SGRS - ADIV
AVRIL 2026 / WWW.SGRS.BE

RAPPORT ANNUEL 2025

QUAERO ET TEGO

LA DÉFENSE

.be

COUVERTURE : Lanceur Ariane 6 développé par l'Agence spatiale européenne

Le monde change, mais notre mission reste identique

TABLE DES MATIÈRES

GÉNÉRAL-MAJOR STÉPHANE DUTRON

CHEF DU SGRS

Quaero et Tego est notre devise ; Protéger notre pays, nos entreprises et nos expatriés par nos Renseignements est notre mission première ; Conseiller judicieusement les autorités est notre devoir envers notre pays, la société et nos concitoyens.

EDITEUR RESPONSABLE

M. Van Hecke Bernard

Quartier Reine Elisabeth
Rue d'Evere 1 à 1140 Evere

Photographies : DG StratCom et personnel SGRS

Mise en page : Quentin Moonen

Par le ADIV-SGRS

"Nous travaillons pour vous, pour notre pays, pour la paix."

Général-major
Stéphane Dutron

P. 36

L'ARRIVÉE DU PREMIER F-35

Le 13 octobre 2025, une étape historique a été franchie avec l'arrivée des premiers avions de combat F-35A Lightning II à la base aérienne de Florennes.

NOTRE MESSAGE

Votre futur.
Notre mission.

Introduction

Dans notre métier de l'ombre, il n'y a pas d'année facile ou légère

Nous en sommes déjà à la quatrième édition de notre rapport annuel. Cette publication survient dans un monde en profonde mutation et le chaos géopolitique a fortement pesé sur les services de renseignements. Les derniers mois ont en effet été le théâtre d'événements marquants qui ont révélé au grand public l'ampleur de changements souvent initiés bien plus tôt. La lutte entre grandes puissances, le recul du multilatéralisme et la mise sous pression de l'ordre international sous-tendent des relations internationales beaucoup plus instables où les intérêts nationaux priment souvent sur toute autre considération. Un monde incertain avec un seuil de violence interétatique de plus en plus bas, même dans des zones jusqu'ici jugées relativement stables. Dans ce contexte, un service de renseignement tel que le nôtre redouble d'importance : nos efforts de collecte et d'analyse nous ont permis de recouper, interpréter et contextualiser moultes situations conflictuelles, offrant aux décideurs la compréhension indispensable à la prise de décision et à l'action, au profit de nos intérêts nationaux. Nous avons agi seuls ou avec l'appui de nos partenaires, en fonction des circonstances et des moyens disponibles.

En 2025, la guerre s'est poursuivie entre l'Ukraine et la Russie et cette dernière a continué à engranger de modestes avancées dans la région du Donbass, malgré une économie de guerre tournant à plein régime. Les dépenses militaires et la sécurité intérieure ont représenté plus de 43 % des dépenses publiques officielles. Cependant, les sanctions internationales et les frappes ukrainiennes sur des installations critiques en Russie produisent lentement et durablement leurs effets. Au prix de pertes humaines effroyables et avec le soutien d'alliés qui continuent à les approvisionner, les armées de Poutine n'ont grapillé que peu de territoires sur un champ de bataille technologiquement en perpétuelle mutation, remettant en question certaines notions tactiques antérieures. La résilience des Ukrainiens ne faiblit pas malgré les attaques incessantes sur leurs installations critiques et leurs villes en territoire ukrainien.

Au Proche-Orient, on a craint un embrasement généralisé de la région lorsqu'Israël a mené des frappes aériennes contre les installations nucléaires de l'Iran en juin. La riposte iranienne n'a en effet pas visé qu'Israël et des missiles balistiques ont entre autres été tirés vers la base américaine d'Al-Udeid au Qatar. A Gaza et en Cisjordanie la situation reste confuse, la fragilité des institutions au Liban et en Syrie est -malgré les efforts déployés- relativement préoccupante tandis que la matérialisation du résultat des élections législatives de novembre en Irak doit nous éclairer sur le futur. L'accès à la Mer Rouge reste bien entendu un point d'attention permanent, de même que la présence de l'Etat

Islamique et de ses alliés qui pourraient essayer de se réinstaller durablement dans la région.

En Afrique, le début de l'année 2025 a été marqué par l'avancée des milices rebelles du M23 dans la région des Grands Lacs à l'Est du Congo. La prise de Goma et Bukavu a provoqué une catastrophe humanitaire ainsi que la décision unilatérale des autorités rwandaises de rompre tout lien diplomatique avec notre pays. Notre Service a été sollicité pour aider à l'évacuation de notre ambassade dans des délais extrêmement courts et je tiens à saluer le professionnalisme et le sang-froid de notre personnel ainsi que celui du SPF Affaires Etrangères. Malgré des accords diplomatiques, le conflit perdure sur le terrain et la prise d'Uvira en décembre a été un nouveau camouflet pour certains belligérants mais aussi pour les pays négociateurs et une partie de la communauté internationale.

A l'Ouest du continent africain, différents groupes terroristes affiliés à Al-Qaïda et, dans une moindre mesure, à l'Etat Islamique poursuivent leur avancée au Sahel. Ces groupes étendent leurs territoires au Mali, au Burkina Faso, au Niger, au nord du Bénin et au nord-ouest du Nigeria. A l'heure d'écrire ces lignes ils menacent toujours plusieurs capitales sahéliennes (Bamako, Ouagadougou et Niamey)

Nous continuons à suivre l'évolution de la situation internationale et ses conséquences en Belgique avec nos analystes, mais également en bonne entente avec le réseau diplomatique, via nos attachés militaires et nos nombreux contacts internationaux.

En Belgique, nous poursuivons de concert nos efforts dans la lutte contre le radicalisme et l'extrémisme avec la Sûreté de l'Etat, notre premier partenaire en matière de renseignement et de sécurité, avec lequel nous renforçons au fil des ans les synergies. Les tentatives d'ingérence ou d'espionnage sont également une source de préoccupation permanente, notamment au sein des milieux scientifiques et de la recherche en lien avec la Défense. Notre service participe activement au renforcement de la coopération interdépartementale fédérale dans la lutte contre ces phénomènes.

Enfin, les tentatives hybrides de déstabilisation par des acteurs étatiques hostiles, au travers d'attaques cyber, de la désinformation, d'incursions dans l'espace arien de l'OTAN ou de tentatives de sabotage sont suivies avec l'attention nécessaire. Néanmoins, même si certains sont enclins à attribuer les nombreux survols de drones au-dessus de nos casernes, aéroports civils ou infrastructures critiques à la Russie, aucun élément matériel ne permet de confirmer cette hypothèse pour l'instant.

Dans notre métier de l'ombre, il n'y a pas d'année facile ou légère. Au contraire, les tensions géopolitiques et la menace hybride en Belgique sont plus marquées que jamais et nous poussent à redoubler d'attention envers la sécurité du personnel et des infrastructures militaires mais aussi en vue de préserver nos intérêts nationaux.

Mais l'intensification et la diversification des menaces nous demandent davantage de flexibilité et de résilience année après année. Ce qui veut dire que nous devons nous réinventer en permanence, au niveau de nos formations, de nos procédures et de notre matériel et c'est la raison pour laquelle l'agilité du Service reste ma priorité.

Nous devons engager plus de moyens dans la technologie et le traitement des données, de plus en plus nombreuses, afin d'accélérer les processus.

Nous devons anticiper les menaces et nous engager, avec tous nos partenaires nationaux et internationaux, pour appuyer la Défense, informer nos décideurs et protéger notre pays, sa population, ses valeurs et ses institutions. Nous nous devons de répondre à la question : « Quid Belgica ? »

Au nom du personnel du SGRS je vous souhaite une bonne lecture !

GÉNÉRAL-MAJOR

SGRS - ADIV / CYBER FORCE

Introduction

Il faut un réseau pour défendre un réseau

C'est avec un immense honneur que j'ai repris la fonction de commandant de la Force Cyber en septembre 2025 après plusieurs années aux côtés du Lieutenant-Général Michel Van Strythem comme directeur des opérations.

Ma priorité c'est le développement de cette nouvelle Force afin qu'elle puisse au mieux remplir ses missions de soutien au SGRS et aux autres Forces de la Défense. Notre diversité de fonctions, de profils et de statuts est non seulement une richesse mais aussi un avantage dans notre capacité à évoluer rapidement au sein de la Défense et de notre réseau de partenaires externes. Nous continuons à grandir jour après jour mais afin de soutenir cette croissance nous devons poursuivre notre effort en matière de recrutement.

A ce titre, la mise en place de la Réserve cyber, la « Joint Cyber Defence Resilience Force Unit » est d'une importance capitale. Plus que jamais, nous avons besoin d'hommes et de femmes issus de tous les horizons, du monde de l'entreprise ou académique afin d'assurer en permanence ce transfert de connaissance et d'expertise entre le monde civil et militaire afin d'assurer la résilience de la Défense et de participer à celle de notre pays.

C'est dans la même optique que nous avons implanté nos « Cyber Defence Factories » qui sont des lieux de rencontre et de recherche au cœur des écosystèmes de cybersécurité locaux. Après Charleroi sur le site d'un incubateur d'entreprises nous avons ouvert en 2025 une nouvelle implantation sur le campus de la Haute Ecole Howest à Bruges. Aujourd'hui une trentaine d'étudiants travaillent sur des projets en cybersécurité en étroite collaboration avec les entreprises du secteur. Et nous avons de l'ambition pour l'avenir.

Un des faits d'actualité marquants de cette année 2025 c'est évidemment la multiplication des apparitions de drones non identifiés au-dessus de différentes casernes, aéroports nationaux ou régionaux ou encore infrastructures critiques.

La Belgique n'a évidemment pas été le seul pays confronté à ce phénomène, mais il est clair que ces opérations ont été planifiées et coordonnées à grande échelle. Il faut replacer ce phénomène dans le concept plus large de guerre hybride, ces drones sont un moyen parmi d'autres : incursions dans l'espace aérien et maritime, campagnes de désinformation, etc.

Une des particularités de cette guerre hybride c'est son rapport coût/bénéfice particulièrement intéressant. Les drones ne coûtent pas grand-chose mais provoquent un impact médiatique et psychologique considérable en créant un sentiment d'insécurité. Sans parler des conséquences économiques liées aux

fermetures de l'espace aérien et à la paralysie des aéroports.

La question des drones met en évidence la nécessité de développer nos moyens de détection et de protection en matière de guerre électronique. Le spectre électromagnétique est devenu un nouveau terrain d'affrontement et c'est particulièrement vrai en Ukraine où les drones permettent d'obtenir un avantage tactique décisif sur l'adversaire.

C'est la raison pour laquelle nous développons le JEWSC (Joint Electronic Warfare Support Center) qui est chargé de programmer les bases de données électromagnétiques qui doivent être chargées dans l'ensemble des systèmes d'armes actuels et futurs. Il permettra également d'analyser toute une série de paramètres enregistrés pendant les opérations.

Je suis persuadé que nous ne pourrons faire face à toutes ces menaces, démultipliées par l'utilisation de technologies disruptives comme l'intelligence artificielle qu'avec l'ensemble de nos partenaires, privés comme publics.

A ce titre, la désignation d'un officier de liaison avec les entités fédérées est une excellente nouvelle qui facilitera les projets en cours. Nous multiplions les initiatives avec les Régions, notamment avec la « cyber week » de l'Agence du numérique. Nous poursuivons notre collaboration avec l'ESA (l'Agence spatiale européenne) et avec IDELUX (intercommunale de la Province du Luxembourg) où nous entrainons des opérateurs de la Force aérienne à affronter dans un simulateur toute une panoplie d'incidents cyber en temps réel.

Plus que jamais il faut un réseau pour défendre un réseau !

GÉNÉRAL-MAJOR

Pierre Cipadisse

Changement de commandement au sein de la Cyber Force le 19 septembre 2025

Proche-Orient : **la crainte d'un embrasement**

Comme 2024, 2025 a été marqué par le conflit entre Israël et le Hamas. Un conflit qui a perduré en 2025 et a impliqué, directement ou indirectement, de nombreux pays de la région, faisant craindre un conflit armé régional.

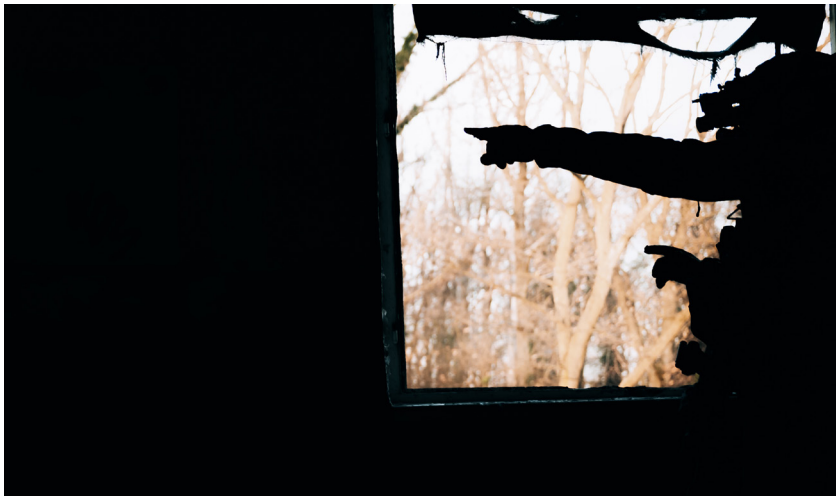
Les craintes d'une escalade régionale sans précédent ont atteint leur paroxysme le 13 juin 2025, jour où Israël a lancé l'opération « Rising Lion » visant à détruire les installations nucléaires iraniennes, ses infrastructures et son commandement militaire. Les jours suivants, une escalade entre les deux pays a mené à de nombreux tirs de missiles balistiques.

Après l'opération américaine «Midnight Hammer» le 21 juin 2025, visant à neutraliser les installations nucléaires iraniennes de Fordow, Natanz et Ispahan, l'Iran a riposté le 23 juin. Elle a tiré une salve de missiles balistiques dirigés vers la base américaine d'Al-Udeid au Qatar. Un cessez-le-feu entre Israël et l'Iran le 24 juin a finalement empêché une nouvelle escalade de la confrontation désormais appelée la « guerre des Douze Jours ».

Affaiblissement de l'Iran

L'Iran a subi de très lourdes pertes. Le potentiel militaire iranien a non seulement été touché, mais le leadership militaire a également été largement atteint. La passivité de plusieurs acteurs de l'«Axe de la Résistance» (considéré comme l'ensemble formé par les proxies de l'Iran, tels que le Hamas palestinien, le Hezbollah libanais ou encore les milices pro-iraniennes en Irak) a confirmé l'affaiblissement de la force de projection de l'Iran. Les Houthis font exception à la règle. Le mouvement yéménite est parvenu à plusieurs reprises à menacer Israël.

Le régime iranien souffre aussi d'une instabilité interne, aggravée par les crises récentes. Cela a conduit à une vague de manifestations importante entamée fin 2025.



Répercussions au Liban et en Syrie

L'instabilité créée par le conflit entre Israël et le Hamas a continué en 2025 à provoquer des répercussions sur le Liban. Malgré l'accord de cessez-le-feu signé fin 2024, des opérations israéliennes contre le Hezbollah ont continué au Sud du Liban et sporadiquement dans d'autres régions telles que Beirut ou la vallée de la Bekaa. L'annonce d'un processus de désarmement début septembre 2025 semble aller dans le sens d'une stabilisation de la situation au Liban, mais le Hezbollah reste politiquement et socialement important. Le choix d'un désarmement forcé comporte donc des risques dans ce pays marqué par la coexistence de nombreuses communautés.

La Syrie reste une zone où des acteurs régionaux essayent de défendre leurs intérêts. La situation y reste précaire. Malgré une politique officielle de démocratisation et d'inclusivité, la question des minorités est encore source de tensions. En outre, le mouvement terroriste État islamique profite lui aussi de l'instabilité du pays pour redévelopper ses activités.

Irak : conflits politiques internes

L'Irak reste quant à lui aux prises avec des conflits politiques internes : conflits entre les différentes composantes ethno-sectaires ; relations avec la Région Autonome du Kurdistan ; (dont les problématiques économiques, entre autres en lien avec les revenus du pétrole) influence des milices pro-iraniennes. En raison de ces défis internes, le pays a essayé de se tenir à l'écart du conflit israélo – iranien, tentative peu évidente étant donné la présence de nombreuses milices alignées à l'Iran. Les élections irakiennes, dont le taux de participation élevé a surpris, se sont déroulées sans encombre. Le résultat des urnes a reconduit l'élite politique traditionnelle. Après l'élection du chef du Parlement le 29 décembre 25, les négociations sont en cours pour former le gouvernement.

De nombreux États de la région s'efforcent, dans la mesure du possible, d'éviter la propagation de l'instabilité sur leur sol. Les attaques iraniennes et israéliennes contre le Qatar en 2025 prouvent qu'en dépit de toutes les tentatives de ne pas se laisser entraîner dans le conflit, plusieurs Etats, dont entre autres les États du Golfe, se trouvent au centre des dynamiques régionales.

Après plus de deux ans de guerre, le conflit entre Israël et le Hamas, qui a eu des répercussions sur toute la région, semble s'orienter vers un scénario de négociations, suite à l'accord de cessez-le-feu annoncé le 30 septembre 2025 par le Président Trump. La situation reste cependant très fragile en raison de nombreux facteurs internes et externes.

Conflit entre la Russie et l'Ukraine : guerre des drones et incertitude géopolitique

Le gouvernement russe a prévu un budget record pour la guerre contre l'Ukraine en 2025.

Les dépenses militaires et la sécurité intérieure ont représenté plus de 43 % des dépenses publiques officielles. Cela montre que la guerre restait la priorité absolue du Kremlin, malgré les pertes importantes sur le front, les difficultés croissantes de l'économie russe et les déficits budgétaires systématiques.

L'attitude hésitante du président américain Donald Trump à l'égard de la Russie et ses positions changeantes sur la guerre et les négociations ont suscité, au sein du camp occidental, une forte pression politique. Mais aussi des attentes élevées d'une part, de l'incertitude et des divisions quant à l'approche à adopter d'autre part. Néanmoins, le président russe Vladimir Poutine a refusé tout compromis. Il a maintenu ses exigences maximales malgré l'intensification de la pression exercée par les États-Unis sur l'Ukraine pour qu'elle fasse des concessions, ainsi que les propositions relativement avantageuses faites à la Russie.

L'évolution des attaques de drones

L'utilisation d'attaques de drones plus sophistiquées et massives s'est poursuivie en 2025. Les drones de reconnaissance et d'attaque rendait impossibles les attaques terrestres à grande échelle sans causer de pertes importantes, tandis que les lignes de défense traditionnelles étaient remplacées par des troupes et du matériel dispersés et décentralisés. La présence constante de drones constituait une menace permanente tant pour les militaires que pour les civils restés près de la ligne de front.

Modeste progression russe

La Russie gagnait lentement mais sûrement du terrain, au prix toutefois de pertes énormes, principalement en personnel militaire. L'avancée russe s'est principalement concentrée dans certaines parties du Donbass et de la région de Zaporijia, où elle a tenté de progresser du terrain en redoublant d'efforts et en recourant intensivement à des unités de drones.

L'Ukraine, quant à elle, souffrait clairement de problèmes de pénurie de personnel. Bien que les gains territoriaux russes aient été plus importants en 2025 que lors des périodes précédentes, l'Ukraine a néanmoins été en mesure de riposter vigoureusement et d'appliquer sa tactique consistant à échanger du territoire contre des pertes russes importantes.

Campagnes aériennes

Outre les combats incessants sur le front, les deux camps se sont concentrés de plus en plus sur les campagnes aériennes afin de déstabiliser l'adversaire au maximum. La Russie s'est principalement concentrée sur les infrastructures énergétiques ukrainiennes dans l'espoir de démoraliser la population ukrainienne et de la laisser littéralement dans le froid. Malgré la situation humanitaire critique dans certaines villes, ces attaques semblaient pour l'instant avoir peu d'effet tangible sur le moral de la population.

Entre-temps, l'Ukraine a continué à bombarder des raffineries et des infrastructures pétrolières russes, mais également les capacités d'exportation de pétrole russe (y compris la flotte fantôme). Cette campagne couronnée de succès a touché, selon les estimations, plus de 20 % de la capacité totale de raffinage russe et a perturbé les exportations de pétrole. Bien que leur incidence directe sur la situation au front soit limitée, ces attaques exercent une pression supplémentaire sur la Russie.

Une attaque russe à Zaporijjia, le 24 février 2026. IMAGO/Smoliyenko Dmytro/Ukrinform/ABACA/IMAGO/ABACAPRESS

Afrique : évolution de la région des **Grands Lacs**

L'année 2025 a connu un début dramatique dans la région des Grands Lacs, et en particulier dans l'Est de la République démocratique du Congo, avec la prise des capitales provinciales Goma en janvier et Bukavu en février par les rebelles de l'Alliance Fleuve Congo (AFC)/Mouvement du 23 mars (M23), soutenus par le Rwanda.

Malgré l'urgence, les corridors humanitaires demeurent un concept théorique.

Cette prise de contrôle a également rendu l'aéroport international de Goma inexploitable pour l'acheminement d'aide humanitaire, et ce jusqu'à nouvel ordre.

Les événements dans l'Est du Congo ont provoqué une certaine nervosité à Kinshasa et ont conduit à l'assaut de l'ambassade belge fin janvier 2025.

Une autre conséquence des événements dans l'Est du Congo pour notre pays a été la décision des autorités rwandaises de rompre leurs relations diplomatiques avec la Belgique. Des comptes (principalement rwandais) sur les réseaux sociaux ont diffusé de la désinformation sur la présence militaire belge au Congo.

Processus de paix

Une nouvelle dynamique dans le processus de paix a conduit à un accord formel entre le Congo et le Rwanda, signé à Washington le 27 juin 2025, et reconfirmé par les présidents des deux pays le 4 décembre 2025. Des pourparlers parallèles entre le gouvernement de Kinshasa et les rebelles de l'AFC/M23 ont été engagés à Doha, dans l'espoir qu'ils aboutissent à un cessez-le-feu permanent. Malgré ces efforts diplomatiques, la situation sur le terrain dans l'Est du Congo demeure fragile. Une éventuelle escalade régionale du conflit reste également préoccupante, compte tenu de la présence militaire du Burundi et de l'Ouganda dans l'Est du Congo.

Le Sahel : progression du terrorisme religieux

Le terrorisme d'inspiration religieuse reste la menace la plus grave pour l'Afrique de l'Ouest. Autour du lac Tchad, l'Islamic State West Africa Province (ISWAP) contrôle une zone trois fois plus grande que la Belgique. Il s'agit du groupe d'État islamique le plus important au monde après les défaites subies par l'EI ailleurs. L'ISWAP tente de créer un pont vers la zone frontalière entre le Mali et le Niger, où opère l'Islamic State Sahel Province (ISSP). Cependant, Jama'at Nusrat al-Islam wa al-Muslimin (JNIM), affilié à Al-Qaïda, est le groupe terroriste dominant au Sahel. Le groupe étend actuellement son territoire au Mali et au Burkina Faso, dans le Nord du Bénin et le Nord-Ouest du Nigeria. Le groupe est responsable du blocus autour de Bamako, la capitale malienne.

Dans les pays du Sahel, nous assistons à un recul systématique de la démocratie et des libertés, associé à un discours anti-occidental. C'est notamment le cas pour les trois juntes qui forment la Confédération des États du Sahel (AES), à savoir le Mali, le Burkina Faso et le Niger, où la Russie (et la Chine) prennent une place importante. La Russie choisit toutefois d'exploiter les richesses minérales et de soutenir les régimes, plutôt que de contribuer efficacement à la lutte contre le terrorisme. Les groupes terroristes poussent de plus en plus les trois juntes AES dans leurs retranchements.

Global Outreach Intelligence : une compétition mondiale accrue

Le bureau Global Outreach Intelligence (GOI) du SGRS analyse les phénomènes transnationaux.

En 2025, le contexte international est marqué par une transformation profonde : les relations internationales, longtemps fondées sur un équilibre entre coopération et compétition, basculent vers une logique de compétition généralisée, parfois jusqu'à la confrontation.

Fragmentation de l'ordre mondial

Les grandes puissances s'affrontent sur des terrains multiples - technologie, énergie, métaux rares, alliances stratégiques - accentuant la fragmentation de l'ordre mondial. Les conflits en Ukraine et dans la bande de Gaza fragilisent la crédibilité occidentale, tandis que le Sud global affirme sa volonté de « désoccidentaliser » l'ordre international.

Montée en puissance des forums alternatifs

Ce mouvement se traduit par le renforcement de forums alternatifs tels que BRICS+ et l'Organisation de coopération de Shanghai (OCS), dont les élargissements et la médiatisation illustrent leur attractivité. Bien que loin de constituer un bloc homogène, ces acteurs contestent l'ordre libéral et revendiquent un système multipolaire.

Chine : acteur central d'un nouvel équilibre

Pilier des deux organisations, elle accroît son influence en proposant une alternative à l'ordre mondial. Cette dynamique intensifie la compétition stratégique entre États-Unis, Chine et Russie, et accroît le poids des régimes autoritaires. Les États du Sud deviennent des terrains de luttes d'influence et de guerres par procuration.

Instabilité et menaces hybrides

La rivalité ne se limite pas à l'économie ou à la politique : elle est aussi identitaire et normative, chaque puissance cherchant à imposer ses règles et son modèle civilisationnel. Cette transition systémique génère instabilité, crises récurrentes et tensions énergétiques, tout en brouillant la frontière entre guerre et paix. Les menaces hybrides contre les pays occidentaux s'en trouvent renforcées.

La **menace hybride** au cœur de nos sociétés

La menace hybride russe demeure aujourd'hui l'un des défis les plus complexes pour la sécurité européenne. Cette menace ne se limite pas au champ de bataille, mais combine des moyens militaires et non militaires pour affaiblir les sociétés occidentales, saper la cohésion politique et perturber les flux d'aide internationale vers l'Ukraine et d'autres régions vulnérables.

La Belgique, en tant que membre de l'OTAN et pays de transit logistique, a également continué d'être la cible de cyberattaques, de tentatives d'espionnage, de sabotage, de désinformation et de reconnaissances maritimes le long d'infrastructures critiques.

Outre notre position diplomatique et logistique centrale, les investissements récents dans la modernisation de notre Défense revêtent également une importance pour la partie adverse. D'un côté, cela renforce la dissuasion collective sur le flanc est de l'Europe vis-à-vis de la Russie. De l'autre, la modernisation de notre Défense offre à la Russie l'occasion de mener des activités d'espionnage concernant nos capacités technologiques, nos processus logistiques et nos partenariats industriels.

« Insider threat »

La protection de nos intérêts exige des restrictions d'accès strictes aux installations sensibles, à la documentation et aux flux d'informations. Au cours des dernières années, nous avons été confrontés à plusieurs incidents au cours desquels des individus ont notamment tenté d'accéder illicitement aux installations de la Défense. Nous avons également constaté diverses activités d'espionnage, telles que le survol par des drones et le repérage d'installations sensibles.

Ces menaces ne proviennent pas uniquement de l'extérieur de notre organisation. L'insider threat est peut-être la menace la plus dangereuse à laquelle nous sommes confrontés aujourd'hui. D'une part, nos militaires peuvent être et sont approchés par des tiers dans le but d'obtenir des informations de manière illicite. D'autre part, le manque de sensibilisation à la sécurité et le laxisme de notre personnel vis-à-vis des restrictions imposées constituent la principale faiblesse de notre dispositif de sécurité.

Les avis émis par la Sécurité militaire visent non seulement à imposer et à contrôler des restrictions, mais aussi à limiter la responsabilité en cas d'incidents de sécurité. En fin de compte, la sécurité est une responsabilité collective, dont le professionnalisme de chaque membre du personnel, militaire ou civil, constitue la pierre angulaire.

Un **nouveau souffle** pour l'industrie de **défense européenne** ?

En mars 2025, l'Union Européenne a annoncé « ReArm Europe », un plan massif d'investissement de 800 milliards d'euros pour donner un nouveau souffle à l'industrie de défense européenne. La Belgique n'est pas en reste, avec une augmentation du budget de la Défense, et de nombreuses initiatives, fédérales et régionales, de financement de projets de recherche et développement militaires.

Protection des industries de défense

Le SGRS intervient dans la protection de ces industries de défense et de ces projets de recherche contre l'espionnage, l'ingérence et la disruption. Il a déjà pu empêcher l'entrée de sociétés contrôlées par des nations hostiles dans ces programmes de recherche, et estime que ces projets vont encore susciter un intérêt certain de la part des officiers de renseignement de tout bord. Le travail du SGRS à ce niveau permet non seulement d'empêcher le transfert de technologies non désiré, mais aussi de protéger la réputation de notre industrie de défense et de nos centres de recherche.

Augmentation de la vulnérabilité à l'espionnage

Une tendance relativement récente et qui complique la donne est la limite de plus en plus floue entre technologie militaire et civile. Les drones en sont un exemple évident, avec les drones FPV (first-person view) petits formats initialement purement à destination civile, et qui sont maintenant une des armes les plus utilisées en Ukraine. Dès lors, beaucoup de sociétés initialement purement « civiles » se tournent vers des programmes de recherche et développement militaires, car leur technologie s'avère être intéressante d'un point de vue militaire. Sans oublier que les budgets disponibles sont conséquents. De plus, énormément de projets de développement se déroulent selon le principe « triple helix », qui implique une collaboration entre privé, public et universités/centres de recherche. Si cette intégration de plusieurs acteurs est très utile pour accélérer l'innovation et le développement, force est de constater qu'elle augmente la vulnérabilité à l'espionnage et l'ingérence. L'implication de plus d'entités et de personnes, dont certaines n'ont pas nécessairement la « culture » de sécurité, augmente logiquement les opportunités d'action pour les services hostiles.

Dépendance technologique et économique

Au niveau des investissements directs à l'étranger, l'exemple de Nexperia montre que tout un secteur économique peut être déstabilisé par la perte de contrôle d'une seule entreprise stratégique dans la chaine d'approvisionnement. Les mêmes problèmes surgissent également lorsque nous dépendons d'un autre Etat pour une technologie indispensable à un secteur économique. C'est donc à juste titre que le SGRS participe, avec ses partenaires nationaux, au filtrage des investissements venant de l'étranger.

Anticiper les **menaces** contre les **intérêts belges**

Pour anticiper toute action de la Défense et conseiller le gouvernement dans sa politique intérieure et étrangère de sécurité et de défense, le SGRS suit, dans la mesure de ses moyens, toutes les tensions dans le monde qui peuvent avoir un impact sur la sécurité nationale et les intérêts belges.

Ce suivi s'exerce avec une approche 360°, pluridisciplinaire et multidimensionnelle pour anticiper les menaces contre les intérêts belges.

Ainsi, il applique les approches ASCOPE-PMESII (Zone, structure, capacités, organisation, personnes, événements - politique, militaire, économique, social, information, infrastructure). Mais aussi multidimensionnelle (les dimensions terre/air/mer/espace/cyber).

Service de renseignement extérieur

Sans que cela ne soit expressément indiqué dans son cadre juridique, le SGRS exerce de facto le rôle de service de renseignement extérieur. Il est en effet le seul acteur belge qui dispose de moyens de collecte importants et intrusifs à l'étranger, tant d'un point de vue du cadre légal que d'un point de vue des capacités techniques (CYBER, SIGINT, IMINT, etc.) et humaines (réseaux de sources et présence de militaires partout dans le monde).

Des besoins supplémentaires se font sentir, comme le suivi de politiques agressives en termes économique (augmentation de taxes douanières) ou en termes d'ambition d'annexion (le Groenland). Ou encore l'émergence de menaces dans l'espace (attaque sur les satellites Galileo) qui ont de potentiels impacts importants sur le Royaume.

Au regard des évolutions récentes et de la guerre hybride en cours, il est important pour la Belgique de disposer d'un service de renseignement extérieur fort capable de suivre les évolutions dans le monde qui peuvent avoir un impact sur les intérêts belges. Il en va de notre sécurité nationale et de notre autonomie stratégique.

Le SGRS envisage donc le suivi de ces nouvelles menaces extérieures dans la mesure où le cadre juridique est adapté à cet effet. Bien entendu, tout est mis en œuvre afin d'obtenir un renfort en personnel avec des profils spécifiques ainsi qu'un matériel à la pointe en matière de nouvelles technologies.

Cyber Rapid Response Teams : La coopération européenne en action

Réagir en 72h : les équipes cyber européennes à l'œuvre

Dans le cadre de la politique européenne de sécurité et de défense, plusieurs projets sont en cours au-travers de la coopération structurée permanente (PESCO) afin de renforcer conjointement les capacités. L'un de ces projets est le PESCO CRRT (Cyber Rapid Response Teams).

La Belgique prend les devants

En 2025, la Belgique a pris la présidence du PESCO CRRT, qui est assurée dans la pratique par le Cyber Command du SGRS. Outre l'organisation d'un council meeting, accompagné d'un cyberexercice, la Belgique était également responsable en 2025 du suivi opérationnel des différentes activations du CRRT. Cela implique notamment que la Belgique fournisse le chef d'équipe pendant l'activation.

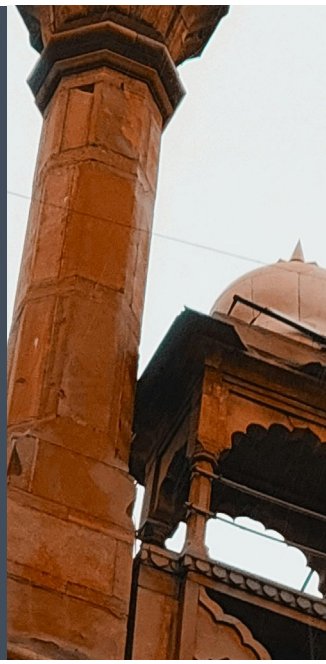
Déploiement en Somalie et en Moldavie

En 2025, le CRRT a été déployée en Somalie sous la supervision de la Belgique. Ils y ont mené des opérations de cybersécurité afin de soutenir l' « European Union Training Mission Somalia » sur le réseau EUTM local, dans le but de formuler des recommandations visant à améliorer la sécurité. Un deuxième déploiement a suivi en appui aux autorités moldaves. Compte tenu de la situation géopolitique, le réseau électoral a dû être analysé. Une équipe internationale d'experts, dirigée par le Cyber Command, a été en mesure d'aider les autorités à garantir le bon déroulement des élections.

Du terrain international à la résilience nationale

L'expérience acquise dans ce cadre international, non seulement en matière de processus, mais aussi d'équipement et de connaissances, est précieuse pour la mise en place du CRRT au niveau national. Une intervention rapide en cas de crise ou de conflit sera essentielle pour garantir notre liberté de mouvement dans le cyberespace. L'objectif est donc de disposer à terme de plusieurs CRRT au sein du Cyber Command.

Renforcement de la **coopération** entre la **Belgique** et **l'Inde** en matière de défense

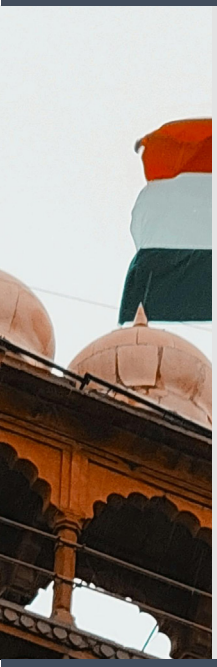


L'émergence de l'Inde en tant que puissance géopolitique est devenue l'une des caractéristiques déterminantes de l'évolution de l'ordre mondial au XXIe siècle. En tant que plus grande démocratie au monde et l'une des économies connaissant la croissance la plus rapide, l'Inde se transforme progressivement, passant du statut d'acteur régional à celui d'acteur central qui façonne l'équilibre des pouvoirs en Asie et dans l'Indo-Pacifique.

Au cours de la dernière décennie, New Delhi a mené une politique étrangère plus affirmée et indépendante, cherchant à diversifier ses partenariats tout en conservant son autonomie stratégique. Ce réajustement reflète l'ambition plus large de l'Inde de tracer sa propre voie sur la scène internationale et se caractérise à la fois par une coopération et des frictions occasionnelles avec ses partenaires traditionnels tels que les États-Unis.

La partie stratégique et commerciale de New Delhi

La pertinence stratégique de l'Inde dépasse largement le cadre économique. Reliant l'Asie du Sud, l'océan Indien et l'Indo-Pacifique, son emplacement en fait un acteur clé de la stabilité régionale. Alors que les tensions s'intensifient dans l'Indo-Pacifique et que l'influence de la Chine s'étend, la posture diplomatique et militaire de l'Inde suscite une attention mondiale accrue. Les efforts déployés par l'Union européenne pour finaliser un accord de libre-échange avec l'Inde d'ici la fin de l'année témoignent d'une reconnaissance plus large du potentiel de New Delhi en tant que partenaire commercial et stratégique.



Diversification des partenariats de défense

Dans le même temps, l'Inde est confrontée à des défis urgents en matière de modernisation de sa défense. Longtemps dépendante des livraisons d'armes russes, New Delhi doit désormais faire face à des perturbations dans l'approvisionnement et à des changements dans les alignements géopolitiques à la suite de la guerre en Ukraine. Cette situation a accéléré la volonté de l'Inde de diversifier ses partenariats en matière de défense, ouvrant ainsi de nouvelles perspectives de collaboration avec les industries européennes. Les entreprises belges de la défense, entre autres, ont déjà pris pied sur le marché indien, offrant des technologies de pointe et des chaînes d'approvisionnement sécurisées qui correspondent aux objectifs de l'Inde en matière d'autonomie et d'amélioration des capacités.

Dans ce contexte en pleine évolution, Bruxelles considère New Delhi non seulement comme un acteur majeur dans le maintien de la stabilité dans l'Indo-Pacifique, mais aussi comme un partenaire essentiel pour faire progresser l'innovation technologique et la résilience industrielle. Dans le cadre de cette reconnaissance croissante, la Belgique vise à approfondir ses relations bilatérales en élargissant sa coopération avec l'Inde dans le secteur de l'armement ainsi que dans le domaine de la coopération militaire.

Ouverture d'un poste d'attaché de Défense à New Delhi

Afin de renforcer encore davantage toutes les collaborations, le SGRS a nommé depuis septembre 2025 un attaché de Défense à New Delhi : Le général de brigade Engels, avec l'adjudant Mertens comme secrétaire.

La nomination par la Belgique d'un attaché de Défense en Inde représente une avancée concrète vers l'objectif de coopération entre les deux pays. Une telle position facilitera le dialogue direct entre les institutions de défense et soutiendra les projets communs entre les entreprises belges et indiennes. Au-delà de la dimension industrielle, cela renforcera également la compréhension mutuelle et la coopération entre les forces armées des deux pays, consolidant ainsi la cohésion et à la durabilité de leur relation de défense.

Le SPF Affaires étrangères : un partenaire-clé de la stratégie de sécurité nationale

Dans un contexte géopolitique particulièrement tendu (multiplication des conflits armés, montée des régimes autoritaires, fragilisation des alliances multilatérales, accroissement des menaces hybrides), le gouvernement Arizona ambitionne de repositionner la Belgique comme acteur stratégique en Europe.

Le SPF Affaires étrangères, à la fois vecteur de projection de puissance douce et acteur de sécurité, occupe un rôle prépondérant dans la formulation et l'exécution de la stratégie de sécurité nationale. La complémentarité stratégique des Affaires étrangères et du SGRS, les deux institutions belges par excellence ayant vocation à travailler à l'extérieur du territoire national, ne peut pas être plus évidente qu'aujourd'hui !

En régime, la coopération entre les deux institutions consiste notamment en :

1. L'organisation de briefings aux diplomates, préalablement à leur mise en poste, afin de les sensibiliser aux enjeux géostratégiques et sécuritaires pour leur zone de responsabilité.
2. La coopération en zone, au sein des postes diplomatiques, par le biais du réseau d'attachés de défense et des postes diplomatiques.
3. L'échange d'informations (demandes spécifiques, rencontres entre analystes, réunions interdépartementales, débriefing des diplomates, etc.) en vue de nourrir la position d'information et renforcer la posture de Contre-Ingérence de nos services respectifs.
4. L'appui par la capacité Cyber du SGRS, tant pour la sensibilisation aux risques dans le cyberespace que pour tenter d' identifier les acteurs derrière les cyberattaques.
5. L'exécution de « sweepings », c'est-à-dire l'inspection approfondie de locaux avant des rencontres sensibles et/ou des réunions classifiées des deux institutions afin de vérifier qu'aucun matériel d'interception n'est présent.

En 2025, le renforcement des synergies et de la coopération entre les Affaires étrangères et la Défense a été couronné par la signature d'un accord-cadre comprenant une série d'annexes techniques impliquant spécifiquement le SGRS. Parmi les développements attendus, une meilleure mobilité du personnel entre les services respectifs et une mobilisation accrue des réseaux diplomatiques pour augmenter la position d'information.

Suite à une cyberattaque qui a durement frappé le réseau d'ambassades belges en 2019, imposant de déconnecter pendant plusieurs jours plus d'une centaine de serveurs situés à l'étranger, le SPF Affaires étrangères a mis en place un « Masterplan Cybersecurity ». La capacité Cyber du SGRS contribue activement à ce plan, y compris sa mise à jour annuelle, notamment en fournissant des évaluations en vue d'adapter les outils et les processus. Plus de 19.000 cyberincidents ont été enregistrés en 2024, dont plus de 1.100 ont été classés à haut risques. Parmi ceux-ci, quatre incidents visant probablement spécifiquement le SPF Affaires étrangères ont été bloqués à temps et n'ont eu aucune conséquence néfaste sur les services du SPF.

Vérifications de sécurité : un rempart contre les menaces

Les vérifications de sécurité garantissent que toute personne accédant à une zone ou une fonction sensible présente les assurances nécessaires pour protéger l'État et la population. Ces contrôles dépassent le cadre de la Défense : les demandes augmentent, les secteurs se diversifient et les analyses se complexifient, dans un contexte marqué par la montée des extrémismes et des menaces hybrides.

Un rôle élargi

Le SGRS intervient dans des domaines variés : aéroports, ports, prisons, centrales, douanes, SNCB. Il conseille les ressources humaines de la Défense pour le recrutement militaire et civil et contrôle les entreprises chargées des infrastructures sensibles. La coopération avec la Police fédérale et la Sûreté de l'Etat s'intensifie pour agir plus vite et plus efficacement.

Ces vérifications permettent d'éviter des scénarios critiques : un docker impliqué dans le trafic de drogue, un hacker prêt à paralyser un réseau ferroviaire ou encore un agent infiltré dans une administration.

Chiffres clés 2025

7000
candidats militaires

700
civils analysés

200
avis négatifs militaires

11
refus civils

10000
demande d'accès entreprises

5,5%
refusées

Habilitations de sécurité : accès strictement contrôlé

Une habilitation de sécurité (HS) donne accès à des zones, réseaux et documents classifiés, selon le principe « Need to Know ». En 2025 :

17 000 enquêtes pour **26 000** entités

Problèmes fréquents : **finances, drogues, alcool, extrémisme, violences, fraudes**

Contribution du SGRS aux plans nationaux et militaires

Depuis l'agression russe contre l'Ukraine, l'OTAN a renforcé sa posture via le concept de dissuasion et défense de la zone euro-atlantique (DDA). En réponse, la Belgique a élaboré trois plans stratégiques – Défense, Enablement et Résilience – pour faire face à des crises majeures ou à l'activation de l'article 5.

En 2025, le SGRS a contribué à cette planification en rédigeant des sections clés sur la cybersécurité, les opérations électromagnétiques, la sécurité et le contre-espionnage, en collaboration avec des partenaires tels que le CCB, l'IBPT, la Sûreté de l'État et l'OCAM. Le service a aussi participé à la préparation de l'exercice OTAN « Steadfast Defender 27 », renforçant la coordination civile et militaire.

Ces efforts visent à intégrer les menaces hybrides et cyber dans la planification nationale et à garantir des procédures robustes pour protéger les infrastructures critiques et soutenir les opérations alliées.

L'industrie belge **se blinde**

Sécurisation accrue des entreprises liées à la Défense

En 2025, le Bureau Industrie a intensifié ses efforts pour protéger les entreprises belges liées à la Défense face à des menaces croissantes telles que les cyberattaques, l'espionnage économique et les intrusions physiques. Cette mission s'est poursuivie en étroite collaboration avec l'Autorité Nationale de Sécurité (ANS), les officiers de sécurité des entreprises et des partenaires internationaux.

Le Bureau a supervisé les habilitations de sécurité pour plus de 1 000 entreprises impliquées dans des projets nationaux et internationaux (OTAN, UE, Organisation conjointe de coopération en matière d'armement), tout en veillant à la conformité des normes de sécurité physique. Il a également organisé une dizaine de sessions de sensibilisation sur la cybersécurité, la protection des informations classifiées et la sécurité des infrastructures sensibles, et a apporté son soutien à la rédaction des cahiers des charges pour les contrats classifiés.

Coopération internationale et rôle d'autorité désignée

En tant que « Designated Security Authority », le Bureau a facilité les échanges de documents sensibles et participé à des groupes de travail internationaux, notamment dans le cadre des projets européens de défense (Fonds Européen de Défense). Il a aussi diffusé des recommandations ciblées sur la sécurité périmétrique, la cybersécurité lors des déplacements, la conformité aux projets EDF et la menace croissante des drones.

Chiffres clés 2025

1500
demandes de visite (Request For Visit)

200
habilitations entreprises délivrées (+25 % par rapport à 2024)

Anticiper la menace par la coopération stratégique

Face à la montée des menaces hybrides, le Bureau Industrie a renforcé la coopération avec les entreprises stratégiques afin d'anticiper les évolutions technologiques et géopolitiques et maintenir un haut niveau de protection.

La Belgique accueille son **premier appareil F-35**

Le 13 octobre 2025, une étape historique a été franchie avec l'arrivée des premiers avions de combat F-35A Lightning II à la base aérienne de Florennes. Cet événement marque le début du déploiement du système d'armes le plus avancé de la Force aérienne belge au-dessus de notre territoire.

En amont de cette « First Aircraft Arrival », le « Special Access Program Central Office » (SAPCO) de la Direction Sécurité a joué un rôle clé. Le SAPCO a assuré l'accompagnement intensif de l'équipe de sécurité locale à Florennes, afin de garantir une réception de l'appareil à la fois sûre et conforme. Cela comprenait notamment le soutien aux activités d'installation par Lockheed Martin, l'élaboration de procédures et de directives pour la sécurité opérationnelle. Mais aussi la poursuite de la préparation des infrastructures et des systèmes de sécurité, ainsi que la coordination permanente avec les partenaires américains du USA Joint Program Office et du Program Security Officer.

Le SAPCO fait office de lien unique entre la Force aérienne belge et les différents services spécialisés au sein du SGRS. La réception réussie du premier appareil F-35 confirme non seulement la préparation technique et opérationnelle de la Défense, mais aussi l'importance stratégique de SAPCO en tant que coordinateur central de tous les aspects liés à la sécurité au sein du programme F-35 belge.

Le premier container TACSAPF F-35

Le TACSAPF constitue une solution avancée pour les déploiements militaires nécessitant rapidité, sécurité et flexibilité. Ces conteneurs sont conçus pour être rapidement déployables dans des conditions difficiles et répondent aux exigences de sécurité les plus élevées liées à l'utilisation du F-35. Les conteneurs ont des fonctionnalités spécifiques telles que la sécurité, la planification des missions et le support IT. Grâce à leur conception modulaire, ils peuvent être facilement adaptés à divers besoins opérationnels.

Blindage électromagnétique

Tous les conteneurs TACSAPF sont dotés d'un blindage électromagnétique assurant une protection contre les attaques électroniques et les interférences. De plus, ils disposent de systèmes autonomes tels que la protection CBRN (chimique, biologique, radiologique et nucléaire), la détection d'intrusion, la protection contre les incendies et le contrôle des accès, ce qui leur permet de fonctionner de manière indépendante sans dépendre d'infrastructures externes.

La combinaison d'un déploiement rapide, d'une protection robuste et d'une grande adaptabilité fait du TACSAPF un instrument essentiel pour les missions militaires modernes avec le F-35, où la fiabilité et la préparation opérationnelle sont primordiales.

Objectif opérationnel

Le premier lot complet de quinze conteneurs a été livré au 2 Wing à Florennes. Il s'agit du résultat d'une période intensive durant laquelle, en à peine un an et demi, non seulement l'ensemble du design review américain a été mené à bien, mais où la production, avec ses règles de sécurité strictes, et la livraison ont également été consolidées. La prochaine étape consiste à faire accréditer le TACSAPF pour un usage opérationnel et à l'employer lors d'un premier déploiement au cours du premier trimestre 2026.

Sécurité militaire : garantir la **sécurité** des **infrastructures de la Défense**

La sécurité militaire représente l'épine dorsale de la protection de la Défense contre les menaces internes et externes, de sorte que les opérations puissent se dérouler efficacement et en toute sécurité. Un véritable « Security by design » permettra d'améliorer considérablement la sécurité militaire à terme.

La construction de nouvelles infrastructures dans les bâtiments de la Défense nécessite davantage d'organisation que le simple processus de construction physique. À cet égard, le SGRS suit activement des dizaines de projets et gère également la réglementation de sécurité. Pensez par exemple au nouveau quartier général, aux infrastructures CAMO, au nouveau Medhub et à la base navale de Zeebruges.

Des Ardennes à la mer, d'Arlon à Ostende, le service de sécurité militaire est impliqué. Chaque nouveau projet présente donc ses propres défis et son propre calendrier.

Un suivi intensif avec coaching est toujours assuré dès notre implication dans la phase initiale.

L'un des principaux objectifs est de continuer à rechercher activement des solutions innovantes pour relever les défis de demain en matière de sécurité. Enfin, nous nous efforçons de réduire autant que possible l'écart entre la base réglementaire et les problèmes concrets rencontrés sur le terrain.

M940 Oostende, premier navire de la nouvelle génération de navires de lutte contre les mines.

L'humain comme première ligne de défense

En 2025, le SGRS a poursuivi l'élargissement de son réseau de capteurs HUMINT au sein des différentes unités militaires en Belgique afin de détecter les menaces relevant du spectre TESSOC (Terrorisme, Espionnage, Sabotage, Subversion, Crime organisé).

Depuis l'entrée en vigueur en 2022 des dispositions légales encadrant la collecte de données auprès des sources humaines, le SGRS a continué à mettre en œuvre des méthodes visant à vérifier leur loyauté et fiabilité. Parallèlement, la procédure interne de gestion des sources en matière de contre-ingérence a été mise à jour et renforcée.

La coopération avec les partenaires nationaux (Sûreté de l'Etat, Police fédérale) et internationaux s'est intensifiée grâce à des formations communes, des entraînements conjoints et le lancement de coopérations opérationnelles.

Electromagnetic Warfare : **passage à la fréquence supérieure en 2025**

La guerre en Ukraine a rappelé l'importance du spectre électromagnétique dans les opérations militaires. Communications, navigation, surveillance, renseignement, commandement et défense reposent sur son exploitation. L'objectif est clair : priver l'adversaire de ces capacités tout en protégeant les nôtres. En 2025, la Défense, le SGRS et le Cyber Command ont engagé une montée en puissance structurée.

La Vision Stratégique 2025 consacre l'EW comme priorité et prévoit plus de 500 M€ d'investissements pour renforcer les moyens. Les Forces ont défini des besoins spécifiques : intégration de capacités EW dans les brigades dès 2027, moyens ESM (Electronic Support Measure) pour la Marine, senseurs avancés pour la Force aérienne et création d'un « Air Warfare Centre ». Cette dynamique s'accompagne de la refonte du centre actuel en un Joint « Electromagnetic Warfare Centre » (JEWC 2.0), destiné à soutenir toutes les opérations et à développer des capacités souveraines de classe internationale. Des discussions sont en cours avec le Royaume-Uni pour s'inspirer de son modèle, tout en scellant des partenariats durables avec l'industrie belge. Le changement sémantique de « guerre électronique » à « guerre électromagnétique » reflète une évolution doctrinale majeure : l'EW couvre désormais l'ensemble du spectre, y compris les technologies spatiales, infrarouges, lasers et micro-ondes, et s'intègre dans une approche multi-domaine. Le Cyber Command belge a contribué activement aux travaux de l'OTAN en la matière.

Des réalisations opérationnelles et technologiques

Sur le plan opérationnel, l'EWC a soutenu des missions clés en 2025 (Iceland Air Policing, déploiements F-16, surveillance en mer Noire, opérations A400M). Elle a également renforcé ses moyens avec un nouveau véhicule, une chambre anéchoïde (chambre destinée à absorber les ondes sonores et électromagnétiques) et des techniques anti-drones. Des progrès ont été réalisés pour l'appui au F-35A et pour la coopération multinationale visant le partage des bases de données et l'interopérabilité totale. Enfin, le projet THREAT marque un premier pas vers des zones d'entraînement dédiées, offrant à la Force aérienne un système déployable de simulation électromagnétique.

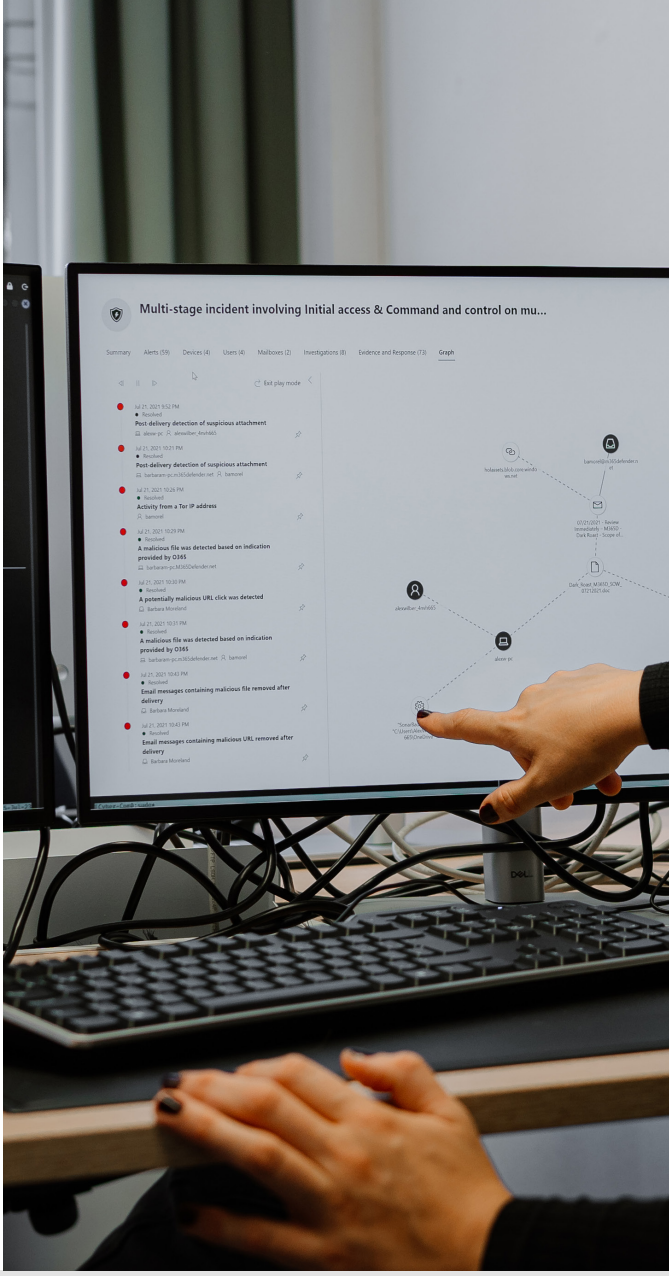
Le Cyber Command et la **défense active des réseaux**

La Force Cyber assure des réseaux de notre organisation au travers de son Security Operations Center (SOC). Cette entité opérationnelle est au cœur de la détection, de l'analyse et de la réponse aux incidents de cybersécurité. Son rôle consiste à surveiller en continu nos infrastructures numériques, à identifier toute activité suspecte et à réagir avec efficacité face aux menaces détectées. Ce dispositif constitue la première ligne de défense de l'organisation contre les attaques informatiques toujours plus sophistiquées.

De SOC à SIC : une transformation guidée par l'Intelligence

Depuis plusieurs années, une évolution majeure a été engagée : le passage d'un modèle de SOC traditionnel à un Security Intelligence Center (SIC), en d'autres termes un SOC guidé par les données et le renseignement Cyber. Cette transformation repose principalement sur une nouvelle architecture intégrant un SOAR (Security Orchestration, Automation and Response).

Cet outil permettra l'automatisation des incidents à faible criticité ainsi que l'orchestration d'incidents à plus haute intensité, réduisant ainsi la charge opérationnelle quotidienne et libérant les analystes pour se concentrer sur les menaces complexes et ciblées. Le SOC devient ainsi un centre proactif, capable de s'appuyer sur la donnée et l'intelligence pour anticiper et contrer les attaques. Cette évolution majeure est actuellement en train de voir le jour.



Renforcement des coopérations et partenariats stratégiques

La montée en puissance du SOC vers un véritable SIC s'accompagne d'un recours accru à l'appui externe. Deux contrats sont en cours d'implémentation : l'un dédié à la surveillance optimalisée du périmètre externe de nos réseaux, l'autre orienté vers la fourniture de l'outillage nécessaire au nouveau modèle de fonctionnement du SIC – incluant le SOAR – ainsi que l'expertise pour une réponse avancée aux incidents. Ces initiatives permettront à notre centre opérationnel de franchir un nouveau cap en matière de maturité et de résilience cyber.

Une année d'activité intense et maîtrisée

L'année écoulée a été marquée par une forte activité opérationnelle. Nos équipes ont contré plusieurs tentatives d'attaque, dont un « password spray » rapidement détecté et neutralisé. Par ailleurs, la vigilance du SOC a permis de découvrir une faille critique avant toute exploitation effective telle que celle subite lors de l'incident majeur de décembre 2021. Le correctif a été appliqué en collaboration avec les autres services d'appui dans des délais courts et maîtrisés, prévenant ainsi un nouvel incident majeur. Ces succès démontrent la robustesse du dispositif de défense et la réactivité exemplaire des équipes face à un environnement de menace toujours plus exigeant.

Construire l'avenir : synergies et compétences

CY. D3F. FACTORY

Les sites de Charleroi et Bruges des Cyber Defence Factories sont les jalons d'une nouvelle perspective En avril 2025, une nouvelle session du « bootcamp » immersif en cybersécurité a été organisée avec la « Cyber Defence Factory » de Charleroi implantée sur le site de l'incubateur d'entreprises A6K/E6K. Cette initiative s'inscrit dans la volonté de renforcer les compétences face aux enjeux numériques.

Comme lors de la première édition, le programme réunit plusieurs acteurs de la triple hélice : la société de cybersécurité NRB, l'ASBL BeCode et le CPAS de Charleroi. Le bootcamp plonge les apprenants et apprenantes dans un cas inspiré de la situation dramatique rencontrée par le CPAS en aout 2023, celle d'un ransomware qui l'a totalement paralysé pendant plusieurs semaines. Les défis concrets du secteur aident les participants à développer leurs compétences et à formuler des recommandations pour mieux protéger les systèmes utilisés par les administrations.

Renforcement des synergies

L'année écoulée s'inscrit comme une année de consolidation, marquée par la structuration des actions et le renforcement des synergies. Grâce à une enveloppe budgétaire dédiée, nous avons pu mettre en œuvre un appel à projets ambitieux, favorisant l'innovation et la coopération entre acteurs. Chaque édition se construit autour d'un thème renouvelé annuellement, décliné en plusieurs volets afin de répondre aux enjeux stratégiques et aux spécificités des écosystèmes dans lesquels les Cyber Defense Factories sont implantées. Cette approche garantit une adaptation fine aux réalités locales tout en consolidant la présence des Factories comme lieux de rencontre entre les activités de la Force Cyber, du SGRS et des écosystèmes civils.

Une deuxième CDF à Howest à Bruges

Le 13 mai 2025, le Cyber Command inaugurait la deuxième « Cyber Defence Factory » sur le campus d'Howest à Bruges en compagnie de nombreuses personnalités du monde académique et politique. La particularité de cette deuxième Factory c'est de se tourner vers les projets de cyberdéfense avec la Marine, notamment avec l'arrivée du premier chasseur de mines de nouvelle génération « M940 Oostende » en novembre 2025 à Zeebrugge.

L'implantation d'une nouvelle Factory sur le site d'Howest était presque une évidence. Tout d'abord parce que le Cyber Command était impliqué depuis longtemps dans ses modules de cours relatifs à la cybersécurité. Ensuite parce que Howest est stratégiquement positionné au cœur de l'écosystème académique et de recherche local, aussi bien public que privé avec une proximité avec les infrastructures de la base de la Marine.

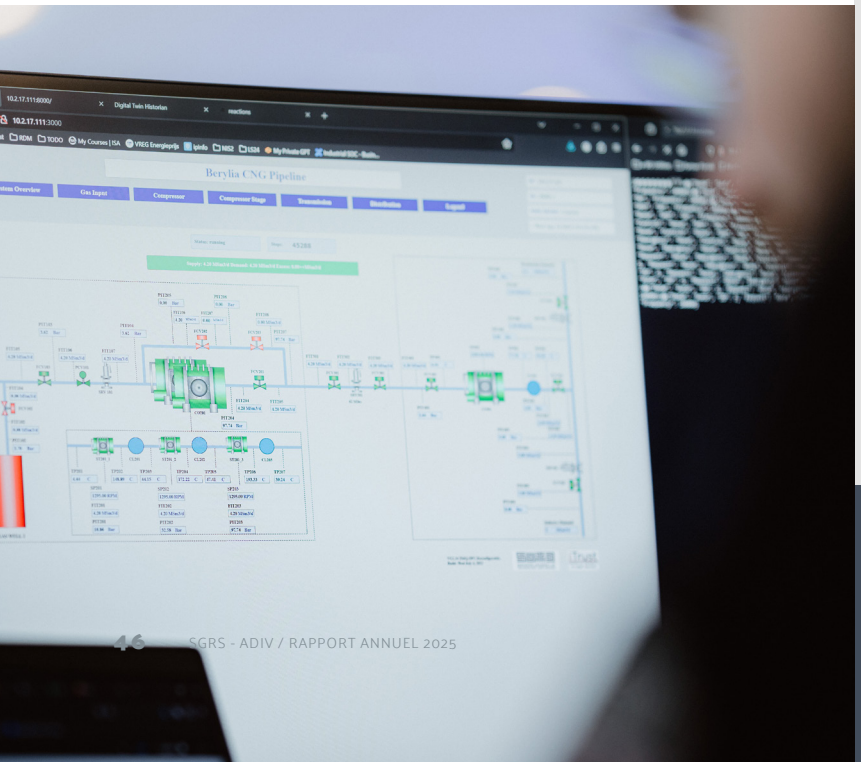
Dès 2026, une troisième Factory verra le jour, renforçant notre maillage territorial et nos capacités d'action. Le financement disponible permettra de soutenir jusqu'à 1,8 million d'euros de projets visant à accroître la cyber-résilience militaires et civile (dual-use). Pour accompagner cette montée en puissance, un Governance Board viendra chapeauter les structures et insuffler une ligne stratégique commune. Enfin, un site web dédié devrait voir le jour, offrant une vitrine et un point d'accès centralisé à nos initiatives. L'adoption d'un nouveau logo illustre cette dynamique : le chiffre 3 y symbolise la triple hélice des partenariats – industriels, académiques et institutionnels – qui constituent le socle de nos Factories.

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

L'année 2025 a marqué le premier jalon opérationnel de la Joint Cyber Defence Resilience Force Unit (JCDRFU). L'unité s'intègre pleinement dans la stratégie nationale de cyberdéfense de la Belgique, en cohérence la Stratégie de Résilience Cyber, et renforce les synergies entre acteurs publics et privés.

Sa mission s'articule autour de trois dimensions complémentaires. Elle soutient les opérations militaires en apportant une expertise cyber et en renforçant le niveau de mise en condition. Elle contribue à la préparation cyber par la mise en place de formations spécialisées et le développement de compétences afin de maintenir un haut niveau d'opérationnalité de la réserve dans la cyberdéfense.

Enfin, elle assure un soutien national et une contribution à la résilience en période de crise, en renforçant le commandement et le contrôle, et en disposant de la capacité d'agir de manière autonome lorsque les circonstances l'exigent.



Le principe directeur de l'unité est résumé dans la devise **PRIME - Promote, Recruit, Implement, Manage, Enhance :**

Promote : instaurer confiance et crédibilité tout en répondant aux défis organisationnels et opérationnels.

Recruit : développer un vivier hybride de militaires, civils et partenaires dotés de qualités techniques et morales.

Implement : ancrer la résilience par une intégration basée sur les rôles permettant une contribution effective aux opérations de routine.

Manage : responsabiliser individus et équipes, tout en exploitant des outils modernes et interopérables pour garantir une gestion efficace des activités et projets.

Enhance : améliorer en continu les capacités afin que la JCDRFU demeure un acteur essentiel de la résilience nationale.

L'année 2025 a été marquée par plusieurs avancées significatives. La première Journée de Cohésion organisée au Fort d'Eben-Emael le 25 mai 2025, en présence du Général Van Strythem et du Colonel Godefridis, a permis de combiner histoire et esprit d'équipe tout en assurant la promotion du recrutement.

L'initiative « bring a friend », lancée à cette occasion, a renforcé notre visibilité et contribué à l'attraction de nouveaux talents. Parallèlement, à l'heure d'écrire ces lignes, plus de quarante collaborateurs militaires locaux ont été recrutés, traduisant la volonté de bâtir un vivier durable de réservistes qualifiés capables de répondre aux défis géopolitiques et opérationnels émergents.

L'unité a également développé de nouveaux outils internes, conçus pour répondre aux défis administratifs et opérationnels. Cette dynamique d'innovation constitue un levier essentiel pour une activation flexible et orientée projet, capable de soutenir à la fois les activités quotidiennes et les missions de contingence.

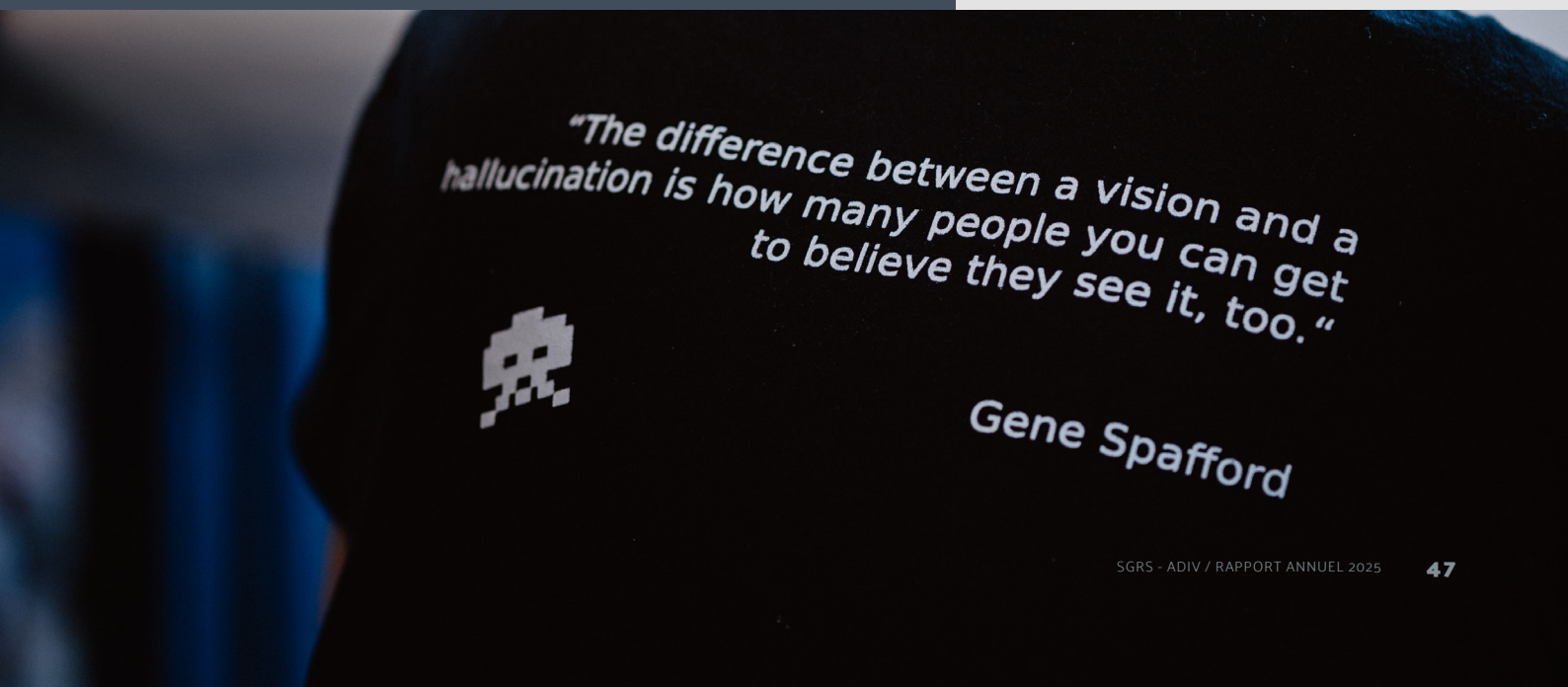
En parallèle, la JCDRFU a multiplié les initiatives de visibilité et d'engagement. Sa participation active aux « jobdays », aux salons de l'emploi, ainsi qu'à des événements académiques et sectoriels, a renforcé la compréhension mutuelle avec l'écosystème cyber belge.

Des synergies ont été créées tant au sein de la Défense que vers l'extérieur. Que ce soit avec les centres d'information de la DG HR et ses différents départements qu'avec les universités, les hautes écoles et les acteurs clés du domaine, consolidant ainsi un partenariat stratégique.

Dans ce contexte, la mise en avant du statut de réserviste étudiant constitue une innovation notable. Elle répond à un triple objectif : contribuer à la formation et à l'expérience des jeunes talents, créer un vivier de recrutement durable et renforcer la résilience nationale par l'intégration progressive de compétences issues du milieu académique.

Enfin, la JCDRFU a pris part activement au Task Force Reserve Work Group durant l'été 2025, contribuant à définir la vision à long terme et la gouvernance des forces de réserve belges selon un principe de travail ascendant (bottom-up).

L'année à venir sera centrée sur l'expansion du recrutement de personnels qualifiés et la consolidation des structures administratives indispensables à l'organisation d'une force moderne et résiliente. Dans un contexte géopolitique et cyber en mutation rapide, la JCDRFU confirme sa détermination à renforcer la posture de défense de la Belgique et à contribuer durablement à sa résilience collective.



Jean-Luc Trullemans : de la sécurité aux spatial et du renseignement aux étoiles

Jean-Luc Trullemans est directeur du Centre européen de sécurité et d'éducation spatiale (ESEC) de l'Agence spatiale européenne (ESA) depuis 2022. Celui qui a eu précédemment une longue carrière dans le domaine de la sécurité à la Police Fédérale nous éclaire sur les enjeux stratégiques du spatial et de la cybersécurité qui sont intrinsèquement liés.

Vous ne vous destiniez pas à une carrière dans le spatial ?

Non, pas du tout. Je suis exclusivement né dans le domaine de la sécurité. J'ai démarré ma carrière comme enquêteur à la Police Judiciaire de Bruxelles. Je suis devenu commissaire à la réforme des Polices et j'ai rejoint l'escadron spécial d'intervention en 2003 qui était une unité de la gendarmerie. En 2014, je suis devenu commissionnaire divisionnaire et conseiller opérationnel du Directeur général de la DG police administrative.

Vous ne vous destiniez pas à une carrière dans le spatial ?

J'ai vécu la réforme des polices de l'intérieur en passant de la PJ à la Police Fédérale de 2000 à 2004 J'étais avec trois collègues responsable de la direction des opérations judiciaires. C'est-à-dire la gestion de l'engagement des unités spéciales et des méthodes particulières de recherche où je collaborais régulièrement avec les collègues du SGRS de l'époque.

Comment avez-vous commencé à l'ESA ?

Quand j'ai pris mes fonctions en 2022, mon directeur m'a donné une mission claire : sortir l'ESEC de son anonymat. Pour y arriver il fallait mettre en place des partenariats et un des points de développement du site était la cybersécurité. Ce qui fait notre force c'est notre capacité à créer des réseaux, c'est ce que j'ai fait dans mon ancienne carrière et j'ai continué à le faire ici. J'ai rencontré Michel Van Strythem et nous avons rapidement trouvé des points d'ancrage et d'intérêt commun. Je l'avais invité lors de la construction du centre et je lui ai dit : « ton projet (le Cyber Command) et le mien ont grandi ensemble. » Il m'a répondu : « oui et ils n'ont plus qu'à faire des enfants ensemble ». Nous avons concrétisé cette collaboration avec la signature d'un accord entre l'ESA et le Cyber Command et la désignation d'un officier de liaison.

En quoi la cybersécurité et le spatial sont-ils liés ?

Le champ de bataille se nourrit de données issues d'infrastructures spatiales qui ont besoin d'être protégées. Et donc, on peut dire que cyber et espace ne font qu'un ensemble cohérent. L'un ne va plus sans l'autre. A l'ESA, tout ce que nous faisons repose sur l'IT. Et tout cela doit être sécurisé. Une architecture spatiale est composée d'un élément qu'on appelle le spatial, d'un deuxième qui est le sol et le troisième c'est la liaison entre les deux. L'élément spatial ce sont nos outils de production autrement dit les satellites. Ils évoluent à des vitesses variables contenues entre 300-350 km et 35 000 km voire plus. Il y a donc toute une couche où de la technologie très spécifique doit être activée pour protéger ces outils. Ils produisent des données qui nourrissent des services télécom, des systèmes d'intelligence ou de reconnaissance, des images, bref toute une série de choses. Ces données sont ensuite transmises au sol et le vecteur doit donc être protégé lui aussi. Au sol, nous devons également traiter ces données brutes pour les rendre exploitables par l'utilisateur final ce qui nécessite encore un élément de transfert. La cybersécurité que nous avons développée est donc tridimensionnelle puisqu'elle intègre le volume qui se trouve au-dessus de la terre, l'espace, le vecteur et la dimension sol. Aujourd'hui, l'outil dont nous disposons pour sécuriser l'ensemble est tout à fait original. Le choix de l'ESA a été de développer un outil spécifique et non pas d'assembler des briques technologiques préexistantes. Mes collègues de la JAXA (agence japonaise spatiale) vont largement s'en inspirer pour la construction de la résilience de leur agence. Nous avons donc été des précurseurs.

Pourquoi la collaboration entre la Défense et le spatial est-elle d'importance stratégique ?

Depuis la conférence ministérielle de novembre 2025, l'ESA a reçu pour la première fois dans le mandat de contribuer à la construction de systèmes de sécurité et de défense. Je vous parle en toute humilité car le simple mot de « défense » était presque un anathème ici à l'agence il y a quelques mois. L'œuvre conjuguée de quelques visionnaires dont le directeur général de l'ESA et du travail de l'ensemble de mes collègues ont permis d'ouvrir cette voie après 50 ans. Aujourd'hui, et ce qui se passe en Ukraine l'a largement démontré, l'utilisation de l'applicatif spatial est quotidien. La démonstration est également faite que des applications au départ développées à des fins civiles ont été intégrées dans le catalogue des outils dont une Défense peut faire usage. C'est ce qu'on appelle les applications duales, civiles et/ou militaires. Aujourd'hui, il faut réfléchir à intégrer l'applicatif qui peut nourrir dès la naissance du programme ou du projet. Ce qui compte dans le cadre des applications duales c'est l'usage que vous allez faire de l'outil. Un couteau peut être une arme si vous le plantez dans le ventre de votre adversaire et peut être un outil si vous l'utilisez pour couper votre pomme.

Plus concrètement, que peut-on citer comme autres applications duales à part la météorologie et le renseignement ?

La cryptographie par exemple, nous l'utilisons globalement pour l'ensemble de nos missions. Les données initialement produites à l'intérieur d'un programme purement scientifique sont cryptées parce qu'elles ont besoin d'être protégées. C'est ce qu'on a commencé à faire ici depuis une petite dizaine d'années. Le centre de cybersécurité que nous avons construit à l'ESEC répond aux normes TEMPEST ainsi qu'aux norme de l'ESA, ce qui nous permet de viser un niveau d'habilitation jusqu'au niveau secret. C'est une petite révolution au sein de l'agence car ce besoin n'était pas reconnu d'emblée. Certains programmes comme GALILEO par exemple intègrent plusieurs services dont une application gouvernementale qui exigent plus de robustesse en matière de cryptographie que les autres. Et, là aussi, on peut parler d'applications duales puisque nos besoins rencontrent ceux des autres.

SGRS & Université de Gand

La cellule Innovation a contribué, en tant que conseillère pédagogique et partenaire enseignant, au programme de certificat en études du renseignement de l'Université de Gand.

Sur la base de ce rôle, d'autres initiatives ont été lancées afin de développer des modules de cours spécialisés et de nouveaux programmes académiques dans les universités belges.

Les thèmes abordés comprennent la radicalisation, l'extrémisme, le terrorisme, l'analyse des risques et la logique argumentative.

GHENT UNIVERSITY

Archives déclassifiées

En 2025, le travail au sein de nos archives classifiées n'a pas cessé. Il a de nouveau été consacré à la conservation, à la gestion et à la déclassification d'archives, dans le respect des dispositions légales et des procédures.

Des archives bien gérées garantissent la préservation des connaissances et du contexte, même lorsque les structures ou les systèmes changent. La déclassification et la mise à disposition de ces documents représentent un processus minutieux, chronophage et laborieux. Chaque dossier doit être évalué individuellement, dans le respect des cadres juridiques, des règles de confidentialité et des intérêts des parties concernées. Cette évaluation exige non seulement une expertise technique, mais aussi de la précision, de la concertation et de la patience.

Des documents d'archives relatifs au passé colonial ont également été déclassifiés :

CONGO : Déclassification de documents sélectionnés à la demande d'un chercheur sur les événements survenus au CONGO en juillet 1960. Il s'agit des fonds COMETRO, VANDERSTRAETEN et GHEYSEN.

RWANDA : Documents relatifs aux événements survenus à ASTRIDA les 21 et 22 juin 1960, en particulier le dossier : « Rapport sur les événements de SOVU (BUFUNDI-ASTRIDA) »

En 2025, de nombreuses archives ont à nouveau été déclassifiées et ouvertes à la recherche (historique) :

Dossiers Agents de Renseignement et d'Action (ARA) et dossiers Services de Renseignement et d'Action (SRA) : en 1993, la Sûreté de l'État a déposé le fonds d'archives « Services de Renseignement et d'Action » auprès du CegeSoma. Ce sont les dossiers des volontaires qui se sont engagés dans des réseaux dans la Belgique occupée pendant la Seconde Guerre mondiale. Après la Seconde Guerre mondiale, un statut distinct a été élaboré au sein de la Résistance : le statut des Agents de Renseignement et d'Action (SRA). Au total, 18 716 personnes ont été reconnues comme SRA après la Seconde Guerre mondiale.

Dossiers de reconnaissance des résistants armés : en 1945, le statut de résistant armé a été instauré afin de rendre hommage à ceux qui avaient pris les armes contre l'occupant. Pour obtenir ce statut, il fallait avoir fait partie d'un groupe de résistance reconnu ou pouvoir prouver que l'on avait accompli individuellement des actes de résistance. Après la guerre, quelque 140 000 personnes pouvaient prétendre à ce statut. À partir de 1946, les dossiers constitués dans le cadre de l'obtention du statut de résistant armé ont été gérés par les services du Ministère de la Défense. Aujourd'hui, ces dossiers sont entièrement déclassifiés. -

Fonds d'archives « Archives du Comité d'acquisition de Liège conservées aux Archives de l'État » (RA LIÈGE)

ADIV · SGRS

QUAERO ET TEGO

Cyber Force
Through Partnerships

WWW.SGRS.BE