DCAF 25 ANS

SSR BACKGROUNDER

LE CONTRÔLE DU RENSEIGNEMENT À L'ÈRE DE LA NUMÉRISATION

À PROPOS DE CE DOCUMENT D'INFORMATION SUR LA RSS

Ce document d'information examine l'impact de la numérisation sur les services de renseignement et souligne l'importance d'un contrôle démocratique de ces derniers dans le contexte de la numérisation. Les technologies numériques permettent de produire des informations crédibles, mais posent des problèmes de protection de la vie privée, de droits de l'homme, de transparence, de gestion des données, de sécurité et de responsabilité. Les organes de contrôle des services de renseignement doivent disposer d'un mandat légal ainsi que des capacités et de l'expertise numériques nécessaires pour surveiller efficacement l'utilisation de ces technologies. Le document explique comment une bonne gouvernance du secteur de la sécurité (GSS) peut renforcer le contrôle démocratique des services de renseignement face aux défis de la numérisation.

CE DOCUMENT D'INFORMATION RÉPOND AUX QUESTIONS SUIVANTES :

À PROPOS DE CETTE SÉRIE

Les documents d'information sur la RSS fournissent une introduction concise à certaines questions liées à la bonne gouvernance du secteur de la sécurité (GSS) et à la réforme du secteur de la sécurité (RSS). Cette série résume les débats actuels, définit les termes clés et révèle les tensions centrales dans ces domaines en s'appuyant sur un large éventail d'expériences internationales. Les documents d'information sur la RSS ne cherchent pas à promouvoir des modèles, politiques ou propositions spécifiques en matière de gouvernance ou de réforme, mais proposent une liste de références additionnelles offrant aux personnes intéressées la possibilité d'approfondir leurs connaissances sur chaque sujet. Ils constituent des ressources utiles pour les acteurs de la gouvernance et de la réforme du secteur de la sécurité qui cherchent à comprendre et à appréhender de façon critique les approches actuelles en la matière.

DCAF, le Centre pour la gouvernance du secteur de la sécurité, Genève se consacre à l'amélioration de la sécurité des États et de leurs citoyens dans un cadre de gouvernance démocratique, d'état de droit, de respect des droits de l'homme et d'égalité des genres. Depuis sa création en 2000, le DCAF contribue à rendre la paix et le développement plus durables en aidant les États partenaires et les acteurs internationaux qui soutiennent ces États à améliorer la gouvernance de leur secteur de la sécurité grâce à des réformes inclusives et participatives. Il crée des produits de connaissances innovants, encourage les normes et les bonnes pratiques, fournit des conseils juridiques et politiques et soutient le renforcement des capacités des acteurs étatiques et non étatiques du secteur de la sécurité.

Le DCAF tient à remercier
Sondra Cheong pour la recherche, la conceptualisation et la rédaction de ce document. Nathalie Gendre, Jean-Michel Rousseau et Gabriela Manea pour l'évaluation par les pairs et les commentaires. Aleksandra Vojvodic pour la traduction en français ; Ioan Nicolau pour l'édition en français ; et Petra Gurtner pour la mise en page et la conception.

Ce document d'information sur la RSS a été élaboré en collaboration avec le Master of Advanced Studies in European and International Governance (MEIG) de l'Université de Genève.

MEIG MASTER OF ADVANCED STUDIES EUROPEAN AND INTERNATIONAL GOVERNANCE

Éditeur de la série
Gabriela Manea

Publication à citer comme suit
DCAF – Centre pour la gouvernance du secteur de la sécurité, Genève. Le contrôle du renseignement à l'ère de la numérisation. Série de documents d`information sur la RSS. Genève: DCAF, 2025.

DCAF – Centre pour la gouvernance du secteur de la sécurité, Genève
Maison de la Paix
Chemin Eugène-Rigot 2E
CH-1202 Geneva
Switzerland

info@dcaf.ch
+41 22 730 94 00

www.dcaf.ch

POURQUOI LE CONTRÔLE DÉMOCRATIQUE DU RENSEIGNEMENT EST-IL PERTINENT DANS LE CONTEXTE DE LA NUMÉRISATION ?

La numérisation a transformé la manière dont les services de renseignement recueillent et produisent des informations, lesquelles éclairent à leur tour des décisions en matière de sécurité nationale. Le travail des services de renseignement est, par définition, confidentiel, secret et classifié. Il est souvent effectué à l'aide de méthodes intrusives de collecte d'informations qui, en raison de la numérisation, deviennent de plus en plus sophistiquées.

Par exemple, l'intelligence artificielle (IA) et l'apprentissage automatique (AA) permettent aux services de renseignement d'accéder à de plus grands volumes de données, de produire des renseignements, de résoudre des problèmes et d'analyser les menaces en temps opportun. Cette tendance pose néanmoins des problèmes dans des domaines tels que la protection de la vie privée, les droits de l'homme, la transparence, la gestion des données, la sécurité et la responsabilité.

→ Pour plus d'informations, voir le Document d'information sur la RSS concernant la numérisation et la gouvernance et la réforme du secteur de la sécurité.

Bien que la nature des services de renseignement rende leur surveillance difficile, il est d'une importance vitale qu'ils fassent l'objet d'un contrôle rigoureux. En l'absence d'un contrôle démocratique efficace des services de renseignement, les technologies numériques peuvent être utilisées pour surveiller les citoyens, contrôler la liberté d'expression et censurer l'information. Ils peuvent également être utilisés par les services de renseignement nationaux et étrangers pour manipuler les décisions politiques et les processus électoraux. Ces actions portent atteinte aux valeurs démocratiques et à la bonne gestion du secteur de la sécurité.

→ Pour plus d'informations, voir le Document d'information sur la gouvernance du secteur de la sécurité dans le cadre de la RSS.

Le contrôle démocratique du renseignement est pertinent pour les raisons suivantes :

- Il établit un cadre juridique clair qui définit les mandats des services de renseignement, y compris leurs domaines spécifiques de responsabilité, les limites et les méthodes de collecte d'informations.
- Il donne aux organes de contrôle le mandat et le pouvoir d'évaluer de manière crédible les activités des services de renseignement, en garantissant à ces organes l'accès, l'indépendance, la discrétion et l'autorité.
- Il garantit que les services de renseignement se conforment à leur mandat légal et, par conséquent, le respect de la gouvernance démocratique, de l'État de droit et de l'égalité entre les hommes et les femmes.
- Il protège contre les abus politiques en mettant en place des services de renseignement professionnels et fondés sur le mérite.

DÉFINITION DES TERMES ET CONCEPTS NUMÉRIQUES

Analyse avancée : une variété de techniques d'analyse de données, telles que l'apprentissage automatique, qui sont employées par des entreprises et organisations afin d'améliorer leur prise de décision.

Intelligence artificielle (IA) : machines ou appareils dotés d'un logiciel qui apprend par l'expérience, s'adapte à de nouvelles données et exécute des tâches semblables à celles de l'homme.

Analyse de l'intelligence augmentée : combine l'IA et l'apprentissage automatique avec le jugement et la prise de décision de l'homme.

Analyse comportementale : utilise l'IA et l'analyse des données massives sur les données comportementales des utilisateurs afin d'dentifier des modèles, des tendances, des anomalies et des informations sur le comportement des clients sur des plateformes numériques telles que les sites web, les courriels et les applications mobiles.

Technologie blockchain : une grande base de données partagée et immuable qui facilite le processus d'enregistrement des transactions et de suivi des actifs dans un réseau d'entreprises.

Informatique en nuage : prestation de services informatiques, y compris les serveurs, le stockage, les bases de données, la mise en réseau, les logiciels, l'analyse et l'intelligence, sur l'internet (« le nuage ») afin d'offrir une innovation plus rapide, des ressources flexibles et des économies d'échelle.

Automatisation cognitive : l'automatisation cognitive utilise des technologies d'automatisation telles que l'IA pour rationaliser et étendre la prise de décision au sein des organisations afin d'améliorer l'efficacité opérationnelle.

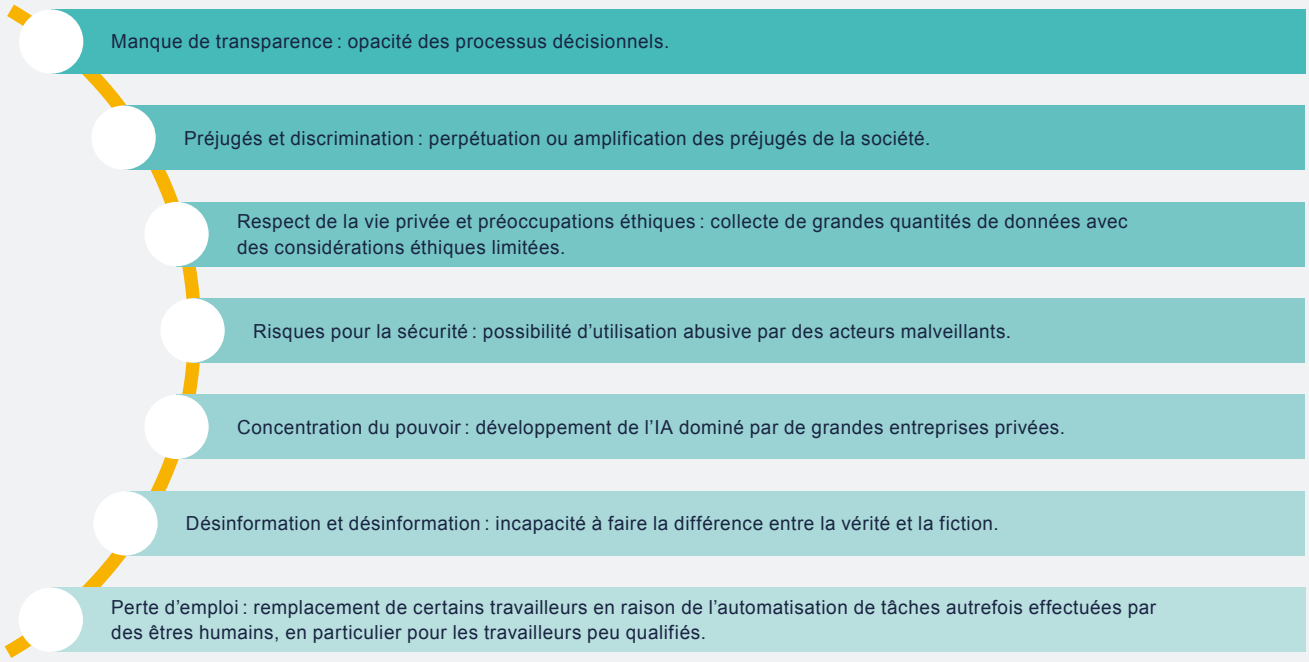
Apprentissage en profondeur : sous-ensemble de l'apprentissage automatique qui établit des corrélations complexes entre les données et apprend à partir d'exemples et d'erreurs antérieures. Il nécessite de plus grandes quantités de données que l'apprentissage automatique.

Numérisation : processus technique de conversion et de stockage de textes, d'images et de sons dans un format numérique, décrivant le passage des données d'un format analogique à un format numérique.

Apprentissage automatique (AA) : discipline de l'IA qui aide les machines à imiter le comportement humain intelligent, en apprenant aux ordinateurs à apprendre à partir de données, à identifier des modèles et à faire des prédictions de leur propre chef.

Principe d' « explicabilité » de l'IA : ensemble de processus et de méthodes qui permettent aux utilisateurs humains de comprendre et de faire confiance aux résultats et aux produits créés par les algorithmes d'apprentissage automatique.

FIGURE 1 RISQUES LIÉS À L'INTELLIGENCE ARTIFICIELLE



- Il renforce la légitimité, l'intégrité et l'efficacité des services de renseignement, car l'obligation de rendre des comptes conduit à une plus grande transparence et à une plus grande confiance des décideurs politiques et du public dans leur travail. Ceci est important afin d'obtenir le soutien politique et public en faveur de l'allocation de ressources afin d'accroître les capacités de réponse des services de renseignement aux défis nouveaux et émergents en matière de sécurité résultant de la numérisation.

→ Pour plus d'informations, voir le **Document d'information de la RSS sur le contrôle des services de renseignement.**

QUEL EST L'IMPACT DE LA NUMÉRISATION SUR LE TRAVAIL DES SERVICES DE RENSEIGNEMENT ?

Les services de renseignement sont principalement chargés de fournir aux gouvernements des informations crédibles sur les éventuelles menaces qui pèsent sur l'État et sa population. Ils définissent et développent des stratégies et des politiques militaires et de sécurité nationale cohérentes et préviennent les menaces à la sécurité nationale. En outre, les services de renseignement sont engagés dans le contre-espionnage défensif et offensif, ainsi que dans des actions secrètes, également connues sous le nom d'actions politiques spéciales.

→ Pour plus d'informations, voir le **Document d'information du RSS sur les services de renseignement.**

La numérisation a offert des possibilités de modernisation des services de renseignement, compte tenu de l'étendue de leur mission et du rythme auquel les renseignements sont produits. Bien que la numérisation soit un phénomène relativement nouveau par rapport au travail des services de renseignement, elle a transformé des activités clés telles que la collecte, le traitement et l'analyse des renseignements.

Avec les technologies numériques, le rôle des services de renseignement a été renforcé, notamment en ce qui concerne leur capacité à produire des informations crédibles et à détourner les menaces pour la sécurité nationale, telles que la cybersécurité, le terrorisme, le cyber espionnage, la désinformation, la biotechnologie, etc. La démocratisation technologique et la mondialisation ont également permis à des individus et à des groupes, travaillant ou non pour des États, ainsi qu'à des acteurs étatiques étrangers, d'exploiter des outils de renseignement technologiques pour mener des activités non détectées, telles des cyberattaques, du piratage, l'installation de logiciels malveillants et le vol de données sensibles. Cette situation complique l'environnement sécuritaire global et amène les services de renseignement à investir dans des nouvelles technologies afin de conserver une longueur d'avance sur ces menaces.

Les services de renseignement se sont ainsi adaptés en utilisant la surveillance et les **technologies d'apprentissage automatique** dans l'analyse du renseignement et l'identification biométrique, même si l'étendue de l'utilisation de ces technologies numériques n'est pas connue en raison de la nature secrète des activités de renseignement.

Collecte d'informations

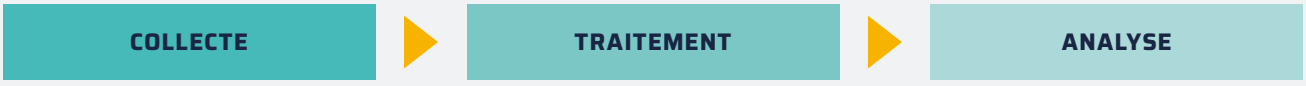
Des technologies telles que l'IA et l'AA, l'**informatique en nuage** et l'**analyse avancée** ont renforcé la capacité des services de renseignement à collecter des données à partir d'un large éventail de sources numériques. L'IA est appliquée afin d'automatiser la reconnaissance aérienne, de même que la surveillance et le suivi de cibles. Les algorithmes d'AA sont utilisés pour vérifier et valider les cibles collectées à partir d'images. Par ailleurs, les activités de surveillance ne se limitent plus à la collecte de données, mais impliquent un suivi en temps réel d'activités en ligne.

Cependant, la collecte d'informations n'est plus seulement l'apanage des services de renseignement. Des entreprises privées, y compris des sociétés militaires et de sécurité privées (SMSP), en tant que propriétaires et moteurs de technologies émergentes, s'engagent dans de la surveillance de masse, le profilage numérique des citoyens et la modification du comportement, rendus possibles par la commercialisation de l'espace et la prolifération de l'imagerie et des capteurs basés sur les satellites. Cela porte atteinte aux droits de l'homme et à l'autorité de l'État en matière de production de renseignements et a de graves implications éthiques et sécuritaires, car les activités des sociétés privées dans ce domaine ne sont pas soumises à un contrôle réglementaire et à une surveillance stricts.

Traitement

L'IA améliore le filtrage de grands volumes de données et d'informations utilisées pour prendre des décisions fondées sur l'intelligence. L'IA est utilisée pour identifier des modèles dans les données et des anomalies qui pourraient être difficiles à détecter par des agents de renseignement humains. Elle a été utilisée pour traiter et automatiser les informations collectées par les satellites et les données aériennes de renseignement, de surveillance et de reconnaissance.

FIGURE 2 ACTIVITÉS CLÉS DE LA COLLECTE DE RENSEIGNEMENTS



Cependant, le traitement de l'information est devenu difficile en raison du volume massif d'informations numérisées, qui est compliqué par le rythme rapide auquel la désinformation se propage sur la multitude de plateformes de médias sociaux. Cette situation met à l'épreuve les capacités de traitement des services de renseignement et les obligera à adopter une approche plus diligente et plus approfondie pour détecter et filtrer les informations erronées qui pourraient avoir des conséquences négatives sur l'analyse et la prise de décision.

Analyse

Les services de renseignement s'appuient sur l'« **intelligence augmentée par l'IA** » pour analyser des informations, à l'aide d'outils tels que l'**automatisation cognitive** et l'**analyse comportementale.** Ces outils sont de plus en plus utilisés et accomplissent même des tâches telles que le traitement du langage, la comparaison des visages, la transcription de textes à partir de fichiers audio et la détection des fraudes, lesquelles étaient traditionnellement effectuées par des analystes humains. Certains services de renseignement ont également commencé à utiliser l'**apprentissage profond** pour améliorer l'efficacité des analystes.

Les analystes doivent acquérir de nouvelles compétences pour mesurer l'authenticité des données dans leurs analyses et se sensibiliser au principe d' **« explicabilité » de l'IA,** qui permet aux décideurs de justifier une décision donnée. Ces compétences permettent aux analystes de détecter les limites de l'utilisation des technologies et de comprendre la logique, les hypothèses et les biais de données de l'IA. Bien que cela soit encourageant, la numérisation continuera à créer une dépendance vis-à-vis des technologies numériques, érodant ainsi l'intuition humaine dans l'analyse et la prise de décision. En outre, l'IA risque de perpétuer les préjugés sociaux liés au genre, à la race et à l'ethnicité tout au long du cycle de vie de la production d'intelligence, par exemple avec l'utilisation de logiciels de reconnaissance faciale ou vocale.

QUELLE EST L'INFLUENCE DE LA NUMÉRISATION SUR LE RÔLE DES ACTEURS DE LA SURVEILLANCE DU RENSEIGNEMENT ?

Dans un système de gouvernement démocratique, le contrôle des services de renseignement comprend les pouvoirs exécutif, judiciaire et législatif, le contrôle interne des services de renseignement et les institutions indépendantes et publiques/informelles, y compris la société civile et les médias.

→ Pour plus d'informations sur les acteurs du contrôle du renseignement, voir le **Document d'information de la RSS sur le contrôle du renseignement.**

La numérisation **renforce l'efficacité des acteurs de la surveillance du renseignement :**

- Les plateformes de communication telles que les sites web et les médias sociaux peuvent permettre aux acteurs de la surveillance du renseignement d'atteindre un public plus large et tenir ce dernier informé de leurs activités.

- Les débats parlementaires et budgétaires, les commissions d'enquête, les réunions d'information des commissions, etc., peuvent désormais être diffusés en direct sur des plateformes en ligne, permettant un engagement en temps réel avec le public. Grâce à la connectivité accrue de l'internet, les acteurs formels et informels de la surveillance peuvent recueillir des informations sur les violations de droits de l'homme dans des endroits autrefois inaccessibles.

- La société civile peut utiliser les plateformes numériques disponibles pour façonner les lois et les politiques par le biais du partage d'informations, de consultations publiques, de l'expression de points de vue, de la mobilisation de campagnes et de manifestation, et de la collecte de fonds.

Toutefois, les acteurs de contrôle du renseignement manquent souvent de la capacité nécessaire pour surveiller les domaines problématiques, tels que la confidentialité, la protection et le partage des données, les violations potentielles des droits de l'homme et la discrimination dans l'espace numérique, ainsi que les risques liés à la sécurité numérique, de manière efficace. Dans l'ensemble, les acteurs de la surveillance du renseignement reçoivent moins d'aide pour se tenir au courant des technologies numériques que les services de renseignement eux-mêmes. En outre, les technologies numériques telles que l'IA ne sont pas soumises à l'examen du public, car elles relèvent de la catégorie des secrets commerciaux.

La numérisation met également à l'épreuve les limites des lois et règlements existants relatifs à l'engagement politique, car elle a un impact direct sur les libertés d'expression, d'association et de réunion, ainsi que sur l'accès à l'information. Certains gouvernements ont été contraints à modifier leur législation pour assurer la protection des données et la sécurité numérique, et à mettre en place des initiatives visant à renforcer le rôle de la société civile pour promouvoir la transparence. Cependant, l'ambiguïté demeure sur la manière dont les technologies émergentes telles que l'IA sont développées et déployées, ce qui rend difficile la mise en place des mécanismes appropriés de contrôle et de responsabilité.

Les acteurs de la surveillance du renseignement doivent :

- avoir le plus haut niveau d'accès au personnel, aux sites et aux informations classifiées. En conséquence, les programmes de classification des informations et les lois sur la liberté d'information devraient favoriser l'accès à ces informations **(Accès).**

- être indépendant des intérêts politiques et de l'influence inappropriée des services de renseignement. Des budgets dédiés et du personnel spécialisé contribuent à garantir un contrôle crédible **(Indépendance).**

- être conçu pour préserver le secret et l'intégrité du processus de renseignement. La fiabilité est nécessaire pour gagner la confiance des services de renseignement afin de sauvegarder les intérêts nationaux **(Discrétion).**

- disposer de pouvoirs d'enquête discrétionnaires, y compris le pouvoir d'obliger à témoigner sous serment. Des tribunaux ou des juges spéciaux doivent être chargés de la surveillance des services de renseignement **(Autorité).**

→ Pour plus d'informations, voir le Document d'information de la RSS sur le contrôle des services de renseignement.

QUELS SONT LES DÉFIS ET LES OPPORTUNITÉS POSÉS PAR LA NUMÉRISATION DANS LE CONTRÔLE DES SERVICES DE RENSEIGNEMENT :

Les obstacles typiques à la mise en place d'un contrôle démocratique des services de renseignement proviennent soit des services de renseignement eux-mêmes (interne), soit du contexte dans lequel ils opèrent (externe).

→ Pour plus d'informations sur ces défis à relever, voir le Document d'information de la RSS sur le contrôle des services de renseignement.

FIGURE 3 DÉFIS ET OPPORTUNITÉS INTERNES

DÉFIS	POSSIBILITÉS
(1) Secret	
• Les technologies numériques renforcent le voile du secret des services de renseignement, ce qui leur permet de violer potentiellement la sphère privée au nom de la sécurité nationale. • Le secret dilue le processus de contrôle des services de renseignement, laissant la qualité du contrôle dépendre presque entièrement de la bonne volonté des services de renseignement, affaiblissant ainsi les démocraties libérales. • Les technologies numériques permettent aux régimes autoritaires de porter atteinte plus facilement aux droits fondamentaux de leurs propres citoyens et des citoyens étrangers.	• Mettre à jour les mandats des institutions de contrôle afin de leur permettre de superviser l'utilisation des technologies numériques par les services de renseignement et renforcer leur accès aux informations secrètes. • Permettre à la société civile de jouer un rôle plus important dans l'élaboration des politiques relatives au travail de renseignement et à la politique en matière de données. • Faire la lumière sur les activités des services de renseignement par le biais du journalisme d'investigation et de la couverture médiatique. • Renforcer l'utilisation des technologies numériques pour permettre aux organes de contrôle et au public d'accéder à l'information.
(2) Pouvoir discrétionnaire	
• Les professionnels du renseignement disposent généralement d'un pouvoir discrétionnaire leur permettant de prendre des décisions indépendantes. En l'absence d'une «explicabilité» et de règles d'engagement appropriées, l'IA brouille la charge de la responsabilité dans la prise de décision en matière de renseignement. • Les systèmes d'IA sont souvent biaisés en termes de sexe et d'appartenance ethnique, ce qui alimente en informations erronées les décisions générées par l'IA. Cela pose des problèmes éthiques et nécessite davantage de capacités et de ressources pour les organes de contrôle, afin de découvrir et de contrer de telles tendances dans le travail des services de renseignement.	• Pour garantir une prise de décision indépendante et responsable, la direction des services de renseignement doit inculquer à tous les niveaux une culture du professionnalisme fondée sur le respect de la bonne gouvernance et de l'État de droit, y compris l'égalité entre les hommes et les femmes. • L'IA et les technologies émergentes doivent être conçues de manière compatible avec les droits de l'homme à tous les stades de la production de l'intelligence.
(3) Perception exagérée des menaces	
• Des menaces telles que la cybersécurité, le terrorisme, le cyber espionnage et la désinformation peuvent justifier une utilisation potentiellement abusive et excessive de technologies telles que l'IA, la reconnaissance faciale et la surveillance par drone, au détriment de la bonne GSS, des droits de l'homme et de l'État de droit. • Il n'existe pas de mécanismes de recours en cas de violation des droits de l'homme par des pratiques de renseignement informatisées, ni de régime de protection pour les lanceurs d'alerte qui mettent au jour des abus.	• Renforcer le professionnalisme et l'indépendance politique, en veillant à ce que l'analyse des renseignements ne surestime ni ne sous-estime les menaces pour la sécurité nationale et s'abstienne de toute violation des droits de l'homme. • Élaborer une définition juridique de l'intrusion et des critères pour la collecte et l'analyse de données non abusives.

FIGURE 4 DÉFIS ET OPPORTUNITÉS EXTERNES

DÉFIS	POSSIBILITÉS
(1) Volonté politique	
• La priorité accordée à d'autres intérêts de sécurité nationale par rapport à la responsabilité des services de renseignement a conduit à un sous-investissement dans le contrôle législatif ou exécutif de ces services, en contraste marqué avec les investissements massifs réalisés par les gouvernements et les entreprises du secteur privé dans le développement de technologies sophistiquées pour la collecte de renseignements et la surveillance. • Le caractère intrusif des technologies de surveillance suscite la méfiance du public en ce qui concerne l'efficacité des organes de contrôle à protéger les droits de l'homme contre les pratiques problématiques des services de renseignement. • En l'absence d'un contrôle efficace, les services de renseignement peuvent faire l'objet de manipulations politiques, et vice versa.	• Élaborer des approches globales qui garantissent une meilleure surveillance grâce à une collaboration accrue entre les organismes de surveillance, le gouvernement et le secteur privé. • Protéger les services de renseignement des manipulations politiques en définissant clairement les chaînes de responsabilité politique des décideurs.
(2) Champ d'application international	
• La numérisation a rendu la coopération internationale en matière de renseignement omniprésente et moins sujette à contrôle. • Les organes de contrôle du renseignement ne disposent pas de connaissances ni de mécanismes de contrôle nécessaires pour déterminer si et comment les services de renseignement nationaux partagent des données avec des services de renseignement étrangers. Ce qui peut en résulter, ce sont des lacunes en matière de responsabilité, des limites à l'examen efficace du partage des données, de la collusion et des déficits démocratiques au niveau international.	• Afin d'éviter les abus et de renforcer la crédibilité des services de renseignement nationaux, les lois et règlements nouveaux ou existants doivent définir la portée et la nature de la coopération internationale en matière de renseignement et de partage des responsabilités.
(3) Développements technologiques	
• Alors que l'innovation technologique a donné des moyens aux services de renseignement, les organes de contrôle du renseignement ont été lents à bénéficier des avancées technologiques, un décalage qui se traduit par des lacunes en matière d'adaptabilité, de responsabilité et de transparence.	• Intégrer une expertise numérique renforcée au sein des organes de contrôle. • IMaintenir les cadres juridiques à jour par rapport aux développements numériques. • IDans les deux cas, les gouvernements doivent investir dans le renforcement des ressources humaines et des capacités et dans des technologies adaptées aux besoins des organes de contrôle.

COMMENT UNE BONNE GSS PEUT-ELLE RENFORCER LE CONTRÔLE DÉMOCRATIQUE DES SERVICES DE RENSEIGNEMENT DANS LE CONTEXTE DE LA NUMÉRISATION :

Il ne fait aucun doute que la numérisation améliore l'efficacité et l'efficience des services de renseignement, mais on peut soutenir que cela a un coût élevé. Pour contrer les effets négatifs potentiels, l'utilisation des outils et technologies numériques par les services de renseignement doit être soumise aux principes démocratiques et respecter les valeurs fondamentales et les droits de l'homme. Par ailleurs, le contrôle du renseignement doit se baser sur les principes d'une bonne GSS (voir figure 3).

Efficacité et efficience

- Les analystes du renseignement, ainsi que les acteurs du contrôle, doivent être formés à l'éthique, à la transparence et à la responsabilité, dans le contexte de la numérisation et des technologies émergentes.

- Le contrôle exécutif doit faire correspondre son investissement (politique, financier et technique) dans le contrôle du renseignement avec un investissement dans l'amélioration des capacités numériques des services de renseignement.

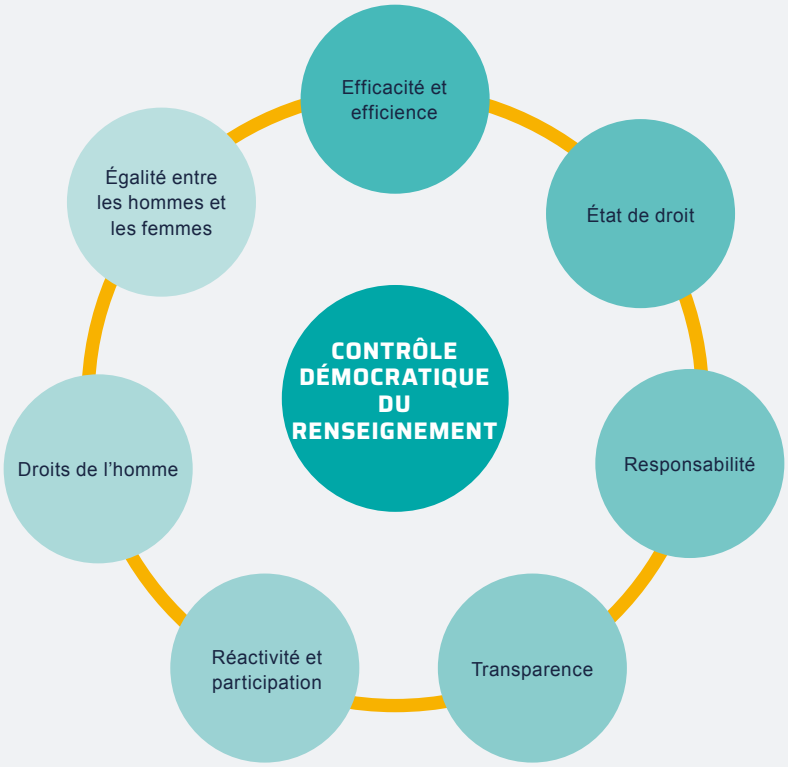
- Le renseignement moderne étant axé sur les données, son contrôle doit l'être également. Les organes de contrôle doivent donc adopter des instruments technologiques leur permettant de§ répondre aux avancées technologiques dans le domaine du renseignement.

État de droit

- Qu'il s'agisse des services de renseignement ou des entreprises privées, l'innovation technologique future doit s'inscrire dans un cadre réglementaire clairement défini, qui fixe des critères justifiables, nécessaires et proportionnés pour la collecte, le traitement et l'analyse d'informations et de données, garantissant à la fois le respect des droits individuels et la protection nécessaire des activités de renseignement.

- Les entreprises technologiques et les décisions algorithmiques doivent être soumises à une bonne gouvernance par le biais de mécanismes de responsabilisation des algorithmes, y compris l'explicabilité de l'IA et la disponibilité du code source ouvert.

FIGURE 5 CONTRÔLE DÉMOCRATIQUE DU RENSEIGNEMENT ET PRINCIPES D'UNE BONNE GSS



- Les lois, les politiques et les budgets relatifs aux services de renseignement doivent faire l'objet d'un examen minutieux, dans la mesure où cela ne menace pas la sécurité nationale. Les organes de contrôle formels et informels doivent être conçus de manière à rendre les services de renseignement « contrôlables ».

- Les lois sur la protection de la vie privée et des données ne devraient pas prévoir de larges exceptions pour les services de renseignement.

- Les pouvoirs exécutif, législatif et judiciaire doivent mettre en place un système viable d'équilibre des pouvoirs et garantir l'indépendance politique des services de renseignement.

Responsabilité

- Les organes de contrôle doivent procéder à des évaluations des technologies émergentes afin de s'assurer que les droits de l'homme, y compris la non-discrimination, le respect de la vie privée et l'égalité des genres, sont respectés dans les opérations des services de renseignement et, surtout, dans le développement et le déploiement d'outils numériques par des entreprises privées. Les organes de surveillance du renseignement doivent également adhérer à ces principes lorsqu'ils utilisent des outils numériques dans le cadre de leurs activités.

- Un système d'audit fondé sur l'éthique doit être mis en place pour exiger des services de renseignement qu'ils expliquent et justifient leurs décisions, y compris celles prises par l'IA, et en particulier les conséquences potentiellement graves de ces décisions.

- Le contrôle interne et l'encadrement supérieur des services de renseignement doivent renforcer la responsabilité en établissant des règles et des procédures garantissant que le personnel agit de manière professionnelle et efficace dans les limites de son autorité, dans le respect de la loi, des droits de l'homme et de l'égalité des genres. Des mécanismes de sanction des actions illégales, de réparation pour les victimes d'abus et de protection des lanceurs d'alerte doivent être mis en place. Le pouvoir judiciaire doit surveiller attentivement l'exercice des pouvoirs spéciaux, statuer sur les accusations de mauvaise conduite portées contre les membres des services de renseignement et poursuivre les éventuelles fautes commises.

- Un environnement propice doit être créé pour permettre à la société civile de signaler les actes répréhensibles et d'obtenir réparation dans de telles situations. Les médias doivent également jouer un rôle plus important dans le journalisme d'investigation afin d'exposer tout acte répréhensible commis par les services de renseignement et de les obliger à rendre des comptes au public.

Transparence

- Il faut établir un cadre juridique qui définisse clairement les mandats, les rôles, les responsabilités et les limites des services de renseignement et des organes de contrôle.

- Les organes de contrôle doivent constamment faire appel aux services de renseignement afin d'instaurer la confiance dans l'accès et l'examen des systèmes opérationnels, ainsi que dans l'examen minutieux des systèmes de collecte et d'analyse des données, de manière précise et opportune.

- Les services de renseignement doivent travailler en étroite collaboration avec les développeurs privés de technologies numériques afin de s'assurer que les données sont collectées uniquement aux fins prévues et de manière sûre, dans le respect de l'état de droit et des droits de l'homme, et sans menace pour la sécurité humaine ou nationale. Les organes de contrôle doivent surveiller de près cette collaboration.

Réactivité et participation

- Le contrôle des services de renseignement doit veiller à ce que la gouvernance et la réglementation des services de renseignement se fassent de manière inclusive et participative, en tenant compte de l'impact que les technologies numériques peuvent avoir sur les groupes rendus vulnérables par la discrimination.

- Les services de renseignement doivent toujours observer une culture de service et de devoir envers la nation, en s'abstenant de toute manipulation, intimidation ou censure.

Droits de l'homme et égalité des genres

- Les droits de l'homme et l'égalité des genres doivent être intégrés dans les activités des services de renseignement et des organes de contrôle, à tous les niveaux.

- Il convient d'élaborer des concepts de formation à l'intention des analystes du renseignement et des acteurs de la surveillance, permettant de sensibiliser à la propension des systèmes liés à l'IA pour afficher d'importants préjugés et discriminations liés au genre et autres, et qui offrent une approche intersectionnelle pour éliminer la discrimination.

QUE LIRE ENSUITE ?

- Ryngaert, Cedric et van Eijk, Nico (2019)
  International Cooperation by (European) Security and Intelligence Services: Reviewing the Creation of a Joint Database in Light of Data Protection Guarantees
  International Data Privacy Law 9 (1) (April)

- Vieth, Kilian et Wetzling, Thorsten (2019)
  Data-driven Intelligence Oversight. Recommendations for a System Update
  Stiftung Neue Verantwortung (November)

- Katz, Brian (2020)
  The Collection Edge: Harnessing Emerging Technologies for Intelligence Collection
  Washington, DC: Centre for Strategic and International Studies (CSIS)

- Born, Hans et Wills, Aidan (2012)
  Supervision des services de renseignement : Une boîte à outils
  DCAF : Genève

- Blanchard, Alexander et Taddeo, Mariarosaria (2023)
  The Ethics of Artificial Intelligence for Intelligence Analysis: a Review of the Key Challenges with Recommendations
  DISO 2, 12.

AUTRES RESSOURCES DU DCAF SUR LA RSS

Les publications du DCAF comprennent une large gamme de manuels et outils spécifiques permettant de guider les praticiens oeuvrant dans le domaine de la RSS et de la bonne GSS, téléchargeables gratuitement à l'adresse suivante : **www.dcaf.ch**

NOTRE MISSION

Aider les États à améliorer le mode de gouvernance de leur secteur de la sécurité.

Donner des conseils sur l'élaboration de mesures de gouvernance du secteur de la sécurité à la fois efficaces et viables.

Favoriser la mise en œuvre par les États de réformes participatives, valorisant la contribution de tous et intégrant la dimension de genre.

NOS ACTIONS

Fournir une expertise technique aux processus de RSS/G menés au niveau national.

Renforcer les capacités des acteurs étatiques et non étatiques.

Diffuser en libre accès des ressources et des résultats de travaux de recherche.

Promouvoir les bonnes pratiques de gouvernance recommandées au niveau international.

Conseiller sur les questions juridiques et politiques liées au secteur de la sécurité.

DCAF – Geneva Centre for Security Sector Governance

Maison de la Paix
Chemin Eugène-Rigot 2E
1202 Geneva
Switzerland

+41 22 730 94 00
info@dcaf.ch
@DCAF_Geneva

www.dcaf.ch