DCAF Le Centre pour la gouvernance du secteur de la sécurité, Genève

SSR BACKGROUNDER

LA DIGITALISATION ET LA GOUVERNANCE ET LA RÉFORME DU SECTEUR DE LA SÉCURITÉ (G/RSS)

À PROPOS DE CE DOCUMENT D'INFORMATION RSS

Ce document d'information sur la RSS traite des répercussions de la digitalisation sur la bonne gouvernance du secteur de la sécurité. En tant que défi émergent en matière de sécurité, la digitalisation et les processus numériques qui y sont associés remodèlent et recadrent les idées traditionnelles de bonne gouvernance, tout en impliquant de nouveaux acteurs émergents de la sécurité dans le secteur de la sécurité. Ce document d'information explore d'abord la digitalisation et ses processus connexes, et explique pourquoi il s'agit d'un nouveau défi en matière de sécurité. Ensuite, il examine comment une bonne GSS pourrait améliorer la sécurité dans l'espace numérique et met en évidence les principaux défis, opportunités et perspectives que la digitalisation pose à une bonne GSS/R. Enfin, il identifie les acteurs spécifiques du secteur de la sécurité qui jouent un rôle important en contribuant à une bonne GSS dans l'espace numérique.

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
Dawn Lui, avec l'aide d'Alexandru Lazar, pour la recherche, rédaction et l`édition de ce document;
Franziska Klopfer, Teodora Fuior, Ann Blomberg pour leurs commentaires et révisions ;
Aleksandra Vojvodic pour la traduction en français; Ioan Nicolau pour l`édition en français et Petra Gurtner pour la mise en forme et la conception de ce document.

Éditrice de la série
Gabriela Manea

Publication à citer comme suit
DCAF – Centre pour la gouvernance du secteur de la sécurité, Genève. « La Digitalisation et la gouvernance et la réforme du secteur de la sécurité (GSS/R). »
Série de documents d'information sur la RSS.
Genève : DCAF, 2023.

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

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

www.dcaf.ch

QU'EST-CE LA DIGITALISATION ?

Le terme de 'digitalisation' désigne un ensemble de processus technologiques, tels que les progrès en matière de communications et infrastructures numériques, qui affectent tous les domaines de la vie publique et privée. En d'autres termes, la digitalisation est l'adoption ou l'utilisation accrue de technologies numériques ou informatiques par des États, des organisations ou des individus. La digitalisation est un domaine très contesté, aux conséquences profondes et incertaines pour la sécurité. La révolution numérique a conduit à une augmentation de la disponibilité et de l'accès à l'information, augmentant le pouvoir des individus et élargissant l'espace démocratique. Par exemple, les services de sécurité peuvent atteindre plus facilement les personnes marginalisées grâce aux technologies numériques. Cependant, cet accès élargi à l'information entraîne également une augmentation de la désinformation, des intox et des campagnes de propagande, qui sapent la confiance dans les autorités publiques. Les autocrates et autocraties, en particulier, ont tendance à utiliser les technologies numériques pour freiner l'opposition et manipuler les récits politiques.

POURQUOI LA DIGITALISATION CONSTITUE-T-ELLE UN DÉFI ÉMERGENT EN MATIÈRE DE SÉCURITÉ ?

Si la digitalisation offre des possibilités d'amélioration et de renforcement de la sécurité et de surveillance, elle peut également être considérée comme un « défi de sécurité émergent » (DSE). Les DSE sont de nouvelles menaces qui ne figuraient pas auparavant dans la conception traditionnelle de la sécurité; Il s'agit notamment de menaces liées à la sécurité transnationale, ainsi que de menaces à la sécurité humaine et sociétale. Pendant plusieurs décennies, les DSE ont été un concept contesté, mais ont maintenant pénétré la pensée et la pratique de la sécurité mondiale, comme l'illustre, par exemple, l'utilisation parallèle de moyens de guerre conventionnels et hybrides dans les conflits contemporains. Les DSE sont des actions ou des événements qui mettent en péril à la fois la structure matérielle et normative des individus, des sociétés et des États. De tels défis sont considérés comme « émergents » lorsque la communauté au sens large des experts et des décideurs les définit comme des risques de sécurité, et que des réponses politiques de sécurité pour les contrer sont alors développées. Premièrement, la digitalisation du secteur de la sécurité a suscité des débats sur l'équilibre entre d'une part un droit individuel et sociétal à la vie privée et d'autre part les obligations et devoirs des États de protéger leurs citoyens. L'intégrité du contrat social entre l'État et la société est mise à rude épreuve en raison de l'infiltration des technologies numériques dans tous les domaines de la vie publique et individuelle. Deuxièmement, les nouveaux outils numériques et les interfaces virtuelles connectées via Internet créent en même temps un paysage complexe de cybermenaces avec un nombre croissant de points de défaillance critiques. Les cybermenaces dépassent les capacités de nombreuses sociétés à les prévenir et à les gérer efficacement. Par exemple, les cyberacteurs utilisant des logiciels de rançon ciblent les services publics, les systèmes de santé et même les organisations non gouvernementales (ONG) qui fournissent de l'aide aux populations vulnérables. Ces acteurs émergents vont des hacktivistes aux cybercriminels et aux cybergroupes parrainés par des États. Ils ciblent aussi bien les représentants de l'État que les militants des droits de l'homme, ce qui entraîne des tensions politiques, des sanctions gouvernementales et des poursuites judiciaires.

FIGURE 1 CLARIFICATIONS CONCEPTUELLES

Digitalisation vs numérisation : La digitalisation ne doit pas être confondue avec la numérisation. La numérisation est le processus technique de conversion et de stockage de texte, d'images et de sons dans un format numérique. Il s'agit de la transition des données d'un format analogique à un format numérique. La numérisation n'entre pas dans le cadre du présent document d'information.

Espace numérique : Il s'agit d'un terme général qui fait référence aux réseaux et aux dispositifs utilisés pour partager de l'information entre personnes, entre institutions, et entre personnes et institutions. Il peut également être conçu comme une arène sociale accessible via une interface virtuelle, permettant utilisateurs d'interagir afin d'accéder ou de partager des données. Contrairement à d'autres espaces tels que la terre, la mer ou l'air, l'espace numérique est considéré comme un nouveau domaine qui s'étend au-delà des frontières nationales (similaire à l'espace extra-atmosphérique).

Cybersécurité : Il s'agit de la pratique consistant à défendre l'infrastructure numérique et les institutions associées contre des menaces numériques et à chercher à garantir une utilisation sûre de l'espace numérique par tous les acteurs impliqués. Toute perturbation de ces services essentiels pourrait entraîner des conséquences dévastatrices pour la population et, à long terme, pour la survie d'un État. La cybersécurité est un lien spécifique et étroit entre la digitalisation et le secteur de la sécurité.

L'avènement de nouveaux outils et acteurs technologiques remet radicalement en question les cadres existants de bonne gouvernance, y compris dans le secteur de la sécurité. Les acteurs du secteur de la sécurité se retrouvent régulièrement à devoir naviguer dans un monde où les développements technologiques dépassent la mise en œuvre des mécanismes de réglementation. Ce nouvel environnement de sécurité a dépassé sa phase « émergente », posant des défis durables à la sécurité nationale et à la démocratie, ainsi qu'aux droits de l'homme et aux libertés civiles des individus.

POURQUOI UNE BONNE GSS EST-ELLE IMPORTANTE POUR LA DIGITALISATION ?

La double nature de la digitalisation – à la fois opportunité et menace – transforme la gouvernance et la prestation de services de sécurité. Cette section explique pourquoi et comment les principes de bonne gouvernance et les questions transversales qui sous-tendent la bonne GSS peuvent aider à mieux gérer les impacts négatifs de la digitalisation sur le secteur de la sécurité et sur la gouvernance démocratique.

Pour de plus amples renseignements sur les principes de bonne gouvernance, veuillez consulter le document d'information 'La Gouvernance du secteur de sécurité'.

Le renforcement de la responsabilité pour des processus numériques dans le secteur de la sécurité suppose des mécanismes de surveillance et de contrôle externes et internes, mis en place par une autorité indépendante. Puisque la digitalisation donne lieu à de nouveaux mécanismes de gestion de données et à de nouvelles techniques de traitement de données, elle permet une surveillance accrue des actions gouvernementales en renforçant la traçabilité, le stockage et la récupération de l'information. Toutefois, il est important de veiller à ce que les évolutions législatives suivent la cadence de ces progrès technologiques, afin qu'il existe des lignes directrices claires sur l'utilisation des outils numériques par le secteur de la sécurité sans aucune violation des droits des personnes.

L'utilisation **transparente** des moyens numériques par le secteur de la sécurité signifie que les informations relatives aux institutions de ce dernier sont accessibles au public et disponibles. La réglementation concernant les renseignements confidentiels et des questions connexes liées à la protection de la vie privée est essentielle pour prévenir des violations de la protection des données. En parallèle, des outils numériques devraient être adoptés pour améliorer la disponibilité, l'accessibilité, le traitement et la sécurité des informations. Les acteurs de la sécurité doivent être prudents lors de la collecte et du traitement des données sur les personnes et veiller à ce que des garanties adéquates soient en place.

Le respect de **l'état de droit** dans le secteur de la sécurité signifie que tous les individus et toutes les institutions, y compris l'État, sont soumis à des lois publiques et impartiales, conformes aux normes internationales et nationales relatives aux droits de l'homme. L'utilisation abusive des technologies numériques peut compromettre la tenue d'élections libres et équitables, mettre en péril la liberté d'expression et limiter l'accès à des informations fiables. La prééminence de la technologie peut menacer de remplacer l'état de droit, en créant des conditions propices à l'autoritarisme numérique dans lequel les technologies numériques sont utilisées pour contrôler ou manipuler des individus dans le pays ou à l'étranger. Les fausses nouvelles, les fausses rumeurs et la propagande haineuse contre les groupes marginalisés peuvent être utilisées pour mobiliser du soutien en faveur d'intérêts autoritaires et peuvent également être instrumentalisées comme prétextes pour promulguer des lois restrictives sur les médias qui ciblent les critiques et les défenseurs des droits humains.

La digitalisation des services de sécurité signifie que davantage de personnes peuvent **participer** au secteur de la sécurité et accéder aux services sur une base équitable et inclusive. Les administrations centrales et locales peuvent mettre en œuvre des outils et mécanismes en ligne pour soutenir les personnes à risque. Les femmes, les membres de minorités raciales et linguistiques, les jeunes et les personnes ayant des emplois mal rémunérés et un faible niveau d'éducation ont tendance à avoir moins accès aux processus démocratiques en raison de facteurs socio-économiques très divers. Les décideurs devront combler les lacunes en matière de littératie numérique, défendre les structures publiques contre le piratage cybernétique, et protéger la sphère privée des citoyens afin de garantir que les groupes défavorisés puissent se connecter à ces services.

La réactivité dans l'espace numérique prescrit que les institutions du secteur de la sécurité soient sensibles aux différents besoins de sécurité de la population et assument leurs rôles et responsabilités dans l'esprit d'une culture du

FIGURE 2 DÉFIS, OPPORTUNITÉS ET PERSPECTIVES DE LA DIGITALISATION DANS LA GSS/R

Défis	Possibilités	Perspectives
Surveillance et processus administratifs		
• Les développements technologiques se produisent plus rapidement que la mise en œuvre législative. • Les normes et réglementations dans l'espace numérique sont en constante évolution. • Il y a un manque de mécanismes de surveillance à jour et tournés vers l'avenir qui protègent les droits de la personne dans l'espace numérique en évolution.	• Le secteur de la sécurité peut adopter des processus tournés vers l'avenir pour s'assurer qu'il n'y a pas de lacunes dans la loi. • Le secteur de la sécurité peut mettre en œuvre des cadres réglementaires de manière réactive, et tenir les acteurs des secteurs public et privé informés de tout développement dans l'espace numérique. • L'information peut être récupérée plus facilement et stockée de manière plus sûre, ce qui évite les retards dans la coopération interministérielle.	• L'examen de la façon dont les décisions sont mises en œuvre peut être prise en charge par des algorithmes. • Les responsables de la sécurité pourraient être moins responsables du personnel et plus en contrôle des processus numériques. • Les citoyens pourraient être en mesure d'accéder à des plateformes en ligne conçues pour leur permettre de soumettre des préoccupations en matière de sécurité et de poser des questions.
Capacités et ressources des institutions du secteur de la sécurité		
• Il y a peu de transparence autour des acquisitions d'outils numériques par différents acteurs du secteur de la sécurité et au moyen de fonds publics, ainsi que peu de questions quant à l'adaptabilité de ces outils face à l'évolution de l'espace numérique. • Les acteurs du secteur de la sécurité et les législateurs ne sont pas au courant des développements technologiques dans l'espace numérique.	• Le secteur de la sécurité peut investir dans des outils et des technologies numériques pour améliorer la sécurité en la rendant plus accessible et ciblée pour la population qu'elle sert. • Le secteur de la sécurité peut adopter des outils numériques pour traiter et analyser les données plus efficacement, éliminer les préjugés humains dans la collecte de données, ainsi qu'améliorer et normaliser les processus administratifs et de surveillance.	• Les tâches journalières sont susceptibles de devenir plus numérisées et nécessitent moins d'intervention humaine, ce qui permet aux experts de travailler sur des tâches plus complexes. • La sécurité pourrait mieux répondre aux besoins spécifiques des différentes communautés en raison de l'amélioration de l'analyse des données et de l'accès à l'information.
Compétences et connaissances techniques du personnel du secteur de la sécurité		
• Le secteur de la sécurité a des compétences numériques limitées et une capacité limitée à s'engager dans l'espace numérique en évolution. • Le secteur de la sécurité n'est pas en mesure d'attirer et de retenir du personnel qualifié.	• Le secteur de la sécurité peut fournir une formation numérique au personnel de sécurité existant afin d'accroître les capacités et d'attirer des employés potentiels. • Le secteur de la sécurité peut recruter du personnel qualifié et alphabétisé au numérique pour s'assurer qu'il n'est pas à la traîne par rapport au secteur privé.	• La digitalisation du secteur de la sécurité pourrait entraîner une course pour suivre le rythme des nouvelles technologies et attirer du personnel qualifié. • L'émergence de nouveaux acteurs de la sécurité pourrait se traduire par des opérations menées dans l'espace numérique.
Participation du public et fracture numérique		
• Les problèmes d'accessibilité, les barrières linguistiques et les infrastructures limitées contribuent à creuser la fracture numérique. • Les femmes, les personnes âgées, les communautés marginalisées et celles des zones rurales sont affectées par ces problèmes de manière disproportionnée. • Les communautés vulnérables et marginalisées ont moins accès aux technologies numériques.	• Il est possible d'élargir la disponibilité de l'information et d'améliorer les méthodes de communication entre le secteur de la sécurité et la population qu'il dessert. • Les nouvelles technologies de réunion peuvent encourager la participation de personnes auparavant exclues en raison des coûts et des défis logistiques. • Les outils numériques peuvent améliorer la participation des femmes à la vie économique, avec un potentiel accru de contournement des obstacles culturels et de mobilité traditionnels	• En raison de la capacité d'organiser des réunions à distance en ligne qui réduisent les coûts et les besoins logistiques, les acteurs de la sécurité pourraient devenir plus réactifs aux besoins de la communauté. • Les plateformes en ligne pourraient accroître la participation du public aux processus de prise de décision et de fourniture de sécurité. • Les individus sont susceptibles d'avoir plus d'occasions de participer à un discours public en ligne sur les décisions qui les concernent.
Droits de la personne, échange d'information et protection de la vie privée		
• Le partage généralisé des données et d'information remet en question les frontières entre les sphères publique et privée. • Il existe un risque élevé de violation de données de sécurité et de fuite d'informations confidentielles. • Il existe des tensions croissantes entre la protection des droits de l'homme et l'empiètement sur la surveillance gouvernementale, en particulier dans des contextes autoritaires.	• Les outils numériques peuvent fournir aux organisations de la société civile et au public des canaux permettant de signaler facilement les violations des droits de l'homme commises par le secteur de la sécurité. • Un équilibre devra être trouvé entre l'accessibilité de l'information et le besoin de secret, ce qui exige la mise en œuvre de normes et de directives claires concernant l'utilisation et la disponibilité de l'information.	• Les défenseurs des droits humains, les activistes et les lanceurs d'alerte pourraient se voir exposés au risque d'une surveillance et d'un suivi accrus. • Les outils numériques devront être associés à une surveillance éthique et à une réglementation stricte pour s'assurer qu'ils n'aggravent pas les inégalités sociales. • Un équilibre devra être trouvé entre la responsabilité d'un État de protéger ses citoyens et le droit individuel à la sphère privée.

service. Les acteurs du secteur de la sécurité peuvent utiliser les technologies numériques pour créer des formulaires de plainte afin de mieux comprendre les griefs et les besoins locaux. Toutefois, les nouvelles initiatives numériques de cette nature ne devraient pas reproduire ou exacerber les préjugés et l'exclusion ou la discrimination existants.

L'efficacité dans l'espace numérique signifie que les institutions du secteur de la sécurité ont clairement défini des objectifs et des politiques de sécurité humaine et qu'elles remplissent leurs rôles, responsabilités et missions respectifs selon des normes professionnelles élevées. Il est crucial d'attirer, de retenir et de former un secteur de la sécurité qualifié avec le personnel possédant des compétences numériques suffisantes pour s'engager efficacement dans l'espace numérique en évolution. Les outils numériques seront également nécessaires non seulement pour intégrer une plus grande variété de méthodes de formation et d'éducation, mais aussi pour cibler, identifier, traiter, analyser et résoudre les problèmes plus efficacement.

L'efficience dans l'espace numérique signifie que les institutions du secteur de la sécurité procèdent à une planification financière solide dans le cadre de laquelle les dépenses de sécurité sont fondées sur des objectifs convenus et réalistes, qui sont hiérarchisés et utilisent au mieux les ressources publiques. Par exemple, l'échange d'informations en temps réel entre les agents de renseignement et de police au-delà des frontières peut lutter contre le trafic de drogue ou les attaques terroristes de manière plus efficace et plus rentable. Les outils numériques peuvent également être utilisés pour assurer une plus grande transparence sur les marchés et l'utilisation des fonds publics par le secteur de la sécurité, ainsi que pour traiter et stocker les données administratives.

Les acteurs du secteur de la sécurité doivent respecter les normes relatives aux droits de l'homme dans la conduite de leurs activités dans l'espace numérique. L'évolution des technologies de l'information et de la communication (TIC) facilite l'accès à l'information, facilite les débats mondiaux et favorise une participation démocratique accrue. Les défenseurs des droits de l'homme peuvent dénoncer plus rapidement et plus complètement les abus. Dans le même temps, cependant, les défenseurs des droits humains peuvent également être victimes de menaces en ligne, d'intimidation et de cyberintimidation, ce qui peut rapidement passer au ciblage, au harcèlement et à la violence dans le monde réel. En outre, les nouvelles technologies sont vulnérables à la surveillance et à l'interception électroniques, peuvent menacer les droits individuels à la vie privée et à la liberté d'expression et d'association et, en fin de compte, peuvent restreindre le libre fonctionnement d'une société civile dynamique.

L'égalité des sexes dans l'espace numérique signifie que les besoins spécifiques des femmes, des hommes, des garçons et des filles en matière de sécurité et de justice sont pris en compte dans la prestation, la gestion et la surveillance de la sécurité. Les problèmes liés à l'accessibilité, à l'abordabilité et au niveau d'éducation, ainsi que les préjugés inhérents et les normes socioculturelles, limitent souvent la capacité des femmes et des filles à bénéficier de la transition vers la digitalisation. Les faibles niveaux de participation des femmes et des filles dans les domaines des sciences, de la technologie, de l'ingénierie et des mathématiques (STIM) continuent de contribuer à creuser les écarts. Néanmoins, la technologie numérique peut améliorer la participation à la vie économique et faciliter l'accès aux services de santé, car ces outils peuvent offrir aux femmes la possibilité de contourner les barrières culturelles et de mobilité traditionnelles. Pour les personnes LGBTQI +, il a été reconnu que les médias sociaux, les applications de rencontres, les réseaux privés virtuels (VPN) et la technologie blockchain ont tous joué un rôle dans la création de nouveaux espaces sûrs, leur offrant plus d'occasions de se connecter et d'explorer les problèmes auxquels leurs communautés sont confrontées.

QUELS SONT LES PRINCIPAUX DÉFIS, OPPORTUNITÉS ET PERSPECTIVES DE LA DIGITALISATION DANS LES DOMAINES CLÉS DE LA R/GSS ?

S'appuyant sur les sections précédentes, la figure 2 présente les principaux défis, opportunités et perspectives inhérents à la digitalisation dans cinq domaines clés essentiels à une bonne GSS/R, à savoir la surveillance, la disponibilité des ressources, la capacité technique, la participation du public et les droits de l'homme.lability, technical capacity, public participation, and human rights.

COMMENT LES ACTEURS DU SECTEUR DE LA SÉCURITÉ PEUVENT-ILS CONTRIBUER À LA BONNE GOUVERNANCE DE L'ESPACE NUMÉRIQUE ?

Cette section met en évidence le potentiel de nouveaux domaines d'engagement pour les acteurs de la sécurité traditionnels et émergents afin d'assurer une bonne G/RSS dans l'espace numérique. La figure 3 présente des recommandations clés sur la manière dont des acteurs de la sécurité spécifique peuvent contribuer à la bonne gouvernance de l'espace numérique.

La légitimité et l'efficacité des **forces armées** dépendent de leur capacité à remplir leur mission de manière responsable dans un cadre de contrôle civil démocratique, d'état de droit et de respect des droits de l'homme. En particulier, le développement et l'utilisation de nouvelles technologies militaires doivent faire l'objet d'un examen rigoureux.

En raison de leur proximité avec la population, les actions et les prises de décisions des organismes d'application de la loi affectent directement la sécurité des individus et des communautés au quotidien. L'utilisation des outils numériques dans les services de police a considérablement augmenté, avec des conséquences discutables pour les droits des individus. L'adhésion aux principes de bonne GSS par les acteurs chargés de l'application de la loi, en particulier dans l'espace numérique, est essentielle car leurs actions ont le potentiel de façonner le caractère démocratique de l'État lui-même.

FIGURE 3 RECOMMANDATIONS À L'ENCONTRE DES ACTEURS DU SECTEUR DE LA SÉCURITÉ

	Acteur de la sécurité	Recommandations
PRESTATAIRES DE SÉCURITÉ	 **Forces armées**	• Partager l'information à l'interne et à l'externe pour faciliter les réponses aux cybermenaces. • Investir dans la modernisation de l'infrastructure numérique et dans les capacités numériques, par exemple en recrutant du personnel ayant des compétences numériques. • Utiliser des outils numériques pour créer des mécanismes de plainte en ligne sensibles au genre afin que le public puisse soulever des préoccupations au sujet des mesures, des politiques et des règlements. • Accroître la transparence en élaborant des processus et des mécanismes d'acquisition de matériel plus solides pour identifier les violations des droits de la personne.
	 **Application de la loi**	• Veiller à ce que l'utilisation et l'accès aux données personnelles ou aux informations sensibles soient correctement réglementés. • Former un réseau d'information et de communication transparent pour échanger des informations, analyser des données et prendre des décisions éclairées. • Utiliser les technologies numériques pour simplifier les processus et assurer des réponses opérationnelles responsables qui répondent aux différents besoins de chaque communauté. • Développer des relations solides avec les institutions de surveillance dans la mise en œuvre de nouvelles politiques et lois qui reflètent les développements technologiques continus. • Accroître la présence en ligne afin de prévenir les abus et sensibiliser davantage le public aux menaces numériques. • Mettre en place des mécanismes de plainte en ligne anonymes et sensibles au genre, et créer des espaces sûrs pour les personnes et les communautés marginalisées afin qu'elles puissent faire part de leurs préoccupations.
SURVEILLANTS DE SÉCURITÉ	 **Ministères exécutifs et gouvernementaux**	• Élaborer des normes opérationnelles pour l'utilisation des technologies numériques par les acteurs de la sécurité et adopter des réglementations plus strictes pour les grandes entreprises technologiques. • Utiliser des outils numériques pour surveiller et évaluer le rendement des fournisseurs de services de sécurité et pour signaler toute inconduite ou autre activité affectant la sécurité des personnes marginalisées. • Établir des mécanismes pour signaler et surveiller les discours haineux, l'extrémisme violent, la cyberintimidation et d'autres formes de harcèlement en ligne. • Créer une politique nationale de cybersécurité sensible au genre et éduquer le personnel de sécurité sur les défis posés par les menaces numériques. • Créer un espace public numérique inclusif et participatif, en veillant à ce que la communication atteigne les femmes, les hommes, les garçons et les filles, ainsi que les personnes marginalisées et les personnes en situation de vulnérabilité.
	 **Parlements**	• Veiller à ce qu'il existe un cadre juridique approprié régissant le secteur de la sécurité dans l'espace numérique et à ce que l'utilisation des outils numériques soit alignée sur les évolutions numériques. • Organiser des interactions participatives et inclusives sensibles au genre avec les citoyens par le biais de plateformes en ligne pour répondre aux questions et recevoir des commentaires au cours du processus de consultation et d'élaboration des lois. • Partager les registres de vote et les activités de surveillance afin de renforcer la responsabilisation et la transparence. • Approuver et surveiller les budgets des fournisseurs de sécurité pour acquérir des ressources numériques.
	 **Organisations de la société civile (OSC)**	• Collaborer avec d'autres OSC pour s'assurer que les fournisseurs de sécurité respectent les normes de protection des données. • Utiliser les technologies numériques pour rationaliser les plaintes contre les agents publics ou les acteurs de la sécurité et pour détecter les violations des droits de l'homme. • Sensibiliser à la sécurité sur Internet et créer des mécanismes pour dénoncer les discours de haine, l'extrémisme violent, la cyberintimidation et d'autres formes de harcèlement en ligne. • Développer des boîtes à outils numériques et du matériel de formation sensibles au genre pour soutenir les activistes et les chercheurs.
ACTEURS ÉMERGENTS DE LA SÉCURITÉ	 **Grandes entreprises technologiques**	• Respecter la législation et les réglementations mises en place par les gouvernements et encourager de meilleures normes pour la protection et l'échange de données privées. • Coopérer avec les gouvernements, les parlements et les acteurs de la sécurité nationale et internationale pour définir des normes, des réglementations et des meilleures pratiques dans l'espace numérique. • Travailler avec les OSC et les gouvernements nationaux pour fournir à ces acteurs les ressources et les connaissances nécessaires pour prévenir les cyberattaques. • Développer des mécanismes sensibles au genre qui permettent de surveiller le contenu publié sur les plateformes en ligne afin de prévenir la désinformation ou le harcèlement en ligne.

Les ministères exécutifs et gouvernementaux gèrent l'administration, l'organisation et le budget des forces de sécurité et ont généralement le dernier mot sur les politiques de sécurité. Les gouvernements ont adopté les technologies numériques de manière transformatrice, qu'il s'agisse de fixer des objectifs administratifs mesurables et d'améliorer la prestation de services, de prendre des décisions fondées sur des données et d'adopter des politiques fondées sur des données probantes qui garantissent une plus grande responsabilisation et transparence des services publics.

Si les **parlements** sont propres à chaque système politique et juridique, ils partagent tous des fonctions similaires qui en font des acteurs centraux de toute démocratie. Les parlements utilisent les technologies numériques pour faciliter l'engagement des citoyens dans le processus décisionnel. Les outils numériques qu'ils utilisent vont des plateformes d'e-parlement aux systèmes de gestion des documents. Cependant, les parlements sont souvent confrontés à des difficultés dans la numérisation de leurs processus, en particulier ceux qui se trouvent dans des contextes à faible revenu.

Les organisations de la société civile (OSC) sont essentielles pour encourager une culture de participation qui renforce la nature démocratique de la prise de décision sur les questions de sécurité. Il existe une myriade de façons dont les OSC ont numérisé leurs activités, y compris l'utilisation d'outils numériques pour travailler plus efficacement dans un large éventail de contextes et la fourniture de services numériques essentiels aux populations vulnérables.

L**es grandes entreprises technologiques** sont considérées comme des « acteurs émergents de la sécurité » car elles jouent un rôle de plus en plus important en facilitant l'accès et en participant au discours public grâce aux technologies numériques qu'elles produisent. Principalement des entités privées avec des priorités distinctes, les grandes entreprises technologiques deviennent plus influentes dans la politique nationale et les affaires internationales.

RESSOURCES ADDITIONNELLES

- Sabrina Ellebrecht and Stefan Kaufmann
  Digitalization and Its Security Manifestations
  European Journal for Security Research (5), 2020.

- Cody Collum and Houssain Kettani
  On Security Implications of Emerging Technologies
  Association for Computing Machinery, 2022.

- Graeme P. Herd, Detlef Puhl, and Sean Costigan
  Emerging Security Challenges: Framing the Policy Context
  GCSP Policy Paper 5, 2013.

- Francesco Mancini (ed.)
  New Technology and the Prevention of Violence and Conflict
  New York: International Peace Institute, April 2013.

- DCAF Research Report
  SSG/R in the Digital Space: Projections into the Future
  Geneva, Switzerland. Forthcoming, 2023.

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**

DCAF Le Centre pour la gouvernance du secteur de la sécurité, Genève

DCAF – le Centre de Genève pour la gouvernance du secteur de la sécurité

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

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

www.dcaf.ch