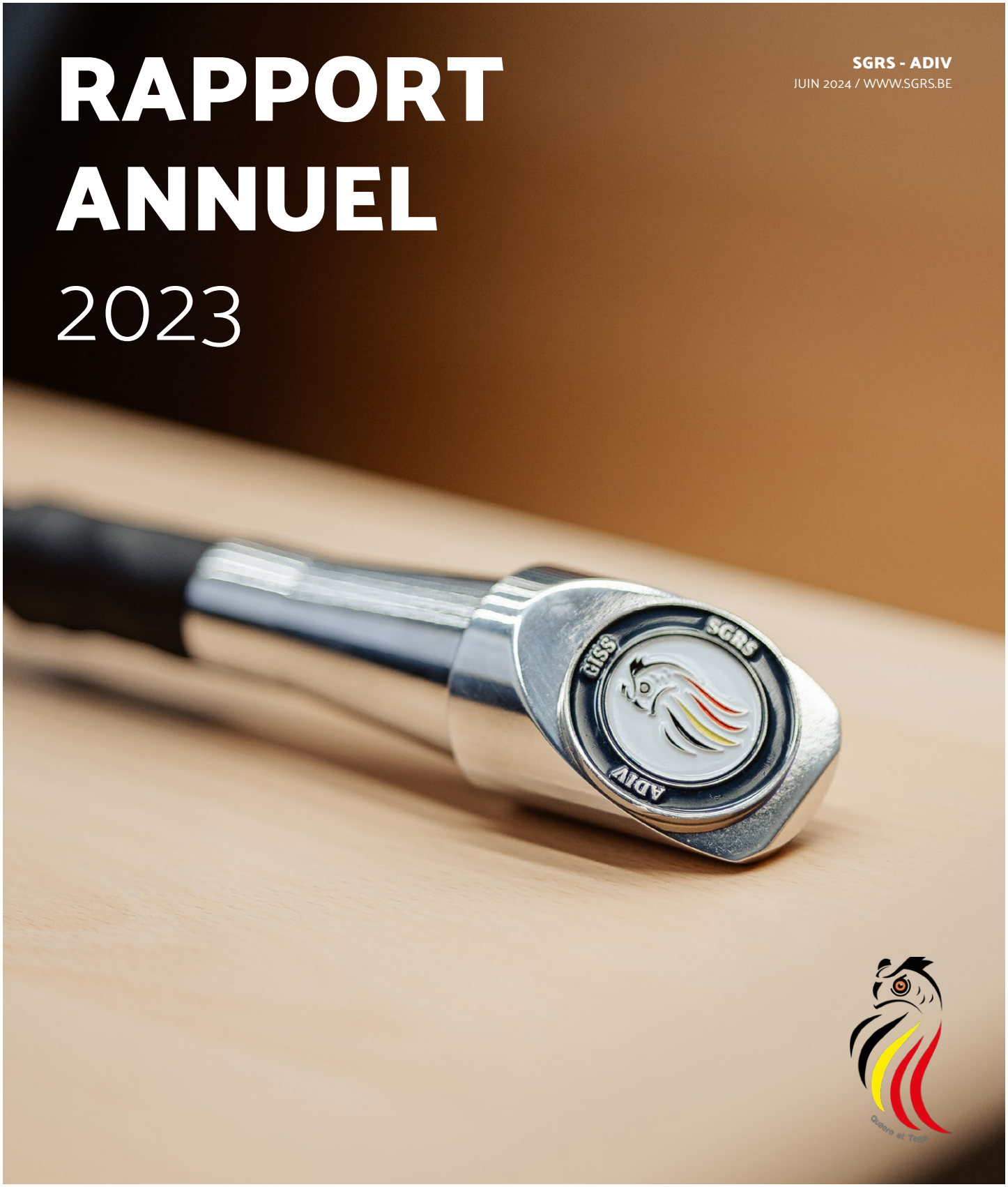
RAPPORT ANNUEL 2023

SGRS - ADIV
JUIN 2024 / WWW.SGRS.BE



LA DÉFENSE

.be

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 : ADIV-SGRS

Par le ADIV-SGRS

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

Général-major
Stéphane Dutron

REMISE-REPRISE DU STICK RSM

L'Adjudant-Major Frédéric Charlot, ancienement Adjudant de Corps a pris son congé et a laissé place au nouvel Adjudant de Corps Dolores Geeraert.

Introduction

L'actualité 2023 fut particulièrement chargée pour les services de renseignement et de sécurité.

Sans être exhaustifs, nous pouvons mentionner les coups d'État successifs en Afrique de l'Ouest, la reprise du conflit israélo-palestinien, la poursuite de la guerre d'agression de la Russie contre l'Ukraine ou encore le conflit dans l'Est de la République Démocratique du Congo.

Au cours de la même période, des phénomènes tels que l'extrémisme, le terrorisme, la criminalité organisée, la prolifération ou encore l'ingérence ont continué de faire peser une menace structurelle sur le continent européen. Nous l'avions déjà souligné lors du premier rapport en 2022 : les activités d'espionnage et d'ingérence étrangère ont atteint des niveaux inédits depuis la guerre froide. Cette tendance s'est confirmée malheureusement en 2023. La Belgique, et Bruxelles en particulier, en tant que siège de nombreuses organisations internationales, ne sont évidemment pas épargnées.

Collaborer pour mieux appréhender

Pour faire face à ces multiples menaces, la collaboration avec les autres services de renseignement et de sécurité est essentielle, tant en Belgique qu'à l'internationale. La collaboration avec la Sûreté de l'Etat est, en particulier, primordiale. Dans le cadre de la mise en œuvre du PSNR[1] , cette volonté de collaboration s'est traduite concrètement par la mise en place de plateformes, communes à nos deux institutions, pour lutter contre l'extrémisme et le terrorisme.

En parallèle, la numérisation de mon Service se poursuit afin de traiter au mieux la denrée première avec laquelle nous travaillons : l'information. Cette information, nous devons la protéger, l'analyser et la mettre en relation avec celles de nos partenaires. Pour cela, nous avons besoin de moyens informatiques modernes et sécurisés, non seulement pour sa collecte, mais aussi pour son traitement et sa diffusion.

La guerre de l'information, une réalité

Le champ informationnel est, d'ailleurs, devenu un nouveau champ de bataille et d'influence, avec la production massive, par des puissances étrangères, de contenus mensongers et/ou visant à promouvoir des narratifs contraires à nos valeurs. L'objectif reste le même, en Belgique comme dans le monde : affaiblir nos démocraties en sapant la confiance dans nos dirigeants et dans nos institutions. Pour ce faire,

[1]Le Programme Stratégique National de Renseignement (PSNR) définit les programmes de coopération structurels renforcés entre le SGRS et la Sûreté de l'Etat.

ces puissances tentent de polariser l'opinion publique en opposant les communautés à coups de « fake news ». Nous avions déjà surveillé le processus électoral en 2019 et nous sommes particulièrement attentifs au scrutin de juin 2024 avec l'ensemble de nos partenaires au Fédéral.

Poursuivre la modernisation du SGRS

J'ai eu l'honneur de prendre la tête du SGRS depuis le 1er janvier 2024. Je tiens à saluer l'immense travail de mon prédécesseur le Vice-Amiral Wim Robberecht qui a occupé la fonction de chef du SGRS pendant près de trois ans. Il a imprimé de profonds changements dans notre organisation et je compte maintenir le cap de la transformation et de la modernisation de notre Service.

Je ressens également une grande responsabilité car nous devons être à la mesure de nos ambitions, dans un monde où les équilibres géostratégiques traditionnels ont été bouleversés, où les défis sécuritaires sont multiples et où les crises se succèdent.

L'assise sociétale est la fondation de notre Service. Le développement de notre communication, qu'illustre ce deuxième rapport annuel, vise à renforcer ce lien avec la société et nos citoyens, dans les limites de transparence que notre métier particulier nous impose.

Ce lien, c'est aussi ce qui nous permettra de continuer à recruter du personnel motivé pour combattre nos adversaires, qu'ils soient chez nous, à l'étranger ou dans le cyberespace. Il existe des signaux positifs dans ce sens ; nous avons par exemple attiré plus de mille candidats lorsque nous avons ouvert quarante postes d'inspecteurs en 2023.

Je vous souhaite une agréable lecture.

GÉNÉRAL-MAJOR

Stephane Buton

VICE-AMIRAL
WIM ROBBERECHT

Chef du SGRS de 2021 à 2023

SGRS - ADIV / CYBER COMMAND

Cyber Command

Jour après jour, le Cyber Command poursuit son développement au sein du SGRS ainsi que l'initiation d'une cinquième composante au sein de la Défense.

Dans notre société qui se numérise de plus en plus, il est primordial de renforcer les capacités de renseignement et de sécurité du SGRS dans le cyberespace, mais également de développer les capacités de cyberdéfense, de guerre électronique et de guerre de l'information en appui de toutes les composantes et de l'ensemble de la Défense.

C'est à la fois une aventure humaine et technologique. Humaine car nous recrutons bon nombre de nouveaux collaborateurs qui proviennent de tous les horizons : de la Défense, du milieu académique ou de la recherche, ou encore du milieu associatif. Nous recrutons des militaires, du personnel civil et des réservistes. Il s'agit de profils STEM (Scientific, Technologic, Engineering, Mathematics) comme non-STEM. Il y a plus de quarante métiers au Cyber Command. Et nous tenons à offrir à chacun de ces profils les mêmes chances de se développer et de grandir avec nous. Ce qui demande non seulement un énorme investissement mais aussi une grande flexibilité. Mais je suis persuadé que cette diversité de profils et de talents fait partie de notre identité et représente la clé de notre réussite.

Dans le cadre de cette « guerre des talents », nous misons énormément sur les jeunes. Nous avons par exemple lancé en 2023 la « Summer School », la première université d'été cyber pour les étudiants. C'est une immersion d'une semaine dans le milieu militaire et dans les coulisses de la cyberdéfense, avec nos experts et ceux de l'Ecole Royale Militaire.

Le bilan du recrutement s'avère pour l'instant très positif. Depuis la création du Cyber Command le 19 octobre 2022, le personnel a augmenté de plus de 15% en valeur nette. C'est une réussite dans la mesure où le marché belge et international du travail est extrêmement tendu en matière de cybersécurité.

C'est aussi une aventure technologique, notamment avec l'émergence des EDT (Emerging and Disruptive Technology) comme l'intelligence artificielle, les applications de cloud souverain ou la cryptographie post-quantique. Ces dernières constituent des opportunités mais elles représentent aussi de puissantes menaces lorsqu'elles sont utilisées à mauvais escient, notamment dans le cyberespace.

Ces technologies sont appelées à jouer un rôle majeur dans le cadre de la cryptographie qui nous permet de sécuriser l'échange d'informations extrêmement sensibles ou de protéger les systèmes de communication et de commandement intégrés aux nouveaux systèmes d'armes de la Défense. Comme par exemple le chasseur F-35, la nouvelle capacité motorisée terrestre ou les futurs navires de la Marine.

Nous avons développé un commandement centralisé et une structure ambitieuse au sein du SGRS pour nous permettre de faire face à ces menaces, de les détecter, d'y répondre et de les anticiper. Le renforcement de nos capacités continuera à s'opérer dans le giron du Renseignement et de la Sécurité car nous y sommes intrinsèquement liés, que ce soit au niveau de notre cadre légal ou de l'exécution de nos missions.

L'aventure se poursuit donc et elle ne fait que commencer. Peut-être avec vous à nos côtés ?

GÉNÉRAL-MAJOR

Signature du protocole d'accord avec l'École Royale Militaire concernant des projets R&D.

Première réunion des cyber ambassadeurs et cyber commandeurs lors de la Présidence belge de l'Union Européenne.

Identifier les menaces extérieures d'aujourd'hui et de demain

Le SGRS est le service belge de référence pour le renseignement extérieur et de défense.

A ce titre, il fournit une expertise en analyse stratégique et de défense à ses clients, au premier chef desquels le gouvernement belge et le ministère de la Défense.

Cette analyse permet au SGRS d'identifier les menaces résultant des développements en cours à l'extérieur du Royaume, dans le cadre des compétences qui lui sont données par la loi du 30 novembre 1998. Il dispose à cette fin d'un réseau diversifié de collecte d'informations. Le SGRS développe une coopération renforcée avec certains partenaires pour ce renseignement extérieur et de défense, dont notamment le SPF Affaires étrangères.

Le monde en 2023

Deux conflits, en Europe de l'Est et au Moyen-Orient, ont particulièrement marqué l'actualité 2023.

En Ukraine, sur le théâtre des opérations militaires, la contre-offensive de l'été 2023 n'a entraîné aucun changement stratégique significatif. Le conflit ukrainien est devenu une guerre d'attrition susceptible de perdurer.

Au Moyen-Orient, du fait de la violence de la réaction israélienne et de l'implication de l'axe iranien via ses proxys, la reprise du conflit israélo-palestinien a accentué les tensions régionales et internationales. La sécurité maritime en Mer rouge s'en est vue impactée, entrainant des répercussions économiques non négligeables.

Des évolutions géopolitiques majeures

Ces deux conflits laissent voir en filigrane des évolutions géopolitiques majeures à l'œuvre dans le monde. Le "Rules-Based International Order", système promu par les démocraties libérales s'appuyant notamment sur les institutions onusiennes et de Bretton Woods, est désormais remis en cause, toujours plus ostensiblement, par des puissances révisionnistes, à l'instar de la Russie et de l'Iran. Le multilatéralisme, moteur des relations internationales ces dernières décennies, est mis à mal. Les puissances occidentales rivalisent avec leurs compétiteurs géopolitiques pour s'allier les puissances dites du Sud Global, cet ensemble hétéroclite de nations du sud qui hésitent dans leur positionnement stratégique.

La compétition entre « grandes puissances » redevient un enjeu majeur des relations internationales.

Si ces deux conflits, de même que la question de la migration, focalisent l'attention du public et des politiques occidentaux, ils ne doivent pas occulter d'autres enjeux ou zones du monde.

Le continent africain poursuit avec difficulté son développement économique. Il demeure confronté à une forte pression démographique, aux coups d'états et à la compétition entre puissances extérieures. Les pays du Sahel et d'Afrique de l'Ouest ont été particulièrement touchés par cette vague de putschs, entrainant des changements d'alliance. La situation sécuritaire y reste précaire. Le Soudan est toujours déchiré par une guerre civile. L'Afrique des Grands Lacs demeure, quant à elle, marquée par le conflit dans l'Est de la République démocratique du Congo.

En Asie, la montée en puissance de l'Inde sur fond de nationalisme se poursuit tandis que son voisin pakistanais, doté de l'arme nucléaire, se débat dans une profonde crise économique. La Chine tente de maîtriser le ralentissement structurel de sa croissance tout en poursuivant son développement technologique et militaire. Le développement et la projection de la puissance chinoise suscitent par ailleurs une inquiétude croissante chez certains pays voisins.

Un champ de bataille en constante mutation

En parallèle à ces crises, des évolutions structurelles, difficile à appréhender parfaitement aujourd'hui, sont à l'œuvre. Ainsi, les évolutions technologiques, comme l'intelligence artificielle, de même que leurs impacts sur la conduite des batailles, avec notamment l'usage accru de drones et moyens cyber, nécessitent de repenser ce que sera le monde de demain afin de mieux s'y préparer. De même, les questions de l'accès aux ressources et de la transition énergétique restent essentielles.

La fragmentation des sociétés occidentales par la poussée de l'extrémisme, la persistance de la menace terroriste et la montée en puissance de groupes criminels continuent par ailleurs d'impacter la situation sécuritaire en Belgique. De même, les menaces relatives à l'espionnage, l'influence et le sabotage, corollaires du retour de la compétition entre grandes puissances, sont appelées à marquer durablement notre paysage sécuritaire.

Retour de la compétition entre « grandes puissances »

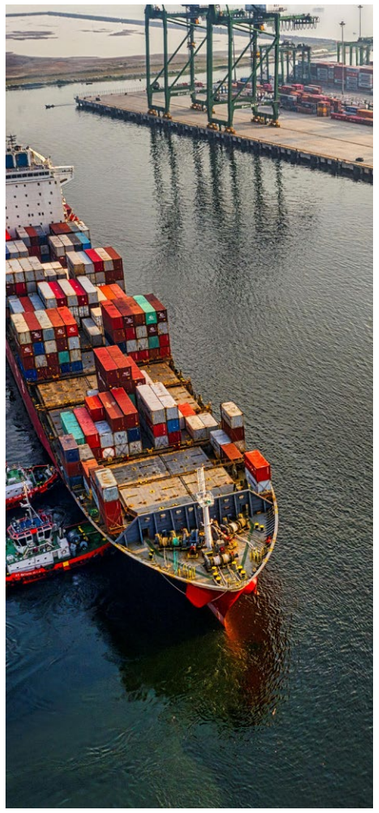
La chute de l'Union soviétique en 1991 avait ouvert une période de quasi-hégémonie de la puissance américaine. La mondialisation de l'économie et la diffusion de la démocratie libérale donnèrent naissance à des concepts tels que la Fin de l'Histoire de Francis Fukuyama.

Si la lutte contre le terrorisme avait marqué la première décennie du 21ème siècle, la compétition entre grandes puissances a progressivement fait son retour comme marqueur principal des relations internationales. Les démocraties libérales font face à des puissances autoritaires et révisionnistes qui remettent en cause aussi bien la puissance occidentale que l'ordre mondial et ses institutions.

Un jeu d'influence et de compétition

La montée en puissance de la Chine sur tous les plans bouleverse les équilibres établis. Dans le jeu d'influence et de compétition internationale, la Chine a lancé à l'échelle mondiale le projet de créer « les nouvelles routes de la soie », consistant à améliorer les voies de communication terrestres et maritimes entre elle et des dizaines d'Etats asiatiques, africains et européens. Et ce par le biais d'investissements économiques d'infrastructures et autres, de relations diplomatiques, de soutien militaire et de projection d'une puissance douce.

La Russie par sa politique d'agression armée en Ukraine a provoqué une rupture majeure avec les démocraties libérales occidentales. Depuis, pour contrer son isolement, elle s'efforce d'accroître son influence dans le monde. Elle manipule à son profit les mouvements de rejet de la domination occidentale, en Afrique notamment, en prenant l'initiative de coopérations militaires et sécuritaires. Sur



le plan diplomatique, la Russie souhaite développer sa vision d'un ordre mondial multipolaire et cherche à cette fin des alliés dans les forums internationaux.

Une question de ressources

La Chine et la Russie ont trouvé des terrains d'entente dans leurs efforts pour contrer la domination des démocraties libérales. Ainsi, juste avant l'invasion russe de l'Ukraine, les chefs d'État de la Russie et de la Chine ont annoncé un "partenariat illimité". Initialement, la Chine, qui défend les principes d'intégrité territoriale et de souveraineté dans ses relations internationales, s'est retrouvée dans une position inconfortable en rejetant les sanctions internationales contre la Russie. Elle a maintenu l'économie russe à flot en lui fournissant des matières premières et en lui offrant une alternative aux échanges monétaires internationaux limités par les sanctions. Pourtant la Chine souhaite maintenir la perception de neutralité et se présenter comme un acteur international responsable.

Pour la Chine, la guerre en Ukraine ne sert pas seulement d'apprentissage en vue d'une éventuelle action future à l'égard de Taïwan. Elle modifie aussi en sa faveur l'équilibre des forces entre elle et la Russie. Cette dernière est devenue dépendante d'elle pour faire fonctionner son industrie militaire. De plus, comme Moscou concentre toute son attention sur le conflit en Ukraine, la Chine peut accroître sa sphère d'influence au détriment de la Russie, par exemple en Asie centrale ou dans la région arctique.

Un jeu de vases communicants

Ce jeu de grandes puissances va bien au-delà des seules puissances américaines, chinoises et russes.

Ainsi, le Moyen Orient demeure marqué par la rivalité entre l'axe iranien et les puissances traditionnelles des pays du Golfe. A cette première ligne de fracture s'ajoutent les tensions entre les puissances proches de l'Islam politique et les puissances sunnites qui considèrent les Frères musulmans comme une menace pesant sur leur stabilité (Egypte, Arabie Saoudite, Émirats arabes unis).

En Asie du Sud, l'Inde est rentrée depuis quelques années de plein pied dans la mondialisation, bénéficiant d'une forte croissance et abritant la plus grande population mondiale. Son rival de toujours, le Pakistan, s'enfonce lui dans une profonde crise économique et politique.

Remise en cause de l'ordre international et du multilatéralisme

L'ordre international fondé sur le "Rules Based International Order" est le système bâti par les démocraties libérales, emmenées par les Etats-Unis. Ce système s'appuie notamment sur diverses institutions internationales et régionales, dont les institutions onusiennes et de Bretton Woods. Il se fonde sur des normes internationales tantôt juridiquement contraignantes, tantôt relevant davantage de la tradition et de codes de bonne conduite. Il englobe les domaines de l'économie, du politique et sécuritaire, et des droits fondamentaux.

Cet ordre international est aujourd'hui ébranlé. La guerre d'agression russe en Ukraine, et l'annexion de la Crimée qui l'a précédée, sont ainsi des violations flagrantes de la Charte des Nations Unies. Des Etats, comme la Chine ou certains pays du Sud Global, remettent en cause l'utilisation qui est faite du cadre juridique développé pour promouvoir les droits fondamentaux.

Autonomisation du Sud Global et recul des démocraties

Les puissances occidentales sont aujourd'hui en compétition avec leurs rivales des BRICS (Brésil, Russie, Inde, Chine, Afrique du Sud) dans le grand jeu d'influence sur les pays dits du Sud Global.

Ce concept, certes mal défini, désigne cet ensemble très hétéroclite de pays non occidentaux, qui partagent peu ou prou les aspirations suivantes : obtenir davantage de développement économique, obtenir davantage de respect de la part des vieilles puissances, obtenir davantage leur mot à dire dans la marche du monde. Certaines de ces nations expriment un malaise voire un rejet des concepts développés en Occident relatifs aux droits fondamentaux et libertés individuelles.

De plus en plus de ces Etats dits du Sud Global font preuve aujourd'hui d'une autonomie croissante quant à leurs positionnements dans la compétition entre grandes puissances, choisissant tantôt les puissances occidentales, tantôt les BRICS, selon ce qu'ils estiment être leurs intérêts.

Il est utile de considérer les coups d'état, putschs militaires et autres changements de pouvoir comme faisant partie d'un mouvement mondial plus large de recul de l'influence des démocraties libérales occidentales sur plusieurs pays du Sud Global, en particulier dans le contexte des grandes luttes de pouvoir opposant les États-Unis d'Amérique et les régimes autoritaires tels que la Russie et la Chine.

INFLUENCE

Réseaux

Quelques exemples de désinformation circulant sur les réseaux sociaux.

Omniprésence de la guerre de l'information au niveau mondial

Des acteurs étatiques comme la Russie et la Chine utilisent la guerre de l'information pour atteindre leurs objectifs stratégiques à long terme. Ils exploitent les failles déjà existantes au sein de certains groupes sociaux et capitalisent sur les faits d'actualité pour accroitre la polarisation et convaincre. Ils ont recours à des activités d'influence aussi bien envers leurs propres publics nationaux qu'externes et internationaux, chacun avec leurs propres accents.

Ces activités visent généralement à modifier les perceptions et systèmes de croyance, contribuent à alimenter les théories du complot au sein de nos sociétés et dans le cadre des conflits actuels, à discréditer les gouvernements occidentaux et semer la méfiance entre les partenaires alliés.

A titre d'exemple, la Chine présente le conflit en Ukraine comme le résultat de l'ingérence occidentale et trouve en la Russie un allié pour modifier l'ordre mondial existant. La Chine amplifie la rhétorique et la désinformation russes en Afrique, en Amérique latine et auprès de ses alliés du Moyen-Orient, souvent économiquement dépendants, pour soutenir la Russie sur le plan diplomatique. La Chine a ainsi sérieusement affaibli les efforts occidentaux visant à isoler et à couper la Russie de l'économie mondiale.

Ces stratégies d'influence ne se limitent pas aux publics étrangers mais s'étend aussi à toute l'Europe. Elles engendrent des effets à long terme et constituent à l'avenir un défi pour nos autorités.

> **NOTRE SERVICE OPÈRE PARTOUT DANS LE MONDE**

Par son renseignement, le SGRS conseille les dirigeants politiques et militaires afin qu'ils puissent réaliser les meilleurs choix, de manière indépendante et souveraine, pour protéger au mieux la Belgique et ses citoyens. A cette fin, en tout temps, notre service opère partout dans le monde où nos intérêts le demandent, en appui aux opérations militaires mais aussi au bénéfice de nos ressortissants, nos politiques et partenaires de la sécurité, aussi bien nationaux qu'internationaux.

L'IMPORTANCE DE NOS ATTACHÉS DE DÉFENSE

Une bonne connaissance du milieu international passe également par le réseau des attachés de Défense. En étroite collaboration avec les Affaires Etrangères, les autorités locales et les armées partenaires, ils assurent la liaison avec le SGRS.

1 Conseiller Militaire à la délégation belge à l'OSCE et attaché de Défense pour l'Autriche, la Slovaquie et la Slovénie.

« En tant qu'attaché de défense, je participe dans les trois pays à des activités bilatérales visant à promouvoir la Défense belge. Le grand défi consiste à identifier l'approche appropriée pour chaque pays. L'appartenance à l'OTAN ou à l'UE, la neutralité de l'Autriche et le climat politique sont autant de facteurs qui entrent en ligne de compte. S'informer sur l'actualité de ces pays et "réseauter" est donc à l'ordre de tous les jours. Ce large éventail de tâches peut constituer un véritable défi, mais c'est aussi ce qui, selon moi, rend ce travail attrayant. »

2 Attaché de Défense en Pologne, également accrédité auprès de l'Estonie, la Lettonie et la Lituanie.

« Je travaille dans une région dont l'importance géostratégique n'est plus à démontrer. Tous ces pays ont une frontière avec la Biélorussie et/ou la Russie et les derniers développements ont eu un impact majeur sur l'aspect sécuritaire et de défense, avec notamment le renforcement de la présence de l'Alliance et l'aide à l'Ukraine.

Dans l'appui à l'Ukraine, la Pologne joue un rôle essentiel, que ce soit pour la fourniture de matériel ou la formation de militaires ukrainiens dans le cadre de la mission européenne EUMAM UKR. Les trois Etats baltes jouent également un rôle clé dans la défense de l'OTAN et notre pays y participe activement dans les trois dimensions, que ce soit au niveau terrestre, aérien ou maritime.

Que ce soit pour l'aide à l'Ukraine ou la défense collective, j'ai un rôle de facilitateur et de coordinateur avec le pays hôte pour permettre le bon déroulement de la mission.

3 Attaché de Défense en Jordanie, également accrédité pour l'Irak.

« Le dialogue est une des clés essentielles à la coopération bilatérale entre la Jordanie et la Belgique. Ancrée au Moyen-Orient, notre équipe dispose d'un vaste réseau qui lui permet de recueillir des informations pour nos deux pays, et ce entre autres dans le domaine du renseignement et de la sécurité. Le développement de cette expertise de la région n'est possible que par une présence dans la zone et des contacts directs.

Au sein de l'Ambassade, j'apporte une valeur ajoutée en tant que conseiller militaire de l'ambassadeur en partageant mon expérience militaire spécifique avec les diplomates, par exemple dans le cas de la planification d'une évacuation de compatriotes d'un pays voisin lors d'une crise. C'est une fonction passionnante et multiforme qui combine diplomatie militaire, coopération bilatérale et opérationnalité »

4 Attaché de Défense en Russie, aussi accrédité pour l'Arménie.

« Les sanctions prises à l'encontre de la Russie ont conduit, entre autres, à l'inscription de tous les États membres de l'UE sur la liste des "pays non amis de la Russie". En conséquence, les relations bilatérales sont actuellement pratiquement inexistantes. Néanmoins, le fait d'être personnellement présent dans le plus grand pays du monde, dont la capitale n'est qu'à 2 500 km de Bruxelles et qui fait quotidiennement la une des médias occidentaux, présente une grande valeur ajoutée. En effet, en temps de crise, il est indispensable de pouvoir observer les événements avec le plus de véracité possible et dans leur contexte spécifique, et ainsi aider les autorités belges à se faire une idée claire de la situation. »

5 Attaché de Défense au Maroc, aussi accrédité au Sénégal et au Cap-Vert.

" Mon mandat dans les pays d'accréditation comporte trois volets. Tout d'abord, il est nécessaire de développer une connaissance de la situation dans la région d'affectation, de construire et d'entretenir un réseau local afin de reconnaître plus facilement les opportunités.

En outre, mon travail consiste à définir chaque année des activités bilatérales avec les forces armées locales et à suivre leur réalisation. De plus en plus, l'industrie belge de la défense me contacte pour que je l'aide à accéder aux forces armées locales.

Enfin, il y a la fonction de conseil. Dans ma fonction, il faut être capable de définir les tendances stratégiques d'une part, mais aussi être prêt à informer l'Etat-major de la Défense en réponse à un incident ou à un goulot d'étranglement dans un dossier particulier. »

Guerre hybride en Ukraine

La guerre d'agression russe contre l'Ukraine s'est transformée en une guerre d'attrition opposant ses belligérants.

Côté russe, bien que soumis à des tensions d'ordre politique et économique depuis février 2022, le régime poutinien vise à se maintenir au pouvoir à tout prix et reste relativement stable. L'année 2023 a été marquée par l'action menée en juin par le chef des mercenaires du Groupe Wagner, Evgueni Prigojine, mais toute tentative de soulèvement populaire est écartée par l'usage de la répression et de la désinformation.

Côté ukrainien, le leadership du président Zelensky reste pour l'instant incontesté, même si les premières failles sont perceptibles. Son charisme et son rôle symbolisant la résistance lui valent un respect indéniable au sein de la société et des institutions ukrainiennes malgré sa forte dépendance aux soutiens extérieurs (politiques, économiques et militaires). Les objectifs maximalistes fixés par ses forces armées n'ont pas été atteint à la suite de l'échec de la contre-offensive de l'été 2023. Dans ce contexte difficile, le leadership ukrainien risque de voir sa légitimité et sa stabilité menacées.

Sur le front militaire, la situation stratégique reste relativement inchangée. En 2023, la Russie a renforcé ses positions sur l'ensemble de la ligne de front de manière à pouvoir mener des opérations offensives mais sans être en mesure d'exécuter une réelle percée militaire. Après l'échec de la controffensive ukrainienne, la Russie a repris l'initiative sur le terrain. Sa propagande, par le biais de campagnes de désinformation, présente la situation comme un échec total de l'Ukraine et par extension, de l'Occident.

Après plus de deux ans de guerre, l'Ukraine et la Russie continuent à faire face aux mêmes défis militaires : recrutement massif et mobilisations d'une partie de la population, manque d'équipements lourds et de munitions. Les deux parties demeurent inaptes à consolider ou exploiter leurs succès militaires. La poursuite d'une guerre d'attrition avec des attaques en profondeur et des conséquences désastreuses pour la population des deux côtés est à craindre. Cette guerre d'attrition élargit d'ailleurs le champ d'action à l'industrie de défense qui sera critique pour la continuité des opérations.

BATTLE GROUP

Depuis juillet 2023,

la Défense belge participe au Battle Group déployé en Roumanie sous commandement français ayant pour objectif de renforcer la présence de l'OTAN sur le flanc Est.

Information sur le rôle du SGRS

En appui direct aux différents détachements de la Défense présents dans les Pays baltes et en Roumanie, le SGRS fournit, tant en Belgique que sur site, une assistance en matière de renseignement, contre-ingérence et sécurité.

De plus, sur le plan stratégique, le SGRS contribue activement à informer tant le gouvernement que ses partenaires de la communauté du renseignement et de la sécurité de l'évolution du conflit en Ukraine, en produisant notamment des notes d'analyses portant aussi bien sur les aspects politiques que militaires. L'expertise du SGRS permet d'accroître la compréhension des décideurs politiques et militaires belges quant aux multiples facettes du conflit.

le drône belge UAV utilisé notamment dans des missions de reconnaissance.

Vers une guerre des drones

L'utilisation des drones, ou Unmanned Aerial Systems (UAS), est longtemps restée aux mains des forces armées conventionnelles, bien que certains groupes terroristes aient utilisé depuis quelques années de petits drones commerciaux à des fins de propagande ou de frappes cinétiques légères. L'usage des drones militaires, quoi qu'en forte croissance, n'avait pas encore un caractère massif.

L'invasion de l'Ukraine par la Russie a rapidement changé la donne, les deux parties ayant multiplié les développements technologiques dans le domaine ainsi que leurs usages. Drones militaires pour la reconnaissance ou les missions cinétiques ; frappes ciblées au moyen de drones « kamikaze », ou « One-way Attack » ; de fabrication industrielle ou improvisée ; utilisation des petits drones commerciaux de type « First-Person View » transportant de petites et moyennes charges explosives pour frapper des véhicules ou du personnel ; Unmanned Surface Vessels (USV) afin de détruire les flottes ennemies… l'emploi des drones sur le théâtre ukrainien s'est diversifié et amplifié. Après plus de deux ans de conflit, ces nouveaux moyens de combats sont devenus le moteur de bon nombre de fabricants dans le monde, et commencent à s'exporter vers d'autres théâtres.

Ces développements et la démocratisation de certains systèmes ont convaincu beaucoup de pays émergents, majoritairement en Afrique ou au Moyen-Orient, d'acquérir des UAS militaires de combat (UCAV) afin de combattre les groupes rebelles ou terroristes sur leur territoire. Parmi les principaux fabricants d'UCAV, des pays comme la Turquie, la Chine ou encore l'Iran, exportent massivement vers ces pays, se souciant peu des sanctions internationales ou des aspects légaux ou éthiques.

De même, les Houtis yéménites, avec le support de l'Iran, utilisent massivement des drones, tant aériens que sous-marins, menaçant le trafic maritime dans le Golfe d'Aden et en Mer Rouge.

Dans le cadre du réinvestissement en cours dans ses forces armées, la Belgique devra tenir compte de cette évolution majeure dans la conduite de la bataille.

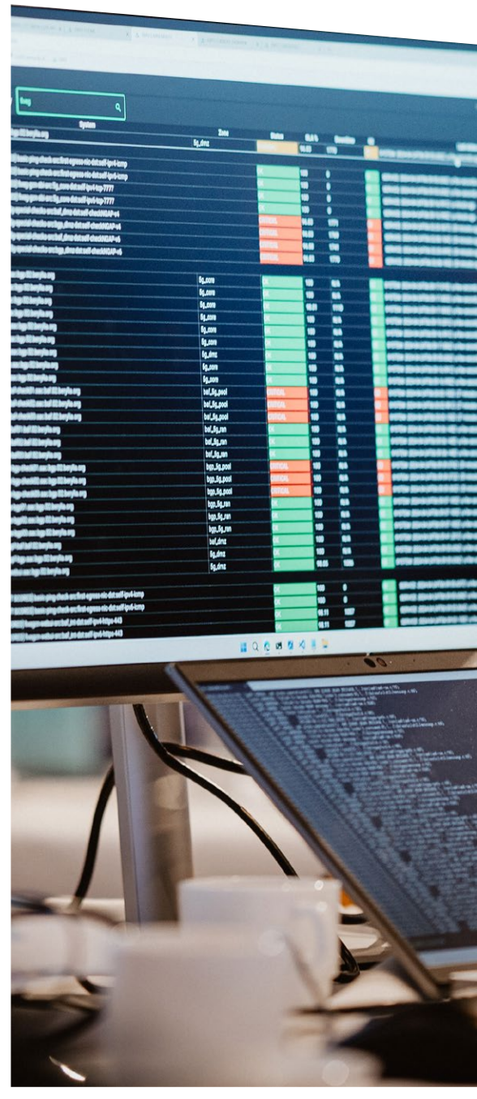
Le projet européen « COURAGEOUS » vise à développer une méthode de test standardisée pour les systèmes anti-drones

Attaques hybrides à l'encontre des infrastructures critiques

En 2023, la Russie a lancé une campagne d'envergure visant les infrastructures critiques ukrainiennes. Cette campagne visait notamment le réseau de production et de distribution électrique, au moyen de de bombardements intensifs et récurrents (missiles de croisière, missiles hypersoniques, drones, etc.) mais aussi d'attaques cybernétiques.

Ainsi, un cyber acteur lié au Service de Renseignement Militaire russe (GRU) a ciblé ses opérations cybernétiques destructrices sur des infrastructures critiques telles que centrales électriques, opérateurs de réseaux et télécommunications. Par ailleurs, des opérations de cyber espionnage russes ont visé à empêcher les efforts de contre-espionnage et les enquêtes menées sur les crimes de guerre.

Une tendance claire peut être observée : les cyber acteurs russes ciblent de manière répétée les mêmes organisations, mènent des attaques soutenues contre les médias ukrainiens et tentent de contourner les capacités, pourtant améliorées, de détection et de récupération de l'Ukraine grâce à une exfiltration plus rapide des données.



Témoignage

« J'ai travaillé sur trois continents en 2023 »

Matthew, 36 ans

En pratique, directement ou indirectement, le SGRS est toujours impliqué dans toutes les opérations de la Défense. Chaque année, elles sont passées en revue et traduites en plan d'opérations. Cela se passe sur terre, en mer, dans les airs et dans le domaine cybernétique. Mais à quoi ressemble une journée de travail dans la vie d'un officier du SGRS à l'étranger et à quoi doit-il faire face au quotidien ?

« Je m'appelle Matthew et je travaille dans les équipes déployables du SGRS. Avec ma petite équipe, je pars pour des périodes plus longues à l'étranger et j'opère dans des endroits où des détachements de la Défense sont également présents.

Qu'est-ce que je fais là-bas au quotidien ? J'ai des contacts réguliers avec les services de sécurité locaux et d'autres partenaires. Le soir, je transforme ces conversations en un rapport qui est envoyé à la fois au quartier général à Bruxelles et aux troupes belges déployées dans ma région. Ensuite, je prépare minutieusement mes entretiens pour le lendemain. De cette manière, je reste à l'écoute et j'aide à détecter les changements de situation. Je peux ainsi tenir les troupes belges informées et contribuer à leur protection.

Mon travail est très varié et passionnant. L'année dernière j'ai travaillé sur trois continents différents : l'Afrique, l'Europe et le Moyen-Orient. Même si la nature du travail ne change pas dans les différents continents, je suis amené à devoir m'adapter à chaque fois aux circonstances locales et à la culture des partenaires locaux.»

Conflit israélo-palestinien une résonnance au-delà des frontières

L'attaque terroriste du Hamas du 7 octobre 2023 a déclenché une série d'événements dont on ne connait pas encore l'issue. Les opérations militaires, incidents armés et protestations se multiplient aussi bien dans la région qu'au niveau international.

Un pays, quatre conflits

Depuis l'éclatement du conflit, les tensions aux frontières d'Israël ne cessent de croître en une situation de plus en plus complexe et aux nombreuses facettes.

A Gaza, la population se trouve entre le marteau et l'enclume. Les opérations israéliennes en réaction de l'attaque du 7 octobre 2023 visent à éliminer ou affaiblir le potentiel militaire du Hamas mais provoquent une profonde crise humanitaire avec de lourdes pertes humaines et des destructions d'envergure.

En Cisjordanie, la température ne cesse d'augmenter. Les clashs sont de plus en plus fréquents et violents entre, d'une part, la population palestinienne, et d'autre part, les forces israéliennes et les colons.

Au Nord d'Israël, la frontière libanaise présente pour l'Etat hébreu tous les risques d'un conflit ouvert avec le Hezbollah. Les incidents et bombardements réciproques se sont multipliés depuis le 7 octobre.

En interne même d'Israël, une quatrième dimension du conflit constitue la polarisation croissante qui divise la population israélienne ainsi que ses politiques.

Veille permanente

Le SGRS suit au jour le jour les différents aspects du conflit israélo-palestinien et ses conséquences régionales, au profit des décideurs politiques et militaires. De plus, doté de moyens de collecte spécifiques, il contribue à l'analyse des répercussions éventuelles sur notre territoire, au profit de ses partenaires belges du renseignement et de la sécurité.

Un jeu mortel de proxys

Le SGRS constate que l'Iran ne s'implique pas seulement en coulisses mais également via son impressionnant réseau de milices et proxys dans la région.

Au Liban, les capacités militaires du Hezbollah sont une menace directe pour Israël. Si le Hezbollah a mené des opérations militaires d'ampleur limités contre Israël après le 07 octobre 2023, entrainant des ripostes des forces israéliennes, un conflit majeur a été évité jusqu'à présent mais menace toujours.

En Syrie, la présence de milices chiites pro-iraniennes et d'éléments du Corps des gardiens de la révolution iranienne illustrent la complexité syrienne. Ces forces, qui ont permis au régime syrien de rétablir son autorité sur de larges pans de son territoire, s'y sont installées durablement. Les forces israéliennes mènent régulièrement des frappes aériennes contre ces milices et ces éléments iraniens, notamment dans l'Est du pays et le long des lignes de démarcation avec le plateau du Golan. Si le Président syrien a officiellement pris position en faveur des Palestiniens, aucune action concrète n'a été réalisée.

En Irak, les milices chiites pro-iraniennes regroupés au sein de la « Résistance Islamique en Irak » font peser une menace tant pour la stabilité irakienne que sur les forces de la coalition internationale. Ces milices ont enclenché en octobre 2023 une série d'attaques contre les bases américaines en Irak, Syrie, ainsi qu'une base américaine en Jordanie. Les Etats-Unis ont répondu par des frappes contre des milices pro-iraniennes en Irak et en Syrie, mais sans affronter directement l'Iran. Au niveau politique, les acteurs pro-iraniens ont exploité l'incident pour réitérer leur demande de retrait des troupes américaines du territoire. Un vote au parlement en ce sens a échoué mais les négociations se poursuivent encore avec les USA.

Au Yémen, le mouvement houthi qui contrôle le Nord du pays et la

capitale a entrepris une série d'actions dans la région qui constituent une menace directe pour la liberté de navigation en Mer Rouge. Ils ont ainsi procédé à des attaques directes sur Israël. Ils ont également mené des actions offensives dans la mer Rouge et le Golfe d'Aden en affichant l'objectif d'attaquer des navires commerciaux ayant des liens avec Israël. Depuis novembre 2023, plus de soixante attaques utilisant majoritairement des missiles et des drones, aussi bien aériens que marins, ont été enregistrées.

Les USA et le Royaume-Uni ont procédé à des frappes ciblant les capacités militaires houthies sur le territoire yéménite, menant le mouvement à élargir ses actions aux navires commerciaux américains et britanniques. Une coalition emmenée par les Etats-Unis a conduit au déploiement de plusieurs navires militaires en mer Rouge.

Protection du trafic maritime

En février 2024, l'Union européenne a officiellement lancé une opération supplémentaire, ASPIDES, de nature purement défensive et visant la protection du trafic maritime. La frégate Louise-Marie est la contribution belge à la fois à ASPIDES et à l'opération European Maritime in de Strait of Hormuz (EMASoH), en cours depuis 2020. Ces deux missions multinationales visent la préservation de la liberté de navigation, respectivement dans la mer Rouge et dans le détroit d'Ormuz. Le SGRS fournit dans le cadre de ce déploiement une assistance renseignement et sécuritaire.

Un conflit impactant les démocraties occidentales

Les polémiques relatives à de possibles crimes de guerre engendrent des tensions au sein même des démocraties occidentales.

Ces tensions internes aux démocraties occidentales et les polémiques sur les crimes de guerre font peser un risque d'un isolement croissant pour Israël.

Réseau de milices, proxys mais aussi hacktivistes

Pour l'Iran, Israël reste une cyber-cible clé. Les cyberattaques destructrices, parfois déguisées en ransomware, ne sont pas en reste. Le régime iranien procède régulièrement à des cyberattaques contre les membres de l'opposition et les dissidents iraniens, tant en Iran qu'en Europe.

La guerre entre Israël et le Hamas montre que dans un nouveau conflit, les hacktivistes peuvent être mobilisés à court terme et, à la demande ou avec la coopération des services de renseignement, tenter de mener des opérations perturbatrices ou destructrices. Dans le cas du conflit entre Israël et le Hamas, ce ne sont pas seulement les services gouvernementaux et les infrastructures critiques qui ont été visés, mais ce sont aussi les systèmes d'alerte en cas d'attaque au missile.

TÉMOIGNAGE

Rachel, 42 ans est « gestionnaire de profils ».

Au quotidien son travail consiste à échanger avec des « sources humaines ». En 2023, elle est partie en opération au Moyen-Orient pour recruter des personnes susceptibles de fournir des renseignements.

« J'ai rencontré une source africaine, une personne très délicate rencontrée dans un pays tiers. Elle ne savait pas que je travaillais pour le SGRS, mais au cours de notre entretien, elle m'a fait part d'informations sensibles susceptibles de nous intéresser.

La difficulté de mon travail réside donc dans le fait que, d'une part, je dois être très souple et, d'autre part, je dois être capable d'agir de manière très discrète. Lors de telles interactions, je recherche toujours les motivations qui pourraient amener ces personnes à nous aider plus concrètement, comme une motivation d'ordre financier, mais le plus souvent cela relève de l'idéologique.

Ce travail m'apporte une immense satisfaction, surtout si, grâce à mes efforts, je peux recueillir des informations vitales qui peuvent être utiles à notre pays. »

AFRIQUE

coups d'état, ingérences et réalignement stratégique

Si les conflits israélo-palestinien et russo-ukrainien accaparent les gros titres de nos journaux, des développements ont lieu en Afrique qui peuvent avoir un impact aussi significatif sur le long terme. Le SGRS doit y consacrer toute son attention et son expertise, afin d'en informer ses clients.

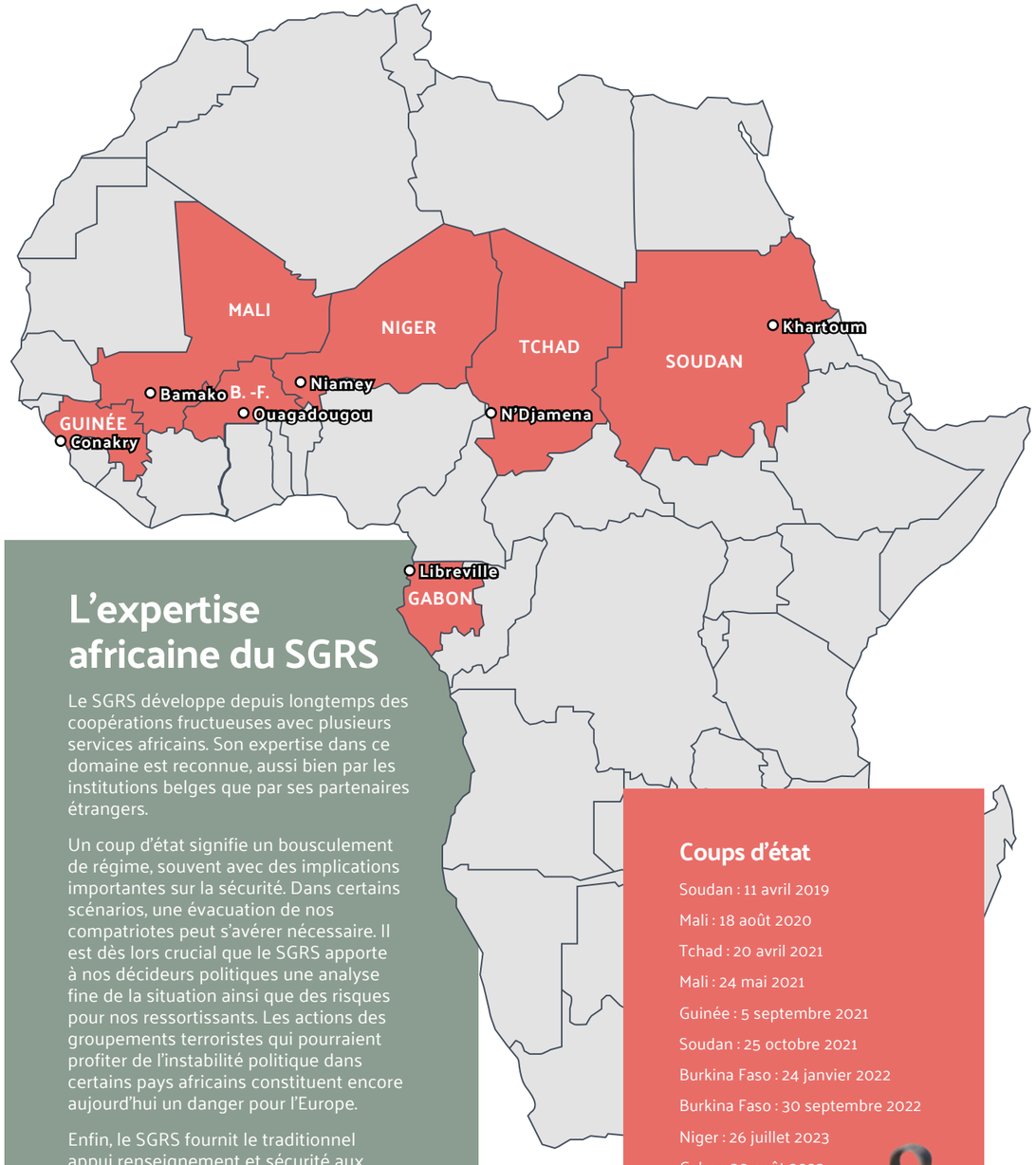
Recrudescence des coups d'État

Ces dernières années, les coups d'état militaires sont redevenus une caractéristique inquiétante du paysage politique africain. L'Afrique en a connu pas moins de huit au cours des trois dernières années, entre autres au Tchad, en Guinée, au Mali, au Burkina Faso et en 2023, au Niger et au Gabon.

La base en est l'incapacité de certains gouvernements à répondre aux défis socio-économiques et sécuritaires d'une partie de la population, cette défaillance perçue dans la fonction régalienne se voyant traduite en actions de putschistes. Deux phénomènes peuvent en découler : premièrement, un putsch peut en cacher un autre, si la qualité de la vie ne s'améliore pas à court terme.

Deuxièmement, les putschistes ont tendance à annoncer assez vite une transition pour ensuite l'envoyer aux calendes grecques.

Bien que l'Union africaine (UA) et les organisations régionales telles que la Communauté Economique des États de l'Afrique de l'Ouest (CEDEAO) aient condamné les coups d'état, leurs décisions politiques et leurs sanctions économiques ont été jusqu'à présent plutôt inefficaces. Leur manque de capacités ainsi que leur lutte souvent incohérente contre les coups d'état et autres changements anticonstitutionnels de gouvernement demeurent inquiétants.



L'expertise africaine du SGRS

Le SGRS développe depuis longtemps des coopérations fructueuses avec plusieurs services africains. Son expertise dans ce domaine est reconnue, aussi bien par les institutions belges que par ses partenaires étrangers.

Un coup d'état signifie un bousculement de régime, souvent avec des implications importantes sur la sécurité. Dans certains scénarios, une évacuation de nos compatriotes peut s'avérer nécessaire. Il est dès lors crucial que le SGRS apporte à nos décideurs politiques une analyse fine de la situation ainsi que des risques pour nos ressortissants. Les actions des groupements terroristes qui pourraient profiter de l'instabilité politique dans certains pays africains constituent encore aujourd'hui un danger pour l'Europe.

Enfin, le SGRS fournit le traditionnel appui renseignement et sécurité aux déploiements militaires belges en Afrique.

Coups d'état

Soudan : 11 avril 2019
Mali : 18 août 2020
Tchad : 20 avril 2021
Mali : 24 mai 2021
Guinée : 5 septembre 2021
Soudan : 25 octobre 2021
Burkina Faso : 24 janvier 2022
Burkina Faso : 30 septembre 2022
Niger : 26 juillet 2023
Gabon 30 août 2023

La guerre aussi en Afrique

Il n'y a pas qu'en Ukraine où une guerre interétatique fait rage. Sur le continent africain aussi, une quasi-guerre interétatique oppose le Rwanda et la RDC. Elle se fait, certes, en partie sous le couvert de supplétifs présents dans l'Est du Congo et manipulés au profit d'un des belligérants, à l'instar des rebelles du M23.

D'autres nations africaines sont frappées par des insurrections armées ou des conflits civils. Le Soudan, en particulier, a vu se déclencher en avril 2023 une guerre opposant deux grandes factions de l'appareil militaire et sécuritaire : les forces militaires et les forces de soutien rapide. Ces deux factions bénéficient, par ailleurs, de leurs propres appuis extérieurs.

Le réalignement stratégique

Le continent africain a connu en 2023 des changements importants témoignant d'un réalignement stratégique en cours dans plusieurs Etats africains. Ces Etats se détournent de leurs partenaires traditionnels, notamment occidentaux, au profit d'autres acteurs.

Ainsi, après l'éclatement de la Force conjointe du G5 Sahel, un retrait progressif de la présence internationale se marque dans la région. La MINUSMA s'est retirée du Mali en décembre 2023 et la présence militaire française au Sahel a également diminué de manière significative.

En Afrique centrale et orientale, la présence internationale s'est aussi réduite : en République démocratique du Congo, les Nations unies préparent la fin de la MONUSCO , tandis qu'en Somalie, l'Union africaine a mis en œuvre le départ d'ATMIS fin décembre.

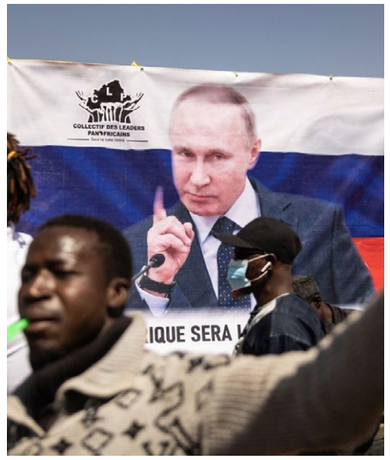
La Chine et la Russie ont accru leur influence dans le « Sud global » et ce, dans divers domaines. Les deux Etats pratiquent cependant une approche différente quant à l'établissement de relations privilégiées avec certains Etats africains. La Russie privilégie des coopérations militaires et sécuritaires tandis que la Chine établit sa coopération d'abord par le secteur de l'économie. D'autres nations, comme la Turquie, l'Iran et les Etats du Golfe, se mêlent également du grand jeu africain et accroissent également leurs implications dans certaines zones africaines.

Il résulte de ce réalignement stratégique un bouleversement du paysage des ingérences étrangères sur le continent africain.

MINUSMA : Mission multidimensionnelle intégrée des Nations unies pour la stabilisation au Mali

MONUSCO : Mission de l'Organisation des Nations Unies pour la stabilisation en République démocratique du Congo

ATMIS : African Union Transition Mission in Somalia



© AFP

La Russie étend sa zone d'influence à l'Afrique

Les pays africains sont dans la ligne de mire de Moscou. La Russie, qui recourt de plus en plus à la désinformation anti-occidentale, à l'utilisation de mercenaires russes et, plus généralement, à l'affaiblissement des institutions démocratiques, cherche à nouer des liens plus étroits avec toute une série d'États africains.

Elle utilise spécifiquement le discours selon lequel les pays occidentaux continuent d'exploiter les populations africaines et impose le modèle russe dit "anticolonialiste". Bien que l'impact économique de la Russie en Afrique soit dérisoire par rapport à celui de l'Occident ou de la Chine, la Russie a réussi - en particulier dans la région instable du Sahel - à se lier plus fortement à un certain nombre de pays, en partie grâce au déploiement de mercenaires (Africa Corps - anciennement Wagner).

Entretemps, à la suite de coups d'état en Guinée, au Mali, au Burkina-Faso, au Niger, au Soudan et en République centrafricaine, plusieurs gouvernements pro-russes sont déjà au pouvoir. Dans la pratique, cela crée une zone plus ou moins contiguë de régimes autocratiques et, en plus des forts sentiments anti-occidentaux dans ces pays, développe également l'insécurité et les flux migratoires illégaux.

En dehors de la région du Sahel, l'influence de la Russie, n'est pas négligeable, même si plus limitée. Par exemple, plusieurs gouvernements africains, tels que l'Afrique de Sud, choisissent également de renforcer leurs liens avec Moscou, malgré l'invasion russe de l'Ukraine. Cela s'explique en partie par le mécontentement suscité par le manque de représentation et de poids dans les institutions internationales mais aussi par des considérations économiques pragmatiques.

QUELQUES RÉALISATIONS EN 2023

Des produits de qualité au bénéfice de nos partenaires

La qualité de plusieurs produits d'analyses du SGRS a été saluée par les institutions otaniennes, comme le montre l'intégration de ces produits aux portefeuilles de lecture recommandées aux membres de l'organisation. Cette mise en avant des produits du SGRS souligne la reconnaissance par des instances internationales de son expertise dans les domaines qu'il couvre.

Coopération avec le monde académique renforcée

Un protocole d'accord a été signé avec l'Ecole Royale Militaire (ERM), notre 'tête de pont' avec les universités civiles, belges et étrangères. Ses champs d'application couvrent différents domaines du cyberespace, comme la 5G ou la cryptographie, et contribuent à soutenir de nombreux projets en recherche et développement sur le long terme, tant au profit de la Défense que de la société civile.

Des efforts de sensibilisation accrus

Qu'il s'agisse des mesures de protection contre les risques d'espionnage, des nouvelles directives de sécurité ou des mesures de cybersécurité, le SGRS a mis l'accent sur la sensibilisation de l'ensemble du personnel de la Défense afin d'accroître la sécurité de l'organisation. Ces actions de sensibilisation se déroulent au travers de campagnes d'information et de communication, au sein du SGRS.

Le Centre d'Excellence belge en cryptographie est né

En partenariat avec l'ERM, sa structure a été définie et des ressources allouées. A terme, ce Centre d'Excellence, inspiré du modèle français, produira une expertise technique au profit de ses partenaires fédéraux et internationaux.

Une expertise en cybersécurité en appui à nos partenaires fédéraux

Le Cyber Command du SGRS, expert en cyber audit et contrôle, a été désigné par le Conseil National de Sécurité pour homologuer le nouveau système classifié fédéral BSC (Belgian Secure Communication) qui sera à l'avenir utilisé par l'ensemble des SPF.

Coopération avec l'IGN consolidée

La signature d'un accord de coopération avec l'IGN en 2023 permet de maximiser les synergies, notamment en favorisant le transfert de personnel, et d'associer structurellement l'IGN à la Stratégie Géo de la Défense en tant que centre d'expertise.

Actualisation des normes de sécurité militaire

Les normes de sécurité militaire ont été actualisées et optimalisées en vue d'améliorer la culture de sécurité de la Défense, conformément aux recommandations du Comité R et au plan d'action émis à la suite de l'« affaire Jurgen Conings ».

Plateforme commune avec la VSSE

Le SGRS et la VSSE ont travaillé tout au long de l'année 2023, permettant d'aboutir à la création d'une plateforme commune pour lutter contre l'extrémisme et le terrorisme, qu'ils soient d'ordre confessionnel ou idéologique.

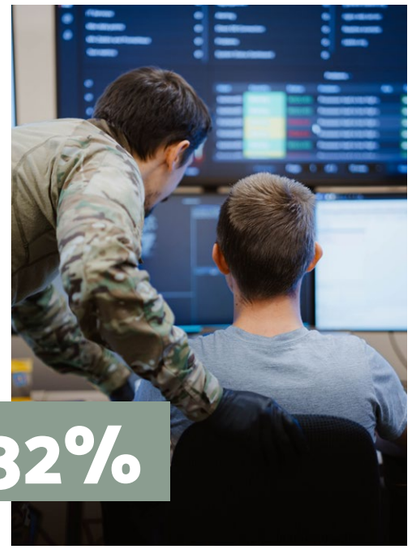
IF5 : engagement fort envers la protection du personnel et des informations classifiées. Agilité et comité d'évaluation permanent.

Première édition du Cyber Summer School

Ce stage d'été proposé par le Cyber Command du SGRS, pour la première fois en 2023, doit permettre aux jeunes d'appréhender les défis de la cyberdéfense d'aujourd'hui et de demain mais aussi contribuer à attirer de nouveaux talents. Le SGRS continue à investir dans son capital humain.

Quelques chiffres en 2023

Augmentation de 6%
du personnel



32%

DE CIVILS AU SEIN DU SGRS

160

PLUS DE 160 RÉSERVISTES EMPLOYÉS PAR LE SGRS

652

« PAPERS » PRODUITS ET VALIDÉS PAR LA DIRECTION RENSEIGNEMENT : DOCUMENTS D'ANALYSE PARTAGÉS AVEC NOS CLIENTS/PARTENAIRES.

7226

« REQUEST FOR INFORMATION » DEMANDÉES PAR NOS PARTENAIRES ET TRAITÉES PAR LE SGRS.

236

NOMBRE DE BIM'S (MÉTHODES EXCEPTIONNELLES D'INVESTIGATION)

5483

VÉRIFICATIONS DE SÉCURITÉ TRAITÉES

NOMBRE D'IMAGES SATELLITAIRES OU CARTES RÉALISÉES POUR LES OPÉRATIONS :

15560
Images prises dont 3154 produites

747
Demandes de support géographique

5
Missions topographiques effectuées

PARTIE 2

Evaluer l'état des menaces, pour s'en protéger

Les conflits au-delà des frontières dessinent le monde de demain et définissent les menaces auxquelles notre pays doit pouvoir faire face.

D'ores et déjà, nous observons un état élevé de la menace d'espionnage ; une augmentation des tentatives d'influence et d'ingérence mais aussi des cyberattaques envers les institutions et entreprises belges et européennes. Notre mission est d'éviter que des forces extérieures à notre société n'instrumentalisent des thématiques clivantes, comme la guerre en Ukraine ou au Proche-Orient, pour déstabiliser notre modèle démocratique.

Désinformation et opérations d'influence

Les opérations d'influence sont en augmentation, les canaux utilisés à cet effet se diversifient et leur impact sur le comportement se fait de plus en plus perceptible. Citons par exemple l'agitation autour de l'EVRAS, plusieurs manifestations d'agriculteurs, des émeutes à la suite de l'affaire "Nahel" en France, qui ont laissé une empreinte tangible et violente sur notre société.

A l'aube des élections belges et européennes entre autres, ces événements mettent nos autorités en état d'alerte face aux efforts d'influence de la part d'acteurs étatiques adversaires tels que la Russie, la Chine ou l'Iran.

Depuis que Twitter est devenu X, le nombre de « comportements inauthentiques coordonnés » est en hausse. L'utilisation de Telegram, canal par excellence des acteurs pro-russes, est en hausse en Belgique avec 12 % d'utilisateurs de la plateforme. Par ailleurs, les groupes anti-vax et conspirateurs COVID sont toujours actifs et d'autres se sont développés autour de nouveaux thèmes tels que le climat, l'énergie ou encore l'immigration. De récents événements ont clairement démontré que la frontière entre le monde virtuel et réel se fait de plus en plus ténue et peut conduire à la violence physique. En lien avec nos missions, ces tentatives d'influence et de désinformation doivent absolument être suivies.

En 2023, le SGRS a pris la direction du SIMII, un groupe de travail composé des principaux acteurs de la sécurité. L'objectif de cette coopération est de développer une approche unifiée et globale autour des Foreign Information Manipulation and Interference (FIMI), en particulier en lien avec les élections de 2024.

2023

Au cours de l'année écoulée,

La SIMII[1] a organisé de nombreuses réunions multilatérales, permettant l'échange d'informations entre les différentes parties prenantes, et un système d'alerte a été mis au point pour détecter rapidement toute activité d'influence étrangère.

Ce projet est appelé à se développer et se renforcer à l'avenir car le monitoring des tentatives de désinformation est permanent.

Conspirations sur Telegram

Les efforts d'influence et l'écosystème de désinformation de la Russie pour atteindre les publics nationaux et européens se concentrent principalement sur Telegram, le canal par excellence pour diffuser des récits pro-Kremlin et alimenter les théories conspirationnistes.

La Russie y exploite habilement tout événement susceptible de polariser l'opinion publique et d'affaiblir la confiance des citoyens envers leurs gouvernements et institutions.

[1]SGRS Interdepartmental Information Manipulation and Interference

Les menaces d'espionnage sont en augmentation

L'espionnage est défini en droit belge comme la recherche ou la fourniture d'informations non accessibles au public et l'entretien de relations secrètes susceptibles de préparer ou de faciliter ces actes.

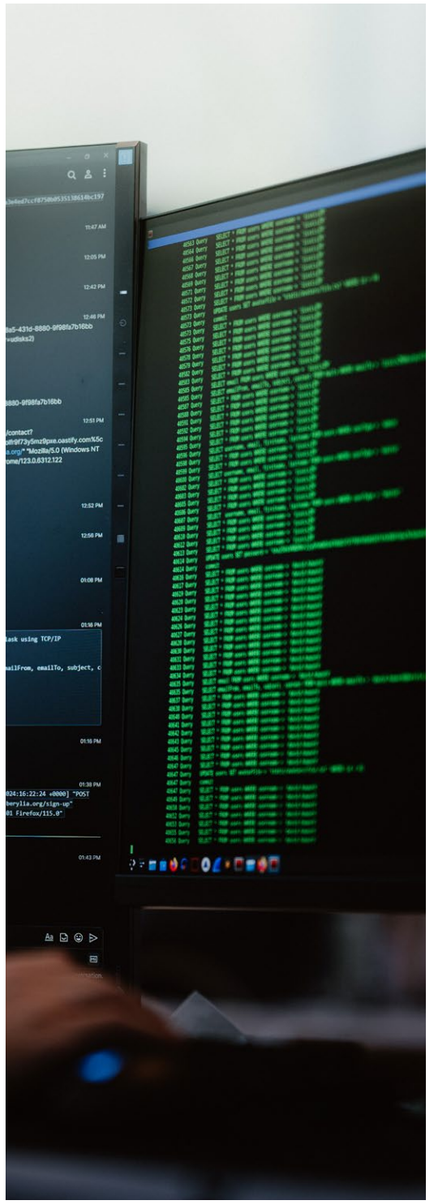
Pour le SGRS, il s'agit de toute information susceptible d'aider une personne extérieure mal intentionnée à entraver l'exécution des missions de défense, et donc pas seulement d'informations secrètes ou confidentielles au sens strict de la loi.

En tant que pays hôte de plusieurs organisations internationales telles que l'OTAN et l'UE, la Belgique est une cible privilégiée et le SGRS est co-responsable de leur protection. Le SGRS estime que le contexte géopolitique actuel se traduit par un très haut niveau de menaces d'espionnage auxquelles nos institutions doivent faire face en termes d'espionnage et d'ingérence. Une tendance qui devrait se poursuivre en 2024.

Tout au long de l'année 2023, le SGRS a mené diverses enquêtes de renseignement dans le domaine du contre-espionnage et de la contre-ingérence. Lorsque nécessaire, le SGRS a pris des mesures pour neutraliser la menace existante, en coopération ou en appui tantôt de sa Direction Sécurité, tantôt de la Direction générale Human Ressources de la Défense, tantôt de ses partenaires belges (Sûreté de l'Etat, Ministère public).

Le SGRS constate que les techniques utilisées dans l'espionnage se diversifient, entre autres grâce à l'évolution technologique, mais l'usage traditionnel des contacts humains comme source d'information reste une méthode très répandue. En 2023, plusieurs cas de tentatives d'espionnage ont pu être identifiés et déjoués.

C'est pourquoi la sensibilisation du personnel aux techniques utilisées par les agents de renseignement étrangers et à la manière de s'en prémunir a fait l'objet d'une attention toute particulière cette année. En 2023 une campagne de sensibilisation interne a été menée à grande échelle. A l'avenir, des outils de prévention seront développés et mis à disposition de tout le personnel de la Défense.



L'espionnage, aussi dans les rouages du cyberespace

Outre le vol de secrets commerciaux et de propriétés intellectuelles, les activités d'espionnage par des cyber acteurs chinois sont en augmentation et ciblent notamment les institutions de l'Union européenne, les agences gouvernementales des pays européens et de l'OTAN. Leur objectif est, entre autres, de connaître les positions des pays européens sur Taiwan et les initiatives européennes visant à réduire les risques associés à la dépendance économique vis-à-vis de la Chine.

Ces acteurs utilisent des structures de réseaux de plus en plus complexes en s'immisçant dans les infrastructures peu sécurisées de particuliers et d'entreprises ou en recourant aux failles de type « zero days ».

Des organismes publics belges, dont la Défense, ont eux aussi déjà été victimes du cyber espionnage chinois. Ces attaques se sont toutefois limitées à des fins d'espionnage et n'ont pas permis d'établir un accès persistant aux données des institutions visées.

Au-delà des cyber acteurs liés aux agences de renseignement chinoises, les entreprises publiques et privées chinoises constituent elles aussi une cybermenace potentielle. En effet, la loi nationale chinoise sur le renseignement permet aux agences de renseignement chinoises d'exiger des entreprises et des citoyens chinois, partout dans le monde, qu'ils coopèrent à tout moment. Les solutions matérielles et logicielles chinoises utilisées dans les secteurs des télécommunications et des transports constituent donc, à présent et à l'avenir, une menace potentielle de cyber espionnage, y compris en Belgique.

Il est du devoir du SGRS de développer les capacités nécessaires à la protection de nos intérêts belges. Le Cyber Command du SGRS contribue activement, aux côtés de ses partenaires tels que le Centre pour la Cybersécurité Belge (CCB), le Centre de crise National (NCCN) et le SPF Justice, à la cyber résilience nationale. Il appuie couramment les efforts conjoints en fournissant un avis technique et dispose de capacités défensives élaborées.

Les menaces cyber : la Belgique et ses alliés, victimes d'hacktivistes pro-russes

Dans le cadre du conflit russo-ukrainien, ls opérations de cyber espionnage russes, menées par un cyber acteur lié au Service de Renseignement Extérieur russe (SVR), ont surtout ciblé les institutions diplomatiques des États membres de l'Union européenne et de l'OTAN. Ces opérations ont engendré une augmentation de la fréquence des attaques et le déploiement continu de nouveaux logiciels malveillants visant à déjouer les outils de détection mis en œuvre. En outre, en raison de leur utilisation croissante par les autorités gouvernementales et entreprises, l'intrusion dans les solutions Microsoft Cloud est devenue un objectif majeur de ce cyber acteur.

En parallèle, des hacktivistes pro-russes ont mené des attaques dites "par déni de service distribué" (DDoS) dans presque tous les États membres de l'OTAN. En surchargeant les sites web par l'envoi de multiples requêtes ou données malveillantes, ils empêchent leur bon fonctionnement. La Belgique a elle aussi été victime de plusieurs de ces attaques, notamment sur les sites gouvernementaux, portuaires et de contrôle du trafic aérien. En général, ces cyberattaques n'ont toutefois eu qu'un impact limité. Les hacktivistes en ont davantage exploité l'attention médiatique pour nourrir les campagnes de désinformation russes.

Diverses sources d'information démontrent que la Russie continue à développer ses capacités de cybersabotage et mener des opérations dans le cyberespace en vue notamment de corrompre les infrastructures critiques.

TÉMOIGNAGE

« La cyberdéfense est avant tout une question de prévention et de détection », Gilda, 40 ans

La Belgique subit presque chaque mois des attaques perturbatrices de la part de "hacktivistes" pro-russes visant les sites internet de diverses agences gouvernementales. En outre, les cyber unités des différents services de renseignement russes tentent continuellement d'exploiter les faiblesses des logiciels ou d'obtenir l'accès des utilisateurs aux systèmes par le biais du phishing et d'autres techniques. Qu'il s'agisse de structures publiques ou privées, les tentatives d'intrusion sont en croissance constante.

En tant que capacité transversale, le Cyber Command du SGRS a pour mission de protéger les réseaux et systèmes d'armes employés par la Défense. Gilda, analyste CSOC (Cyber Security Operations Center) est en première ligne de cyberdéfense.

« Comme data analyst, mon rôle est d'analyser des données dans un but préventif mais aussi réactif. Avec mon équipe, nous monitorons les réseaux et infrastructures ICT de la Défense, générons des systèmes d'alerte visant à repérer les activités anormales et lorsque nous en détectons, nous déterminons les actions et mesures à prendre pour assurer une sécurité optimale.

Mon leitmotiv, c'est contribuer à la protection de notre pays et sa population. Aujourd'hui, dans le cadre de mes fonctions, cela me semble plus vrai que jamais. Au quotidien, je réagis sur des failles de sécurité qui sont bel et bien réelles et je prends des actions concrètes au profit de notre sécurité et donc, celle de notre pays »

Les menaces liées à la prolifération

Dans le domaine de la prolifération, 2023 a été marquée par une tendance accrue de transferts de technologies sensibles entre états et vers des proxys non-étatiques, en ce compris des vecteurs tactiques et stratégiques avancés utilisés en Ukraine et au Moyen-Orient. L'accroissement de la prolifération, en dépit des normes internationales établies, et le recours accru à la coercition nucléaire par la Russie dans le cadre de sa confrontation avec l'Ouest (avec notamment le retrait de plusieurs traités de réduction d'armements stratégiques comme New START – Strategic Armament Reduction Treaty ou CTBT – Comprehensive Test Ban Treaty), accélèrent l'érosion de l'architecture de non-prolifération des Armes de Destruction Massives.

Le déclin de l'architecture de non-prolifération et l'accélération de la compétition entre grandes puissances se traduit par une course à l'armement y compris dans les domaines stratégiques, ainsi qu'un risque accru d'escalade et d'erreur de calcul. Le développement de programmes balistiques et nucléaires de plusieurs pays sensibles (entre autres – mais pas uniquement- Chine, Iran, Corée du Nord) et les difficultés pour les institutions internationales à cadrer ces avancées constituent également une source de préoccupation grandissante.

EU2024BE

Réunion des Cybercommandeurs

Les relations internationales dans le cyberespace

Interagir avec des organisations nationales, internationales et multinationales demeure l'une de nos priorités. Ces interactions permettent non seulement de s'inscrire comme partenaire international fiable mais aussi de suivre l'évolution de la gouvernance en matière de cybersécurité, de soutenir de nouvelles initiatives et de rechercher d'éventuelles opportunités de coopérations ou de synergies.

Des réunions régulières ont lieu avec nos homologues du Centre de Cybersécurité de Belgique, la Représentation permanente de la Belgique auprès de l'OTAN et de l'Union européenne ainsi que le SPF Affaires étrangères afin de mieux coopérer pour répondre aux défis d'aujourd'hui et de demain.

En 2023, un effort particulier a été fourni pour aligner les stratégies et processus nationaux à la nouvelle politique et gouvernance en matière de cybersécurité définie par l'OTAN et l'UE. Une démarche vitale pour assurer une coopération harmonieuse et maintenir l'interopérabilité de nos pays au niveau technique. Le Cyber Command est d'ailleurs devenu en mars 2023 membre effectif du CRRT, "Cyber Rapid Response Teams", un projet qui doit permettre aux États membres de s'entraider pour assurer un niveau plus élevé de cyber résilience et de réagir collectivement aux cyber incidents.

PARTIE 3

Faire face aux menaces et contribuer à la résilience nationale

Le SGRS anticipe les évolutions technogiques, maintient son expertise et contribue avec ses partenaires à la sécurité intérieure.

Pour assurer notre sécurité et contribuer à la résilience nationale, nous devons non seulement maintenir notre expertise dans toute une série de domaines, mais aussi anticiper les évolutions technologiques et sociétales des années à venir. Au travers de partenariats, notre organisation s'adapte dans toutes ses lignes de développement et renforce en permanence sa capacité à répondre aux missions qui lui ont été conférées.

En cas de crise nationale, mais aussi internationale, le SGRS peut être sollicité pour fournir une expertise ou un appui technique. Se tenir à la pointe de la technologie et des dernières tendances est donc, plus qu'une volonté sstratégique, une nécessité. Cela se réalise au travers de partenariats, aussi bien avec le monde du renseignement que le monde industriel, académique et associatif. Optimaliser et innover sont dans ce cadre des maitres-mots.

Des plateformes communes dans la lutte contre l'extrémisme et le terrorisme

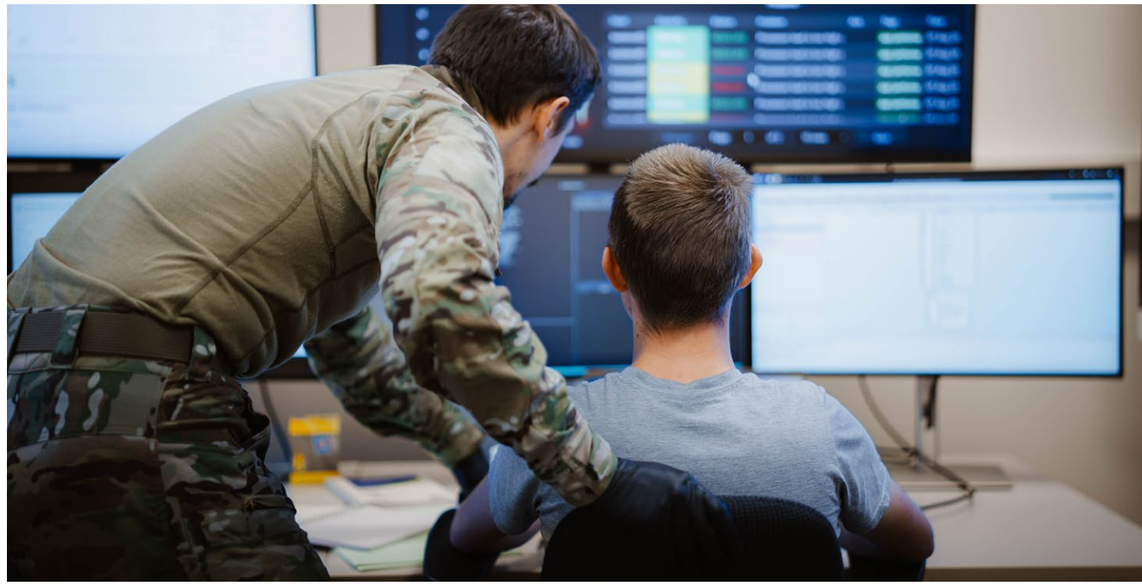
En 2018, le SGRS et la Sureté de l'Etat s'accordaient sur le « plan stratégique national de renseignement » (PSNR), un plan ambitieux de coopération renforcée structurelle afin de mieux lutter contre les menaces communes qui ressortent de leurs compétences. Depuis 2022, il en est à sa deuxième itération, marquée par un renforcement des domaines de coopération et des synergies. Ce dernier vise à faire bénéficier intelligemment chaque service des avantages comparatifs de l'autre, notamment en termes d'expertise et de moyens spécifiques de collecte, et aussi à mutualiser les efforts dans la lutte contre certaines menaces spécifiques.

Début 2024, la plateforme commune de lutte contre l'extrémisme et le terrorisme, tant confessionnels qu'idéologiques (extrémismes de droite et de gauche) est entrée en vigueur. Le personnel du SGRS et de la VSSE travaille maintenant au sein d'une seule entité, optimisant l'échange d'informations et l'emploi du personnel disponible. Il s'agit ici d'une extension majeure d'une plateforme conjointe déjà existante et opérationnelle depuis 2018. Cette dernière, qui se limitait à la lutte contre le terrorisme confessionnel, a permis de nombreuses avancées.

Les attaques terroristes récentes en Europe et en Belgique ayant démontré la nécessité d'une coopération renforcée entre nos différents services de renseignement, cette synergie devrait permettre un échange maximal d'informations, une mutualisation des ressources et une évaluation commune à destination de nos partenaires. Parmi les mesures, des équipes mixtes, mélangeant agents du SGRS et de la VSSE, seront constituées.

A terme, cette coopération concernera aussi d'autres types de menaces, notamment celles de l'espionnage et de l'ingérence, selon des modalités propres à chacune des menaces. Un meilleur partage d'informations et une coordination renforcée devraient faciliter et améliorer le débusquage des espions actifs sur notre territoire ou œuvrant contre nos intérêts nationaux.

En parallèle à ces avancées, le PSNR recouvre aussi les aspects Information and Communication Technologies (ICT) et de formation. Sa mise en œuvre progressive traduit la volonté des deux services de travailler ensemble, toujours plus étroitement, dans le respect mutuel et la confiance, selon la devise nationale « l'union fait la force ».



Sécurité militaire assurée, sécurité nationale renforcée

Suite à l'affaire « Jurgen Conings » de 2021, une série de mesures ont été définies en un plan d'actions visant à améliorer la culture de sécurité de la Défense.

L'année 2023 s'est traduite par la mise en œuvre et la concrétisation d'un certain nombre d'entre elles, à savoir la mise à jour des normes de sécurité militaire de la Défense par un groupe de travail du SGRS.

L'espionnage, la subversion et le sabotage, tout comme le terrorisme, mais aussi le crime organisé, sont des réalités auxquelles l'ensemble de l'organisation doit pouvoir faire face en toute agilité. La mise en œuvre de ces nouvelles normes, pensées sur base des risques éventuels, compte tenu de l'évolution technologique et des nouvelles législations, constitue une étape clé pour garantir la sécurité de la Défense. Mais aussi celle de ses partenaires industriels et institutionnels, aussi bien nationaux qu'internationaux. En cas d'incidents, les actions à mener sont définies pour regagner l'opérationnalité au plus vite.

Des efforts considérables ont été menés dans différents domaines, tels que la sensibilisation à tous les niveaux de commandements, la formation, le suivi des habilitations de sécurité, le renforcement des contrôles de l'armement et des munitions.

L'ensemble des mesures visent à garantir la rigueur mais aussi la flexibilité nécessaire à la Défense pour s'adapter à son environnement sécuritaire en constante évolution ainsi qu'une collaboration accrue entre les diverses autorités compétentes.

Concrètement

1. Introduction du concept « Security by Design", entre autres en matière de cybersécurité, dans la conception des infrastructures de la Défense.
2. Renforcement des échanges entre les unités, le Service Général du Renseignement et de la Sécurité (SGRS) ainsi que la Direction Générale des Ressources Humaines (DGHR).
3. Sensibilisation, formation et contrôles renforcés à tous les niveaux de commandement.
4. Vérification de la fiabilité des collaborateurs de la Défense dès leur embauche et tout au long de leur carrière.
5. Mise en place d'un organe permanent d'évaluation pouvant réaliser des ajustements en fonction, par exemple, des évolutions technologiques ou contextuelles.

TÉMOIGNAGE

« j'ai souhaité me recentrer sur un job aux valeurs fortes » Jean, 30 ans

Au niveau de la Défense, l'ensemble des moyens de communication et systèmes d'armes, actuels et futurs, repose sur l'utilisation de clés cryptographiques. Leur opérationnalité et liberté de mouvement en dépend directement. Jean, 30 ans, ingénieur en informatique spécialisé en cybersécurité, est aujourd'hui responsable d'Audit et Accréditation des systèmes. Après avoir travaillé pour diverses multinationales, il a rejoint le Cyber Command.

« J'ai souhaité me recentrer sur un job aux valeurs fortes. Je me suis donc naturellement porté vers la Défense. Ici, je me sens faire partie d'une équipe et on travaille de façon collégiale pour atteindre un objectif commun. Au quotidien, mon rôle consiste à homologuer des systèmes d'armes ou à m'assurer de leur niveau de sécurité. Ça touche à peu près à tout, aussi bien à une infrastructure réseau que des systèmes liés au F-35, à la nouvelle capacité motorisée (CaMo), ou encore au programme des chasseurs de mines belgo-néerlandais. »

Un officier de l'ERM avant le défilé du 21 juillet.

Mon job est assez diversifié. Demain, je serai à l'Ecole Royale Militaire (ERM) pour une formation, ensuite j'irai faire un contrôle à la caserne de Peutie et la semaine suivante, je vais à Strasbourg pour appuyer le Corps Européen...

Il y a une diversité d'actions et de tâches qui font que le boulot reste intéressant même si ma fonction reste la même.

En fait, le Cyber Command du SGRS a vraiment mis les moyens de ses ambitions sur la table. Il y a cette volonté politique qui se traduit directement dans les faits et ça, ça me plait ».

Jean et son équipe seront aussi impliqués dans la conception du futur Quartier Général d'Evere où il s'agit aussi de contrôler la domotique, les normes de sécurité d'émission électromagnétiques et bien d'autres systèmes.

Ne pas perdre le momentum de l'évolution technologique

Partenariat avec AGORIA, la fédération des entreprises technologiques.

Le cyberespace est devenu l'un des vecteurs les plus puissants de propagation de la menace. Les tentatives d'intrusion au sein des systèmes de défense, tout comme l'explosion des cyberattaques à l'encontre des structures aussi bien publiques que privées, et ce notamment dans le contexte de la guerre d'agression de la Russie contre l'Ukraine, sont en croissance constante. Être en mesure de réagir à ces menaces dans les différents domaines du cyberespace est l'un des rôles fondateurs du Cyber Command.

Le Cyber Command du SGRS s'est vu allouer 140 millions d'euros pour le développement de ses capacités dans le cadre du plan STAR, un plan qui prévoit aussi la mise en place de la stratégie DIRS (Defence, Industry and Research Strategy) pour mettre l'accent sur le développement d'une industrie de Défense forte et technologiquement avancée.

En matière de cyberdéfense, la coopération avec l'industrie, les centres de recherche nationaux et le monde académique est une condition sine qua non au développement de nouvelles technologies. Le Cyber Command, future composante de la Défense et toujours dans le giron des renseignements, doit pouvoir garantir à court et long terme les connaissances et ressources nécessaires afin de répondre aux menaces « high-tech », qu'elles soient actuelles ou encore futures.

Dans ce contexte, un accord de coopération structurelle a été signé avec l'Ecole Royale Militaire le 26 juin 2023, désignant cette dernière comme partenaire privilégié dans le cadre des projets de recherche et de développement dans le domaine cyber. Celui-ci soutient de nombreux projets de recherche et développement à long terme au profit de la Défense et de la société civile. Outre cette coopération, des échanges sont en cours avec d'autres organismes universitaires tels que l'UC Louvain, l'Université de Gand et HOWEST.

Une coopération intensive est également développée avec l'industrie au travers du Cyber Made in Belgium for Defence (CMIB4Def), une initiative conjointe d'AGORIA, la fédération des entreprises technologiques et du Cyber Command. Elle part du constat que l'amélioration de notre cyberdéfense et de notre résilience collective passe nécessairement par un rapprochement entre la Défense et l'industrie.

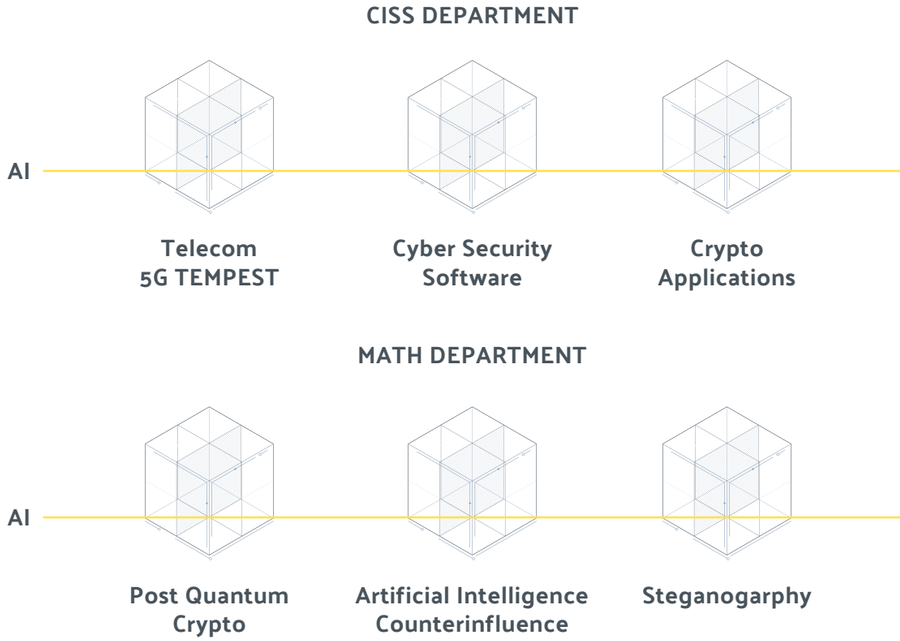
Les réflexions et travaux menés au sein du CMIB4Def portent sur des sujets tels que le soutien aux capacités opérationnelles de la Défense, le renforcement de la chaîne d'approvisionnement en cyberdéfense ou encore le développement des cyber compétences.

ESA

Depuis mai 2023, il existe également une collaboration entre le Cyber Command et l'Agence spatiale européenne dans le cadre du site de REDU, les deux parties voyant la valeur ajoutée d'une coopération structurelle.

NOS SIX DOMAINES DE RECHERCHE

Un exemple : garantir la disponibilité d'un réseau 5G en cas de crise



Investi dans de nombreux projets en collaboration avec le monde académique et industriel, le Cyber Command se prépare constamment à l'avenir. Parmi les domaines essentiels au développement de notre cyber résilience nationale : la protection des réseaux et infrastructures critiques.

L'objectif d'un projet issu du protocole d'accord avec l'Ecole Royale Militaire est d'étudier, en collaboration avec Orange Belgique, l'utilisation d'une installation 5G pour soutenir les réseaux "critiques" des bases de la Défense belge. Ces réseaux doivent en effet pouvoir soutenir en permanence les opérations ou un éventuel support logistique et technique dans le cadre des plans d'urgence. Il est donc important pour la Défense d'analyser quel type d'infrastructure 5G convient à ce besoin en termes de sécurité de l'information (confidentialité, intégrité et disponibilité) et de communication (intégration à nos réseaux existants, services spécifiques, etc.)

Par ailleurs, pour mener son étude, le consortium avec Orange Belgique a reçu à la fois des subventions pour le développement expérimental et pour l'infrastructure de recherche, entre autres en répondant à un appel à subventions lancé par le SPF Economie. Au total, il sera possible de tester et d'intégrer les solutions critiques mais aussi de réaliser une évaluation complète de la cybersécurité et du plan 5G.

PARTIE 4

Continuer à investir dans le capital humain

Nos agents et collaborateurs sont la richesse première du SGRS. La diversité des métiers au sein de notre service et les évolutions technologiques rendent indispensables un investissement continu dans notre capital humain et une ouverture accrue à la société civile.

Sur un marché de l'emploi en pleine mutation se caractérisant par une pénurie de main d'œuvre qualifiée, une guerre des talents croissante et une évolution constante du secteur de la technologie, le SGRS vise à quitter les paradigmes de politiques d'embauche dit « classiques ». Il se tourne vers de nouvelles formes d'accompagnement des talents et ce, en collaboration avec le monde académique, associatif et industriel. En matière de sécurité et de défense collective, l'équation à résoudre et les défis à venir, tant pour les entreprises que le secteur public, sont en effet de taille.

Le monde professionnel de la cyberdéfense reste particulièrement exigeant et compétitif. Et certaines compétences transversales s'avèrent parfois insuffisamment consolidées parmi ceux qui accèdent au marché de l'emploi. Dans ce contexte, toute forme de rigidité en matière de procédures de recrutement et sélection pourrait être préjudiciable.

En 2023, diverses initiatives ont été lancées pour améliorer l'accessibilité, fluidifier les procédures de recrutement et bien entendu proposer un parcours de formation plus en adéquation avec les attentes de toutes les parties prenantes.

VISITE

Cyber Command

En janvier 2024, le Cyber Command du SGRS recevait la visite du Chef de la Défense, l'Amiral Hofman.

Bien conscients de leur valeur ajoutée sociétale au travers de la (re)mise à l'emploi de jeunes « NEET » (Not in Education, Employment or Training), des acteurs pourvoyeurs de parcours formation-emploi s'efforcent désormais de se faire connaître comme de véritables partenaires de recrutement. Leur démarche consiste désormais à former les apprenants, non seulement aux exigences pratiques, mais aussi en prenant soin de répondre au mieux aux attentes et besoins des futurs employeurs. Le SGRS entend soutenir pleinement ces démarches. Déjà partenaire de Molengeek et BeCode, en s'associant à ces pourvoyeurs de talents, il offre aux candidats la possibilité d'intégrer la cyberdéfense de manière plus flexible et d'en apprendre plus tout au long de leur vie professionnelle. Cet effort devrait se poursuivre en 2024 avec entre autres, l'ouverture de ses bureaux civils à Charleroi dans les bureaux de A6K[1].

Parmi les initiatives visant à favoriser le recrutement et former les futurs experts de la cyberdéfense à présent et à venir, le SGRS participe au groupe de recherche et innovation Cyber Made in Belgium for Talents initié par Agoria, déploie ses efforts de communication et d'accessibilité en organisant des événements ciblés mais vise aussi à développer sa Réserve plus en accord avec le monde de l'entreprise.

[1]A6K

A6K est un écosystème unique et stimulant au cœur de l'Europe qui rassemble des leaders industriels, des start-ups émergentes, des universités, des acteurs institutionnels et des centres de recherche en un seul et même lieu afin de stimuler l'innovation dans le domaine de l'ingénierie.

Le Cyber Command entretient des relations étroites avec des ASBL comme BeCode pour le recrutement d'experts cyber sous contrat Rosetta.

Une formule « win – win – win », à court et long terme, pour tous, aussi bien pour les apprenants, jeunes et moins jeunes talents, que les professionnels et industries du secteur de la cybersécurité. A l'avenir, le SGRS souhaite proposer une réelle « proposition de valeur » gagnante pour toutes les parties, et ce toujours dans l'optique de contribuer à la résilience nationale.

Vers un nouveau concept de Réserve ?

Renforcer et promouvoir la Réserve est un moyen de créer du lien avec la population, offrir une réelle « proposition de valeurs » aux professionnels mais aussi de contribuer à la cyber résilience nationale.

Devenir réserviste,

c'est avoir l'opportunité d'intégrer le milieu militaire, de servir son pays mais aussi de partager ses savoirs, d'échanger avec d'autres professionnels, et de développer son expertise en contribuant à des projets innovants.

Au SGRS, les réservistes ont par exemple l'occasion de suivre des formations, de participer à des entrainements tels que « Locked Shields », le plus grand exercice de cyberdéfense à taille réelle organisé par le Centre d'excellence en coopération pour la cyberdéfense de l'OTAN (CCDCOE). En proposant des projets concrets et des possibilités de « formation continue » aux professionnels de la cybersécurité, le SGRS se veut plus en adéquation avec les besoins tant des entreprises, des professionnels que de la Défense.

La Réserve envisagée sous cet angle est un projet triplement « gagnant », aussi bien pour les entreprises, les professionnels que la Défense. Il permet de renforcer le savoir et l'expertise de chaque partie, promouvoir la mobilité des experts en cybersécurité ainsi que la collaboration entre le monde industriel et celui de la cyberdéfense.

Il est aussi un moyen de renforcer la cyber résilience nationale. En cas de crise nationale, le Cyber Command demeure un maillon essentiel, mais en développant cette collaboration avec les entreprises et leurs professionnels, ils seront, à leur niveau, également en mesure d'agir. La première ligne de cyberdéfense demeure les utilisateurs, à savoir les citoyens, et les sensibiliser contribue sans aucun doute à la sécurité de notre nation tout entière.

Développer la Réserve, c'est augmenter notre protection par le développement d'un réseau élargi, tant avec le professionnel que son entreprise.

Première édition de la « Cyber Summer School » et du « Cyber Discovery Day »

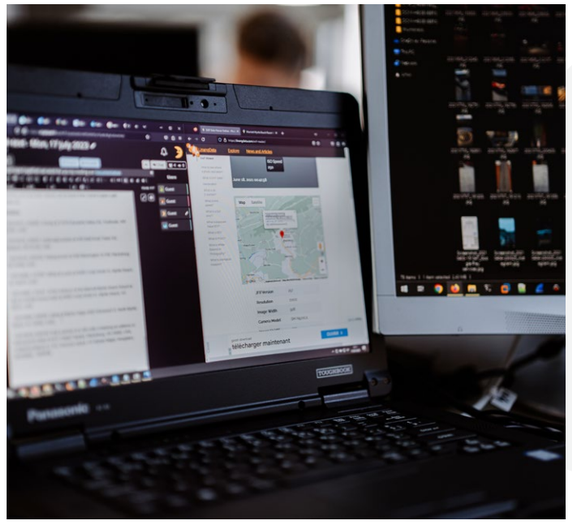
Permettre aux jeunes talents de découvrir l'ADN de leur futur employeur et mieux appréhender les défis que représente la cyberdéfense est certainement l'un des pistes à explorer pour répondre aux défis du marché de l'emploi.

Totalement inscrit dans cette volonté d'ouverture, le Cyber Command a organisé au cours de l'été 2023 sa première édition de sa « Cyber Summer School » et dans la foulée, une version « réduite », à savoir le « Cyber Discovery Day ». Ces deux nouvelles initiatives invitaient les étudiants et jeunes professionnels à découvrir les coulisses du Cyber Command et ses missions de manière plus approfondie, humaine et originale.

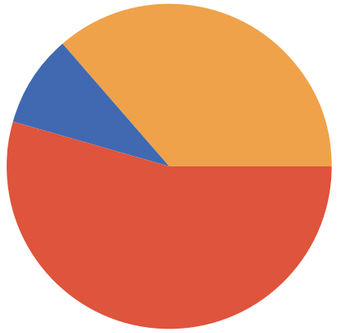
À l'issue d'un processus de sélection poussé, une vingtaine de candidats ont été sélectionnés pour participer au programme de la « Cyber Summer School », un stage d'été en milieu militaire. Accueillis durant cinq jours au sein de l'Ecole Royale Militaire, ils ont eu l'opportunité de découvrir de l'intérieur, au travers d'ateliers pratiques et d'activités ludiques, tant la culture du Cyber Command que ses capacités.

Les participants ont eu l'occasion, entre autres, d'effectuer une analyse médico-légale de smartphones, de disséquer le piratage d'un réseau informatique et d'apprendre des techniques de recherche d'information sur le dark web.

SGRS - ADIV / PARTIE IV



Si l'on en juge par les réactions des participants, cette édition a été couronnée de succès. L'initiative, ciblée et à l'image du Cyber Command, a manifestement suscité de nombreuses vocations car près d'un quart d'entre eux ont déjà rejoint nos rangs, que ce soit en tant que réserviste ou employé à temps plein.



À l'issue de la Cyber Summer School, seriez-vous enclins à vous engager au Cyber Command ? Et si oui, sous quel statut ?

- **MILITAIRE (BLEU)**
- **CIVIL (ROUGE)**
- **RÉSERVE (ORANGE)**
- **PAS INTÉRESSÉ (VERT)**

WWW.SGRS.BE