Enabel

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

# Cybersecurity for a secure and inclusive digital society

In 2024, an unprecedented global computer failure paralysed the aviation, banking, media, healthcare and commercial sectors, resulting in losses estimated at $5 billion according to the World Economic Forum. Strengthening cybersecurity is essential for effective international cooperation.

## Introduction

Internet coverage has grown rapidly in Africa over the last fifteen years. Penetration is currently around 40% and the continued roll-out of Starlink will most likely increase this figure, providing an option for rural and underserved areas. Rapid digitisation has considerably improved access to information, basic services (e.g. government and financial services) and democratic participation, while opening up numerous development opportunities in education, health and agriculture, among others.

However, this development comes with new cyberthreats. Cyberattacks, including ransomware, phishing scams and attacks by state actors targeting critical infrastructures, are on the increase. In 2023, cyberattacks increased by 23% in Africa. Smartphones are particularly targeted and cybercriminals exploit social networks and human weaknesses to carry out their attacks (Interpol, 2024).

Critical infrastructures such as hospitals, financial institutions and internet service providers are increasingly being targeted. The growing sophistication (thanks in part to artificial intelligence and the use of cryptocurrencies) of cybercriminals, who are often organised in networks, poses a major challenge. Worryingly, growing complexity in the cyber landscape is further exacerbating cyber inequity, with small organisations, emerging economies and the public sector finding it hardest to ensure their cyberresilience (World Economic Forum, 2025).

Nevertheless, online scams remain the main form of cybercrime affecting organisations and individuals. The steady rise in mobile penetration and the widespread use of social networks, instant messaging and mobile money services has created fertile ground for these types of attack. Cybercrime is also becoming an attractive option for young people, offering quick profits with limited perceived risk.

The threat of cyberviolence also risks exacerbating existing disparities between men and women. Globally, 38% of women have experienced online violence, and, due to under-reporting, this figure may still be an underestimate (Economist Intelligence Unit, 2021). Insecurity is therefore becoming an increasingly significant barrier to women's use of the internet or digital technologies.

## Cybersecurity, a lever for development

Combating cybercrime requires a multi-dimensional approach. As it stands, such combat embodies ‘the comprehensive approach’ as defined by the Belgian state as it touches various areas such as security, trade, human rights, justice, … (FPS FA, 2017). Similarly, the fight against disinformation will require a comprehensive approach combining practical measures and broader efforts.

In addition to the need for various players to work together to deal effectively with cyberthreats, greater cyberresilience also acts as a lever for development in other areas. For example, via Enabel, Belgium is working with Guinea, Senegal and Mali to digitise civil registry systems in order to improve governance and access to public services. However, these advances can only be fully effective if they are accompanied by an effort to strengthen the cybersecurity of these services.

Moreover, cybercrime is, almost by nature, an international phenomenon. Criminals exploit loopholes in legal frameworks and cybersecurity capabilities, often limited to the national level, to target victims around the world. Without coordinated action, there is a risk that virtual threats will intensify and affect not only African countries, but also Europe and Belgium. With this in mind, the fight against cybercrime suits a ‘Beyond Aid’ approach, which focuses on finding joint solutions to common challenges, rather than using a traditional donor-recipient paradigm. This approach is reconfirmed in the Belgian government's policy priorities (Prévot, 2025).

In short, digitisation is a powerful lever for development in Africa, and strengthening cyberresilience is crucial to achieving safe and inclusive development. The fight against cybercrime is a shared challenge that requires mutually beneficial cooperation.

## How does Enabel strengthen cybersecurity?

Enabel plays an important role in implementing Belgium's policy on international cooperation in cybersecurity and the fight against cybercrime. Its presence on the ground is strengthened by close collaboration between Belgian institutions, international partners and local players. Enabel works in fragile contexts, its actions contribute to achieving the Sustainable Development Goals, and it adopts a human rights-based approach.

### Technical and strategic partnerships

To strengthen resilience in the face of cyberthreats, Enabel is forging partnerships with other organisations to promote a coherent and collective approach to cybersecurity. Enabel has cooperation agreements with various Belgian institutional players such as the Belgian Integrated Police, the Centre for Cybersecurity Belgium, universities, the Belgian Defence, the Belgian judiciary, etc. These agreements foster networking in, among others, the D4D Hub working groups and the EU Practitioners' Network. Enabel and GIZ, the German international cooperation organisation, host the secretariat of the Team Europe Democracy initiative, one of whose priority themes is media and digital.

Furthermore, Enabel has worked with the Moroccan security services, in particular the Directorate General of National Security and the Royal Gendarmerie, on the issue of combating cybercrime, in particular cyberviolence against women and girls. This includes the organisation of immersion courses, such as those carried out with the Regional Computer Crime Units of the Belgian police, to strengthen cybercrime skills and raise awareness of digital rights among women's organisations.

### Local involvement

At the same time, Enabel relies on partnerships with universities, local governments and civil society organisations to ensure that specific needs are better understood and that existing capacities are exploited. The wider digital transformation work is helping to establish a strong network with the private sector to keep abreast of contemporary developments and solutions. To this end, Enabel is developing a specific strategy to strengthen the engagement of the private sector to international cooperation.

Enabel works with Ugandan civil society organisations and local governments to implement strategies to prevent cyberattacks, detect potential vulnerabilities and respond quickly and effectively to incidents. These results were made possible by investment in four sub-regional ‘digital innovation hubs’ in Uganda.

### Promoting cyberhygiene and digital rights

As well as building the technical capacity of governments and civil society organisations, Enabel runs awareness campaigns and offers training in digital security so that all citizens, and vulnerable young people in particular, are able to protect their devices, networks, communications, data, accounts and passwords against the risks and threats of cybercrime.

In Palestine, Enabel is working with the 7amleh organisation to build young people's cyberhygiene skills and teach them best practice in cybersecurity, such as protecting accounts from malware, secure messaging and securing social media accounts. A study was also carried out on the digital security of young Palestinians, at a delicate time when the region is suffering from the growing impact of the ongoing war in Gaza.
cours à Gaza.

### And what about disinformation?

When discussing cybercrime, the issue of disinformation often comes up. Disinformation is the deliberate dissemination of false or misleading information to manipulate public opinion, create social unrest or mislead individuals. It comes close to cybercrime in its use of digital tools and platforms and regularly relies on cybercriminal tactics such as hacking or amplification by bots. But disinformation is not unique to online environments and can also be found in traditional media.

On the other hand, cybercriminals can use disinformation as part of phishing scams, social engineering attacks or fraud schemes. But disinformation is not the exclusive preserve of criminals. Also, authoritarian regimes frequently use it as a tool to control, disseminate propaganda or repress dissent. To add to the complexity of the situation, state-sponsored cybercrime groups can use both hacking and disinformation to destabilise their adversaries.

The fight against disinformation will have to be tackled through cybersecurity measures combined with media education, fact-checking and platform policies. But it must also be part of wider measures to build confidence and support democratic institutions.

### A transformative gender and human-rights based approach

Enabel mainstreams gender equality and the protection of human rights in its projects, particularly the fight against gender-based violence facilitated by technology, for example in Benin and Uganda.

As of 2018, Benin has strengthened its legal framework and has seen several successes in the fight against cybercrime. Yet, a large share of incidents remains unknown to the security forces because victims are ashamed to report them, especially in cases of phishing and sextortion. As a result, appropriate support mechanisms have been identified and developed to better analyse gender-specific issues and find suitable responses.

In partnership with the Women of Uganda Network, Enabel has built the capacity of over one 120 civil society organisations on the intersection of gender and technology, raised awareness of online gender-based violence and developed a unique digital rights platform for reporting and accessing resources on online gender-based violence in Uganda.

Finally, the link with Enabel's internal actions is a key aspect of its approach. It intends to apply the lessons learned from its programmes not only in partner countries, but also for its own digital transformation and organisational cybersecurity. Enabel, considered an essential entity under the NIS2 directive (European Commission, 2022b), uses the 'Cyber Fundamentals Framework' of the Centre for Cybersecurity Belgium to assess and strengthen its cybersecurity maturity.

## Recommendations

### Strategic recommendations

1. Help strengthen partners' legislative and regulatory frameworks to ensure effective protection against cyberthreats, while avoiding measures that could unintentionally harm press freedom;
2. Combat disinformation by promoting synergies between the various sectors and players in the cybersecurity ecosystem to mitigate hybrid threats;
3. Strengthen international and regional cooperation to overcome the lack of cybersecurity capacity in countries with fragile contexts, by promoting the sharing of resources and knowledge.

### Operational and technical recommendations

1. Strengthen the cyber capabilities of law enforcement agencies in terms of people, processes and technologies;
2. Establish formal mechanisms for collaboration between the public and private sectors and with international organisations in the field of cybersecurity, through the creation of platforms for exchanging information on cyberthreats;
3. Organise jointly simulated cyberattacks, developof public-private partnerships to finance critical cybersecurity infrastructures, and participate actively in regional and international initiatives to combat cybercrime;
4. Contribute to efforts to strengthen digital skills, with a specific focus on cyberhygiene and the digital rights of users;
5. Strengthen professional training in cybersecurity for actors of digital transformation processes;
6. Systematically raise awareness on cybersecurity and accompanying measures in digitalisation projects.

Enabel thus contributes, with its partners, to a safer and more resilient digital environment in the cooperation partner countries, and even beyond, while strengthening Belgium's fight against international cybercrime.

## References


- African Union, 2014. African Union Convention on Cybersecurity and the Protection of Personal Data (Malabo Convention), 27 June.
- African Union, 2020. Digital Transformation Strategy for Africa (2020-2030).
- 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.
- FPS Foreign Affairs, 2017. Comprehensive Approach - Strategy Note.
- Interpol, 2022. Global Cybercrime Strategy 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 March.
- World Economic Forum, 2025. Global Cybersecurity Outlook 2025, January.



Enabel

**Belgian agency**
**for international cooperation**
Public-law company
with social purposes

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

**Editing board**
Roberto Resmini, Sebastian Otte, Thijs Braem, Pieter De Schepper

**Edition**
Sonia Gsir

Published in French, Dutch and English.

Belgium
partner in development

Managing editor: Jean Van Wetter, Rue Haute 147, 1000 Brussels - 10/2025