United Nations
Economic Commission for Africa

Cybersecurity for Development in the Fourth Industrial Revolution

Research Report

United Nations
Economic Commission for Africa

Cybersecurity for Development in the Fourth Industrial Revolution

Research Report

Ordering information:
To order copies of this report, please contact: *Cybersecurity for Development in the Fourth Industrial Revolutiont*,
Publications Section
Economic Commission for Africa
P.O. Box 3001
Addis Ababa, Ethiopia

Tel: +251 11 544-9900
Fax: +251 11 551-4416
E-mail: eca-info@un.org
Web: www.uneca.org

First printing January 2025

Cover design, layout and printing: ECA Printing and Publishing Unit. ISO 14001-2015 certified.

Table of Contents

List of Figures

List of Tables

Acknowledgements

The present study, Cybersecurity for Development in the Fourth Industrial Revolution, was commissioned by the Economic Commission for Africa (ECA) under the overall supervision of the Director of the Technology, Climate Change and Natural Resources Management Division, Jean-Paul Adam, and with substantive contributions and coordination provided by the Chief of the Technology and Innovation Section, Mactar Seck.

Special thanks are expressed to the Lead Consultant, Jimson Olufuye, a prominent expert in the national, regional and global information and communications technology industry and the Chairman and Principal Consultant at Kontemporary® Konsulting Ltd., an information and communications technology solution company, for his work in drafting the present study.

Acknowledgement is given to the following stakeholders for their constructive feedback during the ECA cybersecurity side event that was organized on the margins of the seventeenth Internet Governance Forum, held in Addis Ababa on 29 November 2022: Nnenna Ifeanyi-Ajufo, Abdul-Hakeem Ajijola, Toyin Oloniteru, Robinson Sibe, Hossam El-gamal and Emma Theofelus. Additional assistance was provided by Asfaw Yitna, Research Assistant in the Technology and Innovation Section of ECA. Extended thanks are also given to the staff of the Publications and Conference Management Section of ECA for providing editorial and design support in the production of the present report.

In addition, acknowledgement is given to the following organizations, which provide data sources that were used for the present study: the World Bank Open Data Platform for gross domestic product and some Internet penetration data; the International Telecommunication Union for data from its Global Cybersecurity Index; the telecommunications and information and communications technology regulators of the Bahamas, Bahrain, Benin, the Congo, the Dominican Republic, Eswatini, Ghana, Kenya, Lesotho, Mauritius, Mexico, Nigeria, Qatar, Puerto Rico, Rwanda, Saudi Arabia, Sierra Leone, South Africa, Trinidad and Tobago, and Uganda and for the up-to-date information and communications technology industry statistics available on their websites; Internet World Stats and DataReportal for gross domestic product and Internet penetration statistics referenced for the research data validation exercises; and Statista for the available data on cyberattacks and the associated financial losses.

The views expressed in the present study do not necessarily reflect the views of ECA, the wider United Nations, its senior officials, or Member States.

Abstract

Analyses of 40 countries in Africa were conducted for the present study, which was aimed at investigating the relationship between cybersecurity and development in the fourth industrial revolution, which is believed to have commenced in 2011 and is characterized by the Internet of things and innovations. The results of the analyses revealed that the correlation between cybersecurity and Internet penetration was strong at approximately 66 per cent, which demonstrates a measure of cybersecurity, confidence and trust in the use of cyberspace. For countries and areas in Latin America and the Caribbean and in Asia, including Western Asia , the correlations were 60 per cent and 82 per cent, respectively. The results indicate that a 10 per cent increase in Internet penetration led to an increase in gross domestic product (GDP) per capita of between 1 and 8.2 per cent in Africa, between 3 and 5.1 per cent in Latin America and the Caribbean and between 5.5 and 12 per cent in Asia, including Western Asia.

Accordingly, cybersecurity has a good correlation with GDP, such that a 10 per cent rise in cybersecurity maturity leads to an increase of between 0.66 and 5.4 per cent in GDP per capita in Africa. In Latin America and the Caribbean, the increase in GDP per capita is between 1.8 and 3 per cent, while in Asia, including Western Asia, it is between 4.5 and 9.8 per cent. Africa has the weakest cybersecurity maturity index, at 29.1 per cent, followed by Latin America and the Caribbean at 35.6 per cent and Asia, including Western Asia at 61 per cent. Asia, including Western Asia, has the strongest index and the lowest financial losses, which implies that the stronger a country's or area's cybersecurity posture, the lower its financial losses per capita.1 The overall research results underscore the importance of cybersecurity to development in the fourth industrial revolution. ECA remains committed to strengthening cybersecurity in Africa.

1 Comparative data analytics are available at www.cd4ir.africa.

1. Introduction

On 5 July 2012, the Human Rights Council adopted by consensus an important resolution on the promotion, protection and enjoyment of human rights on the Internet (A/HRC/20/L.13). The protection of citizens' rights is a security concern affirmed in the Universal Declaration of Human Rights (United Nations, 1948). Therefore, the need to ensure the online security (cybersecurity) of citizens cannot be overemphasized. Cybersecurity is a concern of all Internet stakeholders (government, the private sector, civil society, technical and academic communities, and young people).

The advent of the Internet has transformed societies, economies and ways of life such that millions of people have been lifted out of poverty. Today, more than 50 per cent of the world population has access to information and communications technologies (ITU, 2021), which is an important target of the World Summit on the Information Society. While there is more to be done, the adverse effect of cybercrime, such as losses in reputation and investment, has cast a wide shadow on the possibility of reaping the full potential of information and communications technologies, especially with the advent of the fourth industrial revolution (World Economic Forum, 2016). There is therefore a need for an investigation into cybersecurity as a tool for development in the fourth industrial revolution.

With billions of devices (systems, sensors and actuators) operating autonomously in the fourth industrial revolution and more than 25 billion devices currently connected (Puglia, 2014; World Economic Forum, 2016), the pervasiveness of online risks is expected to rise geometrically in this fourth phase of the industrial revolution. This underscores the importance of establishing comprehensive security measures online to assure trust and confidence and to enhance continuous and sustainable development, as envisaged by world leaders in the 2030 Agenda for Sustainable Development (United Nations, 2015a) and Agenda 2063: The Africa We Want, of the African Union (2015).

The pace of innovation and transformation in the fourth industrial revolution has the potential to solve diverse development issues in the areas of poverty alleviation, health-care delivery, improvement in literacy levels, and food security, among other things. Indeed, the possibility of achieving the Sustainable Development Goals (United Nations, 2015b) may be real if cybersecurity concerns are holistically addressed. In other words, cybersecurity assurance is an imperative for digital transformation and for the advancement of the digital economy in Africa.

The conduct of the research on cybersecurity for development in the fourth industrial revolution was approved by the Economic Commission for Africa (ECA) at a meeting held on 3 August 2022).

i. Lomé Declaration

The first African Cybersecurity Summit, jointly organized by ECA and Togo, was held in Lomé on 23 and 24 March 2022. The Summit was convened in order to hold a dialogue on effective and efficient measures to foster cybersecurity in Africa through strategies, policies and practices. During the Summit, Heads of State and Government, and representatives of African Governments, in cooperation with ECA, signed the Lomé Declaration on Cybersecurity and the Fight against Cybercrime (Lomé Declaration). African Governments expressed their commitment to establish a framework to efficiently fight against cybercrime and promote aculture of cybersecurity, including the creation of authorities, structures and capacities dedicated to cybersecurity. The vehicle for the realization of the Lomé Declaration is the newly formed African Centre for the Coordination

and Research in Cybersecurity, located in Lomé, through a memorandum of understanding signed on 29 July 2022 by the Government of Togo and ECA.

ii. Place of trust and the need for cybersecurity assurance

Critical to addressing cybersecurity concerns is the issue of trust in the interconnected paradigm of people, process and technology (systems, equipment and devices). When concerns are addressed, trust and confidence in the interrelated economic, social and political systems grow, as do the associated development indices. ECA thus supports African countries in prioritizing cybersecurity and optimizing the benefits of the digital economy in the region. It is in that regard that the research for the present report was conducted.

2. Research justification

Studies indicate that a 10 per cent increase in per capita gross domestic product (GDP) is associated with a 22.6 per cent increase in the number of Internet users (Andrés, Diouf and Serebrisky, 2007). Similarly, a 10 per cent increase in Internet penetration in developing countries points to an increase in GDP per capita of between 2.0 and 2.8 per cent (ITU, 2019). It is in that regard that security, as it enables stability, also generates development. The implication of this is that cybersecurity also engenders Internet-enabled development, especially with more than 25 billion currently connected devices and many billions more projected in this fourth phase of the industrial revolution.

In this paradigm, the likelihood of an increased threat to trust on the Internet, which may impede development, cannot be overlooked. The relationship between cybersecurity and development was investigated in an effort to justify the need to consider cybersecurity as networks become more complicated and sophisticated, and to underscore the urgency for cybersecurity to be taken more seriously by top management and stakeholders in the ever-expanding fourth phase of the industrial revolution. Accordingly, harnessing the full potential of the fourth industrial revolution to enhance human development unimpeded by cyberinsecurity and a lack of confidence in cyberspace use is essential to the attainment of the Sustainable Development Goals and the goals and targets of Agenda 2063.

3. Methodology

The research contained in the present report was managed using the Projects IN Controlled Environments 2 methodology with the lead consultant as project manager and senior supplier; ECA management as corporate management; the Director of the Technology, Climate Change and Natural Resource Management Division, as executive; the Chief of the Technology and Innovation Section as the senior user; project assurance and the data collection consultants as team managers; and the lead consultant's assistant as project support (see figure I for a detailed schema).

As noted earlier, the research was focused on identifying a relationship between cybersecurity and development in the fourth industrial revolution. This was achieved through the following activities:

1. An investigation of cybersecurity gaps in:

- Forty top Internet-ranking countries in Africa, with the attendant losses in organizational reputation and investment. While the loss of data was quite sparse, it was assumed that its effect is reflected in the Global Cybersecurity Index or maturity level of each country and that the level of Internet penetration ranking is a reflection of cybersecurity posture.

- Fifteen top Internet-ranking developed and developing countries or areas in Asia, including Western Asia, and in Latin America and the Caribbean, with the attendant losses in organizational reputation and investment contained in their Internet penetration and cybersecurity maturity metrics.

- Some of the yardsticks, which include compliance with the action lines and targets of the World Summit on the Information Society and the degree of infrastructural readiness as a cybersecurity factor, directly reflect the level of Internet penetration and cybersecurity metrics of the countries or areas concerned. They are contributing factors to the data of the Global Cybersecurity Index of the International Telecommunication Union (ITU) utilized in the present study.

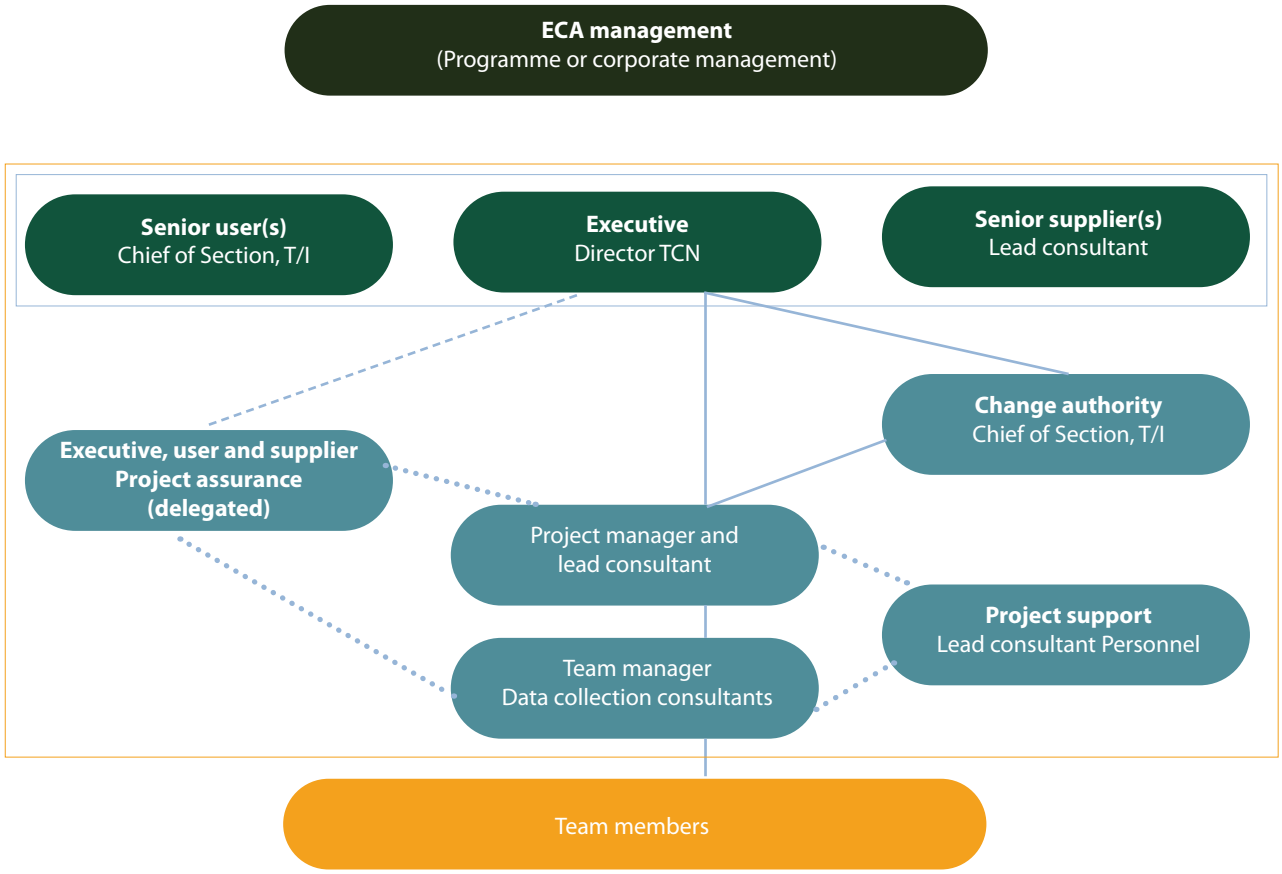
- The state of citizens' awareness of the role of cybersecurity controls. This is a contributing factor to the ITU Global Cybersecurity Index data utilized in the present report. It was also assumed that the level of Internet penetration and cybersecurity maturity is a reflection of how citizens interact with the Internet based on knowledge.

- The presence of a recognized professional career path in cybersecurity, which is an ITU Global Cybersecurity Index variable.

- Institutional cybersecurity and other controls in place. This is also an ITU Global Cybersecurity Index variable.

(a) Metrics on Internet penetration and cybersecurity over a period of 10 years were analysed in conjunction with GDP data to determine the degree of correlation.
(b) Data sets from the World Bank Open Data Platform, ITU Global Cybersecurity Index, national telecommunications and information and communications technology regulators' websites, DataReportal, Internet World Stats, news organizations and other public domain data outlets on the 40 top Internet-ranking African countries and 15 top Internet-ranking developed and developing countries or areas in Latin America and the Caribbean, and in Asia, including Western Asia, were analysed to observe the correlation between cybersecurity posture and development.
(c) A comprehensive literature review of scholarly materials on leading journals and online libraries was conducted on the subject matter.
(d) A quantitative technique was utilized in the research.

Figure I : Project management team structure



Source: Projects IN Controlled Environments 2 Management Methodology.

Abbreviations: T/I, Technology and Innovation Section; TCN, Technology, Climate Change and Natural Resource Management Division.

4. Literature review

i. Introduction

Cybersecurity for development in the fourth industrial revolution is a rather novel research topic judging by the paucity of scholarship materials on the subject matter. There has been significant study in areas of Internet diffusion and penetration and their connection to development. In one such study, Andrés, Diouf and Serebrisky (2007) found that a 10 per cent increase in per capita GDP enabled a 22.6 per cent increase in the number of Internet users, implying that an increase in Internet penetration has a measure of dependency on GDP growth. This showed a mutual association of the two variables.

The Internet is a network of networks encapsulating information and communications technologies and consisting of the communications, services, hardware and software sectors (Olufuye, 2010). Security is an important deliverable for its acceptability in a trust-demanding environment, such as in e-commerce, e-health, e-business, e-transport, supply chain management, banking, e-government, critical infrastructure management and secured data transmission and communications. The open architecture of the Internet, with no initial inbuilt security design, highlighted the limited role of security in its operations, until the Internet became imperative as an enabler of development and a carrier of critical data that require a high degree of confidentiality and integrity. For this reason, there is a limited view that security has no direct link with development (Makridis and Smeets, 2019).

An overwhelming number of scholars have indicated that security is connected to development and, by implication, cybersecurity is linked to development, especially when devices are always connected in critical production scenarios, such as banking, commerce, transportation, transport management, manufacturing, cloud computing, big data analytics and general ledger systems. The possible exploitation of billions of connected devices driving critical life-dependent systems in the evolving fourth industrial revolution presents a serious risk to human life and enjoyment. Taking the mitigation of this risk seriously is the fulcrum of underscoring cybersecurity for development in this fourth phase.

ii. Security and development

Matinuddin (2009) found that, where there is no security, the community falters and development and sustainable development become untenable. As a fundamental requirement of sovereignty, countries are expected to guarantee the security of their citizens. especially within their borders. and to ensure their territorial integrity. Failure to provide this security assurance leads to a failed state phenomenon. In such a situation, living conditions and standards plummet and development turns to regrelopment.2 In this scenario, security and conflict are strongly connected to development, which, in turn, highlights the importance of security to sustainable development.

iii. Cybersecurity and development

In 2012, the Human Rights Council adopted by consensus resolution A/HRC/20/L.13 on the promotion, protection and enjoyment of human rights on the Internet, declaring that every human right that is enjoyed "offline", in accordance with the Universal Declaration of Human Rights, must be upheld online (United Nations, 1948; Article 19, 2018). The Charter made it clear that the global and open nature of the Internet has the potential of facilitating development in its various forms. Since that assertion was made, studies have confirmed the strong relationship between the Internet and development. Where the Internet has been

2 A state of regressive development where development is retarded.

widely deployed, its effect on economic growth and development is evident. In addition, the effect on GDP is more pronounced with the use of giganet broadband. Studies on mature Internet systems with giganet conducted by Mckinsey (2011) reveal that a 3.4 per cent contribution of the Internet to GDP, which resulted in a real per capita increase of $500, on average, over a 15-year period was something that would have taken 50 years for the earlier industrial revolution to accomplish. An interesting phenomenon is the causative relationship between broadband and development such that a 10 per cent increase in broadband raises per capita GDP by $13,036, or a $1,000 increase in per capita income increases broadband penetration by 0.4 per cent.

As the giganet phenomenon catches on in developing countries, helped largely by the coronavirus disease (COVID-19) pandemic, many establishments, including schools, businesses and governments, moved their operations online to such an extent that the contribution of the Internet to GDP soared between 5 and 17.9 per cent in 2021 (Akpan, 2021). Data analysis for a period over 10 years under the present research showed an average GDP rise of $256 per capita in African countries, with a significant correlation between Internet penetration and GDP. It was as high as $1,632 in Seychelles, and as low as -$4,230 in Equatorial Guinea. For African countries, 32 per cent of those sampled recorded a negative correlation between GDP and Internet penetration, owing to economic management issues unrelated to policy inconsistency beyond the influence of Internet penetration. For example, Nigeria suffered a depression in 2014 caused by the economic downturn engendered by the drop in high oil prices and economic management issues, which resulted in the country's GDP shrinking by $100 billion. It did not start to recover from the depression until 2017. Notwithstanding, the strong Internet penetration growth produced a per capita growth of $32.

As dependence on the Internet increases, so does the growing demand for confidence and trust in the network as a consequence of increasing cases of cybercrimes and security gaps on the network. The need to protect the networks and safeguard assets online have become more urgent as the fourth industrial revolution gathers pace. The future plethora and multidimensional risks, such as another COVID-19 pandemic on a bigger scale, a nuclear war, a large-scale attack on critical infrastructure, or an unimaginable environmental disaster on the Internet that may adversely affect the viability of life on Earth prompted the Secretary-General in his report, "Our Common Agenda" (United Nations, 2021) to call for a Global Digital Compact to be agreed by all countries at the Summit of the Future, which is scheduled to be held in September 2024.3

iv. First, second and third industrial revolutions

Industrial revolutions are moments of drastic change in global economies, as compared with revolutions that bring about political change. As an economic change, productivity is transformed from one level to another. The first industrial revolution was marked by the inventions of the spinning jenny, steam engines and coke smelting. It enabled a shift from subsistence production of goods to large-scale production of textiles, consumption goods and machine tools powered by the steam engine invented by James Watt in 1769. It was a revolution that had its beginning in England and covered the period between 1760 and 1830 (Allen, 2011).

The second industrial revolution ushered in steel production, mass assembly lines, petrochemicals and manufacturing engendered by the electricity grid. Germany and the United States of America were leading the innovations during the period 1850 to 1914. The act of scientific management of workflow called Taylorism (after its inventor, Fred

3 More information is available at www.un.org/techenvoy/global-digital-compact.

W. Taylor), influenced mass manufacturing during that period (Wikipedia, n.d.).

The third industrial revolution began in the middle of the twentieth century with the invention of integrated circuits and the automation of product manufacturing. Integrated circuits, also known as chips, led to continuous miniaturization of microprocessors (chips) and the arrival of the Internet, which spurred the global village, digitization and the digitalization of processes. During that revolution, the factories began to use mass assembly lines interfaced with robots, as exemplified by Toyota. The company brought Taylorism to an end and replaced it with the Lean system, which strived for perfection in production and the avoidance of excess production, thereby meeting the exact customer requirements on time (Sesa Systems, 2022).

v. Fourth industrial revolution

The fourth industrial revolution (also known as Industry 4.0) was first mentioned at the Hanover Technology Fair, held in Germany in 2011. It heralded the Internet of things and Connected things, enabling the remote control and tracking of objects through embedded sensors and actuators in utensils, machinery, vehicles, buildings and traffic lights, among other things. It also features artificial intelligence and robotics, cloud computing, big data, 3D printing, blockchain technology, augmented reality and digital twins, all of which are enabled by sensors, actuators and objects driven by giganet. It is an evolving system in which the line between the physical and the virtual world is becoming blurred. The fourth industrial revolution features exceptionally smart manufacturing and the industry and factory of the future beyond planet Earth. It is an industry in which the traditional assembly line manufacturing gives way to on-demand precision manufacturing. According to Schwab (2016), it would be a breathtaking industry with a ubiquitous high-speed mobile-intelligent and connected system, brain and genetic enhancement coupled with exponential events happening at the same time.

More than 25 billion devices are currently connected and billions more are projected to be connected in the immediate future (Puglia, 2014; World Economic Forum, 2016). It is a development that would spur a new level of human development and prosperity. There is, however, concern with the security of the interconnected systems and the risk posed by unauthorized remote access control of the vast network of systems that drives new ways of learning, working, living and playing. That is why the role of cybersecurity in the fourth industrial revolution is so critical.4

vi. Cybersecurity for development in the fourth industrial revolution

Each of the first, second and third phases of the industrial revolution have led to increased prosperity for the global population, especially for countries that have played and are playing active roles through adoption, adaptation and innovation in technology. The fourth industrial revolution of Connected things is no exception. Data from the World Bank show that global GDP rose by 15 per cent, from $61.16 trillion to $84.97 trillion, between 2011 and 2021 (ITU, 2018).

As the fourth industrial revolution accelerates with industrial, business and practically all human endeavours connecting and revolving around the virtual world at an unprecedented speed, the need for continuous trust in the systems cannot be overemphasized. Averting risks of hacks, infiltration by unauthorized entities, especially inherent system failure and human error, has rapidly increased the importance of cybersecurity as a major enabler of development in the fourth industrial revolution.

The Transmission Control Protocol and Internet Protocol open architecture of the Internet has been enhanced with such security features as Internet Protocol security, Secure Socket Layer and Transport

4 More information is available at www.weforum.org/platforms/the-centre-for-cybersecurity.

Layer Security, Secure Shell, domain name system security, symmetry and asymmetry encryption algorithm, including data hashing and the use of complex passwords with multi-factor authentication, to guarantee data confidentiality and integrity. These measures are coupled with continuous system monitoring and filtering to detect and prevent the intrusion of malicious software (malware) and to ensure data and network availability. Notwithstanding the use of technology to tackle cybersecurity, other critical factors include people, in terms of their readiness and capability; and process, which for any country and organization involves legal frameworks, laws to provide deterrence, strategy, policy and regulations, the presence of regulatory institutions, and collaboration among all stakeholders in the global fourth industrial revolution. Despite the best efforts made, to date, losses attributed to cybercrime are still being suffered as a result of various vulnerabilities. Steve Morgan (2020) estimates that cybercrime will cost the world approximately $10.6 trillion annually by 2025. According to ITU, the cost of cybercrime to reach $2 trillion in 2019 and $6 trillion in 2021. By such estimates, cybersecurity failure is costing between 5 and 10 per cent of global GDP (ITU, 2018).

Given the unacceptable losses mentioned above, countries and even mature economies are investing in cybersecurity in order to harden their infrastructure to prevent unnecessary down time, reputation damage, and financial and intellectual property theft to hackers who are State entities and criminal groups. According to Allied Business Intelligence (2014) research, cybersecurity spending on critical infrastructure alone is expected to be in excess of $109 billion by 2020. The Republic of Korea planned to spend $607 million on cybersecurity in 2023, and the United States budgeted $10.9 billion to spend on cybersecurity in 2023. This trend indicates that cybersecurity is top on the agenda of mature economies for sustained economic growth and development.

The fourth industrial revolution provides an opportunity for the digital divide to be bridged in developing countries, as demonstrated by the Republic of Korea, Singapore and the United Arab Emirates, which are economies that have become newly mature and developed in the twenty-first century. African countries have a window of opportunity to ensure that trust, a key deliverable of cybersecurity, in the growing dependence on the virtual giganetworks is sustained to ensure their continuous economic growth and development. It is, again, in this regard, that the present report hypothesizes that cybersecurity, as a major component of the fourth industrial revolution, enables development.

To prove that hypothesis, a three-step approach was employed. The first step was to affirm the already established relationship between Internet penetration and GDP by reviewing available data from 2011 to 2021. The second approach was to investigate the relationship between cybersecurity posture and Internet penetration with data from 2011 to 2021. The third and the most significant approach was to evaluate the relationship between cybersecurity posture and GDP over the same period. The findings show a significant correlation between the pairwise data sets, confirming that cybersecurity enhances development in the fourth industrial revolution. A percentage of cybersecurity posture was computed as an influential rate of a measure of GDP growth.

The use of data on financial loss and attacks were constrained by a lack of real data available for analysis. This is evidence of the lack of regulatory or legal requirements for reporting on financial losses and attack frequency or, if such data exist, the possible weakness of the enforcement mechanism. However, financial loss and attack data were generated using the hot deck imputation method.5 Actual national cybersecurity maturity data of the ITU Global Cybersecurity Index were available for 2014, 2017, 2018 and 2020. Data for the missing years were estimates based on the hot deck imputation method.

5 The hot deck imputation method is a process for handling missing data wherein each missing value is replaced with an observed equivalent from a "similar" data category.

5. Research design, data collation and analysis

i. Introduction

The quantitative research undertaken for the present study was focused on the use of available data on the subject matter to generate numeric values that showed the dependence of one variable to another. Three data variables were of interest, namely, GDP, Internet penetration and the Global Cybersecurity Index data of the 40 countries in Africa and the 15 countries or areas in Latin America and the Caribbean and in Asia, including Western Asia, respectively, with the highest Internet penetration according to the most current available data. Data were gathered over a period of 10 years (2011–2021) from reliable sources, including the World Bank, ITU, telecommunications regulators and DataReportal, among other sources.

ii. Research design and preparation

The year 2011 was considered as the beginning of the fourth industrial revolution. In the research design, that year was the starting point in the research effort. A period of 10 years was considered for data gathering, collation and analysis, with 40 African countries (see subsection 5.3, table 1), along with 15 countries or areas in Asia, including Western Asia (see subsection 5.3, table 2), and 15 countries or areas in Latin America and the Caribbean (see subsection 5.3, table 3) used as samples. To determine the countries or areas used for the research effort, evaluation of the most current Internet penetration data sourced from regulators' websites or, if unavailable, data sourced from DataReportal, were gathered on all countries or areas in Africa, Latin America and the Caribbean, and Asia, including Western Asia. Data were then sorted from highest to lowest to select the number of countries or areas required for the research. Data connected to GDP, Internet penetration and the Global Cybersecurity Index were collected for 70 countries or areas. The processed Internet penetration, Global Cybersecurity Index and GDP data in the 40 African countries were compared with those of the 15 countries or areas in Latin America and the Caribbean and the 15 countries or areas in Asia, including Western Asia, in order to make a case for cybersecurity development in the fourth industrial revolution.

While complete cybersecurity data from 2011 to 2021 were largely unavailable, the hot deck imputation6 and the stochastic regression imputation7 methods (considering the data sets to be homoscedastic) were used to bridge the gap for the missing years in the ITU Global Cybersecurity Index data sets. The Pearson correlation coefficient (see equation 1) computation was used to determine the relationship between the Internet penetration and cybersecurity variables. The closer the value was to one, the stronger the dependence of one variable, for example, Internet penetration, to the other, for example, cybersecurity. The relational proportion was calculated over the review period. This exercise revealed an alignment of Internet penetration data with cybersecurity data for the 10-year period. This alignment could be attributed to:

(1) The increasing adoption of the Internet as a measure of the trust users have in the network;
(2) Confidence in a system as a function of the inherent or associated security measures connected with the system;
(3) The assumption that a breakdown of security on the Internet would imply a breakdown of the usability of the Internet.

6 Hot deck imputation is when a missing value is imputed from a randomly selected similar record.
7 Stochastic regression imputation involves the addition of "noise" to the imputed value obtained from regression imputation to ensure that the variation among imputed values is the same as the variation among observed values.

(4) The trio of people, process and technology as enablers of Internet penetration and the enablers of its security.

As Internet penetration enables GDP growth per capita, the degree of the alignment of Internet penetration with cybersecurity was a determinant factor of cybersecurity to GDP.

Equation 1: Pearson correlation coefficient

$$r = \frac{\sum(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum(x_i - \bar{x})^2 \sum(y_i - \bar{y})^2}} \quad \text{(i)}$$

Where,

r = correlation coefficient

x_i = values of the x-variable in a sample

$\bar{x}$ = mean of the values of the x-variable

y_i = values of the y-variable in a sample

$\bar{y}$ = mean of the values of the y-variable

a. Computational analysis

Computing the effect of Internet penetration on GDP

- For each country or area, the rate of change of Internet penetration (IP) from one year to the other was first computed

$$\Delta IP_{ij} = IP_{ji}+1 - IP_{ji} \quad \text{(ii)}$$

Where,

IP = Internet penetration

Δ = rate of change

i = initial study year (in this case, 2011)

j = computation for a given country or area

- The mean of the rate of change per a above was computed

$$\Delta\overline{IP}_{ij} = \frac{\sum\left(IP_{ji+1} - IP_{ji}\right)}{n} \quad \text{(iii)}$$

Where,

n = number of years (in this instance, 10)

j = computation for a given country or area

- The cumulative year-on-year increase in GDP was computed

$$C\Delta GDP_{ij} = \sum\left(GDP_{ji+1} - GDP_{ji}\right) \quad \text{(iv)}$$

Where,

C = cumulative

GDPij = gross domestic product

- The average GDP per capita increase over the period

$$\Delta\overline{gp}_{ij} = \frac{C\Delta GDP_{ij}}{P_c} \quad \text{(v)}$$

Where,

$\Delta\overline{gp}_{ij}$ = GDP per capita increase

Pc = Population a given country or area

- Calculating the link between IP and GDP per capita

$$\Delta\overline{IP}_{ij} \propto \Delta\overline{gp}_{ij}$$

$$IP_{ij} \propto \frac{\Delta\overline{gp}_{ij}}{\Delta\overline{IP}_{ij}} \quad \text{(vi)}$$

$$_{10p}IP_{ij} \propto \frac{10\Delta\overline{gp}_{ij}}{\Delta\overline{IP}_{ij}} = \frac{10n\sum\left(gp_{ji-1} - gp_{ji}\right)}{P_c\sum\left(IP_{ji+1} - IP_{ji}\right)}$$

Where,

$_{10p}IP_{ij}$ = 10 per cent increase in Internet penetration

$\propto$ = proportional sign

- Calculating the lower range value of 10 per cent increase in IP on GDP per capita in United States dollars

$$_{s}l_{gp} \propto \frac{\sum_{10p} IP_{ij}}{S} \qquad \text{(vii)}$$

Where,

$_{s}l_{gp}$ = lower range value of 10 per cent increase in IP on GDP per capita in dollars

S = number of countries or areas in a sample space

- Calculating the higher range value of 10 per cent increase in IP on GDP per capita in dollars

$$_{s}h_{gp} \propto \frac{\sum\left(_{10p} IP_{ji} \geq 0\right)}{s} \qquad \text{(viii)}$$

Where,

$_{s}h_{gp}$ = higher range value of 10 per cent increase in IP on GDP per capita in dollars

S = number of countries or areas with positive GDP per capita value from IP increase

- Calculating the latest country or area GDP per capita

$$GP_{nj} = \frac{GDP_{nj}}{P_{nj}} \qquad \text{(ix)}$$

Where,

GDP_{nj} = latest GDP of a given country or area in a region

GPnj = latest GDP per capita for a given country or area in a region

j = given country or area

n = year of latest GDP/population data

P_{nj} = latest population of a given country or area in a region

- Calculating the average regional GDP per capita

$$\overline{GP}_{nj} = \frac{\sum GP_{nj}}{S} \qquad \text{(x)}$$

Where,

$\overline{GP}_{nj}$ = average GDP per capita for a region

S = number of countries or areas with data in a region

- Calculating the lower range value of 10 per cent increase in IP on percentage increase in GDP per capita

$$_{10p}l_{gp} = \frac{_{s}l_{gp} \times 100}{\overline{GP}_{nj}} = \frac{100\sum_{10p} IP_{ji}}{\sum GP_{nj}} \qquad \text{(xi)}$$

Where,

$_{10p}l_{gp}$ = lower per cent range of the effect of 10 per cent IP increase on GDP per capita

- Calculating the higher range value of 10 per cent increase in IP on percentage increase in GDP per capita

$$_{10p}h_{gp} = \frac{_{s}h_{gp} \times 100}{\overline{GP}_{nj}} = \frac{100\sum\left(_{10p} IP_{ji} \geq 0\right)}{\sum GP_{nj}} \qquad \text{(xii)}$$

Where,

$_{10p}h_{gp}$ = higher percentage range of the effect of 10 per cent IP increase on GDP per capita

- The 10 per cent IP effect on GDP per capita growth range is provided in equations (xi) and (xii) above and expressed as follows:

Equation 2: Increase of 10 per cent in IP enables GDP per capita

$$_{10p}IP_S \propto \left[{}_{10p}l_{gp} : {}_{10p}h_{gp} \right] \quad \text{(xiiia)}$$

$$_{10p}IP_S \propto {}_{\$}gp_S \geq {}_{10p}l_{gp} \propto \leq {}_{10p}h_{gp} \quad \text{(xiiib)}$$

Where,

$_{10p}IP_S$ = 10 per cent increase in Internet penetration in a region

$\propto$ = proportional sign

$_{\$}gp_S$ = GDP per capita in dollars for the region in perspective

$_{10p}l_{gp}$ = lower percentage range of the effect of 10 per cent IP increase on GDP per capita

$_{p}h_{gp}$ = higher percentage range of the effect of 10 per cent IP increase on GDP per capita

b. Computing the effect of cybersecurity on gross domestic product

The effect of cybersecurity (CS) on GDP was computed based on the strong positive correlation of CS to IP. Using the Pearson correlation coefficient in equation 1, the equation for the effect of CS on GDP is given in Equation 14 below.

Equation 3: Increase of 10 per cent in cybersecurity enables GDP per capita

$$_{10p}CS_S \propto \left[{}_{10p}\beta l_{gp} : {}_{10p}\beta h_{gp} \right] \quad \text{(xiva)}$$

$$_{10p}CS_S \propto {}_{\%}gp_S \geq {}_{10p}\beta l_{gp} \propto \leq {}_{10p}\beta h_{gp} \quad \text{(xivb)}$$

Where,

$_{10p}CS_S$ = 10 per cent increase in cybersecurity maturity in a region

$_{\%}gp_S$ = GDP per capita in percentage increase for the region in perspective

β = correlation factor of CS to IP

$_{10p}l_{gp}$ = lower percentage range of the effect of 10 per cent IP increase on GDP per capita

$_{10p}h_{gp}$ = higher percentage range of the effect of 10 per cent IP increase on GDP per capita

iii. International Telecommunication Union Global Cybersecurity Index

As technology evolves, new cyberthreats continue to be devised. In embracing technology progress, cybersecurity must form an integral and indivisible part of the process (ITU, 2014).

Safeguarding information and communications technology ensures the economic stability of cyberspace and provides a reliable environment that is critical for organizations and individuals to conduct business and freely communicate (ITU, 2015). Safeguarding the integrity of cyberspace must involve the development of cybersecurity.

The ITU Global Cybersecurity Index was informed by country-level surveys, complemented by in-depth qualitative research in all ITU member States. Information was collected on laws, regulations, computer emergency response teams and computer incident response teams, policies, national strategies, standards, certifications, professional training, awareness-raising, and cooperative partnerships. The Index was computed based on five pillars, namely, legal, technical, organizational, capacity development and cooperation. The ITU Global Cybersecurity

Index report was produced for 2014, 2017, 2018 and 2020.

iv. Countries or areas in focus

The following three tables show the Internet penetration rate of the 70 countries or areas (by region) selected for the present study (see tables 1, 2 and 3).

Table 1: Countries with the highest Internet penetration in Africa

	Country	Population June 2022	Internet penetration June 2022	Internet penetration June 2022 (percentage)
1	Morocco	37 560 000	31 587 960	84.1
2	Kenya	55 600 000	46 355 022	83.1
3	Ghana	32 060 000	23 822 911	74.3
4	Egypt	105 200 000	75 660 000	71.9
5	Nigeria	214 100 000	151 021 062	71.4
6	South Africa	60 400 000	41 192 800	68.2
7	Tunisia	11 990 000	7 997 330	66.7
8	Mauritius	1 270 000	824 230	64.9
9	Rwanda	13 618 588	8 348 781	64.4
10	Gabon	2 310 000	1 432 200	62.0
11	Cabo Verde	558 900	345 959.10	61.9
12	Botswana	2 420 000	1 476 200	61.0
13	Algeria	44 980 000	27 280 000	60.6
14	Djibouti	1 010 000	595 900	59.0
15	Seychelles	98 600	57 977	58.8
16	Lesotho	2 170 000	1 126 230	51.9
17	Namibia	2 610 000	1 331 100	51.0
18	Gambia	2 520 000	1 285 200	51.0
19	Libya	7 000 000	3 472 000	49.6
20	Eswatini	1 180 000	554 600	47.0
21	Senegal	17 420 000	8 013 200	46.0
22	Cameroon	27 570 000	10 063 050	36.5
23	Côte d'Ivoire	27 400 000	9 946 200	36.3
24	Mauritania	4 840 000	1 732 720	35.8
25	Sao Tome and Principe	221 300	78 119	35.3
26	Angola	33 400 000	10 354 000	31.0
27	Sudan	45 450 000	14 044 050	30.9
28	Zimbabwe	15 210 000	4 654 260	30.6
29	Mali	21 160 000	6 326 840	29.9
30	Sierra Leone	8 060 000	2 393 820	29.7
31	Uganda	47 770 000	13 901 070	29.1
32	Zambia	19 190 000	5 469 150	28.5
33	Benin	12 290 000	3 490 360	28.4
34	Guinea-Bissau	2 040 000	571 200	28.0
35	Burkina Faso	21 800 000	5 951 400	27.3
36	Equatorial Guinea	1 470 000	385 140	26.2
37	Togo	8 508 000	2 203 572	25.9
38	Congo	5 730 000	1 455 420	25.4

	Country	Population June 2022	Internet penetration June 2022	Internet penetration June 2022 (percentage)
39	Ethiopia	119 300 000	29 825 000	25.0
40	United Republic of Tanzania	62 390 000	15 597 500	25.0

Sources: National telecommunications regulators of Benin, the Congo, Eswatini, Ghana, Kenya, Lesotho, Mauritius, Nigeria, Rwanda, Sierra Leone and Uganda; DataReportal and Internet World Stats (2021 and 2022).

Table 2: Countries or areas with the highest Internet penetration in Asia, including Western Asia

	Country or area	Population June 2022	Internet users June 2022	June 2022 (percentage)
1	United Arab Emirates	10 040 000	9 939 600	99.0
2	Kuwait	4 350 000	4 306 500	99.0
3	Qatar	2 960 000	2 930 400	99.0
4	Bahrain	1 770 000	1 752 300	99.0
5	Republic of Korea	51 320 000	50 290 000	98.0
6	Saudi Arabia	35 590 000	34 842 610	97.9
7	Oman	5 270 000	5 017 040	95.2
8	Brunei Darussalam	443 500	421 300	95.0
9	Japan	125 800 000	118 300 000	94.0
10	Hong Kong, China	7 580 000	7 050 000	93.0
11	Singapore	5 920 000	5 450 000	92.0
12	Israel	8 860 000	7 974 000	90.0
13	Malaysia	32 980 000	29 550 000	89.6
14	Macao, China	662 900	573 400	86.5
15	Kazakhstan	19 146 252	16 410 000	85.9

Sources: National telecommunications regulators of Bahrain, Qatar and Saudi Arabia; DataReportal (2022).

Table 3: Countries or areas with the highest Internet penetration in Latin America and the Caribbean

	Country or area	Population June 2022	Internet penetration June 2022	Internet penetration June 2022 (percentage)
1	Chile	19 120 000	17 700 000	92.0
2	Puerto Rico	3 194 000	2 530 000	89.4
3	Bahamas	393 248	338 900	85.0
4	Uruguay	3 474 000	2 910 000	83.4
5	Argentina	45 380 000	38 020 000	83.0
6	Barbados	287 371	235 400	81.8
7	Costa Rica	5 094 000	4 210 000	81.6
8	Saint Kitts and Nevis	53 192	43 300	80.7
9	Trinidad and Tobago	1 399 000	1 090 000	77.3
10	Brazil	214 700 000	165 300 000	77.0
11	Antigua and Barbuda	97 928	75 300	76.0
12	Ecuador	17 640 000	13 600 000	75.6
13	Paraguay	7 133 000	5 410 000	74.5
14	Mexico	128 900 000	96 870 000	74.0
15	Dominica	72 274	51 992	72.0

Sources: National telecommunications regulators of the Bahamas, Dominica, Mexico, Puerto Rico, Trinidad and Tobago; DataReportal.

v. Data collation

To acquire GDP data for the selected countries or areas in Africa, Asia, including Western Asia, and Latin America and the Caribbean with the highest Internet penetration according to the most current data, relevant data were collated from the World Bank Open Data Platform, national telecommunications regulators, Internet World Stats and DataReportal, published on their websites (see tables 4, 5 and 6).

Table 4 : Gross domestic product data of countries with the highest Internet penetration in Africa

	Country	Internet penetration June 2022 (percentage)	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
1	Morocco	84.1	101 370 474 295	98 266 306 615	106 825 649 872	110 081 248 587	101 179 808 076	103 311 649 248	109 682 728 023	118 096 227 400	119 870 439 114	114 725 065 285	132 725 261 467
2	Kenya	83.1	46 869 457 318	56 396 706 006	61 671 425 370	68 285 768 554	70 120 413 329	74 815 121 315	82 035 800 868	92 202 956 321	100 379 713 697	100 666 542 666	110 347 079 517
3	Ghana	74.3	39 337 314 810	41 270 954 737	62 823 043 706	54 782 847 753	49 406 568 433	56 165 172 899	60 406 382 899	67 299 280 680	68 337 537 816	70 043 199 814	77 594 279 055
4	Egypt	71.9	235 989 672 978	279 116 666 667	288 434 108 527	305 595 408 895	329 366 576 819	332 441 717 791	235 733 695 652	249 712 999 437	303 080 865 604	365 252 651 279	404 142 766 093
5	Nigeria	71.4	404 993 594 134	455 501 524 575	508 692 961 937	546 676 374 568	486 803 295 098	404 650 006 429	375 746 469 539	397 190 484 464	448 120 428 859	432 293 776 262	440 776 971 536
6	South Africa	68.2	458 201 514 137	434 400 545 086	400 886 013 596	381 198 869 776	346 709 790 459	323 585 509 674	381 448 814 653	404 842 116 738	387 934 574 098	335 442 101 366	419 946 428 126
7	Tunisia	66.7	48 122 744 708	47 311 159 485	48 684 187 850	50 271 072 628	45 780 128 467	44 360 614 525	42 164 007 605	42 685 972 269	41 772 900 763	42 514 151 614	46 840 042 941
8	Mauritius	64.9	11 518 393 367	11 668 685 524	12 129 642 296	12 803 445 934	11 692 287 066	12 232 463 656	13 259 351 418	14 181 951 059	14 045 808 843	10 926 820 603	11 156 657 770
9	Rwanda	64.4	6 881 379 762	7 650 671 477	7 815 975 294	8 234 762 201	8 539 424 910	8 690 878 328	9 252 834 120	9 642 440 646	10 356 327 149	10 184 345 442	11 070 356 519
10	Gabon	62.0	18 210 308 748	17 170 465 294	17 595 745 653	18 203 968 002	14 383 107 714	14 023 890 620	14 929 488 771	16 867 325 127	16 874 405 840	15 316 824 039	18 269 350 434
11	Cabo Verde	61.9	1 865 915 544	1 741 809 809	1 850 470 042	1 859 898 513	1 596 800 287	1 663 008 687	1 769 787 215	1 966 501 118	1 981 845 741	1 703 698 677	1 936 174 043
12	Botswana	61.0	15 351 972 361	14 380 004 175	14 901 750 991	15 654 660 710	13 578 754 072	15 082 578 065	16 088 437 675	16 914 245 098	16 695 925 027	14 930 072 799	17 613 846 473
13	Algeria	60.6	200 013 052 199	209 058 991 952	209 755 003 251	213 810 024 944	165 979 279 263	160 034 163 871	170 097 014 589	174 910 878 623	171 767 403 748	145 009 181 491	167 983 141 738
14	Djibouti	59.0	1 239 144 502	1 353 632 942	2 042 817 163	2 214 679 081	2 424 391 785	2 604 955 229	2 762 581 334	2 913 466 732	3 088 853 639	3 181 071 154	3 371 102 124
15	Seychelles	58.8	1 065 823 923	1 059 496 470	1 328 089 686	1 387 577 763	1 415 998 663	1 490 226 454	1 573 428 277	1 636 310 049	1 684 228 529	1 200 634 489	1 320 053 793
16	Lesotho	51.9	2 579 421 686	2 477 702 253	2 367 113 170	2 441 053 176	2 359 759 799	2 114 020 380	2 306 185 361	2 514 146 888	2 451 257 579	2 250 717 718	2 518 468 891
17	Namibia	51.0	12 523 402 329	13 042 007 432	12 043 276 397	12 435 416 060	11 335 179 562	10 721 994 677	12 895 153 160	13 682 062 249	12 543 203 411	10 562 637 376	12 236 250 784
18	Gambia	51.0	1 409 694 554	1 415 006 238	1 375 608 956	1 229 460 602	1 378 176 868	1 484 579 844	1 504 909 753	1 670 670 669	1 813 608 280	1 830 413 000	2 078 070 684
19	Libya	49.6	48 167 374 612	92 538 004 280	75 350 633 011	57 372 445 772	48 717 854 040	49 910 960 875	67 158 415 842	76 684 175 824	69 252 306 372	52 320 215 472	41 879 579 677
20	Eswatini	47.0	4 820 499 924	4 886 533 033	4 597 532 030	4 422 968 340	4 063 245 671	3 816 022 047	4 402 969 226	4 666 784 618	4 466 066 557	3 984 840 580	4 941 373 182
21	Senegal	46.0	17 814 284 622	17 660 871 726	18 918 668 644	19 797 254 643	17 774 766 636	19 040 312 815	20 996 564 752	23 116 897 847	23 398 811 424	24 493 157 583	27 625 388 352
22	Cameroon	36.5	30 630 912 185	30 155 064 574	33 728 622 819	36 386 546 918	32 210 232 912	33 814 337 900	36 098 550 142	39 973 839 065	39 670 977 333	40 804 449 726	45 238 613 480
23	Côte d'Ivoire	36.3	36 693 712 825	36 302 305 578	42 760 237 561	48 843 008 580	45 814 637 971	47 964 234 560	51 588 158 718	58 011 466 451	58 539 424 930	61 348 579 465	69 764 827 467
24	Mauritania	35.8	6 764 627 666	6 728 208 836	7 223 071 177	6 592 537 782	6 166 863 960	6 398 747 532	6 800 135 962	7 352 533 586	7 889 655 284	7 915 985 514	8 227 580 740
25	Sao Tome and Principe	35.3	231 489 270	250 680 846	300 554 484	346 528 329	316 066 072	345 495 615	375 614 126	412 253 810	427 425 040	472 914 470	547 092 915
26	Angola	31.0	109 436 531 427	124 998 158 418	133 401 594 461	137 244 418 013	87 219 290 029	49 840 494 026	68 972 763 787	77 792 940 077	69 309 104 807	53 619 071 176	72 546 985 709
27	Sudan	30.9	78 403 418 360	63 195 499 524	66 026 600 235	76 818 327 442	84 985 132 167	102 943 741 649	129 717 804 935	32 333 780 383	32 338 079 165	26 987 563 444	34 326 058 557
28	Zimbabwe	30.6	14 101 920 300	17 114 849 900	19 091 020 000	19 495 519 600	19 963 120 600	20 548 678 100	17 584 890 937	18 115 543 791	19 284 289 739	18 051 170 799	26 217 726 717
29	Mali	29.9	12 995 112 698	12 442 035 328	13 242 690 790	14 364 937 128	13 104 764 379	14 026 048 334	15 365 713 059	17 070 867 578	17 280 250 805	17 465 392 779	19 143 741 503
30	Sierra Leone	29.7	2 942 546 781	3 801 862 611	4 920 343 195	5 015 157 816	4 218 723 875	3 674 794 530	3 719 369 107	4 085 114 794	4 076 578 543	4 063 289 450	4 200 380 124
31	Uganda	29.1	27 871 725 206	27 305 915 761	28 915 786 997	32 612 397 758	32 387 183 845	29 203 988 815	30 744 473 912	32 927 025 573	35 353 060 634	37 600 368 181	40 434 701 517
32	Zambia	28.5	23 459 515 276	25 503 060 420	28 037 239 463	27 141 023 558	21 251 216 799	20 958 412 538	25 873 601 261	26 311 590 297	23 308 667 781	18 110 631 358	21 203 059 080
33	Benin	28.4	10 693 321 954	11 141 358 945	12 517 845 732	13 284 528 654	11 388 160 958	11 821 066 153	12 701 654 743	14 262 407 011	14 391 686 633	15 651 545 332	17 785 640 079
34	Guinea-Bissau	28.0	1 099 818 652	989 271 230	1 046 087 418	1 054 915 645	1 048 229 629	1 179 004 941	1 350 177 128	1 504 630 121	1 439 638 443	1 431 758 243	1 638 517 533
35	Burkina Faso	27.3	12 078 000 000	12 569 000 000	13 444 000 000	13 947 000 000	11 833 000 000	12 830 000 000	14 102 000 000	16 067 000 000	15 991 000 000	17 378 000 000	19 932 000 000
36	Equatorial Guinea	26.2	21 357 000 000	22 388 000 000	21 949 000 000	21 765 000 000	13 185 000 000	11 241 000 000	12 201 000 000	13 097 000 000	11 417 000 000	10 036 000 000	12 528 000 000
37	Togo	25.9	5 223 000 000	5 229 000 000	5 831 000 000	6 174 000 000	5 641 000 000	6 030 000 000	6 393 000 000	7 115 000 000	7 221 000 000	7 586 000 000	8 493 000 000
38	Congo	25.4	15 653 000 000	17 704 000 000	17 959 000 000	17 918 000 000	11 891 000 000	10 159 000 000	11 110 000 000	13 649 000 000	12 791 000 000	10 329 000 000	12 744 000 000
39	Ethiopia	25.0	31 958 000 000	42 221 000 000	46 544 000 000	54 165 000 000	63 081 000 000	72 120 000 000	76 841 000 000	80 207 000 000	92 608 000 000	96 611 000 000	92 757 000 000
40	United Rep. of Tanzania	25.0	34 067 000 000	39 651 000 000	45 681 000 000	50 002 000 000	47 384 000 000	49 774 000 000	53 227 000 000	56 699 000 000	60 810 000 000	64 403 000 000	69 238 000 000

Sources: World Bank Open Data Platform (2011–2020); DataReportal (2021); national telecommunications regulators, Internet World Stats and DataReportal (2021–2023).

Note: The numbers under each year represent the GDP figures.

Table 5 : Gross domestic product data of 15 countries and areas with the highest and most current Internet penetration in Asia, including Western Asia

	Country or area	Population	Internet users June 2022	Internet penetration June 2022 (percentage)	2011 (thousands)	2012 (thousands)	2013 (thousands)	2014 (thousands)	2015 (thousands)	2016 (thousands)	2017 (thousands)	2018 (thousands)	2019 (thousands)	2020 (thousands)	2021 (thousands)
1	United Arab Emirates	10 040 000	9 939 600	99.0	350 666.06	374 590.66	390 107.53	403 137.21	358 134.94	357 045.16	385 605.51	422 215.04	417 215.56	358 868.77	358 868.77
2	Kuwait	4 350 000	4 306 500	99.0	154 068.12	174 070.38	174 161.14	162 631.41	114 567.30	109 419.73	120 707.44	138 182.40	136 196.76	105 960.23	105 960.23
3	Qatar	2 960 000	2 930 400	99.0	167 775.27	186 833.50	198 727.64	206 224.60	161 739.96	151 732.18	161 099.12	183 334.95	175 837.55	144 411.36	179 570.78
4	Bahrain	1 770 000	1 752 300	99.0	28 776.60	30 749.31	32 539.47	33 387.71	31 050.64	32 234.97	35 473.78	37 802.01	38 653.32	34 723.36	38 868.66
5	Republic of Korea	51 320 000	50 290 000	98.0	1 253 223.04	1 278 427.63	1 370 795.20	1 484 318.22	1 465 773.25	1 500 111.60	1 623 901.50	1 724 845.62	1 651 422.93	1 637 895.80	1 798 533.92
6	Saudi Arabia	35 590 000	34 842 610	97.9	671 238.84	735 974.84	746 647.13	756 350.35	654 269.74	644 935.68	688 586.09	816 578.67	803 616.26	703 367.84	833 541.24
7	Oman	5 270 000	5 017 040	95.2	77 497.53	87 408.84	89 936.02	92 699.09	78 710.79	75 128.74	80 856.70	91 505.85	88 060.86	73 971.39	85 868.63
8	Brunei Darussalam	443 500	421 300	95.0	18 525.32	19 047.94	18 093.83	17 098.34	12 930.39	11 400.85	12 128.10	13 567.35	13 469.42	12 005.83	14 006.57
9	Japan	125 800 000	118 300 000	94.0	6 233 147.17	6 272 363.00	5 212 328.18	4 896 994.41	4 444 930.65	5 003 677.63	4 930 837.37	5 037 835.38	5 123 318.15	5 040 107.75	4 937 421.88

Sources: World Bank Open Data Platform (2011–2021); DataReportal (2021); national telecommunications regulators, Internet World Stats and DataReportal (2021–2023).

Note: The numbers under each year represent the GDP figures.

Table 6 : Gross domestic product data of countries and areas with the highest Internet penetration in Latin America and the Caribbean

	Country or area	Population June 2022	Internet penetration June 2022	Internet penetration June 2022 (percentage)	2011 ('000)	2012	2013	2014	2015	2016	2017	201	2019	2020	2021
1	Chile	19 120 000	17 700 000	92.0	251 224.86	267 175.87	277 239.46	259 405.20	242 496.65	249 298.72	276 364.93	295 402.65	278 584.73	252 727.19	317 058.51
2	Puerto Rico	3 194 000	2 530 000	89.4	100 351.70	101 564.80	102 450.00	102 445.80	103 375.50	104 336.70	103 445.53	100 925.00	104 914.60	103 138.30	103 138.30
3	Bahamas	393 248	338 900	85.0	10 070.45	10 720.50	10 562.80	11 176.10	11 861.90	11 834.60	12 357.60	12 755.80	13 192.80	9 699.50	11 208.60
4	Uruguay	3 474 000	2 910 000	83.4	47 962.44	51 264.39	57 531.23	57 236.01	53 274.30	57 236.65	64 233.97	64 515.04	61 231.15	53 560.76	59 319.55
5	Argentina	45 380 000	38 020 000	83.0	530 163.28	545 982.38	552 025.14	526 319.67	594 749.29	557 531.38	643 628.67	524 819.74	452 818.43	389 591.04	491 492.70
6	Barbados	287 371	235 400	81.8	4 657.70	4 610.10	4 677.25	4 696.34	4 724.69	4 832.81	4 981.59	5 097.28	5 304.16	4 689.53	4 900.80
7	Costa Rica	5 094 000	4 210 000	81.6	42 762.62	47 231.65	50 949.67	52 016.41	56 441.92	58 847.02	60 516.04	62 420.17	64 417.67	62 158.00	64 282.44
8	Saint Kitts and Nevis	53 192	43 300	80.7	836.09	826.23	875.38	954.06	958.41	1 008.94	1 060.64	1 078.51	1 164.88	980.91	976.15
9	Trinidad and Tobago	1 399 000	1 090 000	77.3	25 433.01	25 781.71	27 294.45	27 642.53	25 191.55	22 373.57	23 180.11	23 820.74	23 886.22	21 392.54	21 391.80
10	Brazil	214 700 000	165 300 000	77.0	2 616 156.61	2 465 228.29	2 472 819.36	2 456 043.77	1 802 212.00	1 795 693.27	2 063 514.69	1 916 933.71	1 873 288.16	1 448 565.94	1 608 981.22
11	Antigua and Barbuda	97 928	75 300	76.0	1 137.64	1 199.95	1 181.45	1 249.73	1 336.69	1 436.59	1 467.98	1 605.94	1 687.53	1 370.28	1 471.13
12	Ecuador	17 640 000	13 600 000	75.6	79 276.66	87 924.54	95 129.66	101 726.33	99 290.38	99 937.70	104 295.86	107 562.01	108 108.01	99 291.12	106 165.87
13	Paraguay	7 133 000	5 410 000	74.5	33 737.05	33 296.44	38 651.33	40 377.99	36 211.37	36 089.55	38 997.13	40 225.45	37 925.34	35 432.18	38 986.81
14	Mexico	128 900 000	96 870 000	74.0	1 180 489.60	1 201 089.99	1 274 443.08	1 315 351.18	1 171 867.61	1 078 490.65	1 158 913.04	1 222 408.20	1 269 404.28	1 087 117.78	1 293 037.87
15	Dominica	72 274	51 992	72.0		501.03	486.00	498.30	520.21	540.74	576.23	521.55	554.77	611.54	504.21

Sources: World Bank Open Data Platform (2011–2020): DataReportal (2021); national telecommunications regulators, Internet World Stats and DataReportal (2021–2023).

Note: The numbers under each year represent the GDP figures.

The following three tables show the Internet penetration of the selected countries or areas in Africa, Latin America and the Caribbean, and Asia, including Western Asia (see tables 7, 8 and 9).

Table 7 : Internet penetration data of 40 countries in Africa, in context, 2011–2021

	Country	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	Average of change 2011–2021	Increase per capita GDP resulting from 10 per cent increase in Internet penetration (US dollars)	Increase in per capita GDP resulting from 10 per cent increase in Internet penetration in countries with positive correlation (US dollars)
		Percentage of Internet penetration													
1	Morocco	46	55	56	57	57	58	62	65	74	84	74.4	2.84	294	294
2	Kenya	9	11	13	17	17	17	67	86	84	43	40.0	3.1	368	368
3	Ghana	9	11	15	19	23	28	38	43	53	58	50.0	4.1	291	291
4	Egypt	26	26	29	34	53	52	45	50	57	72	57.3	3.13	511	511
5	Nigeria	14	16	19	21	38	53	51	49	50	42	50.0	3.6	46	46
6	South Africa	34	41	47	49	52	54	56	62	68	70	64.0	3	-211	
7	Tunisia	39	41	44	46	46	50	56	68	67	72	66.7	2.77	-39	
8	Mauritius	35	35	40	45	50	52	63	63	65	68	64.0	2.9	-98	
9	Rwanda	7	8	9	11	18	20	27	30	44	27	31.4	2.44	126	126
10	Gabon	18	24	31	38	46	48	50	60	61	62	62.0	4.4	6	6
11	Cabo Verde	32	35	38	40	43	50	57	60	62	65	61.9	2.99	42	42
12	Botswana	9	16	30	37	37	39	41	58	61	64	47.0	3.8	246	246
13	Algeria	15	18	23	30	38	43	48	50	58	63	59.6	4.46	-160	
14	Djibouti	7	9	13	17	23	31	56	58	59	59	55.7	4.87	433	433
15	Seychelles	43	47	50	51	54	57	59	71	76	79	58.8	1.58	1 632	1 632
16	Lesotho	7	10	15	22	25	32	39	41	42	44	47.9	4.09	-7	
17	Namibia	12	13	14	15	26	31	37	40	41	51	51.0	3.9	-28	
18	Gambia	11	12	14	16	18	21	25	33	35	37	23.7	1.27	209	209
19	Libya	14	15	17	18	19	20	50	59	69	75	46.2	3.22	-279	
20	Eswatini	2	2	3	4	4	5	14	32	32	47	47.0	4.5	23	23
21	Senegal	10	11	13	18	22	26	46	61	59	46	46.0	3.6	156	156

	Country	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	Average of change 2011–2021	Increase per capita GDP resulting from 10 per cent increase in Internet penetration (US dollars)	Increase in per capita GDP resulting from 10 per cent increase in Internet penetration in countries with positive correlation (US dollars)
22	Cameroon	5	8	10	16	18	21	23	30	34	38	34.0	2.9	183	183
23	Côte d'Ivoire	3	4	7	10	17	25	35	38	44	47	36.3	3.33	362	362
24	Mauritania	5	5	6	12	18	24	24	35	37	41	33.1	2.81	108	108
25	Sao Tome and Principe	20	22	23	24	26	28	30	32	32	33	35.3	1.53	932	932
26	Angola	5	8	13	21	22	23	26	29	32	36	31.0	2.6	-425	
27	Sudan	4	7	12	12	13	14	27	29	28	31	30.9	3.09	-314	
28	Zimbabwe	8	12	16	16	23	23	42	40	40	33	33.4	2.54	314	314
29	Mali	2	3	4	7	10	14	19	66	64	27	27.9	2.59	112	112
30	Sierra Leone	1	3	4	6	6	12	13	16	17	25	29.7	2.87	54	54
31	Uganda	5	5	5	5	6	6	41	44	42	24	26.2	2.12	124	124
32	Zambia	4	4	5	7	9	10	21	30	41	24	29.4	2.54	-46	
33	Benin	4	5	5	6	11	15	19	33	33	26	28.4	2.44	237	237
34	Guinea-Bissau	3	3	3	3	6	14	15	16	19	23	25.0	2.2	120	120
35	Burkina Faso	3	4	5	6	8	12	17	19	19	22	25.7	2.27	159	159
36	Equatorial Guinea	12	14	16	19	21	24	26	24	24	26	26.2	1.42	-4 230	
37	Togo	4	4	5	6	7	11	12	16	19	24	23.8	1.98	194	194
38	Congo	6	6	7	7	8	8	10	12	12	28	32.1	2.61	-195	
39	Ethiopia	1	3	5	8	14	15	19	20	22	24	20.6	1.96	260	260
40	United Republic of Tanzania	3	4	4	7	10	14	16	19	38	25	25.0	2.2	256	256
												Average computation	3.54	31	256

DataReportal Hot deck imputed data

Sources: World Bank and national telecommunications regulators of Benin, the Congo, Eswatini, Ghana, Kenya, Lesotho, Mauritius, Nigeria, Rwanda, Sierra Leone, South Africa and Uganda (2011–2021).

Table 8 : Internet penetration data of 15 countries or areas in Latin America and the Caribbean, in context, 2011–2021

	Country or area	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	Average of percentage change 2011–2021	Increase in per capita GDP resulting from 10 per cent increase in Internet penetration (US dollars)	Increase in per capita GDP resulting from 10 per cent increase in Internet penetration in countries or areas with +ve correlation (US dollars)
		Percentage of Internet penetration													
1	Chile	52	55	58	61	77	84	82	85	86	88	82	3	1 148	1 148
2	Puerto Rico	48	69	69	69	63	69	69	71	78	84	77	2.9	301	301
3	Bahamas	65	72	72	77	78	80	81	83	85	87	85	2	1 447	1 447
4	Uruguay	51	54	58	61	65	66	70	81	83	86	77	2.6	1 257	1 257
5	Argentina	51	56	60	65	68	71	74	78	80	86	80	2.9	-294	
6	Barbados	67	71	71	75	76	80	82	80	81	82	82	1.5	564	564
7	Costa Rica	39	48	46	53	66	66	72	73	81	81	81	4.2	1 006	1 006
8	Saint Kitts and Nevis	63	64	65	68	76	77	77	78	78	81	81	1.8	1 463	1 463
9	Trinidad and Tobago	55	58	60	62	65	68	69	73	73	77	77	2.2	-1 313	
10	Brazil	46	49	51	55	58	61	67	70	74	81	75	2.9	-1618	
11	Antigua and Barbuda	52	58	63	68	70	73	88	80	79	76	76	2.4	1 419	1 419
12	Ecuador	31	35	40	46	49	54	56	58	62	65	57	2.6	586	586
13	Paraguay	25	29	37	43	50	53	61	65	69	74	69	4.4	167	167
14	Mexico	37	40	43	44	57	60	64	66	70	72	71	3.4	257	257
15	Dominica	49	50	51	58	65	67	68	68	78	100	100	3.8	0	0
												Average computation	4	447	754

DataReportal

Sources: World Bank Open Data Platform and national telecommunications regulators of the Bahamas, the Dominican Republic, Mexico, Puerto Rico and Trinidad and Tobago (2011–2021).

Table 9 : Internet penetration data of 15 countries or areas in Asia, including Western Asia, in context, 2011–2021

	Country or area	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	Average of percentage change 2011–2021	Increase in per capita GDP resulting from 10 per cent increase in Internet penetration (US dollars)	Increase in per capita GDP resulting from 10 per cent increase in Internet penetration in countries or areas with positive correlation (US dollars)
		Percentage of Internet penetration													
1	United Arab Emirates	78	85	88	90	91	91	95	98	99	100	99	2.1	389	389
2	Kuwait	66	70	75	79	82	86	98	100	100	99	99	3.3	-3 351	
3	Qatar	69	69	85	91	93	95	97	100	100	100	99	3	1 328	1 328
4	Bahrain	77	88	90	91	93	98	96	99	100	100	99	2.2	2 592	2 592
5	Republic of Korea	84	84	85	88	90	93	95	96	96	97	97	1.3	8 174	8 174
6	Saudi Arabia	48	54	61	65	70	75	94	93	96	98	96	4.8	950	950
7	Oman	48	60	66	70	74	77	80	86	90	95	95	4.7	338	338
8	Brunei Darussalam	56	60	65	69	71	90	95	95	95	95	94	3.8	-2 681	
9	Japan	79	79	88	89	91	93	92	91	93	90	93	1.4	-7 357	
10	Hong Kong, China	72	73	74	80	85	87	89	91	92	92	92	2	7 891	7 891
11	Singapore	71	72	81	82	83	84	84	88	89	92	90	1.9	10 458	10 458
12	Israel	69	71	70	75	77	80	82	84	87	90	88	1.9	13 027	13 027
13	Malaysia	61	66	57	64	71	79	80	81	84	90	84	2.3	985	985
14	Macao, China	60	61	66	70	78	82	83	84	86	88	87	2.7	-3 878	
15	Kazakhstan	51	62	63	66	71	75	76	79	82	86	81.9	3.09	41	41
												Average computation	2.8	1 898	4 149

DataReportal

Sources: World Bank Open Data Platform and national telecommunications regulators of Bahrain, Qatar and Saudi Arabia (2011–2021).

The following three tables show the cybersecurity data of the selected countries or areas in Africa, Latin America and the Caribbean, and Asia, including Western Asia, with the highest Internet penetration (see tables 10, 11 and 12).

Table 10 : Cybersecurity data of countries in Africa with the highest Internet penetration (Percentage)

	Country	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	Cybersecurity maturity level	Correlation of cybersecurity with GDP	Correlation of cybersecurity with Internet penetration
1	Morocco	35.9	40.1	45.8	55.9	47.8	55.3	54.1	42.9	50.7	82.4	82.5	53.9	0.7	0.8
2	Kenya	34.4	36.8	40.0	41.2	45.3	50.7	57.4	74.8	78.9	81.7	82.3	56.7	1.0	0.8
3	Ghana	27.5	28.9	29.1	29.4	31.2	32.4	32.6	43.7	56.9	86.7	88.9	44.3	0.8	0.8
4	Egypt	38.3	40.1	45.8	58.8	57.6	65.6	77.2	84.2	90.2	95.5	96.4	68.2	0.5	0.9
5	Nigeria	41.2	43.5	44.0	44.1	45.9	54.2	56.9	65.0	72.7	84.8	85.9	58.0	-0.3	0.7
6	South Africa	35.3	37.6	38.1	38.2	40.0	47.5	50.2	65.2	66.4	78.5	79.6	52.4	-0.2	0.9
7	Tunisia	53.0	55.3	55.8	55.9	57.7	56.4	59.1	53.6	74.1	86.2	87.3	63.1	-0.3	0.7
8	Mauritius	55.9	58.2	58.7	58.8	60.6	80.3	83.0	88.0	84.8	96.9	98.0	74.8	0.1	0.9
9	Rwanda	50.0	52.3	52.8	52.9	54.7	57.5	60.2	69.7	67.9	80.0	81.1	61.7	0.9	0.8
10	Gabon	0.0	2.3	2.8	2.9	4.7	11.2	13.9	31.8	22.3	11.4	12.5	10.7	-0.2	0.8
11	Cabo Verde	0.0	2.3	2.8	2.9	4.7	3.1	5.8	5.1	5.6	17.7	18.8	6.5	0.1	0.7
12	Botswana	14.8	17.1	17.6	17.7	19.5	40.3	43.0	44.0	41.0	53.1	54.2	32.9	0.6	0.8
13	Algeria	14.8	17.1	17.6	17.7	19.5	40.5	43.2	26.2	21.9	34.0	35.1	26.1	-0.7	0.7
14	Djibouti	3.0	5.3	5.8	5.9	7.7	7.2	9.9	6.3	5.6	1.7	2.8	5.6	0.0	0.0
15	Seychelles	8.9	11.2	11.7	11.8	13.6	15.7	18.4	25.9	10.2	13.2	14.3	14.1	0.6	0.4
16	Lesotho	0.0	0.0	0.0	0.0	1.8	6.7	9.4	5.1	6.8	9.1	10.2	4.5	-0.4	0.9
17	Namibia	0.0	0.0	0.0	0.0	1.8	3.9	6.6	12.7	12.0	11.5	12.6	5.5	0.1	0.9
18	Gambia	5.9	8.2	8.7	8.8	10.6	10.9	13.6	28.0	30.0	32.1	33.2	17.3	0.9	0.9
19	Libya	26.5	28.8	29.3	29.4	31.2	19.7	22.4	20.6	25.5	28.8	29.9	26.6	-0.1	-0.2
20	Eswatini	0.1	2.4	2.9	3.0	4.8	7.3	10.0	13.3	16.3	18.2	19.3	8.9	-0.1	1.0
21	Senegal	14.8	17.1	17.6	17.7	19.5	28.7	31.4	30.5	32.2	35.9	37.0	25.6	0.9	0.9
22	Cameroon	38.3	40.6	41.1	41.2	43.0	38.6	41.3	43.2	43.7	45.6	46.7	42.1	0.8	0.8

	Country	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	Cybersecurity maturity level	Correlation of cybersecurity with GDP	Correlation of cybersecurity with Internet penetration
23	Côte d'Ivoire	20.6	22.9	23.4	23.5	25.3	38.9	41.6	45.6	55.7	67.8	68.9	39.5	0.9	0.9
24	Mauritania	11.8	14.1	14.6	14.7	16.5	11.9	14.6	10.7	13.9	18.9	20.0	14.7	0.5	0.3
25	Sao Tome and Principe	3.0	5.3	5.8	5.9	7.7	1.3	4.0	6.4	10.6	15.6	16.7	7.5	0.8	0.7
26	Angola	5.9	8.2	8.7	8.8	10.6	5.1	7.8	9.7	8.0	13.0	14.1	9.1	-0.2	0.6
27	Sudan	41.2	43.5	44.0	44.1	45.9	24.4	27.1	29.4	30.0	35.0	36.1	36.4	-0.1	-0.6
28	Zimbabwe	5.9	8.2	8.7	8.8	10.6	16.5	19.2	18.6	31.5	36.5	37.6	18.4	0.5	0.7
29	Mali	5.9	8.2	8.7	8.8	10.6	3.3	6.0	8.5	8.9	10.1	11.2	8.2	0.4	0.2
30	Sierra Leone	3.0	5.3	5.8	5.9	7.7	11.8	14.5	13.8	20.3	25.3	26.4	12.7	0.0	1.0
31	Uganda	53.0	55.3	55.8	55.9	57.7	50.9	53.6	62.1	65.0	70.0	71.1	59.1	0.9	0.5
32	Zambia	11.8	14.1	14.6	14.7	16.5	26.5	29.2	43.6	63.9	68.9	70.0	34.0	-0.5	0.9
33	Benin	14.8	17.1	17.6	17.7	19.5	4.2	6.9	48.5	75.1	80.1	81.2	34.8	0.9	0.8
34	Guinea-Bissau	0.0	2.3	2.8	2.9	4.7	0.7	3.4	5.5	6.6	9.9	11.0	4.5	0.8	0.8
35	Burkina Faso	29.5	31.8	32.3	32.4	34.2	18.1	20.8	40.0	35.0	40.0	41.1	32.3	0.6	0.4
36	Equatorial Guinea	0.0	0.0	0.0	0.0	0.0	0.0	0.0	3.1	4.2	1.5	2.6	1.0	-0.5	0.5
37	Togo	23.6	25.9	26.4	26.5	28.3	19.1	21.8	8.7	28.2	33.2	34.3	25.1	0.3	0.3
38	Congo	3.0	5.3	5.8	5.9	7.7	1.3	4.0	16.7	9.7	14.7	15.8	8.2	-0.2	0.8
39	Ethiopia	0.0	2.3	2.8	2.9	4.7	24.0	26.7	27.8	22.7	27.7	28.8	15.5	0.9	0.9
40	United Rep. of Tanzania	17.7	20.0	20.5	20.6	22.4	29.0	31.7	64.2	85.6	90.6	91.7	44.9	0.9	0.9
												Average computation	29.1	0.3	0.66

Hot deck imputation method

Sources: ITU data for 2014, 2017, 2018 and 2020 combined with other data using the hot deck imputation method.

Table 11: Cybersecurity data of countries or areas in Latin America and the Caribbean with the highest Internet penetration (Percentage)

	Country or area	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	Cybersecurity maturity level	Correlation of cybersecurity with GDP	Correlation of cybersecurity with Internet penetration
1	Chile	35.3	37.6	38.1	38.2	40.0	34.0	36.7	47.0	56.7	68.8	69.9	45.7	0.5	0.6
2	Puerto Rico	No data													
3	Bahamas	58.9	61.2	61.7	61.8	63.6	11.0	13.7	14.7	14.2	13.4	14.5	35.3	-0.4	-1.0
4	Uruguay	58.9	61.2	61.7	61.8	63.6	62.0	64.7	68.1	69.1	75.2	76.3	65.7	0.4	0.9
5	Argentina	38.3	40.6	41.1	41.2	43.0	45.5	48.2	40.7	44.0	50.1	51.2	44.0	-0.3	0.8
6	Barbados	14.8	17.1	17.6	17.7	19.5	24.6	27.3	17.3	10.8	16.9	18.0	18.3	-0.1	0.3
7	Costa Rica	32.4	34.7	35.2	35.3	37.1	30.9	33.6	22.1	61.4	67.5	68.6	41.7	0.5	0.6
8	Saint Kitts and Nevis	11.8	14.1	14.6	14.7	16.5	3.9	6.6	6.5	6.3	12.4	13.5	11.0	-0.7	-0.4
9	Trinidad and Tobago	17.7	20.0	20.5	20.6	22.4	15.2	17.9	18.8	16.1	22.2	23.3	19.5	0.0	0.2
10	Brazil	67.7	70.0	70.5	70.6	72.4	56.6	59.3	57.7	90.5	96.6	97.7	73.6	-0.5	0.6
11	Antigua and Barbuda	8.9	11.2	11.7	11.8	13.6	15.2	17.9	24.7	22.4	15.6	16.7	15.4	1.0	0.8
12	Ecuador	32.4	34.7	35.2	35.3	37.1	43.9	46.6	36.7	20.2	26.3	27.4	34.2	-0.1	-0.3
13	Paraguay	17.7	20.0	20.5	20.6	22.4	29.9	32.6	60.3	51.0	57.1	58.2	35.5	0.4	0.9
14	Mexico	29.5	31.8	32.3	32.4	34.2	63.3	66.0	62.9	75.6	81.7	82.8	53.8	-0.2	0.9
15	Dominica	3.0	5.3	5.8	5.9	7.7	5.6	10.0	1.9	3.2	4.2	5.3	5.3	-0.2	-0.1
Average computation													35.6	0.3	0.6

Hot deck imputation method

Sources: ITU data for 2014, 2017, 2018 and 2020 combined with other data using the hot deck imputation method.

Table 12: Cybersecurity data of countries or areas in Asia, including Western Asia, with the highest Internet penetration (Percentage)

	Country or area	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	Cybersecurity maturity level	Correlation of cybersecurity with GDP	Correlation of cybersecurity with Internet penetration
1	United Arab Emirates	32.4	34.7	35.2	35.3	37.1	53.9	56.6	80.7	86.0	98.1	99.2	59.0	0.4	0.9
2	Kuwait	3.0	5.3	5.8	5.9	7.7	7.7	10.4	60.0	70.0	75.1	76.2	29.7	-0.5	0.8
3	Qatar	58.9	61.2	61.7	61.8	63.6	64.9	67.6	86.0	89.4	94.5	95.6	73.2	-0.2	0.6
4	Bahrain	26.5	28.8	29.3	29.4	31.2	44.0	46.7	58.5	72.8	77.9	79.0	47.6	0.8	0.7
5	Republic of Korea	60.7	65.1	68.9	70.6	73.5	75.2	78.2	87.3	90.2	98.5	99.1	78.8	0.9	0.9
6	Saudi Arabia	26.5	28.8	29.3	29.4	31.2	54.2	56.9	88.1	94.4	99.5	99.9	58.0	0.5	0.7
7	Oman	73.6	75.9	76.4	76.5	78.3	84.4	87.1	86.8	90.9	96.0	97.1	83.9	-0.2	0.9
8	Brunei Darussalam	35.3	37.6	38.1	38.2	40.0	49.7	52.4	62.4	51.0	56.1	57.2	47.1	-0.7	0.9
9	Japan	67.7	70.0	70.5	70.6	72.4	75.9	78.6	88.0	92.7	97.8	98.9	80.3	-0.4	0.6
10	Hong Kong, China	58.9	61.2	61.7	61.8	63.6	67.7	73.2	76.9	79.4	82.6	83.7	70.0	0.9	0.9
11	Singapore	64.8	67.1	67.6	67.7	69.5	89.8	92.5	89.8	93.4	98.5	99.6	81.8	0.9	0.8
12	Israel	73.6	67.1	67.6	67.7	69.5	66.4	69.1	78.3	85.8	90.9	92.0	74.5	0.9	0.9
13	Malaysia	73.6	75.9	76.4	76.5	78.3	86.6	89.3	89.3	93.0	98.1	99.2	85.1	0.7	0.9
14	Macao, China	No data											0.0		
15	Kazakhstan	14.7	17.0	17.5	17.6	19.4	32.5	35.2	77.8	88.1	93.15	94.3	46.1	0.9	0.9
												Average computation	61.0	0.4	0.82

Hot deck imputation method

Sources: ITU data for 2014, 2017, 2018 and 2020 combined with other data using the hot deck imputation method.

vi. Data validation

Data were validated for quality and consistency through rigorous review and pairwise comparison with data from other sources. For example, GDP data from 2011 to 2021 were sourced and validated on the World Bank Open Data Platform and pairwise checked with data from DataReportal. Data on Internet penetration were sourced from the regulators' websites and therein validated. In certain instances, when data were not available on the regulators' websites, data from DataReportal were used.

vii. Data analyses

Data obtained were analysed in order to determine whether there was a significant correlation between national GDP and Internet penetration and cybersecurity in the selected countries or areas. The Pearson Correlation coefficient of GDP data and those of Internet penetration and cybersecurity were computed. The data are presented in figures II–XIV.

Note: Positive correlation is measured on a 0.1 to 1.0 scale. Weak positive correlation would be in the range of 0.1 to 0.3, moderate positive correlation from 0.3 to 0.5 and strong positive correlation from 0.5 to 1.0. The stronger the positive correlation, the more likely the subject data are to move in the same direction.

Detailed analyses show that:

1. In Africa:

- A 10 per cent increase in Internet penetration yielded average per capita growth of between $31 and $256 (between 1 and 8.2 per cent of per capita GDP) for the sample space of 40 countries (see subsection 5.2, equation 2). When the sample space of the top 15 countries was used, it was between 4.8 and 7.4 per cent. The highest 10 per cent increase in Internet penetration yield was found in Seychelles ($1,632 per capita), while the lowest yield was found in Equatorial Guinea (-$4,230 per capita).

- A 10 per cent increase in cybersecurity maturity yielded average per capita growth of between $20 and $169 (between 0.66 and 5.4 per cent of per capita GDP) for the sample space of 40 countries (see subsection 5.2, equation 3). When the sample space of the top 15 countries was used, it was between 3.36 and 5.18 per cent. The country with the highest 10 per cent increase in cybersecurity maturity yield was Seychelles, with $653 per capita, while the country with the lowest yield was Equatorial Guinea, with (-$2,115 per capita).

- Internet penetration correlates with GDP at 0.32 (32 per cent), a positive correlation for which 68 per cent (27 countries) have positive Internet penetration correlation with GDP.

- Cybersecurity maturity correlates with GDP at 0.3 (30 per cent), a weak positive correlation for which 63 per cent (25 countries) have positive cybersecurity maturity correlation with GDP.

- Cybersecurity correlates with Internet penetration at 0.66 (66 per cent), a strong correlation for which 93 per cent (37 countries) have positive cybersecurity correlation with Internet penetration.

2. In Latin America and the Caribbean:

- A 10 per cent increase in Internet penetration yielded average per capita growth of between $447 and $754 (between 3 and 5.1 per cent of per capita GDP). The highest 10 per cent increase in Internet penetration yield was found in Saint Kitts and Nevis, ($1,463 per capita), while the lowest yield was found in Brazil (-$1,340 per capita).

- A 10 per cent increase in cybersecurity maturity yielded average per capita growth of between $268 and $452 (between 1.8 and 3

per cent of per capita GDP). The highest 10 per cent increase in cybersecurity maturity yield was found in Antigua and Barbuda ($1,135 per capita), while the lowest yield was found in the Bahamas (-$1,258 per capita).

- Internet penetration correlates with GDP at 0.30 (30 per cent), a weak positive correlation for which 47 per cent (seven countries or areas) have positive Internet penetration correlation with GDP.

- Cybersecurity maturity correlates with GDP at 0.3 (30 per cent), a weak positive correlation for which 36 per cent (five countries or areas) have positive cybersecurity maturity correlation with GDP.

- Cybersecurity correlates with Internet penetration at 0.6 (60 per cent), a strong correlation for which 71 per cent (11 countries or areas) have positive cybersecurity correlation with Internet penetration.

3. In Asia, including Western Asia:

- A 10 per cent increase in Internet penetration yielded average per capita growth of between $1,898.15 and $4,149.20 (between 5.5 and 12 per cent of per capita GDP). The highest 10 per cent increase in Internet penetration yield was found in Israel ($11,786 per capita), while the lowest yield was found in Japan (-$7,357 per capita).

- A 10 per cent increase in cybersecurity maturity yielded per capita average growth of between $1,518.52 and $3,319.36 (between 4.5 and 9.8 per cent of per capita GDP). The highest 10 per cent increase in cybersecurity maturity yield was found in Israel, ($10,607 per capita), while the lowest yield was found in Japan, (-$4,414 per capita).

- Internet penetration correlates with GDP at 0.25 (25 per cent), a weak positive correlation for which 60 per cent (nine countries or areas) have positive Internet penetration correlation with GDP.

- Cybersecurity maturity correlates with GDP at 0.4 (40 per cent), a weak positive correlation for which 64 per cent (nine countries or areas) have positive cybersecurity maturity correlation with GDP.

- Cybersecurity correlates with Internet penetration at 0.82 (82 per cent), a strong correlation for which 100 per cent of countries or areas have positive cybersecurity correlation with Internet penetration.

When data for Africa were computed to match the sample population of the top 15 countries or areas with the highest Internet penetration in Latin America and the Caribbean and in Asia, including Western Asia, the result for Africa showed a slight increase in per capita income to $363 from $256 for a 10 per cent increase in Internet penetration. This is still far short of the per capita income of $754 and $4,149 in Latin America and the Caribbean and in Asia, including Western Asia, respectively. Conversely, a sample space of 40 out of 54 countries in Africa (74 per cent) provides more reliable estimates than the sample space of 15 (28 per cent).

Data from table 13 show a strong cybersecurity correlation with Internet penetration, which indicates that cybersecurity is a measure of Internet technology, its acceptability by the people and its positive impact on their income.

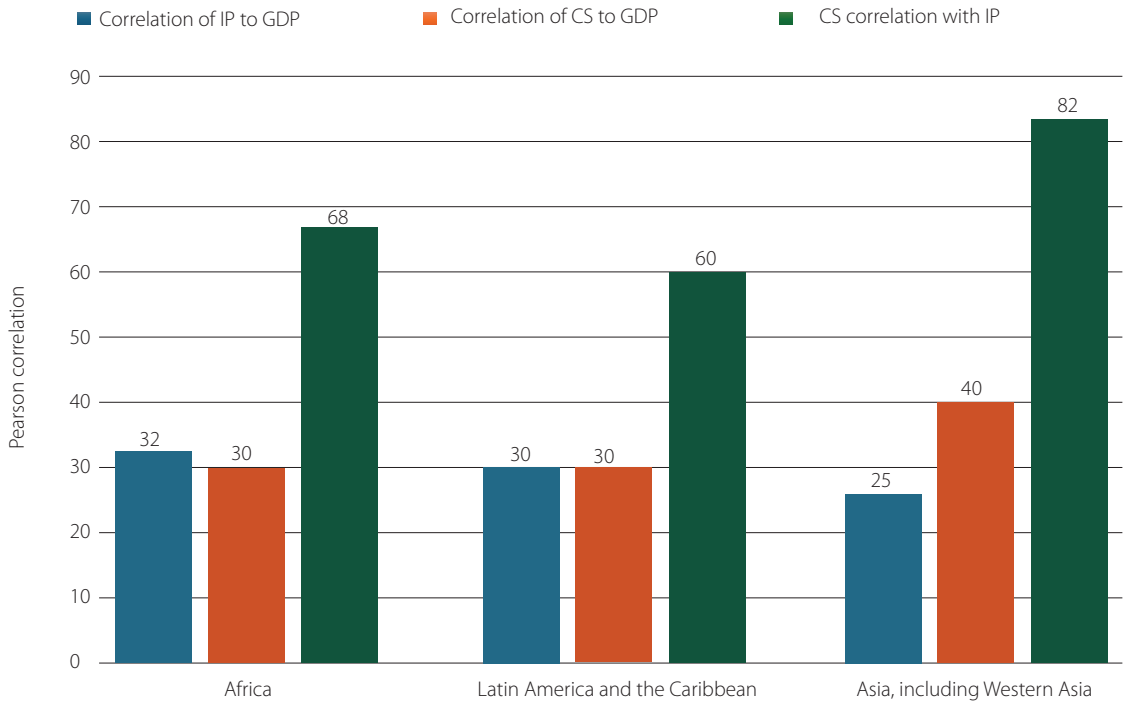
Table 13: Gross domestic product, Internet penetration and cybersecurity correlation with the cybersecurity maturity index in countries or areas in Africa, Latin America and the Caribbean, and Asia, including Western Asia

Continent	Sample population (A)	Correlation of Internet penetration to GDP (percentage) (B)	Correlation of cybersecurity to GDP (percentage) (C)	Cybersecurity correlation with Internet penetration (percentage) (D)	Average per capita GDP resulting from 10 per cent increase in Internet penetration (US dollars) (E)	Average per capita GDP resulting from10 per cent increase in Internet penetration positive correlation countries or areas (US dollars) (F)	Per capita increase resulting from 10 per cent increase in Internet penetration (low percentage – high percentage) (G)–(H)	Per capita increase resulting from 10 per cent increase in cybersecurity (low percentage – high percentage) (DxG)–(DxH)	Cybersecurity maturity index (percentage)
Africa	40	32	30	66	31.00	256.00	1.0–8.2	0.66–5.4	29.1
Latin America and the Caribbean	15	30	30	60	447.00	754.00	3–5.1	1.8–3	35.6
Asia, including Western Asia	15	25	40	82	1 898.15	4 149.20	5.5–12	4.5–9.8	61

Source: author's compilation from ECA data.

Using the same population sample of 15 countries or areas in Africa, in Latin America and the Caribbean and in Asia, including Western Asia, a 10 per cent increase in cybersecurity maturity delivered per capita GDP increases of between 3.36 and 5.18 per cent for Africa, 1.8 and 3 per cent for Latin America and the Caribbean and 4.5 and 9.8 per cent for Asia, including Western Asia (see table 14), provided that there is a continuum in the relevant governance policies of a given country or area so as to avoid political and economic instability leading to policy somersaults, capital flight and loss of confidence in the economy.

Figure II: Gross domestic product, Internet penetration and cybersecurity correlations in 40 countries or areas in Africa, 15 in Latin America and the Caribbean, and 15 in Asia, including Western Asia (Percentage)



Source: author's compilation, based on ECA data.

Abbreviations: IP, Internet penetration; CS, cybersecurity.

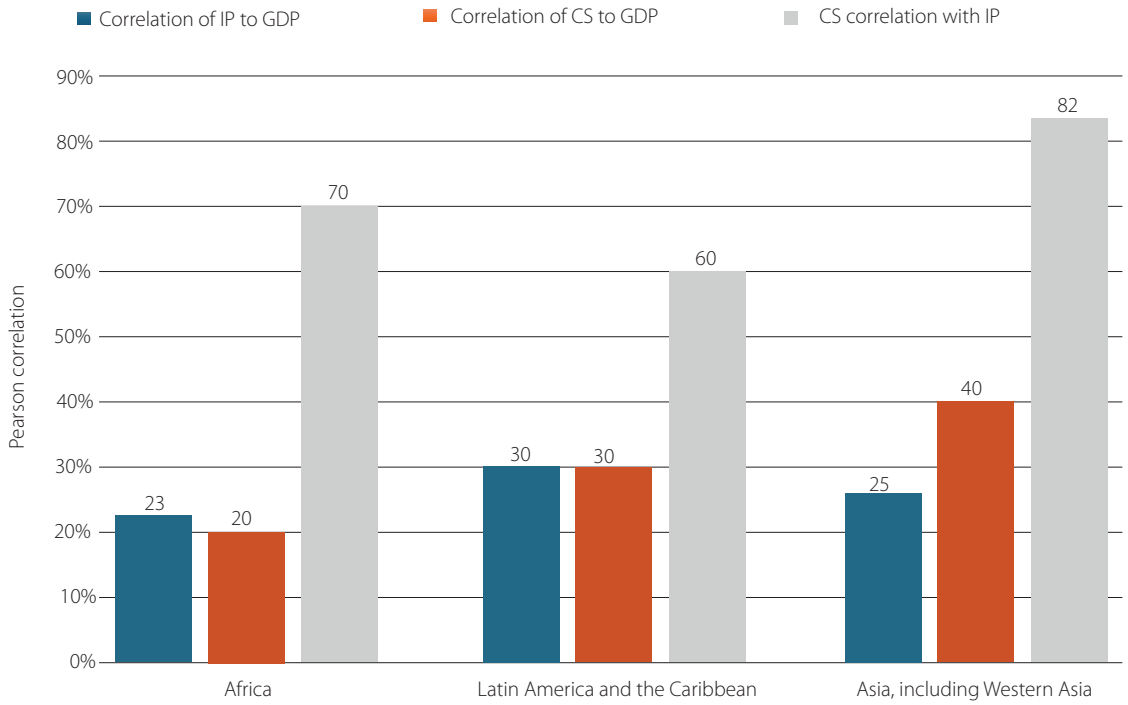
Table 14: Correlation between gross domestic product, Internet penetration and cybersecurity in 15 countries or areas from each continent

Continent	Sample population (A)	Correlation of Internet penetration to GDP (percentage) (B)	Correlation of cybersecurity to GDP (percentage) (C)	Cybersecurity correlation with Internet penetration (percentage) (D)	Average per capita GDP of positive correlation countries or areas resulting from 10 per cent increase in Internet penetration (US dollars) (E)	Per capita increase resulting from 10 per cent increase in Internet penetration (low percentage – high percentage) (F)–(G)	Per capita increase resulting from 10 per cent increase in cybersecurity (low percentage - high percentage) (DxF)–(DxG)
Africa	15	23	20	70	233	4.8–7.4	3.4–5.2
Latin America and the Caribbean	15	30	30	60	754	3.0–5.1	1.8–3.0
Asia, including Western Asia	15	25	40	82	4 149	5.5–12.0	4.5–9.8

Source: author's compilation, based on ECA data.

Using the same population sample of 15 countries or areas each in Africa, Latin America and the Caribbean and Asia, including Western Asia, figure III shows the correlation between gross domestic product, Internet penetration and cybersecurity.

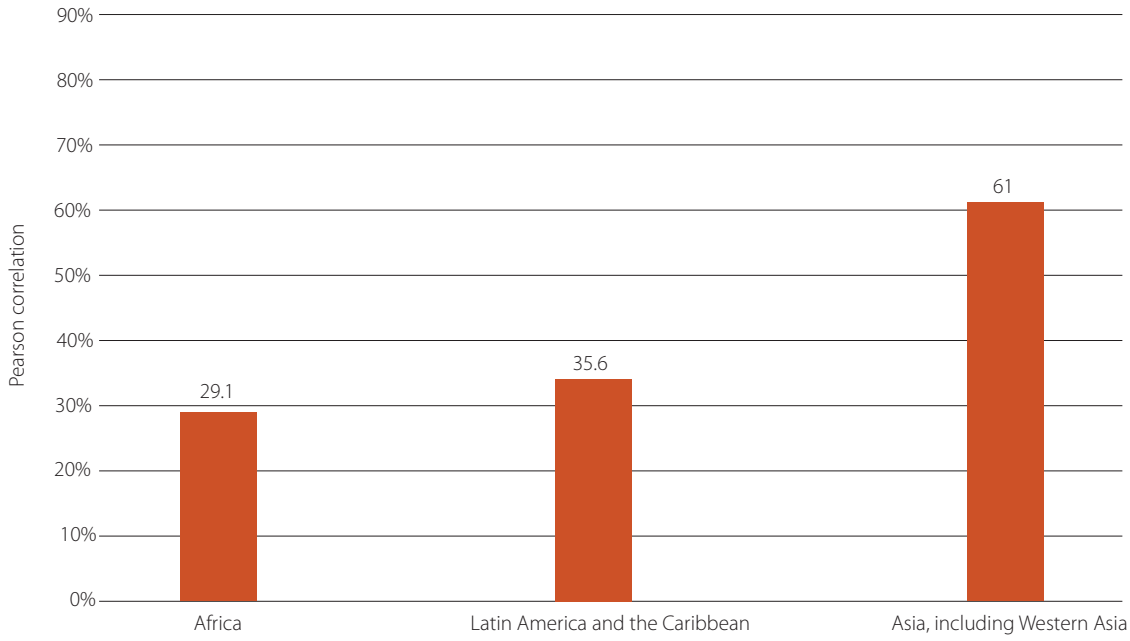
Figure III : Gross domestic product, Internet penetration and cybersecurity correlation in 15 countries or areas from each continent (Percentage)



Source: author's compilation, based on ECA data.

Abbreviations: IP, Internet penetration; CS, cybersecurity.

Figure IV: Regional cybersecurity maturity index (Percentage)



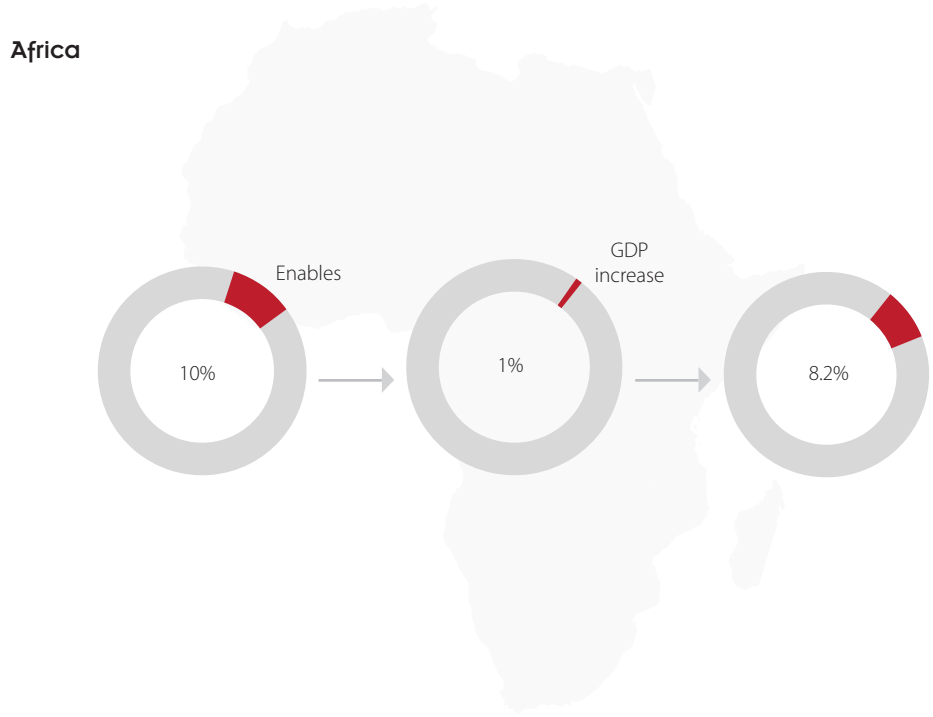
Source: author's compilation, based on ECA data.

iv. Data visualization

When the 40 countries sample space for Africa is used, a 10 per cent increase in Internet penetration enables between 1 and 8.2 per cent increase in GDP per capita (see figure V).

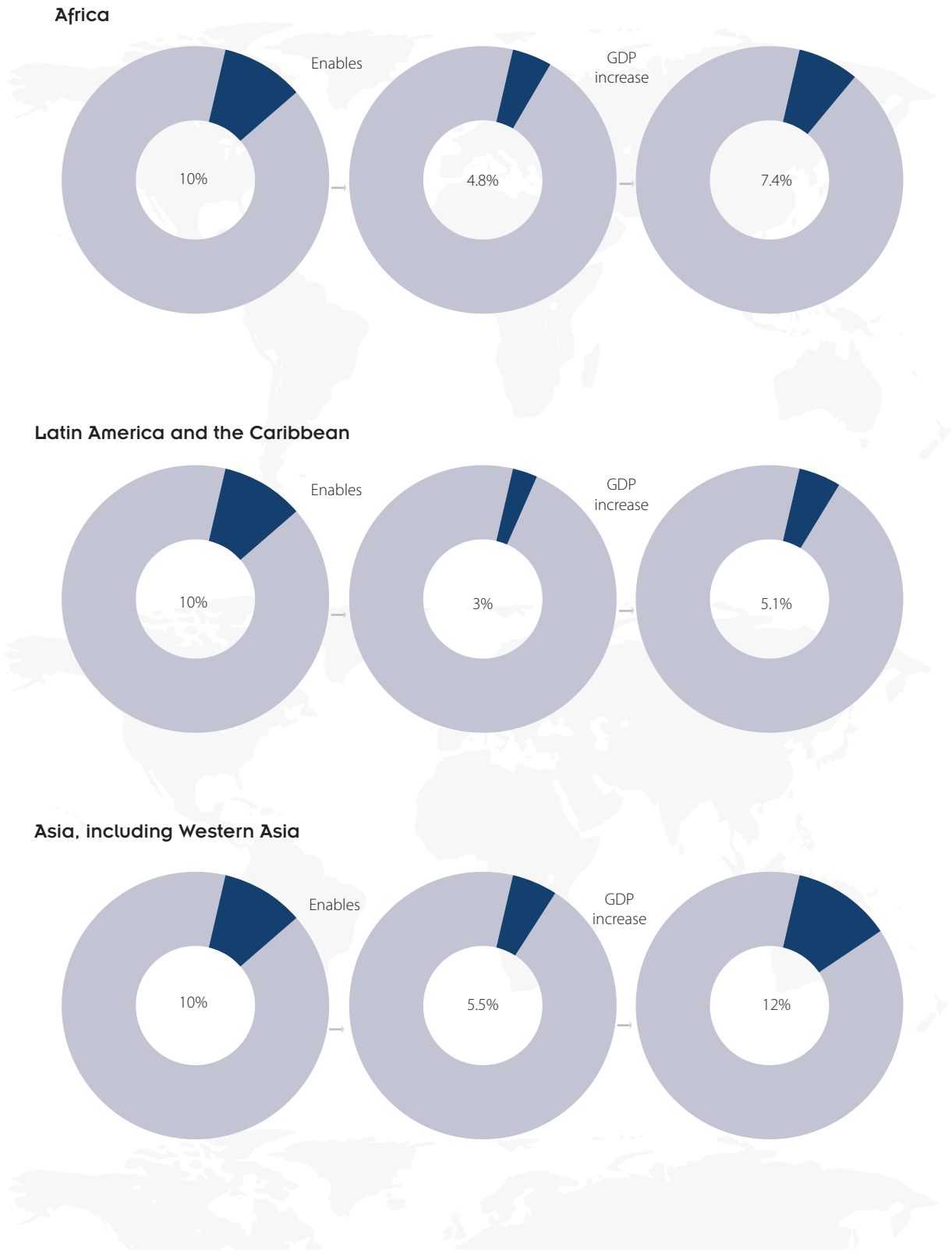
Figure VI shows the Internet penetration when sample space is 15 countries or areas in each region. In Africa, a 10 per cent increase in Internet penetration enables between 4.8 and 7.4 per cent GDP growth. In Latin America and the Caribbean, it enables between 3 and 5.1 per cent GDP growth, and in Asia, including Western Asia, between 5.5 and 12 per cent GDP growth.

Figure V : Internet penetration and gross domestic product growth in 40 African countries



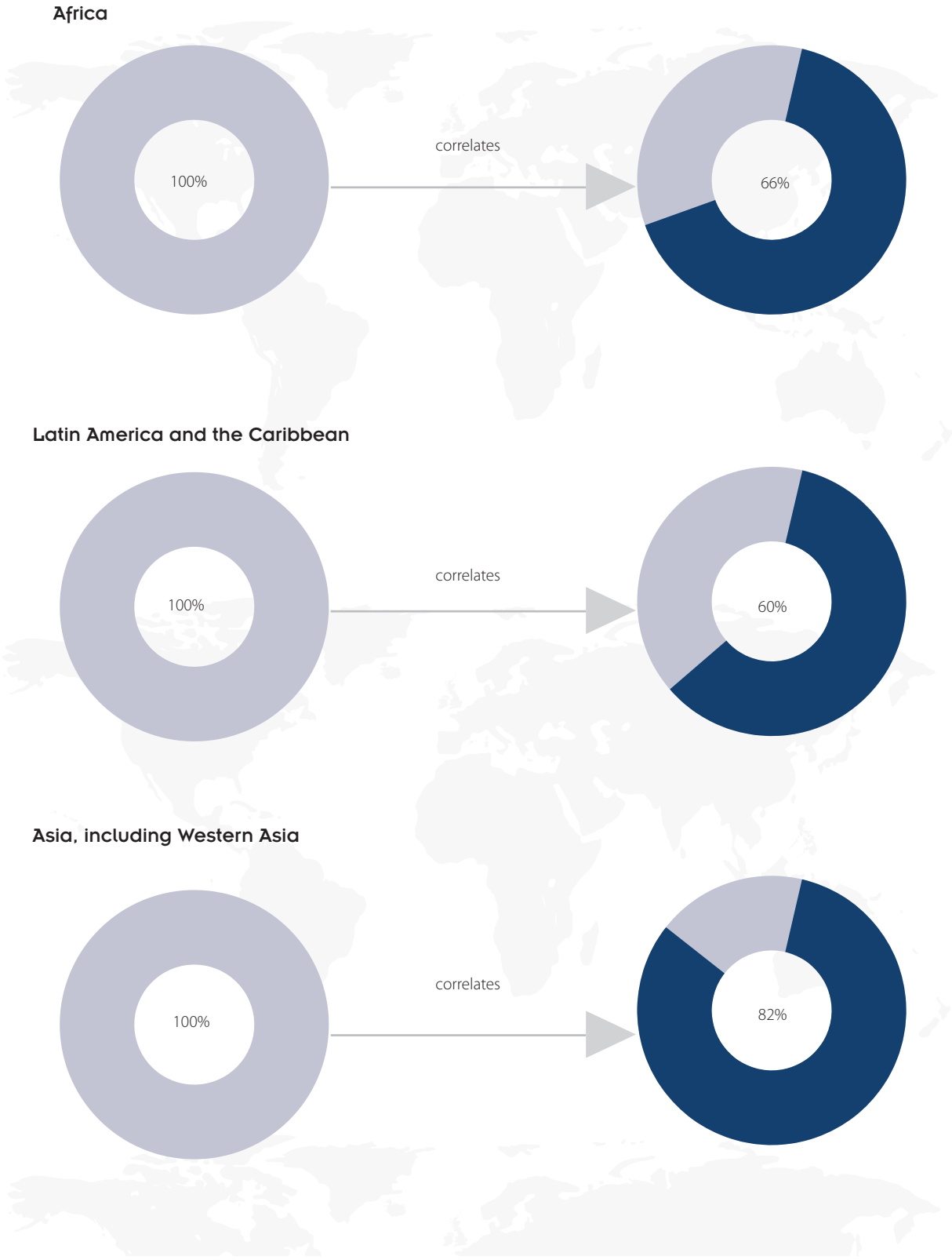
Source: author's compilation, based on ECA data.

Figure VI : Internet penetration and gross domestic product growth on the three continents (Percentage)



Source: author's compilation, based on ECA data.

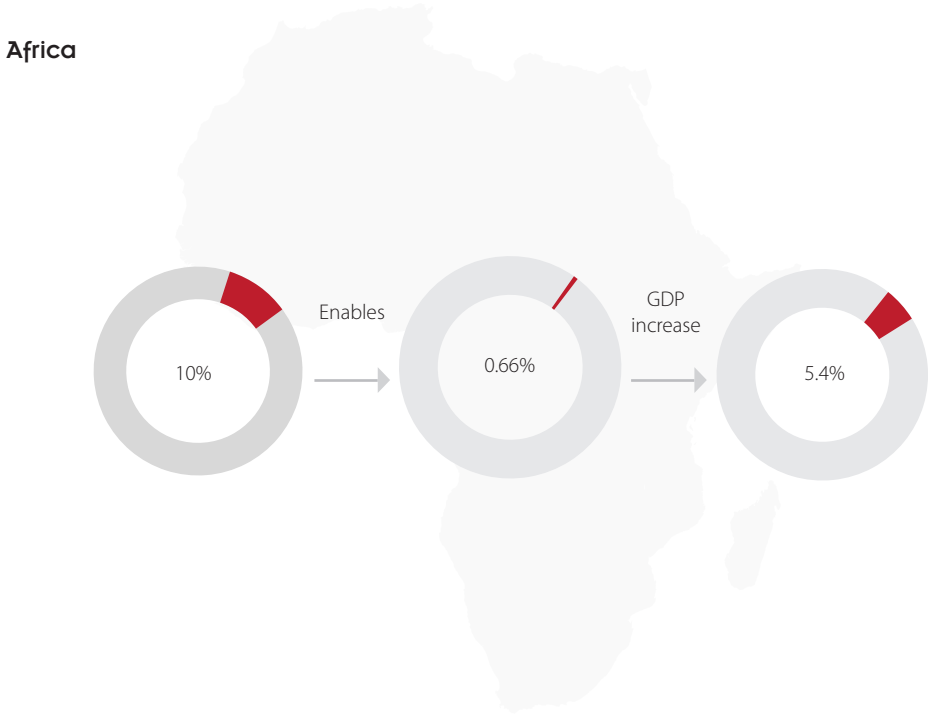
Figure VII : Correlation between Internet penetration and cybersecurity (Percentage)



Source: author's compilation, based on ECA data.

When the 40 countries sample space for Africa is used in the computation, a 10 per cent increase in cybersecurity maturity delivers a per capita GDP increase of between 0.66 and 5.4 per cent (see figure VIII).

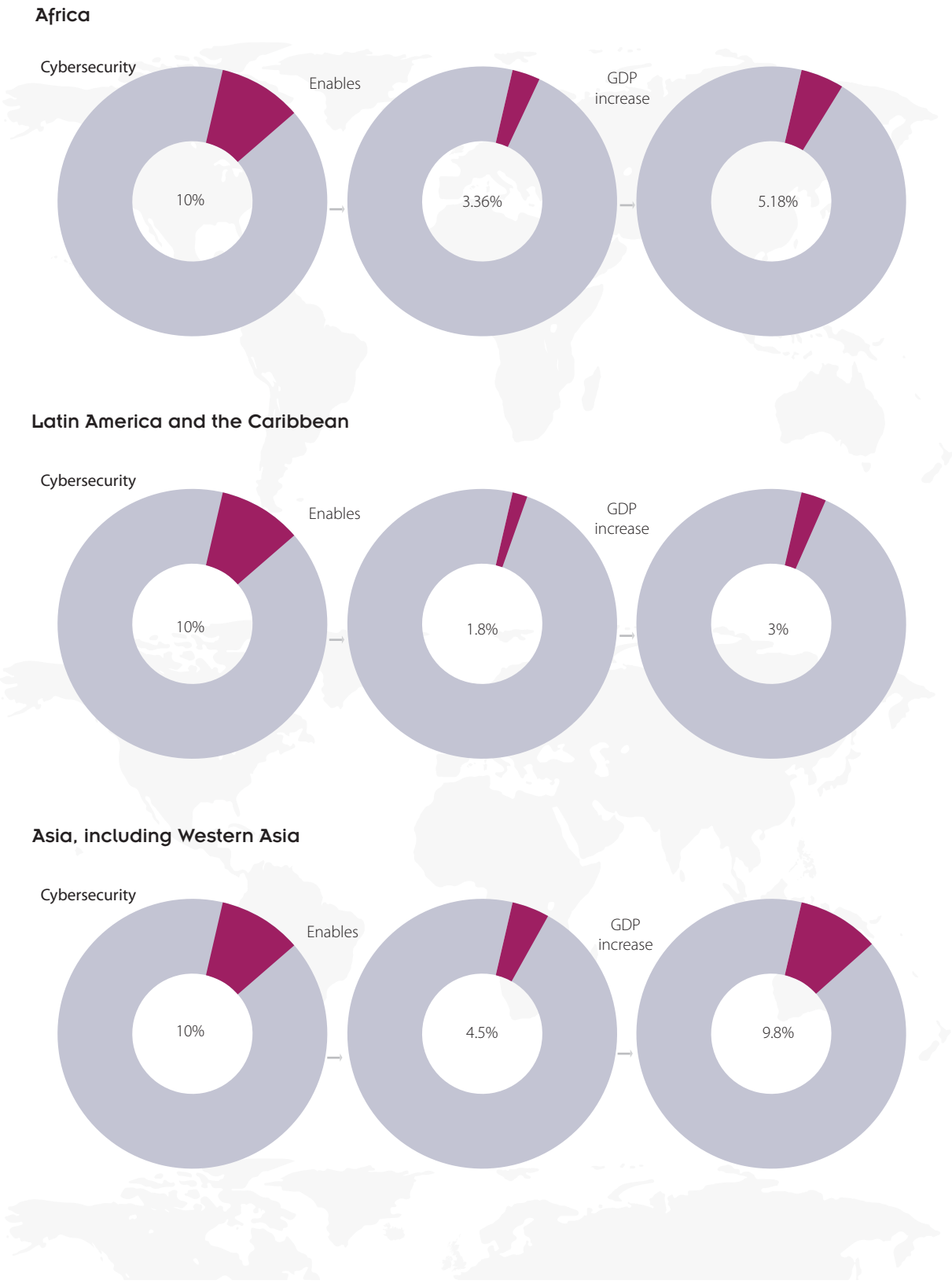
Figure VIII : Cybersecurity and gross domestic product growth in 40 African countries



Source: author's compilation, based on ECA data.

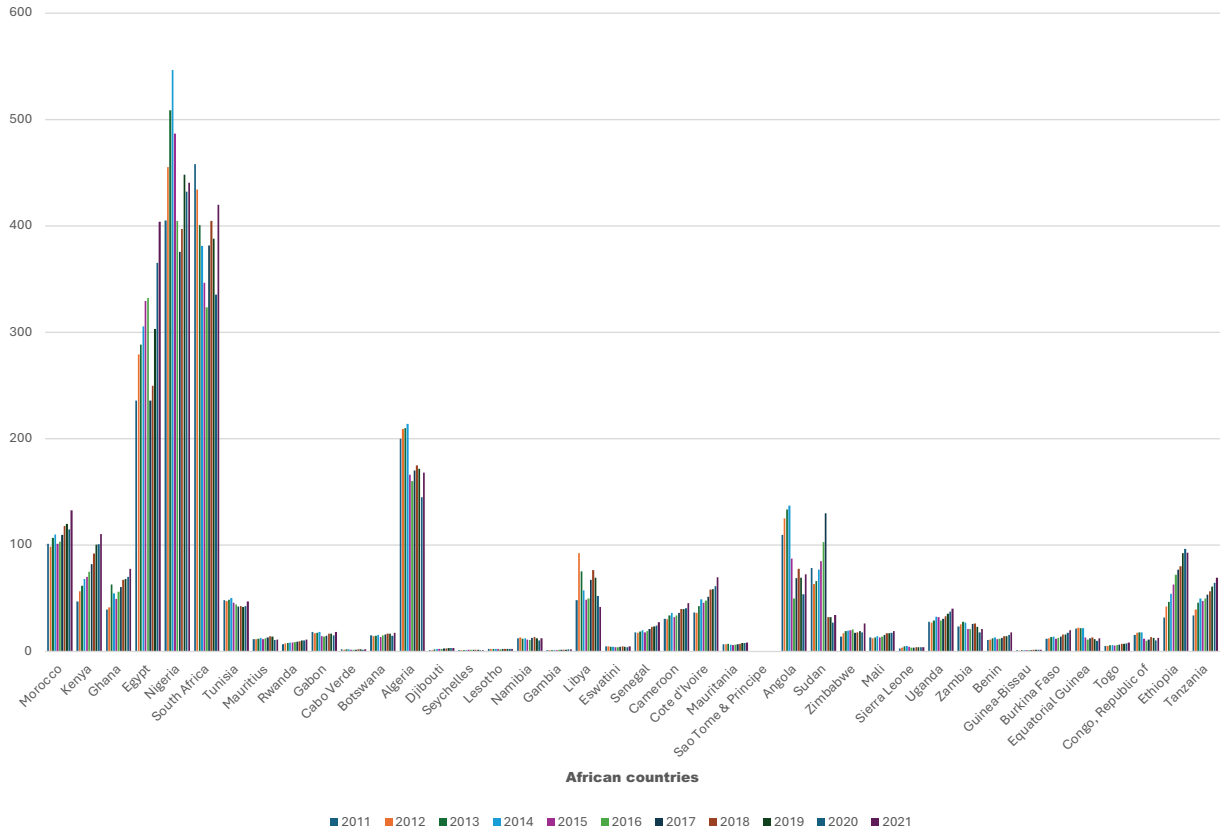
When the sample space is 15 countries or areas, a 10 per cent increase in cybersecurity maturity enables between 3.36 and 5.18 per cent GDP growth in Africa (see figure IX). In Latin America and the Caribbean, it enables between 1.8 and 3 per cent GDP growth, and in Asia, including Western Asia, between 4.5 and 9.8 per cent GDP growth.

Figure IX: Cybersecurity and gross domestic product growth on the three continents



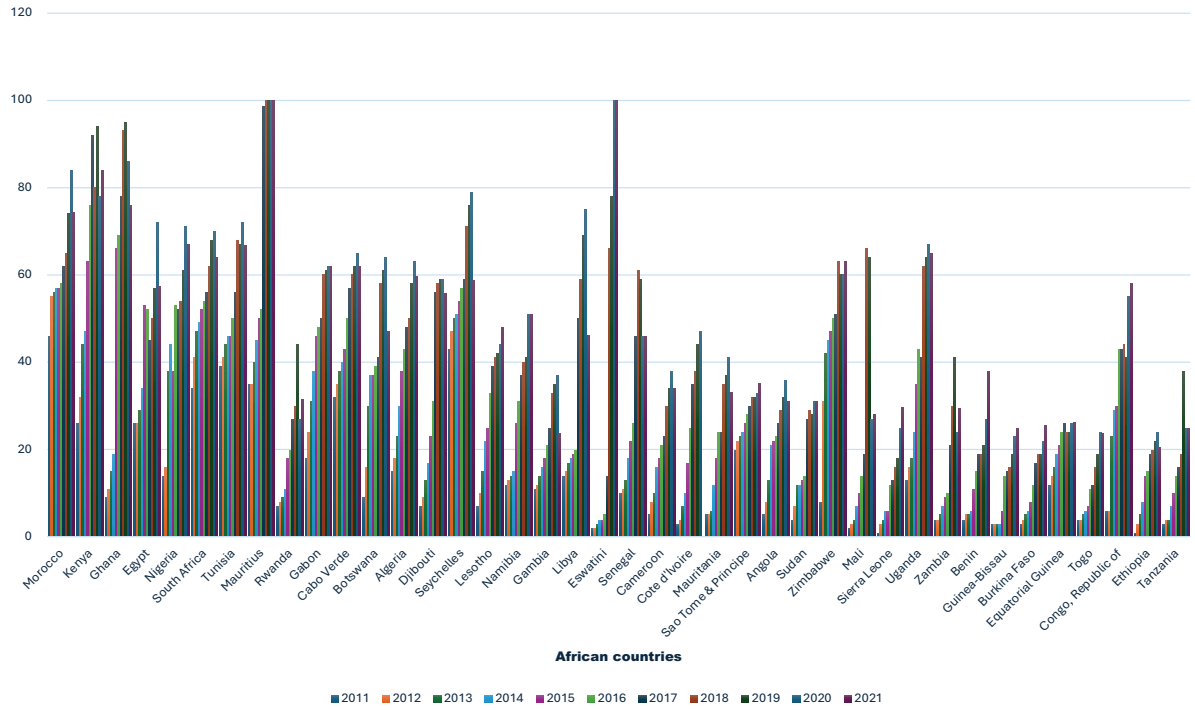
Source: author's compilation, based on ECA data.

Figure X : Gross domestic product growth in 40 African countries, 2011–2021 (Billions of United States dollars)



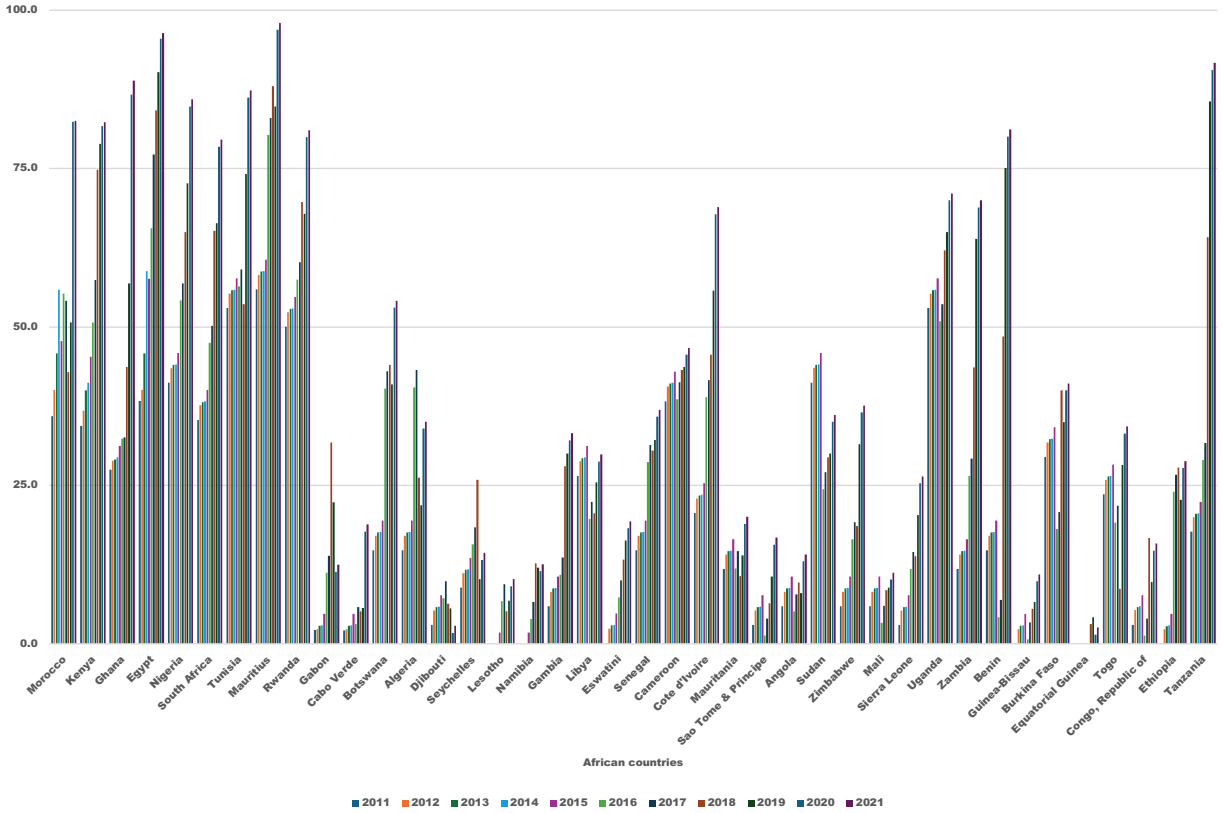
Source: World Bank Open Data Platform (2011–2020); DataReportal (2021). Actual values may be cross-referenced against figures in table 4.

Figure XI: Internet penetration growth in 40 African countries, 2011–2021 (Percentage)



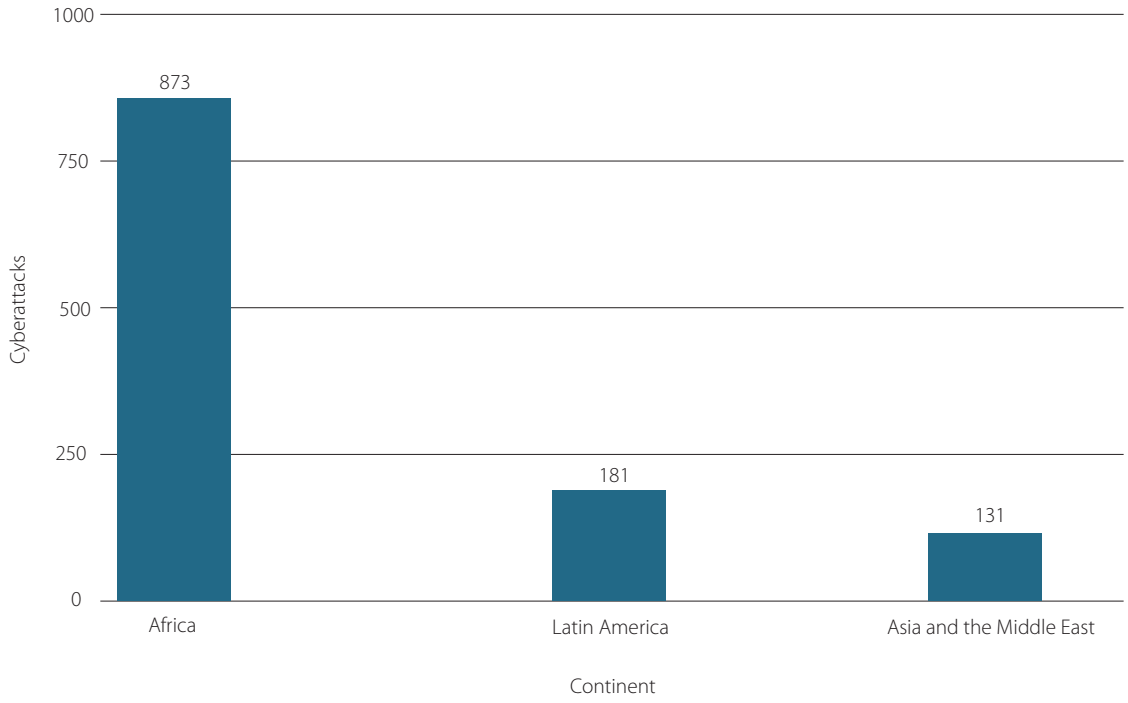
Source: World Bank and national telecommunications regulators of Benin, the Congo, Eswatini, Ghana, Kenya, Lesotho, Mauritius, Nigeria, Rwanda, Sierra Leone, South Africa and Uganda (2011–2021). Actual values may be cross-referenced against figures in table 7.

Figure XII: Cybersecurity maturity growth in 40 African countries, 2011–2021 (Percentage)



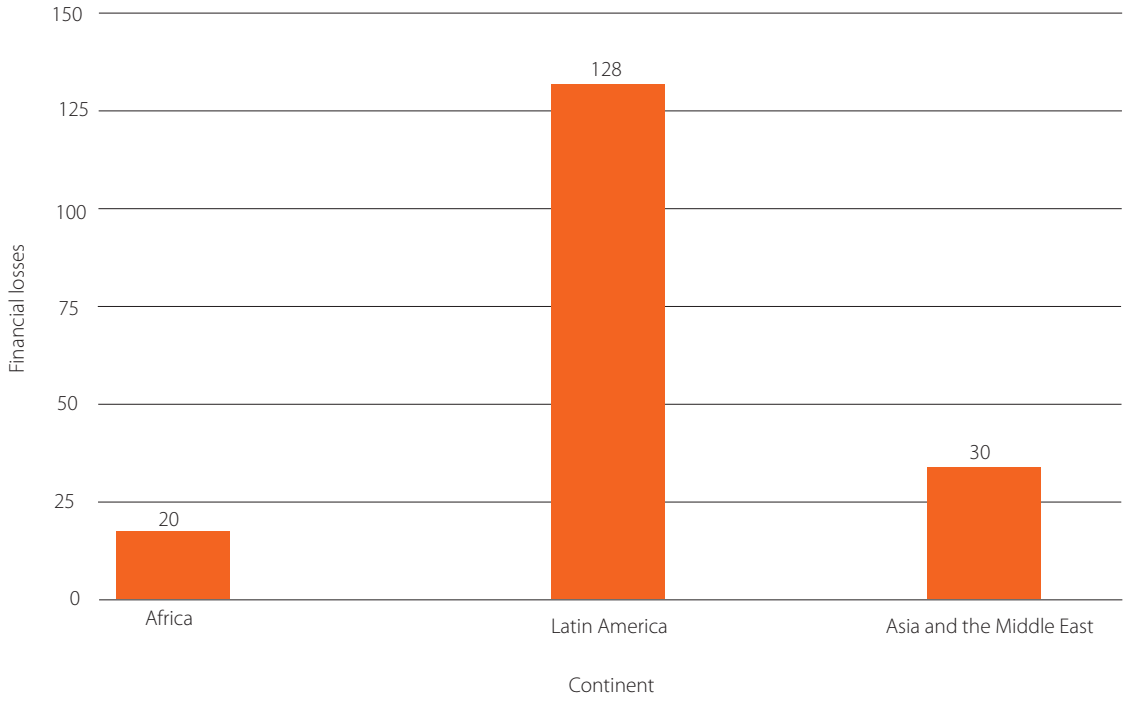
Source: author's compilation, based on ECA data. Actual values may be cross-referenced against figures in table 7.

Figure XIII: Number of cyberattacks (Millions)



Source: author's compilation, based on ECA data.

Figure XIV : Cyberattacks and financial losses (Billions of United States dollars)



Source: author's compilation, based on ECA data.

Table 15: Cyberattacks and financial losses

Continent	Number of countries or areas in sample population	Number of cyberattacks (millions)	Financial losses (billions of United States dollars)
Africa	40	873	20
Latin America and the Caribbean	15	181	128
Asia, including Western Asia	15	131	30

Published data show that Internet cyberattacks and financial losses in Africa for the period 2011–2021 amounted to 873 million and $20 billion, respectively (see table 15). By estimates, the numbers recorded were less than 10 per cent of the actual assuming non-disclosure of many incidents in the absence of legal requirements for disclosure. In Latin America and the Caribbean, the number of cyberattacks and financial losses for the same period amounted to 181 million and $128 billion, respectively; and in Asia, including Western Asia, the number of attacks and financial losses were 131 million and $30 billion, respectively. Although data show that, of the three regions, Latin America and the Caribbean suffered the highest financial losses as a result of cyberattacks, Africa has the weakest cybersecurity maturity index at 29.1 per cent, followed by Latin America and the Caribbean at 35.6 per cent, while Asia, including Western Asia have the strongest cybersecurity maturity index at 61 per cent (see figure IV), with the lowest financial losses per capita.

v. Data evaluation

Data used in the present report were taken from primary sources, including the World Bank, national telecommunications regulators and ITU, and the United Nations system entities responsible for cybersecurity. Those primary sources provided data on GDP, Internet penetration and cybersecurity, respectively, for the evaluation to be carried out. Secondary data sources include DataReportal

and Internet World Stats, which provided pairwise comparison for validation purposes.

The hot deck imputation method was used to account for the missing years in cybersecurity data, and best efforts were made to ensure the use of best fit data approximation for the missing data series for 2011, 2012, 2013, 2015, 2016, 2019 and 2021. The Internet penetration and cybersecurity correlation result reflects the true sense of the connection of cybersecurity maturity to confidence that enables growth in Internet penetration.

6. Design, development and deployment of an analytical platform

i. Introduction

The need for a dynamic development platform in order to view and analyse development data as they evolve is the fulcrum of the web-based data analytics platform. Through a universal resource locator (URL), the outcome of the present research, along with current and future data on GDP, Internet penetration and cybersecurity, will be available on the platform.

ii. Analytics platform

The objective of the data analytics platform is to create an online data-driven platform that reflects changes in national and continental development data relating to GDP, Internet penetration and cybersecurity and the correlation between them; to reflect the progress made towards cybersecurity for development in the fourth industrial revolution; and to utilize the platform as an important management reference point on cybersecurity.

iii. Development structure and framework

The online analytics platform is a content management system designed to project the data used for research and to display the results obtained in a clear way. It is also designed to be a framework for data analysis for periods beyond the coverage of the present research. The platform enables viewers to analyse such development data as GDP, Internet penetration and cybersecurity trends for each of the 70 countries or areas assessed in the present report. The platform is available at https://cd4ir.africa.

iv. Sustainability

The URL for the platform is to be sustained through existing online platform frameworks managed by the owners of the present research.

Conclusion

i. Results of analyses

As security offline is critical to economic development, so is cybersecurity critical to Internet-enabled economic development activities, especially considering the fast pace of the fourth industrial revolution. While the results of the present research indicate a positive Internet penetration and cybersecurity correlation with development across the regions under study, the results also reveal that, when the 40 countries sample space for Africa was used in the computation, a 10 per cent increase in cybersecurity maturity delivered a per capita GDP increase of between 0.66 and 5.4 per cent. The percentage per capita output from Africa, compared with the countries and areas in Latin America and the Caribbean and in Asia, including Western Asia was relatively close at 15 country or area sample space parity. In that regard, a 10 per cent increase in cybersecurity maturity in Africa yielded between 3.36 and 5.18 per cent of per capita GDP. In Latin America and the Caribbean, the percentage increase was between 1.8 and 3 per cent, and in Asia, including Western Asia, between 4.5 and 9.8 per cent.

Further results of the research include the following:

- Some 63 per cent (25 out of 40) of African countries have positive cybersecurity correlation with GDP. This implies that ECA efforts at mainstreaming cybersecurity in Africa is yielding results, but more needs to be done with regard to the remaining 27 per cent of African countries.

- Some 93 per cent (37 out of 40) of African countries have positive cybersecurity correlation with Internet penetration. This is an indication that the more Internet penetration grows, the higher the country's cybersecurity maturity.

- A 10 per cent increase in Internet penetration yields average per capita growth of between $31 and $256 (between 1 and 8.2 per cent of per capita GDP) for the sample space of 40 countries. When the sample space is the top 15 countries, it is between 4.8 and 7.4 per cent. Seychelles has the highest 10 per cent increase in Internet penetration yield ($1,632 per capita), while Equatorial Guinea has the lowest yield (-$4,230 per capita). Compared with other regions, the low per capita output in Africa is a reflection of the lack of proportionate increase in income, implying that African countries need to diversify their income base and boost their intra-African trade. One of the vehicles to achieve that is the African Continental Free Trade Area.

Internet cyberattacks and financial losses in Africa during the period 2011–2021 amounted to 873 million and $20 billion, respectively. By estimates, the numbers recorded were less than 10 per cent of the actual assuming non-disclosure of many incidents in the absence of legal requirements for disclosure. In Latin America and the Caribbean, the number of cyberattacks and financial losses were 181 million and $128 billion, respectively. In Asia, including Western Asia, the number of attacks and financial losses were 131 million and $30 billion, respectively. Although data show that, of the three regions, Latin America and the Caribbean suffered the highest financial losses as a result of cyberattacks, Africa has the weakest cybersecurity maturity index at 29.1 per cent, followed by Latin America and the Caribbean at 35.6 per cent, while Asia, including Western Asia have the strongest cybersecurity maturity index at 61 per cent, with the lowest financial losses per capita. This implies that the stronger a country's or area's cybersecurity posture, the lower the financial losses per capita. Accordingly, countries and areas need to take cybersecurity seriously in order to reduce losses if not completely eliminate them.

ii. Recommendations

In the light of the above research, the following recommendations are made:

1. Countries and areas need to establish a stable and accountable national or organizational governance system over a sustained period of time for cybersecurity to have stronger correlation with development. As confidence and trust in doing business and moving workflow online reflect online security assurance, it is important to note that such assurance is what sustains continuous investment in Internet-enabled businesses and thus, boosts the economic productivity necessary to increase per capita income.

2. Countries and areas need to take their cybersecurity maturity seriously and are encouraged to conduct regular self-assessments. Important regulations, laws and conventions, such as the African Union Convention on Cyber Security and Personal Data Protection, adopted in 2014 in Malabo, should be signed and ratified by other countries without delay, with mechanisms put it place for its follow-up implementation.

3. Laws requiring disclosure of cyberattacks and losses by corporate entities and individuals should be enacted in order to promote transparency and accountability, with a view to improving efforts to address cybersecurity challenges. Mechanisms should be put in place to make it easy for victims to report such cases, for example, an Internet application that enhances ease of reporting with free tips on how to prevent future attacks and recover from losses.

4. Original equipment manufacturers and vendors should uphold the principle of security by design that ensures that, before equipment is produced, at the very least, a change in default passcodes is prompted.

5. As humans remain the weakest link in ensuring an effective cybersecurity framework in any organization, resources should be made available for cybersecurity capacity development at all levels of the education system.

6. Data indicate that cybersecurity challenges concern all countries and areas, which implies that they all need to collaborate, especially under the auspices of the Commission on Science and Technology for Development,8 which comes under the United Nations mandate through the Economic and Social Council,9 for global public policy issues, as cybersecurity is a global public policy issue.

8 Additional information is available at https://unctad.org/topic/commission-on-science-and-technology-for-development/mandate.

9 Additional information is available at www.un.org/en/model-united-nations/economic-and-social-council.

References

Allied Business Intelligence (2014). $US100 billion cybersecurity spending for critical infrastructure by 2020, 28 October.

African Union (2015). Agenda 2063: The Africa We Want, of the African Union. Addis Ababa.

Akpan, Samuel (2021,). "It's unprecedented": FG says ICT contributed 17.9% to Nigeria's GDP in Q2 2021, The Cable, 7 September.

Allen, Robert C. (2011). Why the industrial revolution was British: commerce, induced invention, and the scientific revolution. The Economic History Review, vol. 64, No. 2 (May), pp. 357–384.

Andrés, Luis, Mame Astou Diouf and Tomás Serebrisky (2007). Diffusion of the Internet: a cross-country analysis. Policy Research Working Paper, No. 4420. Washington, D.C.: World Bank.

ARCEP Benin (n.d.). Rapports. Available at https://arcep.bj/rapports/. Accessed on 17 October 2022.

Article19 (2018). UN HRC maintains consensus on Internet resolution, 9 July.

Bahamas, Utilities Regulation and Competition Authority (n.d.). URCA 03/2022 Annual Report 2021 and 2022 Annual Plan. Available at www.urcabahamas.bs/?s=report. Accessed on 17 October 2022.

Chile, Undersecretariat of Telecommunications (2021). Reporte de redes elecciones 2021 (Election networks report 2021). Available at www.subtel.gob.cl/?s=report.

China.org.cn (2022). World Insights: China's sci-tech progress not to be hammered by technology blockade, 14 October.

Citizen TV Kenya (2018). Kenya lost Ksh 20.1 billion cumulative to cyber attacks in 2017. https://www.youtube.com/watch?v=QMSB_Bszib8.

_____ (2019). Cyberattacks cost Kenya Ksh. 29.5B in 2018, video. Available at www.youtube.com/watch?v=DPOElZqPeaY.

Cohen, Matthew, and Charles Freilich Gabi Siboni (2016). Israel and cyberspace: unique threat and response. International Studies Perspectives, vol. 17, No. 3 (2016), pp. 307–321.

Coker, James (2021). Cybercrime cost victims $318 billion annually, Infosecurity Magazine, 11 August.

Colombia, Comisión de Regulación de Comunicaciones (2022). Información Internet móvil. Available at https://postdata.gov.co/informaci%C3%B3n-internet-m%C3%B3vil. Accessed on 17 October 2022.

Communications Authority of Kenya (2018). Annual Financial Reports 2020-2021. Retrieved from: https://www.ca.go.ke/annual-reports

_____(2022). Third quarter sector statistics report sector statistics report for the financial year 2021/2022. Nairobi.

Communications Regulatory Authority of Qatar (2022). CRA issues a telecommunications license to Starlink Satellite Qatar, 18 September.

Communications, Space and Technology Commission of Saudi Arabia (n.d.). Report on internet penetration. Available at https://www.cst.gov.sa/en/research-innovation/Pages/Whitepapers.aspx.

Comparitech (2016). Cybercrime-cost. 19 February. Accessed on 17 October 2022.

_____ (2019). Cybercrime-cost. October. Accessed on 17 October 2022.

_____ (2022). Cybercrime victims lose an estimated $318 billion annually.

Comparitech blog. Available at comparitech.com. https://www.comparitech.com/blog/vpn-privacy/cybercrime-cost/. Accessed on 17 October 2022.

Creese, Sadie, and others (2021). Cybersecurity capacity-building: cross-national benefits and international divides. Journal of Cyber Policy, vol. 6 No. 2, pp. 214–235.

Cyber Security Agency (2018). CSA Singapore cyber landscape 2017: cyber threats in Singapore grew in 2017 mirroring global trend. Available at www.csa.gov.sg/News-Events/Press-Releases/2018/Cyber-threats-in-Singapore-grew-in-2017-mirroring-global-trends.

_____ (2021). Ransomware incidents online scams and COVID-19 related phishing activities dominated cyber landscape in 2020, 8 July.

Daily News Egypt (2020). 12.4 million cyber-threats addressed in Egypt in H1 2020: Trend Micro, 30 September.

_____ (2021). Malware attacks in Egypt increase to 42 million during H1 2021, 18 August.

DataReportal (2021–2024). Digital country reports. Available at https://datareportal.com/reports/.

Eastern Caribbean Telecommunications Authority (n.d.). Annual Reports. Available at https://www.ectel.int/?s=report.

Economic Commission for Africa (2022). The Lomé Declaration on Cybersecurity and Fight against Cybercrime. Cybersecurity Summit, Lomé, 23 and 24 March 2022.

Eswatini Communications Commission (n.d.). Annual Reports. Available at www.esccom.org.sz/publications/reports/. Accessed on 17 October 2022.

Garofalo, Giovanna (2021). Cyber fraud costing millions to Puerto Rico residents. The Weekly Journal, 29 September.

General Authority for Communications and Information Technology (n.d.). Local indicators. www.cim.gov.ly/local-indicators. Accessed on 17 October 2022.

Gerami, Mohsen (2018). Impact of cyber threats on business profitability, ITU Centres of Excellence Network for Asia-Pacific Region, presentation. Available at https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/SiteAssets/Pages/Events/2018/CybersecurityASPCOE/cybersecurity/Impact%20of%20Cyber%20Threats%20on%20Business%20Profitability.pdf.

Giroud, Kayle (2021). Cybersecurity in Ghana: vigilance first. Global Cyber Alliance, 10 November.

Gulf News (2018). Nearly Dh 4 billion lost in the UAE to cybercrime in 2017, 4 February.

_____ (2020). 5.5mn malware attacks recorded in GCC in 2019: trend micro, 12 March.

How we made it in Africa (2019). Africa is fertile ground for cybercrime, 19 October.

Hurel, Louise Marie (2020). Brazil's first national cybersecurity strategy: an analysis of its past, present and future, Internet Governance Project, 5 April.

Information Technology Protective Security Services (2020). Brunei records nearly 40 per cent increase in cybersecurity attacks, 7 February.

Institute for Security Studies (2020). Cybercrime in Nigeria demands public-private action,19 October.

Institute of New Europe (2021). Cybersecurity in Saudi Arabia, 11 August.

Instituto Federal de Telecomunicaciones (n.d.). Reports. Available at https://bit.ift.org.mx/BitWebApp/Reportes.xhtml. Accessed on 17 October 2022

International Telecommunication Union (2014). ITU presents Global Cybersecurity Index: measuring cyber-readiness; promoting capacity-building and knowledge sharing high on the agenda. WTDC-14 Highlights: ITU presents Global Cybersecurity Index, issue No. 5, 2 April. Available at https://www.itu.int/en/newsroom/wtdc-14/Pages/highlights5.aspx.

_____ (2015). Global Cybersecurity Index and Cyberwellness Profiles. Geneva. Available at https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf.

_____ (2018). Global Cybersecurity Index 2018. Available at https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

_____ (2019). Economic Impact of Broadband in LDCs, LLDCs and SIDS: an empirical study. Geneva.

_____ (2020). Global Cybersecurity Index 2020. Available at https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E.

_____ (2021). Facts and figures 2021: 2.9 billion people still offline, 29 November.

KPMG (2021). Cyber security considerations 2022. Available at https://kpmg.com/dp/en/home/insights/2021/12/cyber-security-considerations-2022.html.

Lesotho Communications Authority (n.d.). Annual reports and strategic plans. Available at https://lca.org.ls/annual-reports-and-strategic-plans/. Accessed on 17 October 2022.

LUSA (2022). Cybercrime grows in 2021. Macau Business, 7 March.

Madhyamam (2021). Oman recorded more than 417,000 cybercrimes last year: report, 1 March.

Makridis, C.A., and M. Smeets (2019). Determinants of cyber readiness. Journal of Cyber Policy, vol. 4, No. 1, pp. 72–89. https://doi.org/10.1080/23738871.2019.1604781

Malay Mail (2022). Home Ministry: Malaysia recorded RM560m in losses from cyber crime in 2021, 11 August.

Malayasia, Ministry of Communications (n.d.). Protecting SME from cyber attacks. Available from www.kkmm.gov.my/en/pengumuman-kkmm/233-kpkk-news/19611-protecting-sme-from-cyber-attacks.

Matinuddin, Kamal (2009). Conflict, security, and development. The Pakistan Development Review, vol. 48, No. 4, Part II (Winter), pp. 991–1001.

Mauritius, Information and Communication Technologies Authority (n.d.). Annual report 2020–2021. Available at https://www.icta.mu/?s=report.

McKinsey Global Institute (2011). The great transformer: the impact of the Internet on economic growth and prosperity, 11 October. Available at https://www.mckinsey.com/~/media/mckinsey/industries/technology%20media%20and%20telecommunications/high%20tech/our%20insights/the%20great%20transformer/mgi_impact_of_internet_on_economic_growth.pdf.

Mgbolu, Charles (2010). Is it IT sector or ICT sector? Vanguard, 21 December.

Middle East Monitor (2022). Morocco thwarted hundreds of cyberattacks in 2021, says minister, 11 May.

Mohamed, Duryana (2013). Combating the threats of cybercrimes in Malaysia: the efforts, the cyberlaws and the traditional laws. Computer Law

and Security Review, vol. 29, No. 1 (February), pp. 66–76.

Morgan, Steve (2020). Cybercrime to cost the World $10.5 trillion annually by 2025. Cybercrime Magazine, 13 November.

National Communications Authority of Ghana (2022). Reports: statistical bulletins. Available at https://nca.org.gh/reports/#statistical-bulletins. Accessed on 17 October 2022.

National Telecommunications Commission of Sierra Leone (2019). Annua Report 2019. Available at https://www.natcom.gov.sl/wp-content/uploads/2021/05/natcom-annual-report-2019.pdf.

Negociado De Telecomunicaciones (n.d.). Estadisticas (Statistics). Available at https://jrtpr.pr.gov/category/estadisticas/. Accessed on 17 October 2022.

Nigerian Communications Commission (n.d.). Industry statistics. Available at www.ncc.gov.ng/stakeholder/statistics-reports/industry-overview. Accessed on 17 October 2022.

Nigerian Communications Commission (n.d.). Industry Overview Graphs Table 5.

Nippon (2020). Japan suffers record number of cybercrimes in 2019, 28 February.

Nkurunziza, Michel (2019). Cyber crime cost Rwanda economy Rwf6bn in 2018. The New Times, 29 May.

Olufuye, Jimson (2010). Vision 20-2020: ICT must drive the economy. Vanguard News, 8 June.

Oman Observer (2016). 1.1 million cyber attacks in 2015, 19 December.

_____ (2019). Oman reported 430,000 cyber attack attempts in 2018, 9 September.

Onwuegbuchi, Chike (2020). Nigeria, others facing 'millions of cyber attacks' in 2020. Nigeria Communications Week, 24 September.

Paul, Emmanuel (2020). Nigerian companies record 2nd highest percentage of global cyberattacks. Techpoint Africa, 17 July.

Post and Telecommunications Regulatory Authority of the Republic of the Congo (n.d.).

Publications: reports from the postal and electronic communications sectors. Available at www.arpce.cg/rapports. Accessed on 17 October 2022.

Postal and Telecommunications Regulatory Authority of Zimbabwe (n.d.). Annual reports and strategic plans. Available at www.potraz.gov.zw/?page_id=527.

Ppro.com (2014). Cyberattacks account for up to US8 billion losses in Brazil, 12 June.

Projects IN Controlled Environments 2 (n.d.). Homepage: all training courses. PRINCE2 Certification Training and Information for USA Project Managers: USA. PRINCE2. Available at https://www.prince2.com/zar/what-is-prince2.

Puglia, David (2014). Are enterprises ready for billions of devices to join the Internet? Wired, December.

Regulatory Unit Communications Services of Uruguay (n.d.). Statistics. Available at www.gub.uy/unidad-reguladora-servicios-comunicaciones/datos-y-estadisticas/estadisticas.

Rosch, Carla (2022). A massive cyberattack in Costa Rica leaves citizens hurting. Rest of World, 1 June.

Rotich, Kevin (2021). Cyber-attacks in Kenya up by half to hit 56m in three months. Business Daily, 9 February.

Saunders, Christopher, and Dawn Nagar (2008). Human security and development in Southern

Africa. In Security and Development in Southern Africa. Cape Town, South Africa: Centre for Conflict Resolution.

SciDev.Net (2016). Cybercrime in Africa: facts and figures, 7 July. Available at www.scidev.net/sub-saharan-africa/features/cybercrime-africa-facts-figures/.

Schwab, Klaus (2016). The Fourth Industrial Revolution. Geneva: World Economic Forum.

Security Boulevard (2021). Kuwait Against Cyber Crimes, 8 July.

Sesa Systems (n.d.). Manage your stocks and flows with Lean Manufacturing. Available at www.sesa-systems.com/en/lean-manufacturing-stock-and-flow-management. Accessed on 18 October 2022.

Sesa Systems Digital (n.d.). What is industry 4.0: the fourth industrial revolution? Available at www.sesa-systems-digital.com/en/industry-4-0-fourth-industrial-revolution/. Accessed on 18 October 2022.

Shailbany, Salele al (2017). Cybercrime on the rise in Oman. The National News, 15 April.

Signé, Landry, and Kevin Signé (2018). Global cybercrimes and weak cybersecurity threaten businesses in Africa. Brookings, 30 May.

Statista (2018). Consumer loss through cybercrime worldwide in 2017, by victim country. Available at www.statista.com/statistics/799875/countries-with-the-largest-losses-through-cybercrime/%20-%202017.

_____ (2023). Financial loss due to computer crime in Hong Kong from 2012 to 2022. Available at www.statista.com/statistics/786989/hong-kong-financial-loss-caused-by-computer-crime/.

_____ (2023). Number of hacking cases in South Korea by type 2022. Available at www.statista.com/statistics/1228659/south-korea-online-hacking-cases-by-type/.

_____ (2023). Number of victims of phishing attacks in South Korea from 2017 to 2022. Available at www.statista.com/statistics/1310682/south-korea-number-of-phishing-victims/.

_____ (2023). Total number of computer crime cases in Hong Kong from 2012 to 2022. Available at www.statista.com/statistics/787076/hong-kong-number-of-computer-crime-incidents/.

_____ (2023). Total number of reported computer security incidents in Hong Kong from 2007 to 2021. Available at www.statista.com/statistics/787184/hong-kong-number-of-reported-information-security-incidents/#:~:text=Total%20number%20of%20reported%20computer%20security%20incidents%20Hong%20Kong%202007%2D2021&text=This%20statistic%20depicts%20the%20total,reports%20in%20the%20previous%20year.

_____ (2023). Value of phishing damage in South Korea from 2017 to 2022. Available at www.statista.com/statistics/1310679/south-korea-amount-of-phishing-damage/. Accessed on 17 August 2022.

_____ (2024). Number of cleared cybercrime cases in Japan from 2014 to 2023. Available at www.statista.com/statistics/746963/japan-number-of-cyber-crime-arrests/.

Strategic Foresight Initiative (2013). The third industrial revolution. In Envisioning 2030: US Strategy for the Coming Technology Revolution. Washington, D.C.: Atlantic Council.

Sun, David, and Jessie Lim (2022). Scam victims in S'pore lost $633.3 million in 2021. The Straits Times, 17 May.

Sunday Standard (2017). Botswana is the cyber crime capital of Africa, 28 August.

Tan, Teck-Boon, and Wu Shang-su (2017). The fourth industrial revolution explained. In Public Policy Implications of the Fourth Industrial Revolution for Singapore. Singapore: S. Rajaratnam School of International Studies.

Tech Xplore (2022). Global cost of cybercrime topped $6 trillion in 2021: defence firm, 10 May.

The Media Line (n.d.). Israel suffers 8,600 cyberattacks in 2019. Video. Available at www.youtube.com/watch?v=3ejwdl2UjTw.

The North Africa Post (2019). Cybersecurity: more than 5 million attacks detected in Morocco in second quarter of 2019, Available at https://northafricapost.com/34457-cybersecurity-more-than-5-million-attacks-detected-in-morocco-in-second-quarter-of-2019.html.

Threatcop (2022). How is the need for cybersecurity in the Middle East rising? 2 May.

Uganda Communications Commission (n.d.). UCC market performance report(s). Available at www.ucc.co.ug/?s=report. Accessed on 18 October 2022.

United Nations Trade and Development (n.d.). Commission on Science and Technology for Development. Available at https://unctad.org/topic/commission-on-science-and-technology-for-development.

United Nations (1948). General Assembly resolution 217 A (III). 10 December (Universal Declaration of Human Rights).

_____ (2012). General Assembly resolution A/HRC/20/L.13. 29 June (The promotion, protection and enjoyment of human rights on the Internet).

_____ (2015a). General Assembly in resolution 70/1. 25 September (Transforming our world: the 2030 Agenda for Sustainable Development).

_____ (2015b). The 17 Goals. Available at https://sdgs.un.org/goals.

_____ (2021). Our Common Agenda: Report of the Secretary-General. United Nations publications.

United Nations, Office of the Secretary-General's Envoy on Technology (n.d.). Global digital compact. Available at www.un.org/techenvoy/global-digital-compact.

Utilities Regulation and Competition Authority (2022). Annual Report 2021 and 2022 Annual Plan. Available at www.urcabahamas.bs/wp-content/uploads/2022/05/URCA-2021-Annual-Report-and-2022-Annual-Plan-FINAL-VERSION.pdf.

Wahab, Amirudin Abdul (2016). Facing cyberattacks in 2016 and beyond. The Star, 28 January.

Wikipedia (2013). 2013 South Korea cyberattack. Available at https://en.wikipedia.org/wiki/2013_South_Korea_cyberattack.

_____ (n/d). Scientific management. Available at https://en.wikipedia.org/wiki/Scientific_management. Accessed on 18 October 2022.

World Bank (2020). World Development Indicators. Available at https://datatopics.worldbank.org/world-development-indicators/. Accessed on 18 October 2022.

World Bank Open Data Platform (2011–2021). Data sets. Available at https://datatopics.worldbank.org/world-development-indicators/.

World Economic Forum (2016). The fourth industrial revolution: what it means and how to respond, 14 January.

ZAWYA (2022). Cyber attacks on small businesses jump 348% in Bahrain, 20 May.

Printed in Addis Ababa, Ethiopia by the ECA Printing and Publishing Unit.
ISO 14001:2015 certified. Printed on chlorine free paper.