

# KM 8: Cybersecurity culture, awareness, workforce, and skills

## Outline

<b>Module objectives</b>	<b>2</b>
<b>Cybersecurity skills and culture in Africa (context)</b>	<b>4</b>
Major challenges for nurturing cybersecurity culture on the African continent	5
<b>Capacity building: an overview</b>	<b>7</b>
Theoretical explanation	7
Why is capacity building important in the global context?	9
<b>Cybersecurity capacity building in the broader context in Africa</b>	<b>11</b>
Why is it important for African countries to enhance cybersecurity capacity building and by what means?	12
Skills and culture building	12
Women in cybersecurity	16
<b>Concrete tools for building mature cybersecurity culture: best practices from the GFCE community</b>	<b>20</b>
Awareness-raising campaigns	20
Cybersecurity education	22
Practical tips for developing national cybersecurity capacities - through skills building	26
Case study: How to develop a cybersecurity curriculum for professionals	27
Research and development	28
<b>Conclusion</b>	<b>28</b>

## Module objectives

Welcome to Knowledge Module 4 on cybersecurity culture, awareness, workforce, and skills as part of the GFCE-Africa project. The module was **designed to respond to the need for enhancing cyber capacity building efforts and cybersecurity culture on the African continent**. It aims to guide, support, and equip participants with knowledge of **cyber capacity building that is considered an inevitable component in the overall digital transformation in the region**.

**The overall objective** of this module is to offer a broader context of cybersecurity capacity building in Africa. Cybersecurity capacity building efforts need to be viewed more holistically as these are linked to a broader digital policy reality and have direct spillovers to other developments in the region.

By participating in this module, **participants will acquire an understanding of why it is vital to invest in capacity building projects, with an emphasis on the importance of skills and cybersecurity culture building**. Likewise, this module pays particular attention to the enhancement of gender diversity in the cybersecurity workforce.

**This module also presents and helps participants to** grasp concrete tools for building a mature cybersecurity culture on the African continent.

At the end of this module, participants will have:

1. Knowledge about the impact and necessity of cybersecurity capacity building in their respective countries,
2. Better understanding of related concepts,
3. Better awareness of how capacity building efforts and investment can stimulate job creation, promote socio-economic development, enhance African countries' engagement in international cooperation and negotiations and help them effectively promote their interests in international forums,
4. Developed a vision for enhanced cybersecurity culture and learnt best practices and ideas,
5. Considered engaging more young generations in cybersecurity, especially women and girls at a young age to narrow the gender gap.

Furthermore, you will be able to respond and suggest action on the following questions:

- How do cybersecurity challenges in your country feature in a holistic context?
- How can capacity building efforts contribute to building a mature cybersecurity culture?
- How can early education in cybersecurity and building digital skills contribute to the overall cybersecurity context of your country?

- How can you make the case with your leaders about a longer-term approach to cybersecurity in your country and your region?
- What can be done to attract more women to cybersecurity and narrow the gender gap?
- How can enhanced cyber capacity building help boost economic growth in African countries?
- What are spillovers of having better and more cybersecurity trained professionals in your country to other sectors?

**Target audience:**

This module is particularly relevant for entry to mid-level government officials involved or aspiring to work in the cybersecurity field and/or are working in digital diplomacy. The module will be beneficial and practical for professionals, advisors, engaged in different policymaking related functions and for private sector representatives.

## **1. Cybersecurity skills and culture in Africa (context)**

---

## **GFCE Mission Statement**

*Every citizen of the world should be able to fully reap the benefits of ICT through a free, open, peaceful and secure digital world. Building cyber capacity provides the necessary foundation for countries to strengthen their cyber resilience through developing skills and capacity that addresses threats and vulnerabilities arising from cyberspace. It is therefore our mission to strengthen cyber capacity and expertise globally through international collaboration and cooperation*

---

**Africa's active participation in digital policy and cybersecurity discussions** is beneficial not only for Africa but also for a **more inclusive, impactful, and informed global digital policy**. Building cyber capacity for African stakeholders is an urgent necessity. Cyber capacity building can facilitate the process of **harnessing digital technologies and innovation to generate inclusive economic growth, stimulate job creation, and promote socio-economic development**. At the same time, capacity building will positively contribute to the **engagement of African stakeholders in global digital policy discussions, effectively promoting African interests in the international arena**.

The theme Cybersecurity Culture and Skills was endorsed by the GFCE community in the **Delhi Communiqué** as one of the five prioritised themes (cybersecurity policy and strategy, cyber incident management and critical infrastructure protection, cybercrime, cyber security standards) for cyber capacity building to:

- 1. Promote comprehensive awareness across all stakeholders of cyber-related threats and vulnerabilities and empower them with the knowledge, skills, and sense of shared responsibility to practice safe and informed behaviours in the use of ICTs, and to*
- 2. Involve all stakeholders to create a workforce with a set of cybersecurity skills and knowledge employers require.*

**GFCE Working Group D (WG D) focuses on the following topics:**

- Cybersecurity awarenesses
- Education and training, with a focus on cybersecurity workforce development

See more at <https://thegfce.org>

## Major challenges for nurturing cybersecurity culture in the African continent

### Reflection point

**What do you think are the biggest hurdles and challenges for building a mature cybersecurity culture in African countries?**

*Leave your comment below.*

Several cybersecurity specificities of the African region are linked to gaps in capacity building:

- **Technology adoption** is rising fast in Africa, especially thanks to its young population ([62% of Africans are under 25](#) in 2021). **Youth**, in particular, are very keen to adopt technology. Yet, in 2019, [ITU](#) estimated that only 28.6% of Africans were using the internet, which is low compared to the global average rate of 51.4%. Nevertheless, in the future, most of the new internet users are expected to be coming from Africa. The **potential for internet adoption** on the continent is huge. **Developing a corresponding cybersecurity culture and ensuring that the population has the necessary cybersecurity skills** needs to be a priority.
- This is obviously related to the **high cost of the internet in Africa**. The mobile pricing update by the Alliance for Affordable Internet ([A4AI](#)) indicates that on average, **the cost of the internet in Africa is very high** at about 6% of monthly income. Many African countries cannot be compared with other low- and middle-income countries such as those in Asia-Pacific, Latin America, and the Caribbean, where the mean cost of mobile internet is about 1.5% of monthly income. The pricing update measures the cost of 1GB of data on a prepaid mobile as a percentage of gross national income (GNI) per capita. **Understanding and working to mitigate underlying reasons for the high costs of the internet** is an important focus of **building the corresponding cybersecurity culture** of the future.
- African governments have stated **policies on increasing internet access and lowering its cost**. However, they are progressively targeting the digital space for taxation to raise revenues. This potentially has the effect of slowing the uptake of the internet as many internet users in Africa have other competing needs as noted in the [mobile broadband affordability index](#). It follows then that for the internet to be really affordable, **African economies have to grow and provide disposable income that can be used to purchase internet data**.
- Africa is a **leader in mobile financial services globally** (14% of Africans are using mobile money). The rate of access to financial services in Africa has increased

significantly since the 2000s after mobile money services started according to [Matthieu Aucante](#). The GSMA 2021 [Report](#) estimated that the transaction volume in sub-Saharan Africa alone was US\$27.4bn, while the global one was US\$41.1bn. This is important for financial inclusion as 'individuals and businesses have access to useful and affordable financial products and services that meet their needs - transactions, payments, savings, credit and insurance - delivered in a responsible and sustainable way' ([World Bank Group](#)). [The ACRC](#) estimates that the future of this 'success story will also depend on the **attention and resources that will be devoted to the issue of cybersecurity**'.

- There is a rise of **mobile malware**, especially targeting android phones (89% of smartphones in Africa run on Android), resulting in [stealing of personal data and money extortion](#). While it is common to undertake security measures on their laptops or desktop computers, in most cases, Africans are not doing the same on their smartphones. A study conducted by [Peter Elia Mosha \(2019\)](#) on university students of Arusha in Tanzania concluded that a small number of them use security features. **Educational activities will improve the secure use of digital devices.**
- In 2018, [Mcafee](#) estimated the **financial losses due to cybercrime in Africa** at US\$ 2 billion. Moreover, [Interpol in its report](#), claims that **90% of African businesses are operating without the necessary cybersecurity protocols in place**. This puts the industry at significant risk and opens the door for cybercriminals to exploit these vulnerabilities. Consequently, businesses suffer significant financial losses. The report also asserts that in 2016, the Kenyan economy lost about US\$36 million, the South African economy US\$573 million and the Nigerian economy US\$500 million as a result of cybercrime. Furthermore, during the Book Talk hosted by the Economic Commission for Africa (ECA), it was stressed that [cybercrime is one of the top risk factors likely to jeopardise Africa's economy](#), a concern that is particularly relevant when the continent is transitioning to e-commerce under the Africa Continental Free Trade Area (AfCFTA).
- Access to the internet is not an irrelevant connection. **Should development support focus on affordable access for the 'next billion' or the 'bottom' billion users?** The next billion users are easier to connect to, as they are likely to be closer to networks and have basic digital literacy skills compared to the bottom billion users who will certainly sink further down the poverty line without digital inclusion. Thus, building digital skills is essential and spills over into the issue of access to the internet.

## How can I make the case with my leaders to focus on efficient capacity development programmes?

The specific context and challenges in Africa link back to the **needs for concentrated capacity building efforts**. The advancement of cybersecurity culture will positively impact the African continent as well as the rest of the global community (possibly [decreasing cyber attacks conducted abroad from the African continent](#)). The growing centrality of cybersecurity has led many governments and international organisations to [focus on building the capacity of nations](#) to withstand threats to the public and its digital resources.

Therefore, cybersecurity awareness in Africa should put an emphasis on basic digital skills (such as the safe use of [mobile devices/smartphones](#)), as well as on understanding cybersecurity more holistically - among all stakeholder groups.

It is essential to focus on people's skills in the first place and continually build a better cybersecurity culture. Policymakers need to better understand and be aware of the **alarming links between the lack of cyber capacity and, for instance, economic growth or security**. It is essential to **invest resources into capacity building programmes**.

One exciting motivation for your country's leaders can be to build the image of your country as a champion in cybersecurity capacity building. As the *GFCE Global Good Practices* overview document remarked, countries that have previously benefited from capacity building activities, that have reached a certain level of maturity, and have the experience to share may serve as a regional hub for sharing their experience with their respective regions. Establishing capacity in one country of a region could help strengthen capacity in neighbouring countries as well.

**Having a local hub and a champion** in a region can facilitate awareness-raising of the opportunities for accessing a global programme. The support provided through local hubs can reduce costs and increase responsiveness to the needs of those requesting support and resources for capacity building.

## 2. Capacity building: an overview

### Theoretical explanation

If you really want to be good at something, you need to **understand the issues at hand thoroughly**. You need to be able to see the context, connect the dots, and apply your knowledge in practice. That is the idea behind capacity development - **enabling individuals to grasp the subject in question in its full complexity**. This is vitally important in the world of digital policy and cybersecurity, in which the pace of development (of both solutions and issues) is increasing. **Raising capacities in digital policy helps various stakeholders better navigate through developments related to ICTs and the associated policy implications**.

---

## Capacity building or capacity development?

Capacity development and capacity building are two terms often heard in development discussions. The term **capacity building** was in use before capacity development. One of the primary reasons for the shift in terminology is that capacity building is now seen by some to imply starting at a zero point with the use of external expertise to create something that did not previously exist. This concept does not acknowledge or respect the inherent capacity and ongoing development processes that exist everywhere.

**Capacity development**, on the other hand, emphasises the existence of endogenous development processes in all countries and communities, and addresses the need to support and/or facilitate processes that are already underway. Although there is no universal agreement about which is the most appropriate term, and both are still in common usage, many organisations have moved away from capacity building in favour of capacity development.

---

**Capacity development is much more than training.** Capacity development is often defined as the improvement of knowledge, skills, and institutions for the effective use of resources and opportunities. Widespread on the agendas of international development agencies, capacity development programmes range from institutional and societal to the individual level and include a variety of strategies, from fundraising to targeted training.

**Cyber capacity building** by definition according to Geneva Centre for Security Sector (DCAF) refers to the [development and reinforcement of processes, competences, resources and agreements aimed at strengthening national capabilities, at developing collective capabilities and at facilitating international cooperation and partnerships in order to respond effectively to the cyber-related challenges of the digital age.](#)

Cyber capacity building activities are particularly important when it comes to the prevention of cyber risks and malicious activities in cyberspace such as the protection of systems, infrastructures and more importantly, the protection of citizens. Overall, it comprises both **strengthening of institutional capacities** (in particular for technical deployment, policymaking, and implementation) and the **development of individual competences** (skills and abilities pertaining to the information society, including computer literacy, privacy safeguards, etc.). The effectiveness and legitimacy of digital policy and cybersecurity depend on the capacity of nations, organisations, and individuals to meaningfully participate in policy processes. Sufficient capacity in digital policy issues results in more informed policy decisions.

### Reflection point

**Can you explain in your own words what is capacity building and cyber capacity building?**



Leave your comment below.

## Resources

Read more about the relationship between cybersecurity capacity building, norms and confidence building measures in a [paper by Robert Collet](#). He argues that international cybersecurity capacity building emerged in the mid-2000s as a mechanism for countries and organisations to assist each other, across borders, in protecting the safe, secure, and open use of the digital environment. In parallel with this practical cooperation, the international community negotiated norms and confidence building measures to support peace and stability in cyberspace. The proposed framework shifts capacity building beyond developed-developing country relationships and stresses the many goals that it serves. The paper explores the relationship between cybersecurity capacity building, norms and confidence building measures. It contends that capacity building does not just support norms and confidence building measures, but is also an instance of them, and it benefits from norms of its own.

## Why is capacity building important in the global context?

Capacity building is inherently linked to the current debates taking place in international forums when it comes to stability and peace in cyberspace.

In the outcome documents of the [World Summit on Information Society \(WSIS\)](#) (2003/2005), **capacity development is underscored as a priority for developing countries**. Likewise, the [outcome document of the high-level meeting of the UN General Assembly \(UNGA\) on the overall review of the implementation of the outcomes of WSIS](#) calls for further investments into capacity development. More recently, the importance of capacity development has been raised in the [report of the UN High-level Panel on Digital Cooperation](#).

Capacity development in the area of ICTs has also featured highly on the agenda of the UNGA. At the 74th session of the UNGA, ICT capacity building was addressed mainly by national delegates from developing countries who stressed the importance of international support and partnerships, investment in human capital, and adequate training.

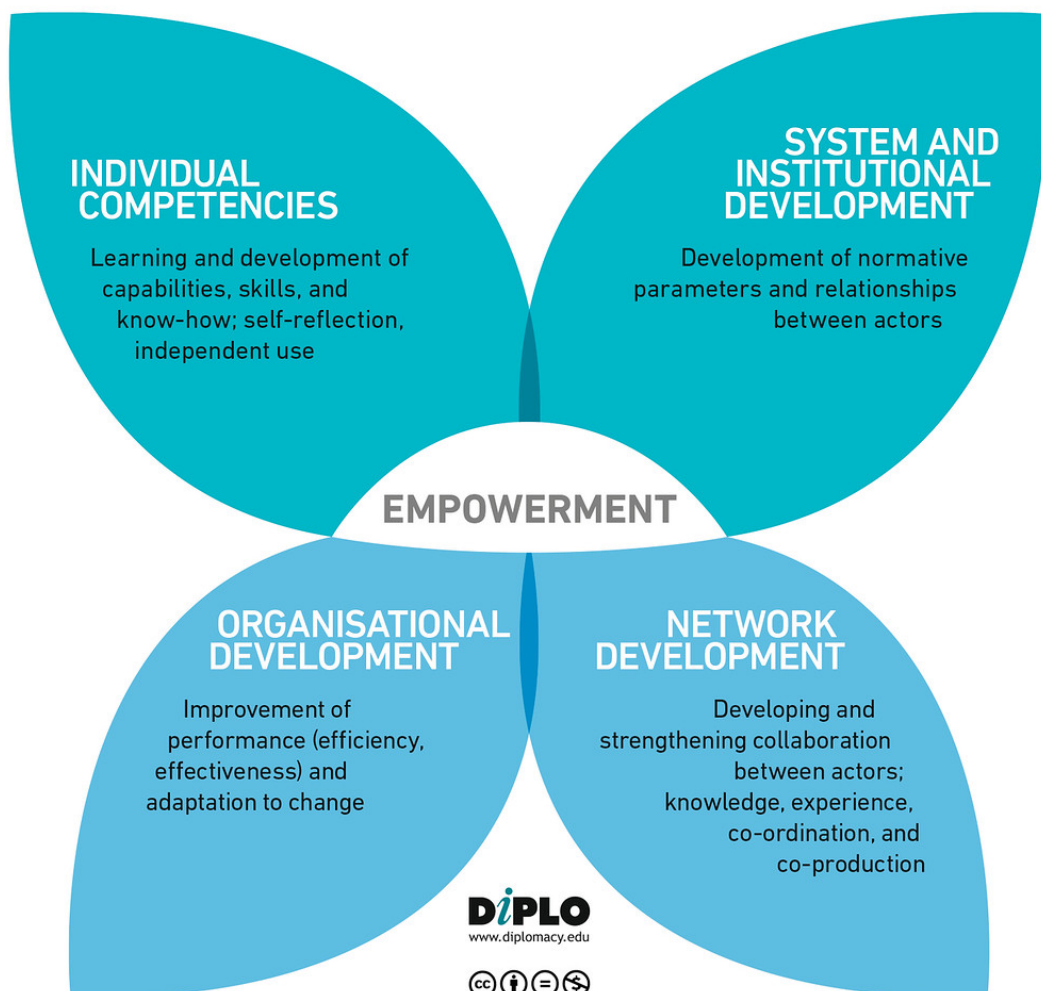
The United Nations Open-ended Working Group and the United Nations Group of Governmental Experts also have useful principles on capacity development. [See more](#).

The shift towards a more mature phase of digital policy would require a stronger focus on organisational development by ensuring sustained participation in policy processes. This includes **developing the organisational capacities of governments, civil society, businesses, and academia**. Organisational and system-level capacity development is becoming particularly relevant in dealing with issues such as cybersecurity.

**Research on capacity development in general and past experience highlights the following:**

- While the internet is a global facility, internet policy is often very local. It is shaped by local cultural and social specificities (e.g. cultural sensitivity to content, relevance of privacy protection). Therefore, **capacity development should follow local dynamics**, taking into consideration local political, social, cultural, and other specific conditions in developing and implementing capacity development programmes and activities.
- The urgency for capacity development could be addressed by providing **just-in-time learning as part of policy processes**.
- The growing need for capacity in the digital policy field has to be addressed at a more systemic level, by **including internet governance, cybersecurity, and related topics in the curriculum of academic postgraduate studies**.

Genuine and sustainable empowerment can be achieved through **holistic capacity development at the individual, organisational, system, and network levels**, as visualised in the capacity development butterfly below.



Generally, the **lack of sufficient resources, political will, and the limited sustainability of initiatives remain the main challenges for capacity development**.

Another challenge lies in the **delicate line between neutral capacity development and advocacy**, as capacity development activities do not aim to influence political decisions.



### Link of the pressing issues in Africa to cybersecurity

Often, other problems the region is facing seem more urgent (let us say, building a school). However, these challenges are not disconnected from cybersecurity. For instance, access to education is a priority, but not having sufficient digital skills can exacerbate the problem we experienced during the COVID-19 pandemic when the whole world suddenly shifted to online learning.

In Africa, in many cases, the lack of basic digital skills and the unfavourable cybersecurity culture have resulted in many children not continuing their education.

## 3. Cybersecurity capacity building in the broader context in Africa

The African continent has been a target of malicious cyber activities in the past couple of years. Many countries have seen a significant rise in sabotaged public infrastructures, illicit financial flows, ransomware attacks or even national security breaches, such as espionage or intelligence theft, to mention a few.

### Case study

According to the [Global Cybersecurity Index \(GCI\)](#), released by ITU in 2021, which measured and combined the score of each country on the 5 pillars of cybersecurity: legal; technical; organisational; **capacity development measures**; and cooperation measures, [all but six countries in Africa lack capacity development incentives for cybersecurity](#).

According to the [ranking made in 2020](#), Mauritius ranked best in 17th place globally, followed by Egypt in 23rd; Tanzania being the third best African country in 35th place. Six African countries are among the 10 lowest scores.

**The major drawback in Africa is the limited public awareness and knowledge about the potential risk that cyberspace brings.** The problem is further complicated by the poorly developed digital infrastructure and limited institutional capacity to implement and develop cybersecurity laws and policies as a result of the lack of fully-equipped cybersecurity professionals.


**Scarce financial resources** often limit readiness of countries in the Global South to invest into more robust cybersecurity infrastructure and measures. A recently published [paper](#) from

the University of Oxford analyses what good risk-based approaches to national cybersecurity should aim at achieving, especially in resource-constrained environments and provides guidance on what to prioritise when investing in cybersecurity.

Moreover, **government officials also lack comprehension of the substantive interconnection between cyber and national security and what it implies.**

**Cybersecurity capacity building aims to explicitly address these shortcomings** and close the cybersecurity skills gap that African countries need in order to adequately respond to cybersecurity risks. It aims to [bridge the digital divide, build institutional knowledge, or address policy awareness limitations and skills shortages for cyber protection.](#)

Members of the Global Forum on Cyber Expertise (GFCE) work together on several practical cyber capacity building initiatives. In 2017, a number of **global good practices of GFCE members were mapped**. They provide a rich set of experiences and knowledge. Collecting and sharing global good practices - in the form of a catalogue - ensures that other cyber capacity building initiatives can benefit from this experience and expertise in their own efforts.

 **Resources**

*GFCE [Cybil Portal](#) is an online repository for international cyber capacity building projects and hosts a large library of resources for projects to use. The portal helps to improve the effectiveness of capacity building, its coordination, and transparency.*

*Diplo's study and report titled [Sustainable Capacity Building: Internet Governance in Africa](#) and [recording in English and French](#)*

<https://africacenter.org/spotlight/africa-evolving-cyber-threat>


## Why is it important for African countries to enhance cybersecurity capacity building and by what means?

### A) Skills and culture building

African countries are not well-prepared for a cyberattack. Generally, **Africa ranks low on cybersecurity legislation**. According to a [report by AUC and Symantec from 2016](#), only 20% of African countries have developed legal frameworks to counter cybercrime, which is expected to grow due to the rapid rise of Africa's e-commerce market and is expected to reach [US\\$75 billion by 2025](#).

One of the reasons for the **poor adoption of cybersecurity laws**, in general, is the **lack of holistic awareness of cybersecurity** resulting in some governments treating cybersecurity

solely as cybercrime; the use of the term 'cybercrime' in different kinds of law, or the use of existing laws to prosecute cybercrimes.

 **Reflection point**

Are you or the security leaders in your country fully-aware of the intersection between digital security and national security? How can the lack of cybersecurity professionals hinder economic growth? What would be the spillover effects of more cybersecurity professionals on overall economic prosperity in African countries?

*Leave your comment below.*

**SCENARIO: CYBERSECURITY AND DIGITAL SKILLS GAP**

**Have you or your colleagues ever come across a situation where the lack of digital skills has hindered more advanced policy discussions on cybersecurity in your country?**



**RESULT:** Over the past few years, cyberattacks have skyrocketed. Africa likewise has witnessed a dramatic rise in cyberattacks during the COVID-19 pandemic.

**First**, the lack of digital skills has a direct and significant impact on organisations or public organisations and results in higher exposure to potential risks and malicious cyber activities.

**Second**, the shortage of adequately trained professionals impedes a nation's overall economic prosperity. The absence of skilled cybersecurity personnel can endanger a company's success: cyberattacks can cause huge financial losses, disrupt operations, services and supply chains, and can compromise personal privacy and data. Overall, the impacts of cyberattacks are grave and have the potential to thwart business success at all levels. For instance, the [African business community is estimated to have lost about US\\$3.5 billion in 2017 to cyber fraud and theft, and cybercrime is consistently ranked as one of the top threats faced.](#)

**Third**, the shortage of a cyber-aware workforce hinders African countries from meaningfully participating and expressing their needs in international forums, often resulting in their absence when discussions are taking place and policies being shaped. This is especially due to the deficits in capacities and the lack of basic awareness that are, inter alia, combined with lagging cyber policies in place.

**Fourth**, at the national level, public administrations desperately need cybersecurity personnel to protect their systems, data, and confidential information in order to increase the country's capacity to respond to threats arising from cyberspace. In other words, cybersecurity professionals are vital to [national security](#) and to prevent digital threats ranging from espionage, critical infrastructure sabotage, and organised crime. Besides, due to the lack of expertise, governments fail to monitor incidents and ultimately prosecute cyber criminals.



**ACTION:** Industry and the public sector should invest time and money in **cybersecurity education, longer-term training, awareness and mentorship programmes. The focus should be on multiple stakeholder groups. However, it should be taken into account that skills and culture building is a long-term process.** The situation will progressively improve by investing in capacity development programmes ranging from basic digital skills for children and young people through lifelong learning and targeted capacity building support of professionals, including policymakers.



**SPILLOVER TO:** Enhanced cybersecurity skills and culture will make people fit for the job market better and would address youth unemployment in Africa.

The OECD looked into [e-skilling of workers in Africa and the reality of self-employed individuals in Africa](#). According to the OECD, by 2040, own-account and family workers in Africa will represent 65% of employment under current trends. Their number could increase by 163%, to reach 529 million people in 2040, compared to an estimated 325 million people in 2020. Even in the best-case scenario where manufacturing and digital sectors expand substantially, own-account work will likely remain the mainstay for most African youth. A significant proportion of the continent's young labour force is outside the education and training systems, is jobless or works in the informal sector. Policies need to help them embrace digital transformation. Making digitalisation benefit informal and own-account workers requires increasing opportunities for lifelong learning and skills development.

The OECD study draws attention to the emergence of new forms of own-account work via the use of e-platforms and digital applications calling for improving regulatory frameworks and social protection schemes to prevent precarious working conditions. In South Africa, for example, the number of gig workers is growing by over 10% each year and could reach millions within the next decades.

#### Reflection point

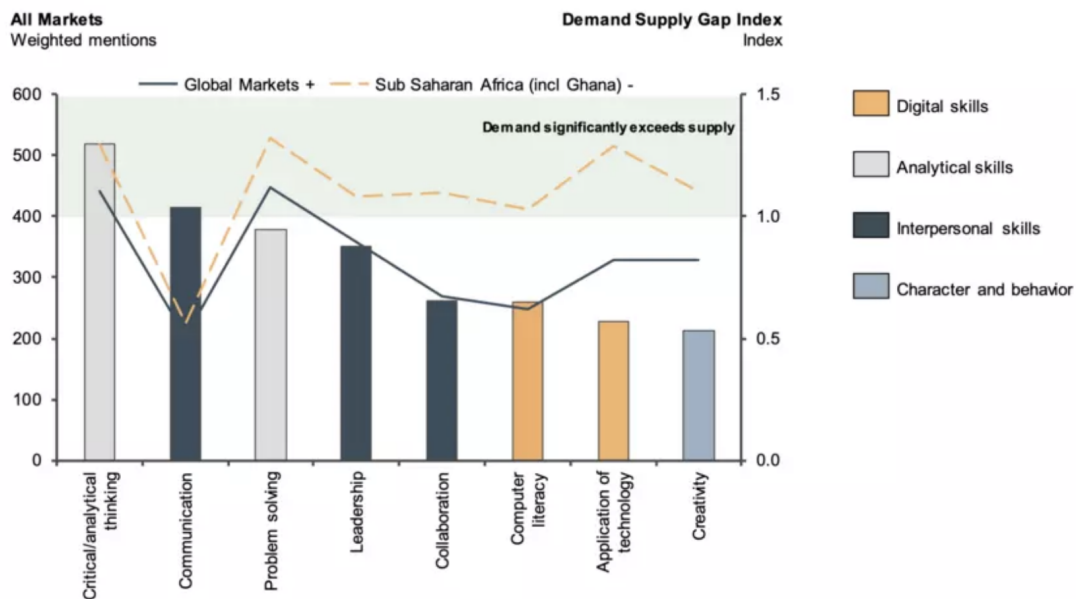
According to a [study](#) by the International Finance Corporation (IFC), a member of the World Bank Group and the largest global development institution focused on the private sector in emerging markets, around 230 million jobs across the continent will require some level of digital skills by 2030. In other words, there is a potential for 650 million training opportunities and an estimated US\$130 billion market.

The study looked at the Côte d'Ivoire, Kenya, Mozambique, Nigeria and Rwanda markets and in its preliminary findings reveals that by 2030 some **level of digital skills will be required for 50-55% of jobs in Kenya, 35-45% in Côte d'Ivoire, Nigeria, and Rwanda,**

and 20-25% in Mozambique.

Can you think of what level of digital skills will be required in your own country? Why?

Leave your comment below.



Source: WEF: [Supply and demand for the most important workforce skills](#)

## ! SOFT SKILLS MATTER

In addition to technical skills, **cybersecurity professionals need soft skills in the pursuit of their cybersecurity careers.**

The [NICE Cybersecurity Workforce Framework](#) made a list of the knowledge, skills, and abilities (KSAs) needed to complete tasks that can strengthen the cybersecurity posture of an organisation.



**NICE**  
NATIONAL INITIATIVE FOR  
CYBERSECURITY EDUCATION

Source : [About NICE](#)

***NICE** is a partnership between government, academia and the private sector, led by the National Institute of Standards and Technology (NIST) in the US Department of Commerce. Since its inception, its mission has been to expand the cybersecurity workforce by accelerating learning and skills development, nurturing a diverse learning community, and guiding career development and workforce planning. One of the initiatives set up by NICE is the **NICE Cybersecurity Workforce Framework** (launched in 2017). The initiative attempts to provide further guidance to employers on how to build a capable and ready cybersecurity workforce.*

Following a request for comment, the GFCE submitted some suggestions to improve the NICE Cybersecurity Workforce Framework. Among others, the GFCE suggested **adding soft skills to the training of future cybersecurity professionals such as critical thinking, communication skills, teamwork, etc.**

[Employers are looking for additional soft skills](#) when recruiting cybersecurity professionals: leadership, communication (translating technical subjects into business terms), critical/analytic thinking, teamwork, and creativity. Likewise, the report on [Development of Soft Skills That Are In Demand by Cybersecurity Employers](#) mentioned soft skills needed by cybersecurity professionals.

A new project on the **development of cybersecurity as a profession** has been launched in the **GFCE Working Group on Cybersecurity Culture and Skills (WG D)** . The project team circulated a [survey](#) to gather international views, which is now being evaluated.

## B) Women in cybersecurity

### Reflection point

**Can you estimate the percentage of women working in the cybersecurity field on the African continent?**

*Leave your comment below.*



Several specificities of the African region are linked to gaps in the inclusion of women and girls in digital transformation:

- Women are still largely underrepresented in the cybersecurity workforce around the globe. In Africa, [9% of cybersecurity professionals are women](#).
- In addition, [African women and girls have lower digital literacy and less access to the internet than African men](#). It is crucial to address the gender digital divide in order for women to have the possibility of starting businesses, getting education, finding jobs, obtaining health care, finding banking and other financial services, or engaging in a wide variety of activities in the digital post Covid-19 recovery.
- [According to Amnesty International](#), women of colour are 34% more likely to be targeted by online hate speech than their white peers.

### Contribute and engage

ITU's initiatives to [involve more women and girls in the digital transformation of economies and societies](#) include:

[CISCO EQUALS Learning Space](#), a free online digital skills training on topics such as cybersecurity, entrepreneurship and the internet of things;

[The Innovation Challenge: Women in Technology](#), a competition that supports standout tech innovators whose solutions are making a difference for women and who are helping and empowering women to excel in accessing and using ICTs to improve their productive and economic capacity in different sectors;


[World Summit on the Information Society Forum](#) (WSIS) special track on ICTs and gender mainstreaming;

[Generation Equality Technology and Innovation Action Coalition](#): In 2020, ITU became a co-leader of the Action Coalition and together with other partners, ITU is committed to working hard to leverage partnerships and the power and breadth of our membership to make Generation Equality concrete, focused, and above all, impactful.

[Talking Tech: Girls and Women in ICT](#), a series of interviews in which girls and young women, aspiring for a career in the technology sector, get a chance to interview leading women and role models in the field.

The GFCE continues to sensitise the global community about the role of women in cybersecurity capacity building. It helps to celebrate women in the field, by sharing their achievements and experiences, as well as discussing areas of opportunities for encouraging

women communities to become even more involved in CCB processes and how the GFCE can facilitate this.

 **Reflection point**

**What type of people work in cybersecurity? Do your women colleagues or peers consider a career in cybersecurity?**

*Leave your comment below.*

**SCENARIO: CLOSING THE GENDER GAP IN CYBERSECURITY**

**Have you ever heard from your women colleagues or peers that cybersecurity jobs are purely technical and are better suited for men to accomplish them successfully?**



**RESULT:** In general, there is a perception among girls at a young age that a cybersecurity career is an overly technical one. Although, partially, it might be true, there are far more job positions that require more interpersonal and soft skills (such as team work, leadership and communications skills, etc.) that women encompass.

Moreover, women tend to be less inclined to perceive cybersecurity as a viable career path because of the wrong judgement that it is a masculine profession.



**ACTION:** Taking into account that almost [60% of Africa's population is under the age of 25](#), making Africa the world's youngest continent and women accounting for more than 50% of Africa's combined population, it is of utmost importance to focus on young girls and women and encourage them to enter and keep working in the cybersecurity sector. Ultimately, it would open up the world of options for the unemployed African female population to generate high income and help shrink the cybersecurity workforce gap that is particularly worrying and upsets the digital and technological advancement in the region.

Like for any other working environment, the greater the diversity (background, thinking, perceptions, ideas), the greater the success of a company. The same rule applies to the cybersecurity field – having more women present will ensure and bring more perspectives and outlooks.

The action should start with the right women mentors and role models who would openly speak up about their success and capabilities and ultimately about the great potential the fields bring.

Women cyber leaders should start leveraging awareness, e.g. by creating a network of women working in tech or cybersecurity fields. Organisations that already have some cybersecurity maturity should start training their women employees or hiring women employees and offering them training or mentorship programmes.

### Contribute and engage

The [Women in Cyber Mentorship Programme](#) run by ITU is open to women in Africa and Arab regions working in cybersecurity at junior levels, as well as women in ICT/STEM seeking to enter the cybersecurity workforce.

[Women in Africa and Deloitte developed a mentoring programme](#) whose main objective is to develop women's leadership in Africa and help each mentor and mentee achieve their professional goals.

[CyberGirls is a one-year fellowship programme](#) that equips girls with globally sought-after cybersecurity skills, helping them seize work opportunities within Africa and across the world.

**Women in Cybersecurity (WiCyS)** provides different [training programmes for women](#) around the world.

### Reflection point

**Can you explain how society will benefit from the recruitment of more highly-qualified women in cybersecurity?**

**Can you think of any cybersecurity female role model in your country?**

*Leave your comment below.*

*Dr Katherine Getao, Chief Executive Officer of the ICT Authority in Kenya, explained the reasons why there are few women involved in the field of cyber security and cyber capacity building in Kenya. First of all, there is a lack of educational awareness regarding this field given to young girls when they choose what career they desire to follow in their lives. Secondly, as cybersecurity is at premium in Kenya, women involved in this domain are not fully aware of the different career paths that they can follow in this field, and only a few of them get involved in the CCB domain. Thirdly, young female professionals lack assertiveness in the working environment and are not encouraged to stand up for themselves and their professional achievements. Dr Getao not only highlighted the need for celebrating women's achievements and contributions, especially as part of the UN GGE, towards global security in the area of ICT and cyber capacity building, but also pointed out the importance of training women at the highest level, giving them opportunities to build*

confidence in order to be pushed to achieve more in the field, get strategic positions, and acquire the visibility they need to progress and show their actual contribution to cybersecurity and capacity building.

## Resources

[GFCE Delhi Communiqué](#) - GFCE global agenda for cyber capacity building, endorsed by all GFCE members and reaffirms their shared commitment to strengthen cyber capacity and expertise globally.

[GFCE Cybil Portal](#) - online repository for international cyber capacity building projects and hosts a large library of resources for projects to use. The portal helps to improve the effectiveness of capacity building, its coordination, and transparency.

Report: [Sustainable Capacity Building: Internet Governance in Africa](#) - the report was commissioned by the African Union and is part of the IG track of the Policy and Regulation Initiative for Digital Africa (PRIDA).

Report: [Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities](#) - publication by the Norwegian Institute of International Affairs.

<https://dig.watch/topics/capacity-development> at Geneva Internet Platform Digital Watch online observatory.

[UN database on cyber training opportunities](#) - a UN effort as an answer to the Roadmap on Digital Cooperation.

Short [video explaining online learning benefits and capacity development](#)

Short [video on methodology and development of online courses](#)

[The African Cyberthreat Assessment Report 2021](#)

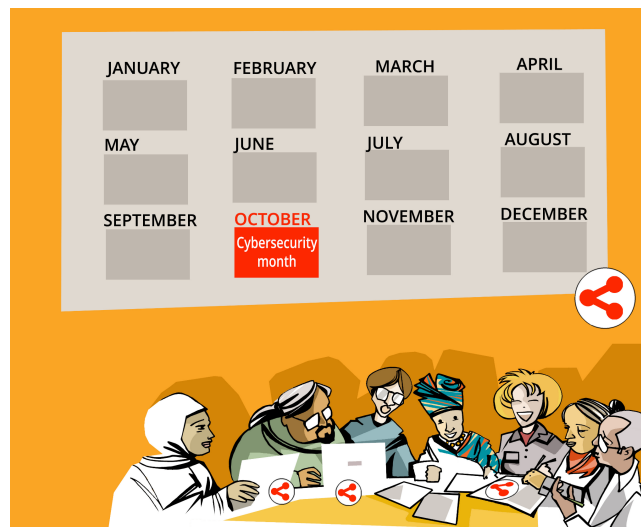
## 4. Concrete tools for building mature cybersecurity culture: best practices from the GFCE community

### A) Awareness-raising campaigns

One tool for building a more mature cybersecurity culture is through **awareness campaigns**. Your awareness campaign is probably not the only one – other campaigns are taking place locally, nationally, and/or internationally. It is advisable to align them to have a greater impact and use resources more efficiently. Aligning campaigns supports the ultimate goal of raising awareness of cyber-threats through safe online behaviour. ([GGP](#))

**Here are a few examples:**

- Experiences from 8 different awareness campaigns conducted in Africa ([Tips for running public awareness campaigns in Africa](#)) show some tips for successful awareness campaigns such as understanding the issue and what you want to achieve, making sure the topic is of a concern to people outside of your organisation, involving the target group in campaign planning, using language and media of your target group, making it easy for the target group to participate, using mainstream media and networks to amplify your message, being accurate, being flexible about the campaign plan, and making sure you can sustain the campaign over the planned period.
- A cyber hygiene campaign called ‘[CyberSmartBW](#)’ was conducted in Botswana in 2020. The aim was to counter the issue of increasing cyber scams targeting young people.
- Get Safe Online (which works with 25 countries including Rwanda) to raise awareness of cybercrime and other online harms has compiled a report of best practice examples of awareness raising, which can be accessed [here](#).
- Declaring a month dedicated to cybersecurity awareness can help focus the efforts of many stakeholders and enhance their collaboration, while delivering a strong message to the public and increasing the effectiveness of capacity building efforts. (GGP) Example: [European Union Cybersecurity Month](#) (ECSM in October 2019) and other years, led by ENISA. See also overview of this [global good practice of the GFCE](#).



Source: Diplo

**Practical tips for preparing an efficient cybersecurity campaign (GGP):**

- Gather stakeholders for dialogue and make efforts to coordinate events and activities. Align the vision, messages, and themes of the campaign among partners.
- Ensure that there is a shared vision.
- While the substance and information are the same for all, make sure to conceptualise campaigns for a specific constituent base. Often, it cannot be just copied and pasted.

- Cooperate and align with stakeholders at a variety of levels: domestically across stakeholder communities, bilaterally and/or regionally, and internationally.
- Coordinate cyber-focused events both in person or via social media while promoting the concept of multistakeholder involvement in the implementation of national awareness-raising initiatives.
- Work on sharing materials and toolkits, and proactively promote existing available resources. Reuse existing materials to reduce the cost of campaigns and to avoid reinventing the wheel. In this way, contextualised and repurposed materials can be used for other domestic and/or international campaigns. This also contributes to lower costs.
- Consider sharing the materials for free.
- Prepare a partner package with basic instructions, and point your partner to available resources. Direct partners to specific sections rather than sharing overwhelming amounts of information with them.
- Try to tailor the partner resources to the region (for instance, in Africa, mobile phones are very popular – tailor the format of your resources accordingly).
- Fit your message and campaign style to the context of the message. Be prepared for the fact that other partners may want to share their message in a different way.
- Consider local specificities, including the culture of the organisation you are working with.
- Utilise existing sharing platforms, for example, the Stop.Think.Connect.™ Cyber Awareness Coalition.
- Measure your campaign in terms of reported successes and participation.
- It is important to be aware of obstacles, such as the language of the campaign. Other obstacles are trademarks and copyrights, which can be a challenge when looking to repurpose and contextualise other organisations' material.

### Reflection point

**Are you aware of any cyber-related awareness campaigns in your own country? If yes, can you share what are its main features and main objectives?**

*Leave your comment below.*

## B) Cybersecurity education

**Creating a mature cybersecurity culture is a long-term process.** It is a shift. It is of utmost importance that governments in African countries embed cybersecurity education

along with digital skills **needed for being secure in cyberspace and make it part of national curricula, as early as the primary school level.**

Cyber skills are specialist digital skills, but in many countries the education system is not fully-equipped to provide students with the necessary digital skills in sufficient depth and scope. The objective for a number of countries is to fund initiatives that create and develop a sustainable pipeline for cybersecurity talent both now and in the future to meet the growing global need for individuals to possess cyber skills. Many countries are working to develop cyber skills amongst young people. However, many countries are not aware of what other countries are doing in this space and are unable to learn from best practices. [See more](#) about this identified knowledge gap.

The GFCE is well aware of the need to look into good practices in cybersecurity education for young people. WG D commissioned a research project by the University of Kent **Pre-University Cyber Security Education: A report on developing cyber skills amongst children and young people.** The [report](#) summarises research results from mapping pre-university cybersecurity education in a global context. The results learned from the research led to the following key findings and main recommendations, which we hope can help stakeholders around the globe to better cybersecurity education in a pre-university setting. South Africa features among the countries mapped.

**The Research Agenda** is a new tool developed for and by the GFCE community. The overarching aim of the Research Agenda is to **help the capacity building community design and run more effective projects by identifying knowledge gaps and filling gaps through research.**

Those skills are even more needed today due to the fact that the Covid-19 pandemic obliged more **children to go online for remote schooling.** Children increasingly use the web for educational purposes. While there are a number of advantages associated with gamification, the rapid increase in exposure to ICTs brings many drawbacks and risks arising from cyberspace due to the lack of awareness among children on how to use cyberspace safely and properly.

The Norton Group has listed these cyber [main threats](#) to children when they are online: **inappropriate content, chat room ‘friends’, cyberbullying and online scams.** In addition, [Kaspersky](#) puts other threats such as **posting private information, phishing, accidentally downloading malware, and posts that come back to haunt a child later in life.** It is vital, therefore, to introduce specific cybersecurity skills in their curricula aimed at countering these threats and ensuring cyber safety among children.

As for teaching methodology, [children are better motivated and focussed](#) on the learning activity when the used learning material is interactive and exciting. This can be done through the design of an educational [cyber safety game as noted by Kritzinger A](#) (2017). It is, however, important to create tailored games that allow learners to reach desired learning outcomes and to combine games with other materials.

## Some examples:

- The [CyberPatriot Elementary School Cyber Education Initiative](#) (ESCEI) has three fun, interactive learning modules for K-6 students about cyber safety.

**Security Showdown 2:** Strangers are asking about you, but is it safe to share with them? Learn the basics of sharing personal information with family, friends, and strangers in this simple point-and-click game. Will you share your information correctly and win the security showdown certificate? Featuring charming voxel graphics, simple game mechanics, and voice overs in both English and Spanish, this game is highly accessible and great for young players..

Key Topics: Personal Information

Grade Levels: K-2



**JeffOS:** Join Jeff, your helpful sidekick, as he guides you through his operating system and covers everything from basic computer skills to dealing with complex issues like phishing and malware. JeffOS delivers actionable advice for safer computing in the real world and breaks down advanced topics into digestible pieces all while providing players with fun, interesting interaction. Players will walk away from JeffOS with a more developed set of computer skills and a grasp on the importance of cybersecurity in their everyday lives.

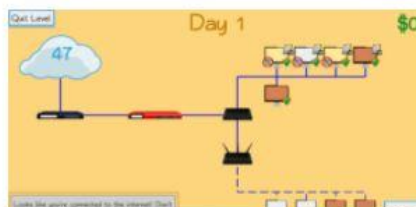
Key Topics: Phishing, Malware, Firewalls

Grade Levels: 3-6



**Packet Protector:** Build a computer network to mine for cryptocurrency and use this money to expand and secure your network! Watch how your decisions affect the security and effectiveness of a network in this educational simulation. Along the way, you will learn about some basic networking components, malware, security software, and discover some of the ways that you can protect your network from cyber threats..

Key Topics: Malware, Defenses, Passwords



Source: [US Cyber Patriot](#)

- [Webrangers](#) is a South African initiative led by Media Monitoring Africa. It is a digital literacy programme designed to allow young people to gain critical skills and knowledge around online safety that they use to create innovative campaigns that promote safe internet usage and champion their rights in the digital world.





Web Rangers is a digital literacy programme designed to allow young people to gain critical skills and knowledge around online safety that they use to create innovative campaigns that promote safe internet usage and champion their rights in the digital world. The programme is about creating young digital citizens who know how to use the internet responsibly and encourage their peers to do the same.

Source: [Web Rangers](#)

→ [Kids in the Know](#) is the [Canadian Centre for Child Protection's](#) interactive safety education programme designed for students from kindergarten to grade 9. The programme is available in French, too.

### About Kids in the Know

*Kids in the Know* is the [Canadian Centre for Child Protection's](#) interactive safety education program designed for students from Kindergarten to Grade 9. **The purpose of the program is to help educators teach children and youth effective personal safety strategies in an engaging, age-appropriate and interactive way that builds resiliency skills and reduces their likelihood of victimization in the online and offline world.** It is research and evidence-based, balances empowerment with protection, communicates without value statements, builds from past experiences, involves activity-based learning, and facilitates important discussions about personal safety without the use of fear.

The program is used in thousands of schools across Canada and has received the nationally-recognized Curriculum Services of Canada seal of approval. Lessons are matched to outcomes mandated by Departments of Education in all jurisdictions across Canada. Topics include healthy relationships, safe and responsible use of technology, addressing high-risk behavior, picture permanence online, as well as building capacity to handle difficult situations and knowing when to seek help.



DOWNLOAD

[KIK Overview Guide](#)



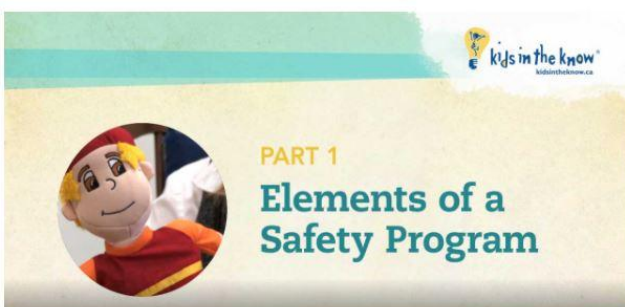
View Our Products

Free Resources



KIK Safety Sheet: 7 Root Safety Strategies

Sign Up!



Source: [About Kids in the Know](#)

As the internet may be slow in some parts of Africa, games and educational programmes should have offline components in addition to the online ones.

For a successful implementation of cybersecurity training in schools, we have to underline the importance of teacher training. For example, an initiative of the United States

Department of Homeland Security equips K-12 teachers with cybersecurity curricula and education tools ([Cybersecurity Education Training Assistance Program](#)). [Kids for Cyber](#) is a ready-to-use kit for educators to create a workshop and explore cyberspace with future generations.

Parents have to be involved in the cybersecurity education process for their children. As a parent, [Corbin Roof shares some tips and best practices](#) on how to teach cybersecurity basics to children. From his personal experience, parents should stress the importance of safeguarding their identity, assess progress made by the child regularly, start the conversations early, engage with their children regularly, foster their curiosity, be the administrator of their household, teach children that they are accountable for their actions.

The GFCE is aware of this need and within its Research Agenda has provided space and funding for project mapping cybersecurity education for young people in several countries/regions.

See the [report](#) on the *Cybil* portal.

While interactive elements in learning and training are important for children, they should not be evaded by professionals. For instance, Kaspersky has prepared an [online simulation game for diplomats and professionals to best understand the technicalities of how and why cyberattacks happen, without surviving such an attack](#).

## Practical tips for developing national cybersecurity capacities - through skills building

The number of malicious activities in cyberspace is rising. Therefore, there is a **need for skilled professionals** to be able to address this situation. According to the white paper by the Organisation of American States [Cybersecurity Education: Planning for the Future Through Workforce Development](#), the needed skills for these professionals include among others, the ability 'to optimally design and operate applications and systems with the capacity to identify and respond to cyber threats'.

The cybersecurity skills gap in Africa and the Middle East is estimated at 142,000 according to the report [Addressing the cybersecurity skills gap through cooperation, education and emerging technologies](#). A report produced by the Serianu Cyber Intelligence team [2018 Africa Cyber Security Report - Kenya](#) states that 60% of surveilled companies are facing a shortage of cybersecurity professionals. That shortage exists both in the public sector and the business sector.

In addition to the shortage, **even trained professionals need to continue upskilling and reskilling in order to adapt to emerging threats**, and that comes at a price. Unfortunately,

many businesses consider such an expense with no clear return on investment as noted in the Seriamu report above.

Different governments in Africa are working to implement e-government services, and financial institutions in Africa have implemented mobile financial services. Unfortunately, the shortage of cybersecurity skilled personnel in Africa places those projects at high risk of cyberattacks.

**The following concrete steps can be considered:**

- The public and private sectors already have IT personnel. That **personnel can receive additional ad hoc training on cybersecurity.**
- **Tertiary educational institutions have to set up cybersecurity sections** within their departments of computer sciences aiming to fill the gap between the needs and the workforce for the future.
- **Building partnerships, either public-private partnerships, or other kinds of partnerships** in order to overcome different obstacles to the building of a cybersecurity workforce. In that aspect, Africa can get inspiration from other initiatives such as:
  - a) NICE ([National Initiative for Cybersecurity Education](#)) - see above.
  - b) The Kingdom of Saudi Arabia has set up a governmental initiative as a result of collaboration between different ministries / departments. It is called the [National Cybersecurity Authority](#) (NCA). Among other duties, the NCA aims at developing the national cybersecurity workforce. For this specific task, the NCA has set up an initiative called [The Saudi Cybersecurity Higher Education Framework \(SCyber-Edu\)](#), a result of collaboration and coordination between the NCA, the Ministry of Education, and the Education and Training Evaluation Commission. SCyber-Edu goals are the development of education and training programmes, preparation of professional standards and frameworks and professional assessment tests related to cybersecurity.
  - c) The National School of Cybersecurity for Regional Training ([Ecole Nationale de cybersécurité à Vocation Régionale](#)) has been established in Dakar through cooperation between France and Senegal. It has the ambition to be a regional hub where learners from other African countries can get enrolled and build their capacities.



**Reflection point**

Can you think of an example from your own country of a public-private link in cybersecurity that has provided a win-win solution?

*Leave your comment below.*

## Case study: How to develop a cybersecurity curriculum for professionals

Several GFCE members have developed cybersecurity training courses and we encourage them to explore the [clearing house function of the GFCE](#) to find the right fit.

Several African stakeholders have developed and delivered capacity development programmes. The African technical community is remarkably [active in the field of capacity building in the region](#). This stakeholder group also presents a high degree of coordination when compared to other groups. Capacity building is not at the core mandate of most civil society organisations, but many of them present some activities within their projects, aiming to enhance capacities. The target audiences for civil society initiatives vary.

The identification of capacity building initiatives provided by universities through desk research is challenging, however, there are several programmes with cybersecurity elements. Some universities try to build a strong connection with the job market by diversifying the types of courses they offer. This is the case, for example, of the [University of Witwatersrand Johannesburg, which offers certificate courses](#), short courses of approximately one week, targeted at professionals.

The private sector contributes to capacity building in mainly two different manners: a) indirectly, supporting the efforts of other stakeholder groups; b) directly, as the main provider of capacity building. In the first case, the support from the private sector for initiatives aimed at capacity building specifically in the field of IG is clear. In the second case, the main motivation seems to be strengthening competencies valued by the job market and leveraging local talent. The relationship with IG is, therefore, less clear. The goal of this section is to provide a few selected examples of the two modalities of support provided by the private sector.

▶ Report: 'Sustainable Capacity Building: Internet Governance in Africa' (2021)

▶ Développement durable des compétences : Gouvernance de l'internet en Afrique

Yet, there is no universal guidebook on how to develop a cybersecurity curriculum. Any successful training programme needs to take into account the objectives of the programme, target group, duration, as well as resources available and mode of delivery (online, hybrid, in person). In terms of methodological approach, face-to-face initiatives were largely predominant in Africa before the COVID-19 pandemic.

## C) Research and development

The roles of research centres are to assist decision makers from either the government sector or the private sector by providing innovative solutions aiming at addressing actual and future cybersecurity challenges. These centres can take the form of national or even regional cybersecurity laboratories whose role is to solve the most pressing cybersecurity issues.

[From different experiences](#), research and development initiatives in cybersecurity work better when they are multistakeholder. It is therefore desirable to include higher education institutions into holistic cybersecurity capacity building efforts.

## Main takeaways

Congratulations, you have reached the end of the module. In the concluding part, we will reflect on the key takeaways from this module, leaving some additional space for you to write down the points that seem important to you and are not included above.

- Cyber capacity building can facilitate the process of **harnessing digital technologies and innovation to generate inclusive economic growth, stimulate job creation, and promote socio-economic development**. Likewise, capacity building will positively contribute to the **engagement of African stakeholders in global digital policy** discussions, effectively **promoting African interests in the international arena**.
- The major difference between capacity building and capacity development is explained by the fact that capacity building encompasses the start at a zero point with the use of external expertise to create something that did not previously exist; capacity development, on the other hand, focuses rather on the existence of endogenous development processes and supports the processes that are already underway.
- Cyber capacity building focuses on developing collective capabilities and facilitating international cooperation and partnerships with the aim to effectively respond to cyber challenges.
- According to the ITU's Global Cybersecurity Index (GCI), which measured and combined the score of each country on the 5 pillars (cybersecurity, legal, technical, organisational, capacity development measures, and cooperation measures) all but 6 countries in Africa lack capacity development incentives for cybersecurity.
- Limited public awareness, knowledge about the potential risk that cyberspace brings and lack of government officials' understanding of the interconnection between cyber and national security is the major hindrance for African countries when it comes to cybersecurity.

- A shortage of adequately trained professionals impedes a nation's overall economic prosperity. The absence of skilled cybersecurity personnel can endanger a company's success: cyberattacks can cause huge financial losses, disrupt operations, services and supply chains, and furthermore, can compromise personal privacy and data. Besides, it hinders African countries from meaningfully participating and expressing their needs in international forums, often resulting in their absence when discussions are taking place and policies being shaped.
- In addition to technical skills, cybersecurity professionals need soft skills in the pursuit of their cybersecurity careers such as leadership skills, communication (translating technical subjects into business terms), critical/analytic thinking, teamwork, and creativity.
- Capacity building efforts should target women who are still largely underrepresented in the cybersecurity workforce. In Africa, 9% of cybersecurity professionals are women. Taking into account that almost 60% of Africa's population is under the age of 25, making Africa the world's youngest continent and women accounting for more than 50% of Africa's combined population, it is important to focus on young girls and women and encourage them to enter and keep working in the cybersecurity sector. Ultimately, it would open up the world of options to generate high income and help shrink the cybersecurity workforce gap, which is particularly worrying and upsets the digital and technological advancement in the region.