van technologieën worden vermeden, maar kan ook de reputatie van onze defensie-industrie en onze onderzoekscentra worden beschermd.

Toename van de kwetsbaarheid voor spionage

De steeds vager wordende grens tussen militaire en civiele technologie is een betrekkelijk nieuwe tendens die de zaken nog ingewikkelder maakt. Drones zijn daarvan een voor de hand liggend voorbeeld, met de kleine FPV-drones (first-person view) die oorspronkelijk louter voor civiel gebruik waren bestemd en die thans een van de meest gebruikte wapens in Oekraïne zijn. Bijgevolg richten veel oorspronkelijk louter “civiele” ondernemingen zich op militaire onderzoeks- en ontwikkelingsprogramma’s, want hun technologie blijkt interessant te zijn vanuit militair oogpunt. En laten we niet uit het oog verliezen dat er aanzienlijke budgetten beschikbaar zijn. Bovendien vinden enorm veel ontwikkelingsprojecten plaats volgens het “triple helix”-principe, wat een samenwerking tussen de private sector, de publieke sector en universiteiten/onderzoekscentra impliceert. Hoewel deze integratie van verschillende actoren zeer nuttig is om de innovatie en de ontwikkeling te versnellen, dient te worden vastgesteld dat ze de kwetsbaarheid voor spionage en inmenging vergroot. De betrokkenheid van meer entiteiten en personen, waarvan sommige niet noodzakelijk de “veiligheidscultuur” bezitten, vergroot logischerwijs de mogelijkheden voor vijandige diensten om actie te ondernemen.

Technologische en economische afhankelijkheid

Wat de rechtstreekse investeringen in het buitenland betreft, toont het voorbeeld van Nexperia aan dat een volledige economische sector gedestabiliseerd kan worden door het verlies van de controle van een enkele strategische onderneming in de bevoorradingsketen. Dezelfde problemen rijzen ook, wanneer wij afhangen van een andere staat voor een technologie die onontbeerlijk is voor een economische sector. Het is dan ook terecht dat de ADIV, samen met zijn nationale partners, meewerkt aan de screening van buitenlandse investeringen.

Anticiperen op **dreigingen** tegen **Belgische belangen**

Om te anticiperen op eventuele maatregelen van het Ministerie van Defensie en de regering te adviseren over haar binnenlands en buitenlands veiligheids- en defensiebeleid, volgt de ADIV, voor zover haar middelen dat toelaten, alle spanningen in de wereld die van invloed kunnen zijn op de nationale veiligheid en de Belgische belangen op.

Deze monitoring gebeurt vanuit een 360°-benadering, die zowel multidisciplinair als multidimensionaal is, om te anticiperen op bedreigingen voor de Belgische belangen. Zo past het de ASCOPE-PMESII-benaderingen toe (Zone, structuur, capaciteiten, organisatie, personen, gebeurtenissen – politiek, militair, economisch, sociaal, informatie, infrastructuur), maar ook multidimensionaal (de dimensies land/lucht/zee/ruimte/cyber).

Buitenlandse inlichtingendienst

Hoewel dit niet uitdrukkelijk in zijn wettelijk kader is vastgelegd, vervult de ADIV de facto de rol van buitenlandse inlichtingendienst. Het is immers de enige Belgische speler die over aanzienlijke en ingrijpende middelen voor het verzamelen van informatie in het buitenland beschikt, zowel vanuit juridisch oogpunt als wat betreft de technische (CYBER, SIGINT, IMINT, enz.) en personele capaciteiten (netwerken van bronnen en de aanwezigheid van militairen overal ter wereld).

Er doen zich nieuwe behoeften voor, zoals het voeren van een agressief economisch beleid (verhoging van de douanerechten) of het nastreven van annexatieplannen (Groenland). Of nog: het ontstaan van dreigingen in de ruimte (aanvallen op de Galileo-satellieten) die mogelijk grote gevolgen hebben voor het Koninkrijk.

Gezien de recente ontwikkelingen en de aanhoudende hybride oorlog is het voor België van belang te beschikken over een sterke buitenlandse inlichtingendienst die in staat is om ontwikkelingen in de wereld op te volgen die van invloed kunnen zijn op de Belgische belangen. Onze nationale veiligheid en onze strategische autonomie staan op het spel.

De ADIV is dan ook van plan om deze nieuwe externe dreigingen in de gaten te houden, voor zover het wettelijk kader daarvoor geschikt is. Uiteraard wordt er alles aan gedaan om extra personeel met specifieke vaardigheden aan te trekken en om te beschikken over de allernieuwste technologische apparatuur.

Cyber Rapid Response Teams : Europese samenwerking in actie

Binnen 72 uur reageren: Europese cyberteams in actie

In het kader van het Europese veiligheids- en defensiebeleid zijn er verschillende projecten lopende via permanente gestructureerde samenwerking (PESCO) om gezamenlijk capaciteiten op het gebied van defensie binnen de EU op te bouwen. Een van die projecten is het PESCO CRRT project (Cyber Rapid Response Team).

België neemt het voortouw

In 2025 nam België het voorzitterschap in handen, wat in praktijk wordt uitgevoerd door het Cyber Command van de ADIV. Naast het organiseren van een council meeting, met een bijhorende cyber-oefening, was België in 2025 ook verantwoordelijk voor het operationeel opvolgen van de verschillende activaties van het CRRT. Dit houdt onder meer ook in dat België de teamleader levert tijdens de activatie.

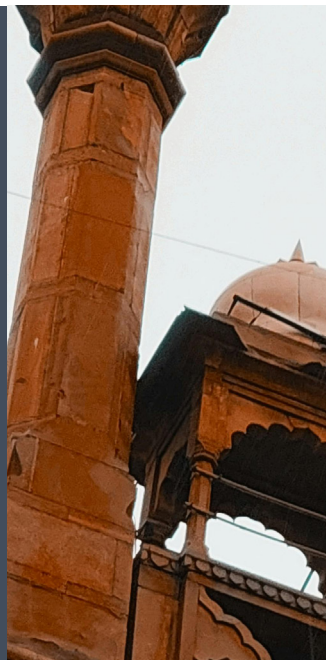
Inzet in Somalië en Moldavië

In 2025 werd het CRRT onder Belgische begeleiding ontplooid in Somalië. Daar voerden ze cyber security operaties uit in ondersteuning van European Union Training Mission Somalia op het lokale EUTM netwerk om zo aanbevelingen en advies te kunnen geven om de beveiliging te verbeteren. Een tweede ontplooiing volgde in steun van de overheid van Moldavië. Gezien de geopolitieke situatie moest het verkiezingsnetwerk geanalyseerd worden. Een internationaal team van experten, onder leiding van het Cyber Command, was in staat om de overheid bij te staan zodat de verkiezingen correct konden plaatsvinden.

Van het internationale toneel naar nationale veerkracht

De ervaring die wordt opgedaan in dit internationale kader, niet alleen op het gebied van processen, maar ook op het gebied van uitrusting en kennis, is waardevol voor het ontwikkelen van Cyber Rapid Response Teams in een nationaal kader. Snel kunnen ingrijpen in geval van crisis of conflict zal essentieel zijn om onze bewegingsvrijheid in cyberspace te garanderen. Het is daarom het doel om op termijn verschillende Cyber Rapid Response Teams beschikbaar te hebben binnen het Cyber Command.

Versterking van de **defensie-samenwerking** tussen **België** en **India**



De opkomst van India als geopolitieke macht is een van de bepalende kenmerken geworden van de verschuivende wereldorde in de 21ste eeuw. Als 's werelds grootste democratie en een van de snelst groeiende economieën transformeert India gestaag van een regionale speler tot een centrale speler die het machtsevenwicht in Azië en de Indo-Pacifische regio mee vormgeeft.

In het afgelopen decennium heeft New Delhi een assertiever en onafhankelijker buitenlands beleid gevoerd, waarbij het zijn partnerschappen probeert te diversifiëren terwijl het zijn strategische autonomie bewaart. Deze herkalibratie weerspiegelt de bredere ambitie van India om zijn eigen koers te varen op het wereldtoneel en wordt gekenmerkt door zowel samenwerking als occasionele wrijving met traditionele partners zoals de Verenigde Staten.

Het strategische en commerciële belang van New Delhi

Het strategische belang van India reikt veel verder dan alleen de economie. Door zijn ligging, die Zuid-Azië, de Indische Oceaan en de Indo-Pacifische regio met elkaar verbindt, is het land een belangrijke stakeholder in de regionale stabiliteit. Nu de spanningen in de Indo-Pacifische regio toenemen en de invloed van China groeit, krijgt de diplomatieke en militaire positie van India wereldwijd meer aandacht. De inspanningen van de Europese Unie om tegen het einde van het jaar een vrijhandelsovereenkomst met India te sluiten, duiden op een bredere erkenning van het potentieel van New Delhi als zowel een commerciële als strategische partner.

Diversificatie van partnerschappen op defensiegebied

Tegelijkertijd staat India voor dringende uitdagingen op het gebied van de modernisering van zijn defensie. New Delhi, dat lange tijd afhankelijk was van Russische wapenleveringen, wordt nu geconfronteerd met verstoringen in de aanvoer en verschuivingen in de geopolitieke verhoudingen als gevolg van de oorlog in Oekraïne. Deze situatie heeft India ertoe aangezet om zijn defensiepartnerschappen sneller te diversifiëren, wat nieuwe mogelijkheden voor samenwerking met Europese industrieën heeft gecreëerd. Belgische defensiebedrijven hebben onder meer al voet aan de grond gekregen op de Indiase markt door geavanceerde technologieën en veilige toeleveringsketens aan te bieden die aansluiten bij de doelstellingen van India op het gebied van zelfredzaamheid en capaciteitsversterking.

In dit veranderende landschap beschouwt Brussel New Delhi niet alleen als een belangrijke speler in het handhaven van stabiliteit in de Indo-Pacifische regio, maar ook als een cruciale partner in het bevorderen van technologische innovatie en industriële weerbaarheid. Als onderdeel van deze groeiende erkenning streeft België ernaar de bilaterale banden te verdiepen door de samenwerking met India op het gebied van bewapening en militaire samenwerking uit te breiden.

Defensieattachépost geopend in New Delhi

Om alle samenwerkingen nog meer te versterken, heeft de ADIV sinds september 2025 een defensieattaché (DA) op post geplaatst in New Delhi: brigadegeneraal Engels, met Adjudant Mertens als secretaris.

De benoeming van een defensieattaché door België in India is een concrete stap in de richting van samenwerking tussen beide landen. Een dergelijke functie zal een directe dialoog tussen defensie-instellingen vergemakkelijken en gezamenlijke projecten tussen Belgische en Indiase bedrijven ondersteunen. Naast de industriële dimensie zal dit ook het wederzijds begrip en de samenwerking tussen de strijdkrachten van beide landen versterken, wat zal bijdragen tot een hechtere en duurzamere defensierelatie.

FOD Buitenlandse Zaken : een belangrijke partner in de nationale veiligheidsstrategie

In een bijzonder gespannen geopolitieke context (toename van gewapende conflicten, opkomst van autoritaire regimes, verzwakking van multilaterale allianties, toename van hybride dreigingen) wil de Arizona-regering België herpositioneren als strategische speler in Europa.

De FOD Buitenlandse Zaken, die zowel een instrument voor het uitdragen van soft power is als een veiligheidsactor, speelt een bepalende rol in de formulering en uitvoering van de nationale veiligheidsstrategie. De strategische complementariteit van Buitenlandse Zaken en de ADIV, de twee Belgische instellingen bij uitstek die buiten het nationale grondgebied actief zijn, kan vandaag de dag niet duidelijker zijn!

In de regel bestaat de samenwerking tussen beide instellingen met name uit:

1. De organisatie van briefings voor diplomaten, voorafgaand aan hun aanstelling, om hen bewust te maken van de geostrategische en veiligheidsuitdagingen voor hun verantwoordelijkheidsgebied.
2. De samenwerking in het gebied, binnen de diplomatieke posten, via het netwerk van defensieattachés en diplomatieke posten.
3. Uitwisseling van informatie (specifieke verzoeken, ontmoetingen tussen analisten, interdepartementale vergaderingen, debriefing van diplomaten ...) om de informatiepositie te voeden en de contra-inmengingshouding van onze respectieve diensten te versterken.
4. Ondersteuning door de cybercapaciteit van de ADIV, zowel voor bewustmaking van de risico's in cyberspace als voor het identificeren van de actoren achter cyberaanvallen.
5. De uitvoering van "sweepings", d.w.z. grondige inspectie van lokalen vóór gevoelige ontmoetingen en/of geclassificeerde vergaderingen van beide instellingen om te controleren of er geen afluisterapparatuur aanwezig is.

In 2025 werd de versterking van de synergieën en de samenwerking tussen Buitenlandse Zaken en Defensie bekroond met de ondertekening (NB: nog niet ondertekend op de datum van opstelling, 24 Okt 2025) van een kaderovereenkomst met een reeks technische bijlagen waarin de ADIV specifiek betrokken is. Tot de verwachte ontwikkelingen behoren een betere mobiliteit van het personeel tussen de respectieve diensten en een grotere mobilisatie van de diplomatieke netwerken om de informatiepositie te versterken.

Na een cyberaanval die het netwerk van Belgische ambassades in 2019 zwaar trof en waardoor meer dan honderd servers in het buitenland gedurende meerdere dagen moesten worden losgekoppeld, heeft de FOD Buitenlandse Zaken een "Masterplan Cybersecurity" opgesteld. De cybercapaciteit van de ADIV levert een actieve bijdrage aan dit plan, met inbegrip van de jaarlijkse bijwerking ervan, met name door beoordelingen te leveren met het oog op de aanpassing van de instrumenten en processen. In 2024 werden meer dan 19.000 cyberincidenten geregistreerd, waarvan er meer dan 1.100 als hoog risico werden geclassificeerd. Vier van deze incidenten waren waarschijnlijk specifiek gericht tegen de FOD Buitenlandse Zaken, maar werden tijdig geblokkeerd en hadden geen nadelige gevolgen voor de diensten van de FOD.

Veiligheidsverificaties : een bolwerk tegen dreigingen

Veiligheidsverificaties verzekeren dat ieder persoon die toegang krijgt tot een gevoelige zone of functie, de nodige garanties biedt om de staat en de bevolking te beschermen. Deze controles gaan verder dan het kader van Defensie: de vraag neemt toe, de sectoren diversifiëren en de analyses worden complexer, in een context die gekenmerkt wordt door de opkomst van extremisme en hybride dreigingen.

Een grotere rol

De ADIV is actief op verschillende gebieden: luchthavens, havens, gevangenissen, centrales, douane, NMBS... De dienst adviseert de HR-afdeling van Defensie bij de aanwerving van militairen en burgers en controleert bedrijven die verantwoordelijk zijn voor gevoelige infrastructuur. De samenwerking met de federale politie en de VSSE (Veiligheid van de Staat) wordt intensiever om sneller en efficiënter te kunnen optreden.

Deze verificaties maken het mogelijk kritieke scenario's te voorkomen: een havenarbeider die betrokken is bij drugshandel, een hacker die klaarstaat om een spoorwegnetwerk lam te leggen of een infiltrant in een overheidsdienst.

Kerncijfers 2025

7000
militaire kandidaten geanalyseerd

700
burgers geanalyseerd

200
negatieve militaire adviezen

11
geweigerde burgers

10000
Toegansaanvragen van bedrijven

5,5%
geweigerd

Veiligheidsmachtigingen: strikt gecontroleerde toegang

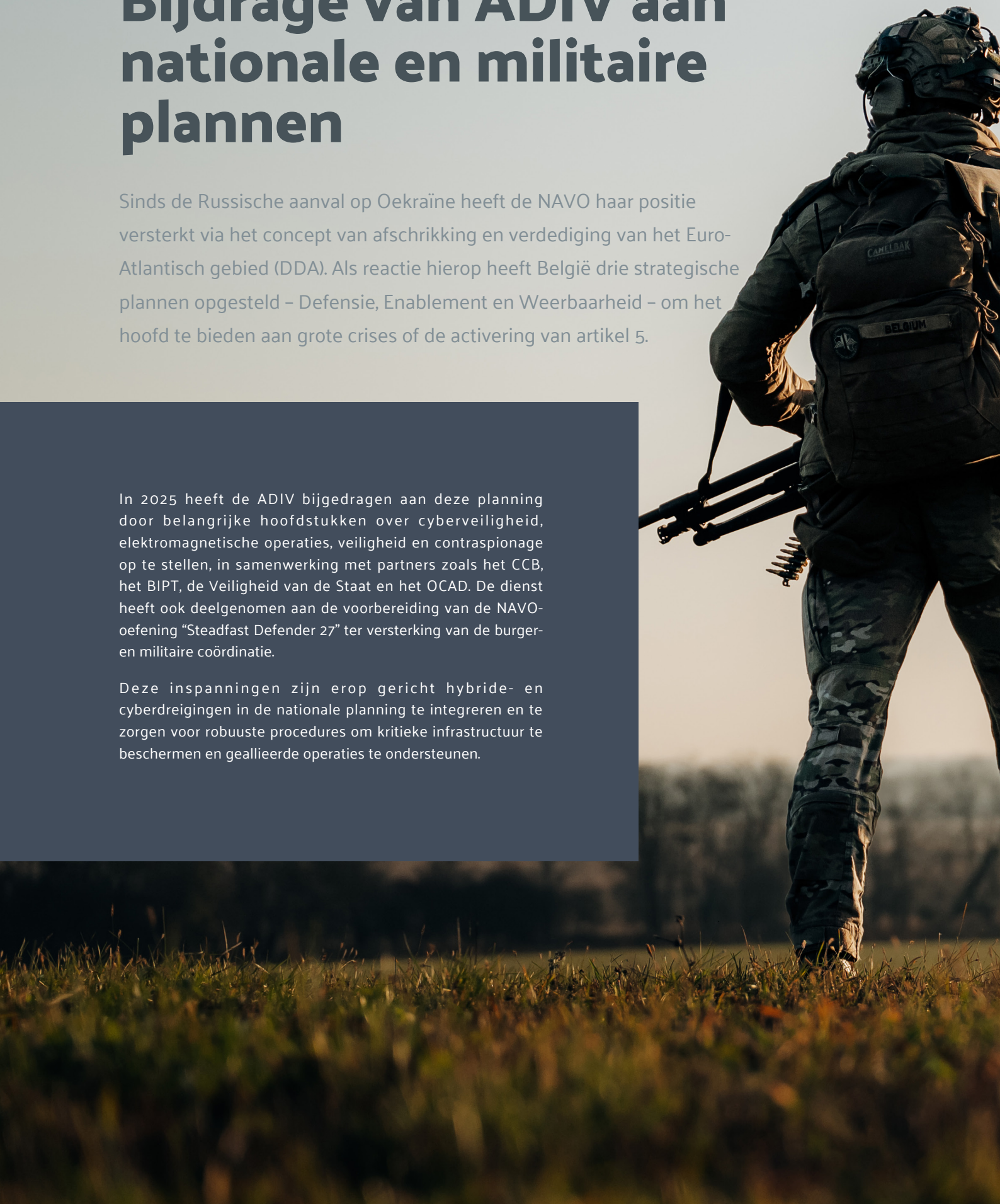
Een veiligheidsmachtiging geeft toegang tot geclassificeerde zones, netwerken en documenten, volgens het "need-to-know"-principe. In 2025:

17 000 onderzoeken voor **26 000** entiteiten

Veelvoorkomende problemen : **financiën, drugs, alcohol, extremisme, geweld, fraude**

Bijdrage van ADIV aan nationale en militaire plannen

Sinds de Russische aanval op Oekraïne heeft de NAVO haar positie versterkt via het concept van afschrikking en verdediging van het Euro-Atlantisch gebied (DDA). Als reactie hierop heeft België drie strategische plannen opgesteld – Defensie, Enablement en Weerbaarheid – om het hoofd te bieden aan grote crises of de activering van artikel 5.



In 2025 heeft de ADIV bijgedragen aan deze planning door belangrijke hoofdstukken over cyberveiligheid, elektromagnetische operaties, veiligheid en contraspionage op te stellen, in samenwerking met partners zoals het CCB, het BIPT, de Veiligheid van de Staat en het OCAD. De dienst heeft ook deelgenomen aan de voorbereiding van de NAVO-oefening “Steadfast Defender 27” ter versterking van de burger- en militaire coördinatie.

Deze inspanningen zijn erop gericht hybride- en cyberdreigingen in de nationale planning te integreren en te zorgen voor robuuste procedures om kritieke infrastructuur te beschermen en geallieerde operaties te ondersteunen.

De Belgische industrie **wapent zich**

Verbeterde beveiliging van bedrijven in de defensiesector

In 2025 heeft het Bureau Industrie zijn inspanningen opgevoerd om Belgische bedrijven die met Defensie samenwerken, te beschermen tegen toenemende dreigingen zoals cyberaanvallen, economische spionage en fysieke inbraken. Deze opdracht werd uitgevoerd in nauwe samenwerking met de Nationale Veiligheidsoverheid (NVO), de veiligheidsofficieren van bedrijven en internationale partners.

Het Bureau hield toezicht op de veiligheidsmachtigingen voor meer dan 1.000 bedrijven die betrokken zijn bij nationale en internationale projecten (NAVO, EU, Gezamenlijke Organisatie voor Samenwerking op Defensiematerieelgebied) en zag tegelijkertijd toe op de naleving van de fysieke veiligheidsnormen. Het organiseerde ook een tiental bewustmakingssessies over cyberveiligheid, de bescherming van geclassificeerde informatie en de veiligheid van gevoelige infrastructuren, en verleende ondersteuning bij het opstellen van bestekken voor geclassificeerde contracten.

Internationale samenwerking en rol als aangewezen instantie

Als “Designated Security Authority” heeft het Bureau de uitwisseling van gevoelige documenten vergemakkelijkt en deelgenomen aan internationale werkgroepen, met name in het kader van Europese defensieprojecten (Europees Defensiefonds). Het heeft ook gerichte aanbevelingen verspreid over perimeterbeveiliging, cyberveiligheid tijdens verplaatsingen, overeenstemming met EDF-projecten en de toenemende dreiging van drones.

Kerncijfers 2025

1500
bezoekaanvragen (Request For Visit)

200
afgegeven machtigingen voor bedrijven (+25 % ten opzichte van 2024)

Door strategische samenwerking op de dreiging anticiperen

Gezien de toename van hybride dreigingen heeft het Bureau Industrie de samenwerking met strategische bedrijven versterkt om op technologische en geopolitieke ontwikkelingen te anticiperen en een hoog beschermingsniveau te handhaven.

België verwelkomt zijn **eerste F-35-vliegtuig**

Op 13 oktober 2025 werd een historische mijlpaal bereikt met de aankomst van de eerste F-35A Lightning II-gevechtsvliegtuigen op de luchtmachtbasis van Florennes. Deze gebeurtenis markeert het begin van de inzet van het meest geavanceerde wapensysteem van de Belgische luchtmacht boven ons grondgebied.

In de aanloop naar deze “First Aircraft Arrival speelde” het “Special Access Program Central Office” (SAPCO) van de afdeling Veiligheid een sleutelrol. Het SAPCO heeft het lokale veiligheidsteam in Florennes intensief begeleid om een veilige en conforme ontvangst van het vliegtuig te garanderen. Dit omvatte met name ondersteuning bij de installatiewerkzaamheden door Lockheed Martin, het opstellen van procedures en richtlijnen voor de operationele veiligheid, maar ook de verdere voorbereiding van de infrastructuur en de veiligheidssystemen, evenals de permanente coördinatie met de Amerikaanse partners van het USA Joint Program Office en de Program Security Officer.

SAPCO fungeert als enige schakel tussen de Belgische luchtmacht en de verschillende gespecialiseerde diensten binnen de ADIV. De succesvolle ontvangst van het eerste F-35-toestel bevestigt niet alleen de technische en operationele paraatheid van Defensie, maar ook het strategische belang van SAPCO als centrale coördinator van alle veiligheidsgerelateerde aspecten binnen het Belgische F-35-programma.

De eerste TACSAPF F-35 container

De TACSAPF biedt een geavanceerde oplossing voor militaire operaties waarbij snelheid, veiligheid en flexibiliteit vereist zijn. Deze containers zijn ontworpen om snel inzetbaar te zijn onder zware omstandigheden en voldoen aan de strengste veiligheidseisen die gelden voor het gebruik van de F-35. De containers beschikken over specifieke functionaliteiten zoals beveiliging, missieplanning en IT-ondersteuning. Dankzij hun modulaire ontwerp kunnen ze eenvoudig worden aangepast aan diverse operationele behoeften.

Elektromagnetische afscherming

Alle TACSAPF-containers zijn voorzien van een elektromagnetische afscherming die bescherming biedt tegen elektronische aanvallen en storingen. Bovendien beschikken ze over autonome systemen zoals CBRN-bescherming (chemisch, biologisch, radiologisch en nucleair), inbraakdetectie, brandbeveiliging en toegangscontrole, waardoor ze zelfstandig kunnen functioneren zonder afhankelijk te zijn van externe infrastructuur.

De combinatie van snelle inzetbaarheid, robuuste bescherming en grote aanpasbaarheid maakt de TACSAPF tot een essentieel instrument voor moderne militaire missies met de F-35, waarbij betrouwbaarheid en operationele paraatheid van cruciaal belang zijn.

Operationele doelstelling

De eerste volledige partij van vijftien containers wordt eind december geleverd aan de Tweede Wing in Florennes. Dit is het mooie resultaat van een intensieve periode waarin in amper anderhalf jaar tijd niet alleen de volledige Amerikaanse design review is afgerond, maar ook de productie – met haar strenge veiligheidsvoorschriften – en de levering zijn geconsolideerd. De volgende stap bestaat erin de TACSAPF te laten accrediteren voor operationeel gebruik en deze in te zetten tijdens een eerste inzet in het eerste kwartaal van 2026.

Militaire veiligheid : de **veiligheid** van de **Defensie-infrastructuur** waarborgen

Militaire veiligheid vormt de ruggengraat van de bescherming van Defensie tegen interne en externe dreigingen, zodat operaties efficiënt en veilig kunnen verlopen. Een echte “Security by design”-aanpak zal op termijn de militaire veiligheid aanzienlijk verbeteren.

De aanleg van nieuwe infrastructuur in de gebouwen van Defensie vereist meer organisatie dan alleen het fysieke bouwproces. In dit verband volgt de ADIV tientallen projecten op de voet en houdt zij ook toezicht op de veiligheidsvoorschriften. Denk bijvoorbeeld aan het nieuwe hoofdkwartier, de CAMO-infrastructuur, de nieuwe Medhub en de marinebasis in Zeebrugge.

Van de Ardennen tot aan de kust, van Aarlen tot Oostende, is de militaire veiligheidsdienst hierbij betrokken. Elk nieuw project brengt dan ook zijn eigen uitdagingen en zijn eigen tijdschema met zich mee.

Vanaf het moment dat wij bij de beginfase betrokken raken, is er altijd sprake van intensieve begeleiding met coaching.

Een van de belangrijkste doelstellingen is om actief te blijven zoeken naar innovatieve oplossingen voor de veiligheidsuitdagingen van de toekomst. Ten slotte streven we ernaar de kloof tussen de regelgeving en de concrete problemen in de praktijk zo veel mogelijk te verkleinen.

M940 Oostende, het eerste schip van de nieuwe generatie mijnenjagers.

De mens als eerste verdedings-linie

In 2025 heeft de ADIV zijn netwerk van HUMINT-sensoren (Human Intelligence) binnen de verschillende militaire eenheden in België verder uitgebreid om dreigingen op het gebied van TESSOC (terrorisme, spionage, sabotage, subversie, georganiseerde misdaad) op te sporen.

Sinds de inwerkingtreding van de wettelijke bepalingen inzake het verzamelen van gegevens bij menselijke bronnen in 2022 is de ADIV methoden blijven toepassen om hun loyaliteit en betrouwbaarheid te controleren. Tegelijkertijd werd de interne procedure voor het beheer van bronnen op het gebied van contra-inmenging bijgewerkt en versterkt.

De samenwerking met nationale (VSSE, federale politie) en internationale partners is intensiever geworden dankzij gezamenlijke opleidingen en trainingen en de lancering van operationele samenwerkingsverbanden.

Electromagnetic Warfare : **overgang naar een hogere frequentie in 2025**

De oorlog in Oekraïne heeft het belang van het elektromagnetische spectrum in militaire operaties benadrukt. Communicatie, navigatie, bewaking, inlichtingen, commando en verdediging zijn allemaal afhankelijk van het gebruik ervan. Het doel is duidelijk: de tegenstander deze capaciteiten ontnemen en tegelijkertijd onze eigen capaciteiten beschermen. In 2025 zijn Defensie, de ADIV en het Cyber Command begonnen met een gestructureerde opschaling.

De Strategische Visie 2025 wijst EW aan als prioriteit en voorziet in meer dan 500 miljoen euro aan investeringen om de middelen te versterken. De machten hebben specifieke behoeften bepaald: integratie van EW-capaciteiten in de brigades vanaf 2027, ESM-middelen (Electronic Support Measure) voor de Marine, geavanceerde sensoren voor de Luchtmacht en de oprichting van een "Air Warfare Centre". Deze dynamiek gaat gepaard met de hervorming van het huidige centrum tot een "Joint Electromagnetic Warfare Centre" (JEWC 2.0), dat bedoeld is om alle operaties te ondersteunen en soevereine capaciteiten van wereldklasse te ontwikkelen. Er zijn besprekingen aan de gang met het Verenigd Koninkrijk om inspiratie te putten uit hun model, terwijl tegelijkertijd duurzame partnerschappen met de Belgische industrie worden gesmeed. De semantische verandering van "elektronische oorlogvoering" naar "elektromagnetische oorlogvoering" weerspiegelt een belangrijke doctrinaire evolutie: EW bestrijkt nu het hele spectrum, met inbegrip van ruimtevaart-, infrarood-, laser- en microgolftechnologieën, en maakt deel uit van een multidomeinaanpak. Het Belgische Cyber Command heeft actief bijgedragen aan de werkzaamheden van de NAVO op dit gebied.

Operationele en technologische verwezenlijkingen

Op operationeel vlak heeft het EWC in 2025 belangrijke opdrachten ondersteund (Iceland Air Policing, F-16-inzet, toezicht op de Zwarte Zee, A400M-operaties). Het heeft ook zijn middelen versterkt met een nieuw voertuig, een echovrije kamer (een kamer die geluids- en elektromagnetische golven absorbeert) en anti-dronetechnieken. Er is vooruitgang geboekt op het gebied van steun aan de F-35A en multinationale samenwerking met het oog op het delen van gegevensbanken en volledige interoperabiliteit. Ten slotte betekent het THREAT-project een eerste stap naar specifieke trainingszones, waardoor de Luchtmacht beschikt over een inzetbaar systeem voor elektromagnetische simulatie.

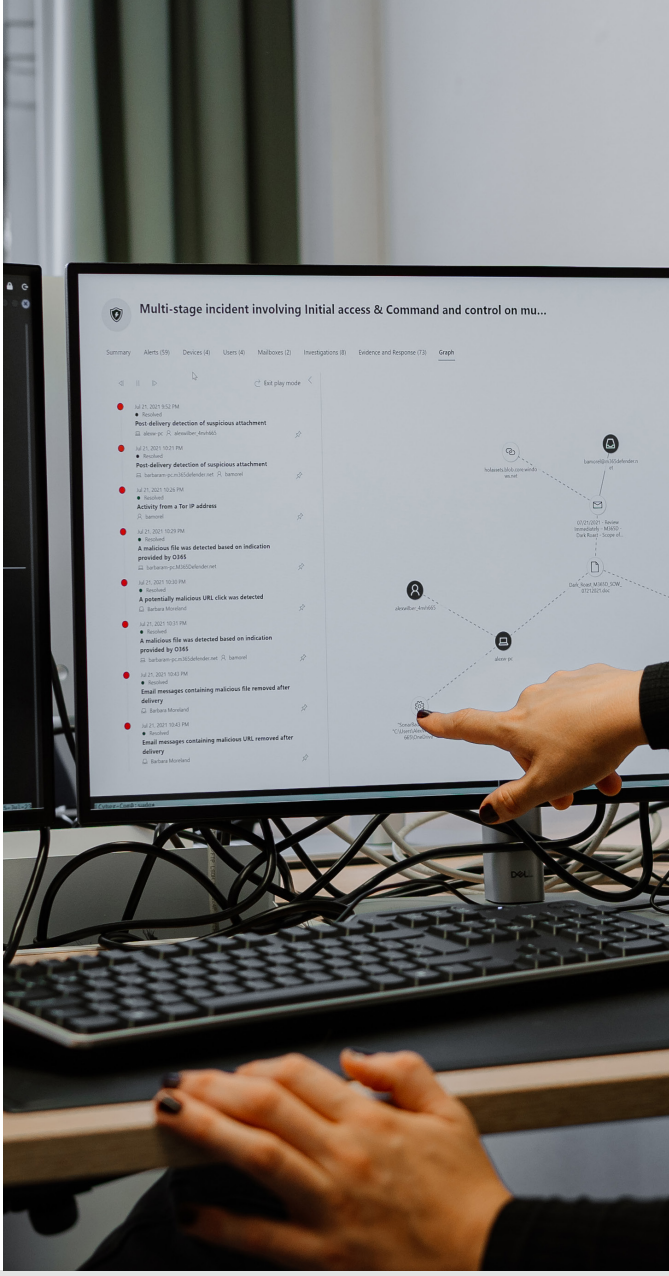
Het Cyber Command en **de actieve verdediging van de netwerken**

De Cyber Force beveiligt netwerken van onze organisatie via haar Security Operations Center (SOC). Deze operationele entiteit speelt een sleutelrol bij het opsporen en analyseren van en het reageren op cyberveiligheidsincidenten. Haar rol bestaat erin onze digitale infrastructuren permanent te bewaken, verdachte activiteiten op te sporen en doeltreffend op de waargenomen bedreigingen te reageren. Dit instrument vormt de eerste verdedigingslinie van de organisatie tegen alsmaar geavanceerdere cyberaanvallen.

Van SOC naar SIC: een door inlichtingen gestuurde transformatie

Sinds enkele jaren is er een belangrijke evolutie gaande: de overgang van een traditioneel SOC-model naar een Security Intelligence Center (SIC), met andere woorden een door data- en cyberinlichtingen gestuurd SOC. Deze transformatie is voornamelijk gebaseerd op een nieuwe architectuur waarin een SOAR (Security Orchestration, Automation and Response) geïntegreerd is.

Dit instrument maakt het mogelijk om incidenten met een lage ernst te automatiseren en incidenten met een hogere intensiteit te coördineren, waardoor de dagelijkse operationele belasting wordt verminderd en analisten zich op complexe en gerichte dreigingen kunnen concentreren. Het SOC wordt zo een proactief centrum dat zich kan beroepen op gegevens en inlichtingen om op aanvallen te anticiperen en ze tegen te gaan. Deze belangrijke ontwikkeling is momenteel in volle gang.



Versterking van Samenwerkingsverbanden en Strategische Partnerschappen

De krachtige evolutie van het SOC naar een echt SIC gaat gepaard met een toenemend beroep op externe ondersteuning. Twee contracten zijn momenteel in uitvoering: één gericht op de geoptimaliseerde bewaking van de externe perimeter van onze netwerken, en het andere gericht op het leveren van de benodigde instrumenten voor het nieuwe werkingsmodel van het SIC – inclusief de SOAR – evenals de expertise voor een geavanceerde incidentrespons. Deze initiatieven zullen ons operationeel centrum in staat stellen een nieuwe mijlpaal te bereiken op het gebied van cybervolwassenheid en cyberveerkracht.

Een jaar van intense en beheerste activiteit

Het afgelopen jaar werd gekenmerkt door een hoge operationele activiteit. Onze teams hebben verschillende pogingen tot aanvallen tegengehouden, waaronder een snel opgespoorde en geneutraliseerde password spray. Bovendien heeft de waakzaamheid van het SOC het mogelijk gemaakt om een kritieke kwetsbaarheid te ontdekken voordat deze daadwerkelijk kon worden misbruikt, zoals gebeurde tijdens het ernstige incident in december 2021. De correctie werd in samenwerking met de andere ondersteunende diensten binnen een kort en beheersbaar tijdsbestek doorgevoerd, waardoor een nieuw ernstig incident werd voorkomen. Deze successen tonen de robuustheid van het verdedigingssysteem en het voorbeeldige reactievermogen van de teams in een omgeving die steeds veeleisender wordt op het gebied van dreigingen.

Bouwen aan de toekomst: synergieën en competenties

CY. D3F. FACTORY

De sites van Charleroi en Brugge van de Cyber Defence Factories vormen de bouwstenen voor een nieuwe toekomstvisie.
In april 2025 werd een nieuwe sessie van de immersieve 'bootcamp' over cyberveiligheid georganiseerd met de 'Cyber Defence Factory' van Charleroi, gevestigd op de site van de bedrijfsincubator A6K/E6K. Dit initiatief past in het streven om competenties op het gebied van digitale uitdagingen te versterken.

Net als bij de eerste editie brengt het programma verschillende spelers uit het triple helix-model samen: het cyberbeveiligingsbedrijf NRB, de vzw BeCode en het OCMW van Charleroi. De bootcamp dompelt de cursisten onder in een scenario dat is geïnspireerd op de dramatische situatie waarmee het OCMW in augustus 2023 te maken kreeg, namelijk een ransomware-aanval die het gedurende meerdere weken volledig lamlegde. De concrete uitdagingen van de sector helpen de deelnemers om hun competenties te ontwikkelen en aanbevelingen te formuleren om de door de overheden gebruikte systemen beter te beschermen.

Oproep voor ambitieuze projecten

Het afgelopen jaar was een jaar van consolidatie, gekenmerkt door het structureel aanpakken van acties en het versterken van synergieën. Dankzij een speciaal daarvoor bestemde financiële enveloppe konden we een ambitieuze projectoproep lanceren, die innovatie en samenwerking tussen actoren bevordert. Elke editie is opgebouwd rond een jaarlijks wisselend thema dat in verschillende onderdelen wordt uitgewerkt om tegemoet te komen aan de strategische uitdagingen en specifieke kenmerken van de ecosystemen waarin de Cyber Defense Factories zijn gevestigd. Deze aanpak garandeert een fijnmazige afstemming op de lokale realiteit en versterkt tegelijkertijd de aanwezigheid van de Factories als ontmoetingsplaatsen voor de activiteiten van de Cyber Force, de ADIV en de civiele ecosystemen.

Een derde CDF in 2026

Op 13 mei 2025 huldigde het Cyber Command de tweede 'Cyber Defence Factory' in op de campus van Howest in Brugge, in aanwezigheid van talrijke prominenten uit de academische en politieke wereld. Het bijzondere aan deze tweede Factory is dat ze zich richt op cyberdefensieprojecten met de Marine, met name met de komst van de eerste mijnenjager van de nieuwe generatie, de 'M940 Oostende', in november 2025 in Zeebrugge.

De vestiging van een nieuwe Factory op de site van Howest was bijna een vanzelfsprekendheid. Eerst en vooral omdat het Cyber Command al lang betrokken was bij haar lesmodules over cyberveiligheid. Ten tweede omdat Howest strategisch gelegen is in het hart van het lokale academische en onderzoeksecosysteem, zowel publiek als privaat, en dicht bij de infrastructuur van de basis van de Marine.

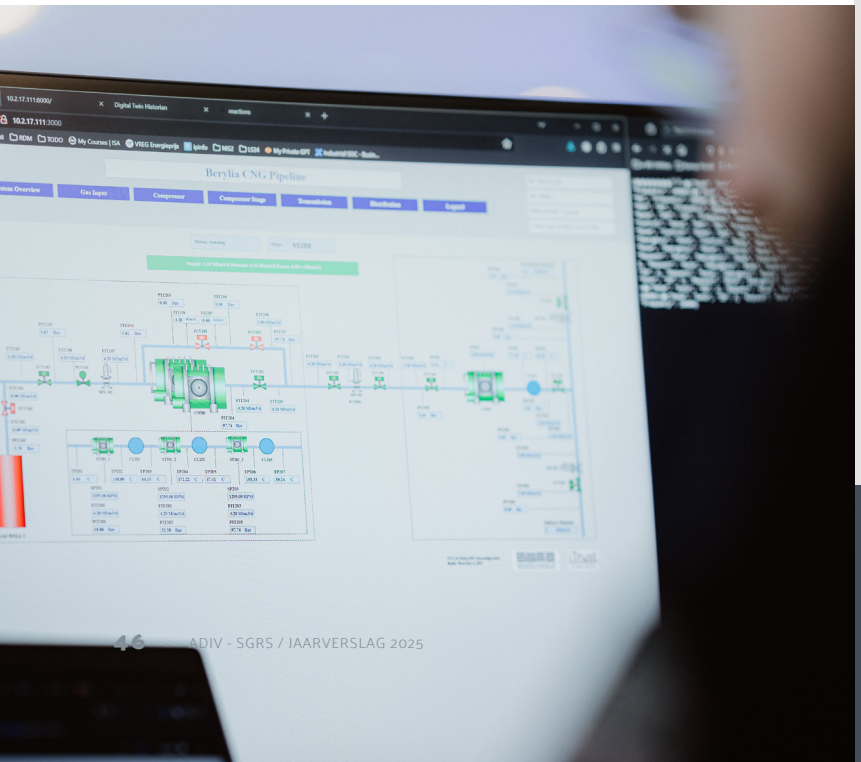
Vanaf 2026 wordt een derde Factory opgericht, waardoor ons territoriale netwerk en onze operationele capaciteit worden versterkt. Met het beschikbare budget kan tot 1,8 miljoen euro aan projecten worden ondersteund die erop gericht zijn de militaire en civiele (dual-use) cyberveerkracht te vergroten. Om deze krachtige evolutie te begeleiden, zal een Governance Board de structuren overkoepelen en een gemeenschappelijke strategische lijn uitzetten. Ten slotte zou er een speciale website moeten komen die een etalage en een centraal toegangspunt voor onze initiatieven biedt. De keuze voor een nieuw logo illustreert deze dynamiek: het cijfer 3 symboliseert de triple helix van de partnerschappen – industrieel, academisch en institutioneel – die de grondslag van onze Factories vormen.

De Joint Cyber Defence Resilience Force Unit **(JCDRFU)**

Het jaar 2025 markeerde de eerste operationele mijlpaal van de Joint Cyber Defence Resilience Force Unit (JCDRFU). De eenheid past volledig in de nationale cyberdefensiestrategie van België, in overeenstemming met de Cyberveerkrachtstrategie, en ze versterkt de synergieën tussen publieke en private spelers.

Haar opdracht steunt op drie onderling elkaar aanvullende pijlers. Ze ondersteunt de militaire operaties door cyberkennis in te brengen en het niveau van paraatstelling te verhogen. Ze draagt bij aan cybervoorbereiding door gespecialiseerde opleidingen te organiseren en competenties te ontwikkelen om een hoog operationeel niveau van de reserve in de cyberdefensie te handhaven.

Ten slotte biedt ze nationale ondersteuning en draagt ze bij aan de veerkracht in tijden van crisis door het commando en de controle te versterken en door te beschikken over de capaciteit om autonoom te kunnen optreden wanneer de omstandigheden dat vereisen.



Het leidende principe van de eenheid wordt samengevat in het devies **PRIME - Promote, Recruit, Implement, Manage, Enhance :**

Promote : vertrouwen en geloofwaardigheid tot stand brengen en tegelijkertijd organisatorische en operationele uitdagingen aangaan.

Recruit : een hybride pool van militairen, burgers en partners met technische en morele kwaliteiten uitbouwen.

Implement : de veerkracht verankeren via een op rollen gebaseerde integratie die een effectieve bijdrage aan de routinematige operaties mogelijk maakt.

Manage : Individuen en teams responsabiliseren, terwijl moderne en interoperabele instrumenten worden ingezet om een doeltreffend beheer van activiteiten en projecten te garanderen.

Enhance : de capaciteiten voortdurend verbeteren zodat de JCDRFU een essentiële speler op het gebied van nationale veerkracht blijft.

Het jaar 2025 werd door verschillende belangrijke ontwikkelingen gekenmerkt. De eerste cohesiedag, die op 25 mei 2025 werd georganiseerd in het Fort Eben-Emael in aanwezigheid van Generaal Van Strythem en de directeur D&R, Kolonel Godefridis, bood de mogelijkheid om geschiedenis en teamgeest te combineren en tegelijk het rekruteringsbeleid in de kijker te zetten.

Het initiatief 'bring a friend', dat bij deze gelegenheid werd opgezet, heeft onze zichtbaarheid vergroot en aan het aantrekken van nieuw talent bijgedragen. Tegelijkertijd zijn er op het moment van schrijven meer dan veertig lokale militaire medewerkers aangeworven, wat de wil weerspiegelt om een duurzaam reservoir van gekwalificeerde reservisten op te bouwen die in staat zijn om het hoofd te bieden aan de groeiende geopolitieke en operationele uitdagingen.

De eenheid heeft ook nieuwe interne instrumenten ontwikkeld om administratieve en operationele uitdagingen aan te pakken. Deze innovatiedynamiek vormt een essentiële hefboom voor een flexibele en projectgerichte mobilisatie, die zowel de dagelijkse activiteiten als de noodmissies kan ondersteunen.

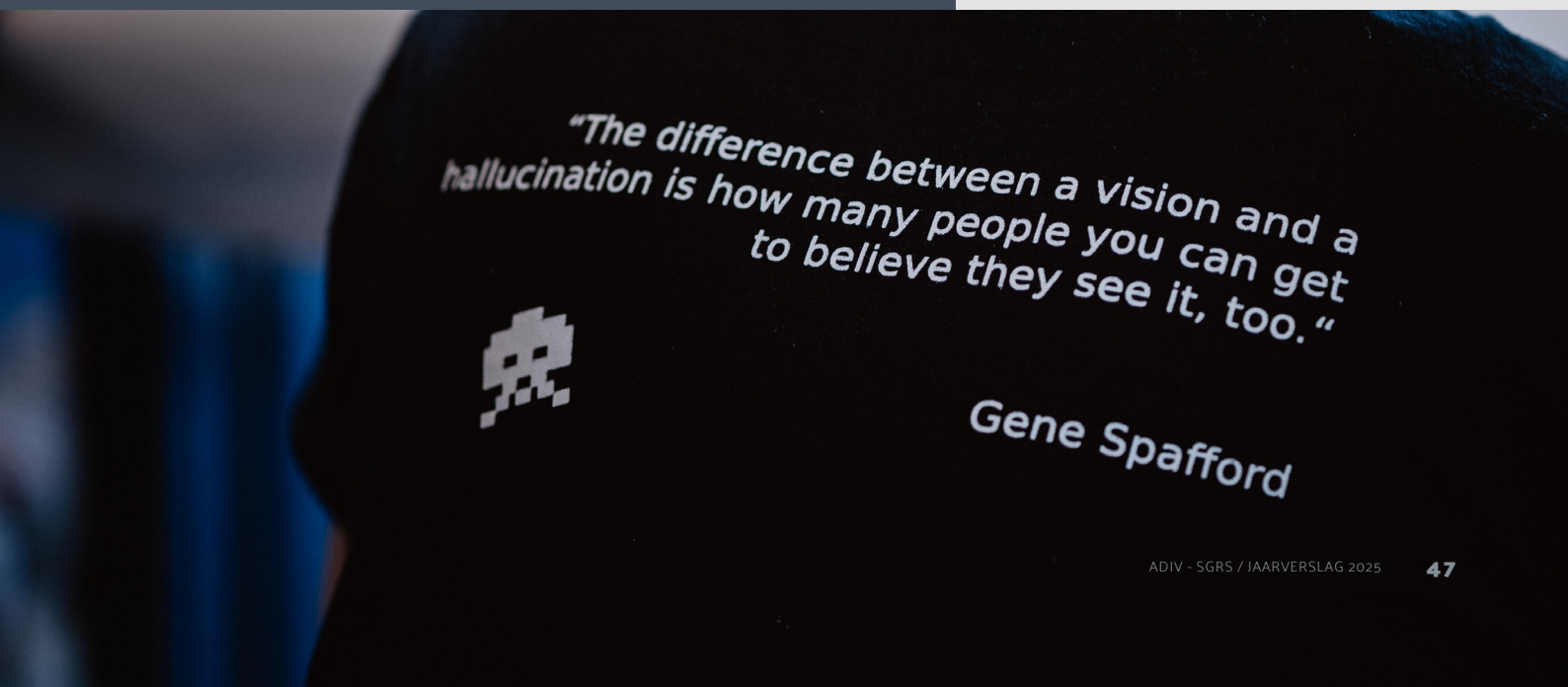
Tegelijkertijd heeft de JCDRFU haar initiatieven op het gebied van zichtbaarheid en engagement verder uitgebreid. Haar actieve deelname aan 'jobdays', jobbeurzen en diverse academische en sectorspecifieke evenementen heeft de wederzijdse verstandhouding met het Belgische cyber-ecosysteem versterkt.

Er zijn, zowel binnen Defensie als daarbuiten, synergieën tot stand gebracht. Zowel met de informatiecentra van DG HR en zijn verschillende departementen als met universiteiten, hogescholen en belangrijke spelers op dit gebied, waardoor een strategisch partnerschap wordt versterkt.

In deze context is het onder de aandacht brengen van het statuut van student-reservist een opvallende vernieuwing. Het dient drie doelen: bijdragen aan de vorming en ervaring van jonge talenten, een duurzame kweekvijver voor rekrutering opbouwen, en de nationale veerkracht versterken door stapsgewijs expertise uit de academische wereld te integreren.

Ten slotte nam de JCDRFU in de zomer van 2025 actief deel aan de Task Force Reserve Work Group en hielp ze zo om een lange-termijnvisie en een vorm van governance voor de Belgische reservemacht, vanuit een bottom-upbenadering, uit te tekenen.

Het komende jaar zal in het teken staan van de uitbreiding van de werving van gekwalificeerd personeel en de consolidatie van de administratieve structuren die onmisbaar zijn voor de organisatie van een moderne en veerkrachtige krijgsmacht. In een snel veranderende geopolitieke en cybercontext bevestigt de JCDRFU haar vastberadenheid om de Belgische defensiehouding te versterken en blijvend bij te dragen aan de collectieve veerkracht van het land.



Jean-Luc Trullemans: van veiligheid tot ruimtevaart en van inlichtingen tot de sterren

Jean-Luc Trullemans is sinds 2022 directeur van het Centrum voor Ruimtevaartveiligheid en -opleiding (ESEC) van het Europees Ruimteagentschap (ESA). Hij heeft een lange carrière achter de rug bij de federale politie op het gebied van veiligheid en geeft ons inzicht in de strategische uitdagingen van ruimtevaart en cyberveiligheid, die onlosmakelijk met elkaar verbonden zijn.

Was u voorbestemd voor een carrière in de ruimtevaart?

Nee, helemaal niet. Veiligheid is altijd mijn vakgebied geweest. Ik ben mijn carrière begonnen als speurder bij de gerechtelijke politie van Brussel. Ik werd commissaris bij de politiehervorming en trad in 2003 toe tot de Directie van speciale eenheden, voorheen het Speciaal Interventie Eskadron, wat een eenheid binnen de Rijkswacht was. In 2014 werd ik hoofdcommissaris en operationeel adviseur van de directeur-generaal van de Algemene directie van de bestuurlijke politie.

U heeft dus de politiehervorming meegemaakt?

Ik heb de politiehervorming van nabij meegemaakt door de overstap van de gerechtelijke Politie naar de federale Politie tussen 2000 en 2004. Samen met drie collega's was ik verantwoordelijk voor de Directie gerechtelijke operaties. Dat wil zeggen het beheer van de inzet van de speciale eenheden en van de bijzondere opsporingsmethoden, waarbij ik regelmatig samenwerkte met collega's van de ADIV uit die tijd.

Hoe bent u bij de ESA begonnen?

Toen ik in 2022 in dienst trad, gaf mijn directeur mij een duidelijke opdracht: het Centrum voor Ruimtevaartveiligheid en -opleiding uit de anonimiteit halen. Om dat te bereiken moesten er partnerschappen worden opgezet en een van de ontwikkelingspunten van de site was cyberveiligheid. Onze kracht ligt in ons vermogen om netwerken op te bouwen. Dat deed ik ook in mijn vorige carrière en dat ben ik hier blijven doen. Ik ontmoette Michel Van Strythem, die toen nog kolonel was. We vonden al snel raakvlakken en gemeenschappelijke interesses. Ik had hem uitgenodigd tijdens de bouw van het centrum en ik zei tegen hem: "Jouw project (het Cyber Command) en het mijne zijn samen gegroeid." Hij antwoordde me: "Ja, en dan hoeven ze alleen nog maar samen kinderen te krijgen." We hebben deze samenwerking concreet gemaakt met de ondertekening van een akkoord tussen de ESA en het Cyber Command en de aanstelling van een verbindingsofficier.

Hoe zijn cyberveiligheid en ruimtevaart met elkaar verwant?

Het speelveld wordt gevoed door gegevens uit ruimtevaartinfrastructuur die beschermd moet worden. We kunnen dus stellen dat cyber en ruimte één coherent geheel vormen. Het ene kan niet meer zonder het andere. Bij ESA is alles wat we doen gebaseerd op IT. En dit alles moet beveiligd worden. Een ruimtelijke architectuur bestaat uit een element dat we 'de ruimte' noemen, een tweede element dat de grond is, en een derde element dat de verbinding tussen beide vormt. Het ruimtelijke element zijn onze productiemiddelen, met andere woorden de satellieten. Ze bewegen zich voort met variabele snelheden tussen 300-350 km/u en 35.000 km/u of zelfs meer. Er is dus een hele laag waar zeer specifieke technologie moet worden geactiveerd om deze instrumenten te beschermen. Ze produceren gegevens die worden gebruikt voor telecommunicatiediensten, systemen voor inlichtingen of verkenning, beelden, kortom een hele reeks zaken. Deze gegevens worden vervolgens naar de grond verzonden en daarom moet ook de vector worden beveiligd. Op de grond moeten we deze ruwe gegevens ook verwerken om ze bruikbaar te maken voor de eindgebruiker, wat opnieuw een overdrachtselement vereist. De cyberbeveiliging die wij hebben ontwikkeld is dan ook driedimensionaal, omdat ze zowel het luchtruim boven de aarde, de ruimte, de vector als de grondcomponent omvat. Vandaag beschikken we over een heel origineel instrument om het geheel te beveiligen. De ESA heeft ervoor gekozen om een specifiek instrument te ontwikkelen in plaats van bestaande technologische bouwstenen samen te voegen. Mijn collega's van JAXA (het Japanse ruimteagentschap) zullen hier veel inspiratie uit putten voor het opbouwen van de veerkracht van hun agentschap. We zijn dus voorlopers geweest.

Waarom is de samenwerking tussen Defensie en de ruimtevaart van strategisch belang?

Sinds de ministeriële conferentie van november 2025 heeft de ESA voor het eerst de opdracht gekregen om bij te dragen aan de bouw van veiligheids- en defensiesystemen. Ik spreek in alle nederigheid, want het woord 'defensie' was hier bij het agentschap een paar maanden geleden nog bijna een vloekwoord. Het gezamenlijke werk van enkele visionairs, waaronder de directeur-generaal van de ESA, en dat van al mijn collega's heeft ervoor gezorgd dat deze weg na 50 jaar eindelijk is vrijgemaakt. Vandaag de dag, en wat er in Oekraïne gebeurt heeft dat duidelijk aangetoond, is het gebruik van ruimtevaarttoepassingen aan de orde van de dag. Er is ondertussen ook aangetoond dat toepassingen die oorspronkelijk voor civiele doeleinden zijn ontwikkeld, nu zijn opgenomen in de catalogus van instrumenten waarvan Defensie kan gebruikmaken. Dit worden duale toepassingen genoemd, civiel en/of militair. Vandaag de dag moet er worden nagedacht over de integratie van toepassingen die vanaf het begin van het programma of het project ingezet kunnen worden. Wat bij duale toepassingen belangrijk is, is het gebruik dat u van het instrument gaat maken. Een mes kan een wapen zijn als je het in de buik van je tegenstander steekt, en een stuk gereedschap als je het gebruikt om je appel te snijden.

Welke andere duale toepassingen zijn er concreet naast meteorologie en inlichtingenwerk?

Cryptografie gebruiken we bijvoorbeeld globaal voor al onze opdrachten. De gegevens die aanvankelijk binnen een puur wetenschappelijk programma worden geproduceerd, worden versleuteld omdat ze moeten worden beschermd. Dat is wat we hier sinds een tiental jaar zijn begonnen te doen. Het centrum voor cyberbeveiliging dat we bij ESEC hebben gebouwd, voldoet zowel aan de TEMPEST-normen als aan de ESA-norm, waardoor we een machtigingsniveau tot het niveau 'geheim' kunnen nastreven. Dit is een kleine revolutie binnen het agentschap, omdat deze behoefte niet meteen werd onderkend. Sommige programma's, zoals GALILEO, omvatten meerdere diensten, waaronder een overheidsapplicatie die meer robuustheid op het gebied van cryptografie vereist dan andere. Ook hier kunnen we spreken van duale toepassingen, aangezien onze behoeften overeenkomen met die van anderen.

ADIV & Universiteit van Gent

De innovatieafdeling heeft als pedagogisch adviseur en onderwijspartner bijgedragen aan het certificaatprogramma Inlichtingenstudies van de Universiteit Gent.

Op basis van deze rol zijn er andere initiatieven gestart om gespecialiseerde cursusmodules en nieuwe academische programma's aan Belgische universiteiten te ontwikkelen.

De behandelde onderwerpen omvatten radicalisering, extremisme, terrorisme, risicoanalyse en argumentatie.

GHENT UNIVERSITY

Gedeclassificeerde archieven

In 2025 is het werk binnen ons vertrouwelijke archief onverminderd doorgegaan. Het was opnieuw gericht op het bewaren, beheren en vrijgeven van archiefstukken, met inachtneming van de wettelijke bepalingen en procedures.

Een goed beheerd archief zorgt ervoor dat kennis en context bewaard blijven, zelfs wanneer structuren of systemen veranderen. Het vrijgeven en beschikbaar stellen van deze documenten is een nauwgezet, tijdrovend en arbeidsintensief proces. Elk dossier moet afzonderlijk worden beoordeeld, met inachtneming van de wettelijke kaders, de vertrouwelijkheidsregels en de belangen van de betrokken partijen. Deze beoordeling vereist niet alleen technische expertise, maar ook nauwkeurigheid, overleg en geduld.

In 2025 zijn opnieuw talrijke archiefstukken vrijgegeven en opengesteld voor (historisch) onderzoek:

Dossiers van de Agents de Renseignement et d'Action (ARA) en dossiers van de Services de Renseignement et d'Action (SRA): in 1993 heeft de Staatsveiligheid het archiefbestand Services de Renseignement et d'Action bij CegeSoma gedeponeerd. Dit zijn de dossiers van de vrijwilligers die zich tijdens de Tweede Wereldoorlog in bezet België bij verzetsnetwerken hadden aangesloten. Na de Tweede Wereldoorlog werd binnen het verzet een aparte status uitgewerkt: de status van Agents de Renseignement et d'Action (SRA). In totaal werden na de Tweede Wereldoorlog 18.716 personen als SRA erkend.

Dossiers voor de erkenning van gewapende verzetsstrijders: in 1945 werd de status van gewapende verzetsstrijder ingevoerd om eer te bewijzen aan degenen die de wapens hadden opgenomen tegen de bezetter. Om deze status te verkrijgen, moest men deel hebben uitgemaakt van een erkende verzetsgroep of kunnen aantonen dat men individueel verzetsdaden had verricht. Na de oorlog kwamen ongeveer 140.000 mensen in aanmerking voor deze status. Vanaf 1946 werden de dossiers die waren aangelegd in het kader van het verkrijgen van de status van gewapend verzetsstrijder beheerd door de diensten van het Ministerie van Defensie. Tegenwoordig zijn deze dossiers volledig vrijgegeven.

Archiefcollectie «Archieven van het Comité d'acquisition de Liège bewaard in de Rijksarchieven» (Rijksarchief LUIK)

Ook zijn er archiefdocumenten met betrekking tot het koloniale verleden vrijgegeven:

CONGO : Vrijgave van documenten die op verzoek van een onderzoeker zijn geselecteerd en betrekking hebben op de gebeurtenissen in CONGO in juli 1960. Het gaat om de archiefbestanden COMETRO, VANDERSTRAETEN en GHEYSEN.

RWANDA : Documenten met betrekking tot de gebeurtenissen in Astrida op 21 en 22 juni 1960, in het bijzonder het dossier: "Verslag over de gebeurtenissen in Sovu (Bufundi-Astrida)"Sovu (Bufundi-Astrida) »

ADIV · SGRS

QUAERO ET TEGO

Cyber Force
Through Partnerships

WWW.SGRS.BE