

Cyberveiligheid voor een veilige en inclusieve digitale samenleving

In 2024 legde een ongeken­de wereldwijde computerstoring de luchtvaart, het bankwezen, de media, de gezondheidszorg en de commerciële sector lam, wat volgens het World Economic Forum tot een geschat verlies van 5 miljard dollar leidde. Het versterken van cyberveiligheid is essentieel voor effectieve internationale samenwerking.

Inleiding

De internetdekking in Afrika nam snel toe de afgelopen vijftien jaar. De penetratie ligt momenteel rond de 40% en de verdere uitrol van Starlink zal dit cijfer hoogstwaarschijnlijk verhogen door een optie aan te bieden in landelijke en onderbediende gebieden. De snelle digitalisering heeft de toegang tot informatie, basisdiensten (bv. van de overheid en financiële diensten) en democratische participatie aanzienlijk verbeterd en tegelijkertijd talrijke ontwikkelingsmogelijkheden gecreëerd in onder andere onderwijs, gezondheidszorg en landbouw.

Deze evolutie gaat echter gepaard met nieuwe cyberdreigingen. Cyberaanvallen, waaronder ransomware, phishing scams en aanvallen door staatsactoren gericht op kritieke infrastructuur, nemen toe. In 2023 is het aantal cyberaanvallen in Afrika met 23% gestegen. Vooral smartphones zijn een doelwit. Cybercriminelen maken gebruik van sociale netwerken en menselijke zwakheden om hun aanvallen uit te voeren (Interpol, 2024).

Kritieke infrastructuur zoals ziekenhuizen, financiële instellingen en internetproviders zijn steeds vaker het doelwit. De toenemende vaardigheid van cybercriminelen en hun netwerken, versterkt door hun gebruik van artificiële intelligentie en cryptomunten, vormt een grote uitdaging. Zorgwekkend is dat de toenemende complexiteit op cybergebied de ongelijkheid vergroot. Kleine organisaties,

opkomende economieën en de publieke sector hebben het het moeilijkst om hun cyberweerbaarheid te verzekeren (World Economic Forum, 2025).

Online oplichting blijft de belangrijkste vorm van cybercriminaliteit. Ze treft zowel organisaties als individuen. De gestage toename van mobiele penetratie en het wijdverbreide gebruik van sociale media, instant messaging en mobiele betalingen vormen een vruchtbare bodem voor dit soort oplichting. Cybercriminaliteit is een aantrekkelijke optie voor jongeren, omdat het om snelle winst gaat met een ogenschijnlijk beperkt risico.

Cybergeweld draagt dan weer bij tot het risico dat de bestaande ongelijkheden tussen mannen en vrouwen toenemen. In totaal meldden 38% vrouwen persoonlijke ervaringen met online geweld. Dit cijfer is waarschijnlijk hoger doordat die ervaringen niet altijd gemeld worden (Economist Intelligence Unit, 2021). Onveiligheid wordt daarom een steeds belangrijkere barrière voor internetgebruik of gebruik van digitale technologieën door vrouwen.

Cyberveiligheid als hefboom voor ontwikkeling

De bestrijding van cybercriminaliteit vereist een multidimensionale aanpak en belichaamt zo de ‘Comprehensive Approach’ zoals gedefinieerd door de Belgische Staat (FOD BZ, 2017) waarbij over beleidsdomeinen heen (zoals veiligheid, handel, mensenrechten en justitie) wordt samengewerkt. Ook de strijd tegen desinformatie vereist een alomvattende aanpak die praktische maatregelen en bredere inspanningen combineert.

Naast de noodzaak voor de verschillende spelers om samen te werken om cyberdreigingen effectief aan te pakken, fungeert een grotere cyberweerbaarheid ook als hefboom voor ontwikkeling op andere gebieden. Via Enabel werkt België bijvoorbeeld samen met Guinee, Senegal en Mali aan de digitalisering van de burgerlijke stand om het bestuur en de toegang tot openbare diensten te verbeteren. Deze vooruitgang kan echter alleen volledig effectief zijn als deze gepaard gaat met een inspanning om de cyberveiligheid van die diensten te versterken.

Bovendien is cybercriminaliteit bijna per definitie een internationaal fenomeen. Criminelen maken gebruik van lacunes in de wetgeving en cyberveiligheids capaciteit, die



vaak beperkt zijn tot het nationale niveau, om over de hele wereld slachtoffers te maken. Zonder gecoördineerde actie bestaat het risico dat virtuele bedreigingen intensiever worden en niet alleen Afrikaanse landen treffen, maar ook Europa en België. Zo sluit de strijd tegen cybercriminaliteit beter aan bij de 'Beyond Aid'-benadering die gericht is op het vinden van gezamenlijke oplossingen voor gemeenschappelijke uitdagingen, in plaats van het klassieke paradigma van donor en begunstigde. Deze benadering werd opnieuw bevestigd in de beleidsprioriteiten van de Belgische regering (Prévot, 2025).

Kortom, digitalisering is een krachtige hefboom voor ontwikkeling in Afrika en een sterkere cyberweerbaarheid is cruciaal voor het bereiken van een veilige en inclusieve ontwikkeling. De strijd tegen cybercriminaliteit is een gemeenschappelijke uitdaging en vereist wederzijds voordelige samenwerking.

Hoe versterkt Enabel de cyberveiligheid?

Enabel speelt een belangrijke rol in de uitvoering van het Belgische beleid van internationale samenwerking op het vlak van cyberveiligheid en de strijd tegen cybercriminaliteit. De aanwezigheid van Enabel op het terrein wordt versterkt door een nauwe samenwerking tussen Belgische instellingen, internationale partners en lokale spelers. Enabel werkt in fragiele contexten, stemt zijn acties af op de Duurzame Ontwikkelingsdoelstellingen en hanteert een aanpak die gebaseerd is op de mensenrechten.

Technische en strategische partnerschappen

Om de weerbaarheid tegen cyberbedreigingen te versterken, gaat Enabel partnerschappen aan met andere organisaties om een samenhangende en collectieve aanpak tot cyberveiligheid te bevorderen. Enabel heeft samenwerkingsovereenkomsten met verschillende Belgische institutionele spelers zoals de Belgische Geïntegreerde Politie, het Centrum voor Cybersecurity België, universiteiten, de Belgische Defensie, de Belgische rechterlijke macht, enz. Deze relaties bevorderen de integratie in verschillende netwerken zoals de D4D Hub-werkgroepen en het EU Practitioners' Network. Enabel en GIZ huisvesten het secretariaat van het initiatief Team Europe Democracy, waarvan media en digitalisering een van de prioritaire thema's zijn.

Enabel heeft samengewerkt met de Marokkaanse veiligheidsdiensten, met name het Directoraat-generaal voor Nationale Veiligheid en de Koninklijke Gendarmerie, op het gebied van de bestrijding van cybercriminaliteit, in het bijzonder cybergeweld tegen vrouwen en meisjes. Het ging daarbij om de organisatie van inleefstages, zoals die uitgevoerd met de Regional Computer Crime Units van de Belgische politie, om de vaardigheden op het gebied van cybercriminaliteit te versterken en het bewustzijn van digitale rechten onder vrouwenorganisaties te vergroten.

En hoe zit het dan met desinformatie?

Als we het hebben over cybercriminaliteit, komt de kwestie van desinformatie vaak ter sprake. Desinformatie is het opzettelijk verspreiden van valse of misleidende informatie om de publieke opinie te manipuleren, sociale onrust te creëren of individuen te misleiden. Het lijkt op cybercriminaliteit door het gebruik van digitale tools en platformen en doordat het regelmatig vertrouwt op cybercriminale tactieken zoals hacking of versterking door bots. Maar desinformatie beperkt zich niet tot online omgevingen, ze komt ook voor in traditionele media.

Aan de andere kant kunnen cybercriminelen desinformatie gebruiken als onderdeel van phishing, social engineering-aanvallen of fraudeconstructies. Desinformatie wordt niet enkel verspreid door criminelen. Autoritaire regimes gebruiken het vaak als controlemiddel of propaganda of bij de onderdrukking van opstand. Om de situatie nog ingewikkelder te maken, kunnen door de staat gesponsorde cybercriminale groepen zowel hacking als desinformatie gebruiken om tegenstanders te destabiliseren.

De strijd tegen desinformatie zal moeten worden gevoerd door middel van cyberveiligheidsmaatregelen in combinatie met media-educatie, fact-checking en richtlijnen voor de verschillende platformen. Maar het moet ook deel uitmaken van bredere maatregelen die helpen om democratische instellingen te ondersteunen en het vertrouwen erin te vergroten.

Nabijheid

Tegelijkertijd vertrouwt Enabel op partnerschappen met universiteiten, lokale overheden en het maatschappelijk middenveld om ervoor te zorgen dat specifieke behoeften beter worden begrepen en dat bestaande capaciteiten worden benut. Het bredere werk op het gebied van digitale transformatie helpt bij het opzetten van een sterk netwerk met de private sector om op de hoogte te blijven van hedendaagse ontwikkelingen en oplossingen. Hiertoe ontwikkelt Enabel een specifieke strategie om de betrokkenheid van de private sector bij internationale samenwerking te versterken.

Enabel werkt samen met Oegandese maatschappelijke organisaties en lokale overheden aan de implementatie van strategieën om cyberaanvallen te voorkomen, mogelijke kwetsbaarheden op te sporen en snel en doeltreffend te reageren op incidenten. Vermeldingswaardig is dat dit in Oeganda gerealiseerd werd via investeringen in vier lokale digitale innovatiehubs.

Cyberhygiëne en digitale rechten bevorderen

Enabel bouwt niet alleen aan de technische capaciteit van overheden en maatschappelijke organisaties, maar voert ook bewustmakingscampagnes en biedt opleidingen aan op het gebied van digitale veiligheid zodat alle burgers, en kwetsbare jongeren in het bijzonder, in staat zijn om hun apparaten, netwerken, communicatie, gegevens, accounts en wachtwoorden te beschermen tegen de risico's en bedreigingen van cybercriminaliteit.

In Palestina werkt Enabel samen met de organisatie 7amleh om jongeren vaardigheden bij te brengen op het gebied van cyberhygiëne en hen de beste praktijken op het gebied van cyberveiligheid aan te leren, zoals het beschermen van accounts tegen malware, veilig berichtenverkeer en het beveiligen van accounts op sociale netwerken. Er werd ook een onderzoek uitgevoerd naar digitale veiligheid bij jonge Palestijnen, op een delicaat moment, nu de regio lijdt onder de toenemende impact van de aanhoudende oorlog in Gaza.

Een transformatieve genderaanpak gebaseerd op de mensenrechten

Enabel integreert gendergelijkheid en de bescherming van mensenrechten in zijn projecten, bijvoorbeeld in Benin en Oeganda, met name in de strijd tegen door technologie gefaciliteerd gendergerelateerd geweld.

Sinds 2018 heeft Benin zijn wettelijke kader versterkt en verscheidene successen geboekt in de strijd tegen cybercriminaliteit. Maar een groot deel van de incidenten blijft onder de radar van de veiligheidsdiensten omdat slachtoffers zich schamen om die te melden, vooral in gevallen van phishing en sextortion. Daarom is gezocht naar aangepaste ondersteuning om beter in te spelen op genderkwesties.

In samenwerking met het Women of Uganda Network heeft Enabel de capaciteit van meer dan 120 maatschappelijke organisaties vergroot op het vlak van gender en technologie, het bewustzijn van online gendergerelateerd geweld vergroot en een uniek digitaal rechtenplatform ontwikkeld voor het melden van en toegang krijgen tot bronnen over online gendergerelateerd geweld in Oeganda.

Tot slot is de link met interne acties een belangrijk aspect van de aanpak van Enabel. Enabel wil de lessen uit zijn programma's niet alleen in partnerlanden toepassen, maar ook bij de eigen digitale transformatie en cyberveiligheid van de organisatie. Enabel, dat wordt beschouwd als een essentiële entiteit onder de NIS2-richtlijn (European Commission, 2022b), gebruikt het Cyber Fundamentals Framework van het Centrum voor Cybersecurity België om het maturiteitsniveau te meten en te versterken.

Aanbevelingen

Strategische aanbevelingen

1. Bijdragen aan de versterking van de wet- en regelgevingskaders van partners om effectieve bescherming tegen cyberbedreigingen te waarborgen, waarbij maatregelen worden vermeden die de persvrijheid onbedoeld zouden kunnen schaden;
2. Bestrijden van desinformatie door het bevorderen van synergieën tussen de verschillende sectoren en spelers in het ecosysteem van cyberveiligheid om hybride bedreigingen te beperken;
3. Versterken van internationale en regionale samenwerking om het gebrek aan cyberveiligheids capaciteit in landen met een kwetsbare context te verhelpen, door het delen van middelen en kennis te bevorderen.

Operationele en technische aanbevelingen

1. Versterken van de cybercapaciteiten van wetshandhavingsinstanties wat betreft personen, processen en technologieën;
2. Instellen van formele mechanismen voor samenwerking tussen de publieke en private sector en met internationale organisaties op het gebied van cyberveiligheid, met name via de creatie van platformen voor het uitwisselen van informatie over cyberbedreigingen;
3. Gezamenlijk organiseren van simulaties van cyberaanvallen, de ontwikkeling van publiek-private partnerschappen voor het financieren van kritieke cyberbeveiligingsinfrastructuren, en actieve deelname aan regionale en internationale initiatieven ter bestrijding van cybercriminaliteit;
4. Bijdragen aan inspanningen om digitale vaardigheden te versterken, met specifieke aandacht voor cyberhygiëne en de digitale rechten van gebruikers;
5. Versterken van de beroepsopleiding op het gebied van cyberveiligheid voor actoren die werken aan digitale transformatie;
6. Systematisch opnemen van bewustzijn rond en maatregelen voor cyberveiligheid in digitaliseringsprojecten.

Enabel draagt zo samen met zijn partners bij aan een veiligere en meer veerkrachtige digitale omgeving in onze partnerlanden en zelfs daarbuiten. Tegelijk helpen we België in zijn strijd tegen internationale cybercriminaliteit.

Referenties

- 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.
- FOD Buitenlandse Zaken, 2017. Strategienota Comprehensive Approach
- Interpol, 2022. Lutte contre la cybercriminalité, Stratégie mondiale 2022-2025.
- Interpol, 2024. African Cyberthreat Assessment Report, April.
- Prévot, M., 2025. Beleidsverklaring, Buitenlandse Zaken, Europese Zaken en Ontwikkelingssamenwerking, 10 maart.
- 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.



**Belgisch agentschap
voor internationale samenwerking**
Naamloze vennootschap van publiek
recht met sociaal oogmerk

Hoogstraat 147
1000 Brussel, België
T + 32 (0)2 505 37 00
info@enabel.be
www.enabel.be



Redactie

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

Eindredactie

Sonia Gsir

Gepubliceerd in het Nederlands, Frans en Engels.



België

partner in ontwikkeling