Enabel

**Position** Paper
**N° 08** - octobre 2025

# La cybersécurité, pour une société numérique sûre et inclusive

En 2024, une panne informatique mondiale sans précédent a paralysé les secteurs aérien, bancaire, médiatique, sanitaire et commercial, entraînant des pertes estimées à 5 milliards de dollars selon le Forum économique mondial. Renforcer la cybersécurité est essentiel pour une coopération internationale efficace.

## Introduction

La couverture internet a progressé rapidement en Afrique au cours des quinze dernières années. Le taux de pénétration est actuellement d'environ 40 % et la poursuite du déploiement du fournisseur d'accès internet Starlink augmentera très probablement ce chiffre, en offrant une option pour les zones rurales et moins desservies. La digitalisation rapide a considérablement amélioré l'accès à l'information, aux services de base (par exemple, les services gouvernementaux et financiers) et à la participation démocratique, tout en ouvrant de nombreuses opportunités de développement dans divers secteurs tels que l'éducation, la santé et l'agriculture.

Cependant, cette évolution s'accompagne de nouvelles menaces cybernétiques. Les cyberattaques, y compris les rançongiciels, les escroqueries par hameçonnage et les attaques menées par des acteurs étatiques ciblant les infrastructures critiques, se multiplient. En 2023, les cyberattaques ont augmenté de 23 % en Afrique. Les smartphones sont particulièrement visés et les cybercriminel·les exploitent les réseaux sociaux et les faiblesses humaines (Interpol, 2024).

Les infrastructures critiques telles que les hôpitaux, les établissements financiers et les fournisseurs d'accès à internet, sont de plus en plus ciblées. La sophistication croissante, grâce, entre autres, à l'intelligence artificielle et à l'utilisation de cryptomonnaies, des cybercriminel·les souvent organisé·es en réseaux, pose un défi majeur. Il est inquiétant de constater que cette complexité croissante du cyberespace exacerbe les inégalités dans ce domaine, car les petites organisations, les économies émergentes et le secteur public sont ceux qui ont le plus de mal à assurer leur cyberrésilience (World Economic Forum, 2025).

Les escroqueries en ligne restent la principale forme de cybercriminalité, affectant à la fois les organisations et les individus. La progression constante du taux de pénétration mobile et l'utilisation généralisée des réseaux sociaux, de la messagerie instantanée et des services d'argent mobiles a créé un terrain fertile pour ces types d'attaques. La cybercriminalité devient également une voie attrayante pour les jeunes, offrant des gains rapides avec un risque perçu comme limité.

Enfin, la menace de la cyberviolence risque également d'exacerber les disparités entre les hommes et les femmes. Globalement, 38 % des femmes ont déclaré avoir subi personnellement de la violence en ligne et, en raison de la sous-déclaration, ce chiffre pourrait encore sous-estimer les taux de prévalence réels (Economist Intelligence Unit, 2021). L'insécurité devient donc un obstacle de plus en plus important à l'utilisation d'internet ou des technologies numériques par les femmes.

## La cybersécurité comme levier de développement

La lutte contre la cybercriminalité nécessite une approche multidimensionnelle. En tant que telle, cette lutte incarne « l'approche globale » définie par l'État belge en couvrant différents domaines comme la sécurité, le commerce, les droits humains, la justice, (SPF AE, 2017). D'une manière similaire, la lutte contre la désinformation nécessitera une approche globale combinant des mesures pratiques et des efforts de plus grande envergure (voir encadré page suivante).

Au-delà de la nécessité pour les différents acteurs de travailler ensemble pour faire face efficacement aux cybermenaces, une cyberrésilience accrue agit aussi comme un levier de développement dans d'autres domaines. La Belgique via Enabel collabore ainsi avec la Guinée, le Sénégal et le Mali en matière de digitalisation des systèmes d'état civil afin d'améliorer la gouvernance et l'accès aux services publics. Cependant, ces avancées ne peuvent être pleinement efficaces que si elles s'accompagnent d'un effort visant à renforcer la cybersécurité de ces services.

De plus, la cybercriminalité est, presque par nature, un phénomène international. Les criminel·les exploitent les failles des cadres juridiques et des capacités de cybersécurité, souvent limités à l'échelle nationale, pour cibler des victimes à travers le monde. Sans une action coordonnée, les menaces virtuelles risquent de s'intensifier et d'affecter non seulement les pays africains, mais aussi l'Europe et la Belgique. Dans cette optique, la lutte contre la cybercriminalité s'inscrit dans l'approche « Beyond Aid », qui privilégie la recherche de solutions conjointes pour des défis communs, plutôt que le paradigme traditionnel bailleur-bénéficiaire. Une approche qui a été reconfirmée dans les priorités politiques du gouvernement belge (Prévot, 2025).

En résumé, la digitalisation est un puissant levier de développement en Afrique, et renforcer la cyberrésilience est fondamental pour permettre un développement sécurisé et inclusif. La lutte contre la cybercriminalité constitue un défi commun qui requiert une coopération mutuellement bénéfique.

## Comment Enabel renforce-t-elle la cybersécurité ?

Enabel joue un rôle important dans la mise en œuvre de la politique belge de coopération internationale en matière de cybersécurité et de lutte contre la cybercriminalité. Sa présence sur le terrain est renforcée par une forte collaboration entre institutions belges, partenaires internationaux et acteurs locaux. L'agence belge de coopération internationale œuvre dans des contextes fragiles, aligne ses actions sur les Objectifs de développement durable et adopte une approche basée sur les droits humains.

### Partenariats techniques et stratégiques

Pour renforcer la résilience face aux cybermenaces, Enabel établit des partenariats avec d'autres organisations afin de promouvoir une approche cohérente et collective de la cybersécurité. L'agence dispose d'accords de coopération avec divers acteurs institutionnels belges tels que la Police intégrée belge, le Centre pour la cybersécurité Belgique, les universités, la Défense belge, les acteurs judiciaires belges, etc. Ces relations favorisent l'intégration dans divers réseaux comme les groupes de travail du D4D Hub et le Practitioner's Network de l'Union européenne. Enabel et la GIZ, l'agence de coopération internationale allemande hébergent le secrétariat de l'initiative Team Europe Democracy, dont l'un des thèmes prioritaires est « les médias et le digital ».

Par ailleurs, Enabel a collaboré avec les services de sécurité marocains, notamment la Direction générale de la Sûreté nationale et la Gendarmerie royale, sur la thématique de lutte contre la cybercriminalité, en particulier les cyberviolences à l'égard des femmes et des filles. Cela inclut l'organisation de stages d'immersion, comme ceux réalisés avec les Regional Computer Crime Units de la police belge, pour renforcer les compétences en cybercriminalité et la sensibilisation des organisations de femmes aux droits numériques.

### Qu'en est-il de la désinformation ?

Lors des discussions sur la cybercriminalité, la question de la désinformation revient souvent. La désinformation consiste à diffuser délibérément des informations fausses ou trompeuses pour manipuler l'opinion publique, créer des troubles sociaux ou tromper les individus. Elle se rapproche de la cybercriminalité par l'utilisation d'outils et de plateformes numériques et s'appuie régulièrement sur des tactiques cybercriminelles telles que le piratage ou l'amplification par des bots. Mais la désinformation n'est pas unique aux environnements en ligne et peut également être présente dans les médias traditionnels.

Par ailleurs, les cybercriminel·les peuvent utiliser la désinformation dans le cadre d'escroqueries par hameçonnage, d'attaques par ingénierie sociale ou de systèmes de fraude. Néanmoins, la désinformation n'est pas l'apanage des criminel·les, les régimes autoritaires l'utilisent fréquemment comme outil de contrôle, de propagande et de répression de la dissidence. Pour ajouter à la complexité de la situation, les groupes cybercriminels parrainés par des États peuvent se livrer à la fois au piratage et à la désinformation pour déstabiliser leurs adversaires.

La lutte contre la désinformation doit être abordée par le biais de mesures de cybersécurité combinées à l'éducation aux médias, à la vérification des faits et aux politiques des plateformes. Elle doit également s'inscrire dans le cadre de mesures plus larges visant à instaurer la confiance et à soutenir les institutions démocratiques.

### Proximité

Simultanément, l'agence s'appuie sur des partenariats avec des universités, des gouvernements locaux et des organisations de la société civile pour assurer un ancrage et une meilleure compréhension des besoins spécifiques et la valorisation des capacités existantes. Le travail plus large de transformation numérique aide à établir un réseau solide avec le secteur privé et permet d'être informé des solutions et développements récents. En ce sens, Enabel développe une stratégie spécifique pour renforcer l'engagement du secteur privé dans la coopération internationale.

Par exemple, Enabel travaille avec des organisations de la société civile et des gouvernements locaux ougandais pour mettre en œuvre des stratégies visant à prévenir les cyberattaques, à détecter les vulnérabilités potentielles et à répondre rapidement et efficacement aux incidents. Ces résultats ont été rendus possibles grâce aux investissements dans quatre « digital innovation hub » sous-régionaux en Ouganda.

### Promotion de la cyberhygiène et des droits numériques

Outre le renforcement des capacités techniques des gouvernements et des organisations de la société civile, Enabel mène des campagnes de sensibilisation et propose des formations à la sécurité numérique afin que tou·tes les citoyen·nes, et les jeunes, plus vulnérables en particulier, soient en mesure de protéger leurs appareils, réseaux, communications, données, comptes et mots de passe contre les risques et les menaces de cybercriminalité.

En Palestine, Enabel collabore avec l'organisation 7amleh pour renforcer les capacités des jeunes en termes de cyberhygiène et leur apprendre les meilleures pratiques en matière de cybersécurité, comme la protection des comptes contre les logiciels malveillants, la messagerie sécurisée et la sécurisation des comptes de médias sociaux. Une étude a également été réalisée sur la sécurité numérique des jeunes Palestinien·nes, et ce, à un moment délicat, alors que la région souffre de l'impact croissant de la guerre en cours à Gaza.

### Approche transformatrice de genre et basée sur les droits humains

Enabel intègre l'égalité de genre et la protection des droits humains dans ses projets, en particulier dans la lutte contre les violences basées sur le genre facilitées par la technologie, par exemple au Bénin et en Ouganda.

À partir de 2018, le Bénin a renforcé son cadre légal et a connu plusieurs réussites dans la lutte contre la cybercriminalité. Cependant, de nombreux incidents échappent à l'attention des forces de sécurité car les victimes hésitent à les signaler, souvent par sentiment de honte, notamment lorsqu'il s'agit d'hameçonnage ou de sextorsion. Par conséquent, des mécanismes adaptés de prise en charge ont été identifiés et développés pour mieux analyser les spécificités liées au genre et y trouver des réponses spécifiques.

En partenariat avec le Women of Uganda Network, Enabel a renforcé les capacités de plus de cent-vingt organisations de la société civile sur l'intersection du genre et de la technologie, a sensibilisé à la violence sexiste en ligne et a développé une plateforme unique de droits numériques pour le signalement, mais aussi pour l'accès aux ressources sur la violence sexiste en ligne en Ouganda.

Enfin, le lien avec les actions internes d'Enabel est un aspect clé de son approche. L'agence entend appliquer les enseignements tirés de ses programmes, non seulement dans les pays partenaires, mais aussi pour sa propre transformation numérique et sa cybersécurité organisationnelle. Enabel, considérée comme une entité essentielle selon la directive NIS2 (European Commission, 2022b), utilise à cet effet le « Cyber Fundamentals Framework » du Centre pour la cybersécurité Belgique pour évaluer et renforcer sa maturité en cybersécurité.

## Recommandations

### Recommandations stratégiques

1. Contribuer à renforcer les cadres législatifs et réglementaires des partenaires afin d'assurer une protection efficace contre les cybermenaces, tout en évitant des mesures qui pourraient nuire involontairement à la liberté de la presse ;
2. Lutter contre la désinformation en favorisant les synergies entre les différents secteurs et acteurs de l'écosystème de la cybersécurité pour mitiger les menaces hybrides ;
3. Renforcer la coopération internationale et régionale pour pallier au manque de capacités en cybersécurité des pays aux contextes fragiles, en favorisant le partage des ressources et des connaissances.

### Recommandations opérationnelles et techniques

1. Renforcer les cybercapacités des forces de l'ordre aux niveaux des personnes, des processus et des technologies ;
2. Etablir des mécanismes formels de collaboration entre les secteurs public et privé, ainsi qu'avec les organisations internationales en matière de cybersécurité, notamment par la création de plateformes d'échange sur les cybermenaces ;
3. Organiser conjointement des simulations de cyberattaques, le développement de partenariats public-privé pour le financement d'infrastructures critiques de cybersécurité, et la participation active aux initiatives régionales et internationales de lutte contre la cybercriminalité ;
4. Contribuer à l'effort de renforcement des compétences numériques, avec une attention spécifique à la cyberhygiène et aux droits numériques des utilisateur·rices ;
5. Renforcer les formations professionnelles en matière de cybersécurité des acteurs de la transformation numérique ;
6. Intégrer systématiquement la conscientisation à la cybersécurité et aux mesures attenantes dans les projets de digitalisation.

Enabel contribue ainsi, avec ses partenaires, à un environnement numérique plus sûr et plus résilient dans les pays partenaires de la coopération, voire au-delà, tout en renforçant la lutte de la Belgique contre la cybercriminalité internationale.

## Références


- Council of Europe, 2001. Convention on Cybercrime, 23 November.
- Economist Intelligence Unit, 2021. Measuring the prevalence of online violence against women, 1 March.
- European Commission, 2022a. The Strengthened Code of Practice on Disinformation, 13 February.
- European Commission, 2022b. Directive of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, 2022/2555 (NIS2).
- European Commission, 2023. Operational Guidance for the EU's International Cooperation on Cyber Capacity Building, Second Edition.
- Interpol, 2022. Lutte contre la cybercriminalité, Stratégie mondiale 2022-2025.
- Interpol, 2024. African Cyberthreat Assessment Report, April.
- Prévot, M., 2025. Exposé d'orientation politique, Affaires étrangères, Affaires européennes et Coopération au Développement, 10 mars.
- SPF Affaires étrangères, 2017. Note stratégique Approche Globale.
- Union Africaine, 2014. Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel (Convention de Malabo), 27 juin.
- Union Africaine, 2020. Stratégie de transformation numérique pour l'Afrique (2020-2030).
- World Economic Forum, 2025. Global Cybersecurity Outlook 2025, January.



Enabel

**Agence belge**
**de coopération internationale**
Société anonyme de droit public
à finalité sociale

Rue Haute 147
1000 Bruxelles, Belgique
**T** + 32 (0)2 505 37 00
info@enabel.be
www.enabel.be

**Rédaction**
Roberto Resmini, Sebastian Otte, Thijs Braem, Pieter De Schepper

**Édition**
Sonia Gsir

Publié en français, néerlandais et anglais.

Belgique
partenaire du développement

Éditeur responsable : Jean Van Wetter, rue Haute 147, 1000 Bruxelles - 10/2025