ANCy
Agence Nationale
de la Cybersécurité

RÉPUBLIQUE TOGOLAISE

National Cybersecurity Strategy

2024-2028

National Cybersecurity Agency (NCA)

63 Bd du 13 janvier
Nyékonakpoe, Lomé-TOGO
07 BP 7878

+228 97 52 58 58
+228 70 60 60 83

secretariat.ancy@ancy.gouv.tg
https//www.ancy.gouv.tg

H.E.M. Faure Essozimna GNASSINGBÉ
President of the Togolese Republic

Ladies and Gentlemen,

Cybersecurity is a major challenge for Togo, which has made digital technology an essential lever in its economic and social transformation. Cybersecurity is vital to ensure that citizens, businesses and administrations have confidence in digital services, to fight the threats to our national security and to preserve our national sovereignty.

The implementation of the National Cybersecurity Strategy is a crucial step in the government's commitment to anticipating and dealing with digital threats of all kinds, in order to ensure that citizens, businesses and critical infrastructures and services are protected against digital threats.

I invite you to take ownership of this strategy and implement it with determination and efficiency, to make Togo a model country in terms of cybersecurity.

Victoire S. TOMEGAH-DOGBE
Prime Minister, Head of Government

Co-preface

Under the strong leadership of the President of the Republic, His Excellency Mr Faure Essozimna GNASSINGBE, information and communication technologies (ICT) have, within a decade, deeply transformed our personal and professional habits, raised the competitiveness of businesses to an unprecedented level, brought administrations closer to users and fostered transparency in the life of our country's institutions.

This massive use of ICTs is part of our country's stated ambition to become a prime logistics hub and business centre by 2025, in line with the objectives of the National Development Plan (NDP 2018-2022) and the government's roadmap "TOGO 2025".

However, this global information society, a real "Tower of Babel", which opens the way to infinitely unseen possibilities, certainly for the better, but it would seem also, for the worse, also offers new opportunities for cyber-attacks, which are acquiring limitless capacity to harm the resilience of our infrastructures and essential networks, and national economic prosperity.

These cyber-attacks, which are increasingly varied and sophisticated in their origins, are based on various reasons: They are the work of individuals and activists pursuing political goals, of criminal organisations resorting to fraud or blackmail, of spies working for other nations or of terrorist organisations seeking to disrupt or destabilise our State and our society.

In response to this situation, although we have not yet all collectively grasped the full extent of the challenges and cyber risks, the Government, in order to preserve the integrity of our physical borders and the national cyberspace, to guarantee the security of our fellow citizens, to protect our essential infrastructures and keep our economy growing, has decided to include the security and defence of information systems among the national priority sectors.

This National Cybersecurity Strategy (NCS), drawn up in accordance with international best practice in the field and submitted to the various stakeholders for their approval, will enable our country to effectively deal with the serious threats to the availability, integrity and confidentiality of systems, data and national digital processes.

It aims to prevent and effectively respond to cyber-attacks by improving our country's resilience in this area by building national capacities, supporting digital trust, promoting international cooperation, with a view to ultimately consolidate Togo's digital leadership in the sub-region.

Even though much remains to be done, we remain convinced that the simple and concrete, yet very ambitious objectives we have set ourselves are equal to the major challenges posed by the technological innovations that are more necessary than ever in order to guarantee our country a place of choice in the community of nations.

Dear compatriots, dear partners, if the great challenge of cybersecurity, launched at the end of 2018 with the promulgation of the law on cybersecurity and the fight against cybercrime, already revealed a strong political will to take this issue head on, the present NCS confirms in every aspect the privileged place that the Government attribute to this issue.

It therefore calls on us to participate to its implementation for a safe and reliable cyberspace, in order to "skip" several stages of our digital transition, thanks to the participatory approach that is developed in the action plan of this strategy.

Ambassador
Calixte Batossie MADJOULBA,
Minister of Security
and Civil Protection

Cina LAWSON
Minister of Digital Economy
and Digital Transformation

Dear Readers,

Our world is changing at an unprecedented speed, with digital technology at the heart of every aspect of our lives. This transformation comes with a complex set of challenges and threats, with malicious actors seeking to exploit our vulnerabilities.

In response to these challenges, it is with pride and determination that I present to you the National Cybersecurity Strategy (NCS 2024-2028), an essential milestone in our ongoing commitment to participate in our country's national security and digital sovereignty.

The National Cybersecurity Strategy is based on four main pillars:
Promoting a culture of cybersecurity by raising awareness and training the population, considering that awareness is the first line in the defence against cybersecurity threats.

Protecting critical information systems will be a reality, by strengthening existing protection measures, identifying and mitigating vulnerabilities, implementing appropriate security controls and consolidating our defences against sophisticated attacks.

Strengthening the IT incident response system: We will implement an effective and coordinated incident response system capable of detecting, analysing and reacting quickly to cyber security incidents.

Finally, we will ensure that the perpetrators of cybersecurity crimes and offences are prosecuted and brought to justice to answer for their actions, through mechanisms for the effective prosecution of cybersecurity crimes.

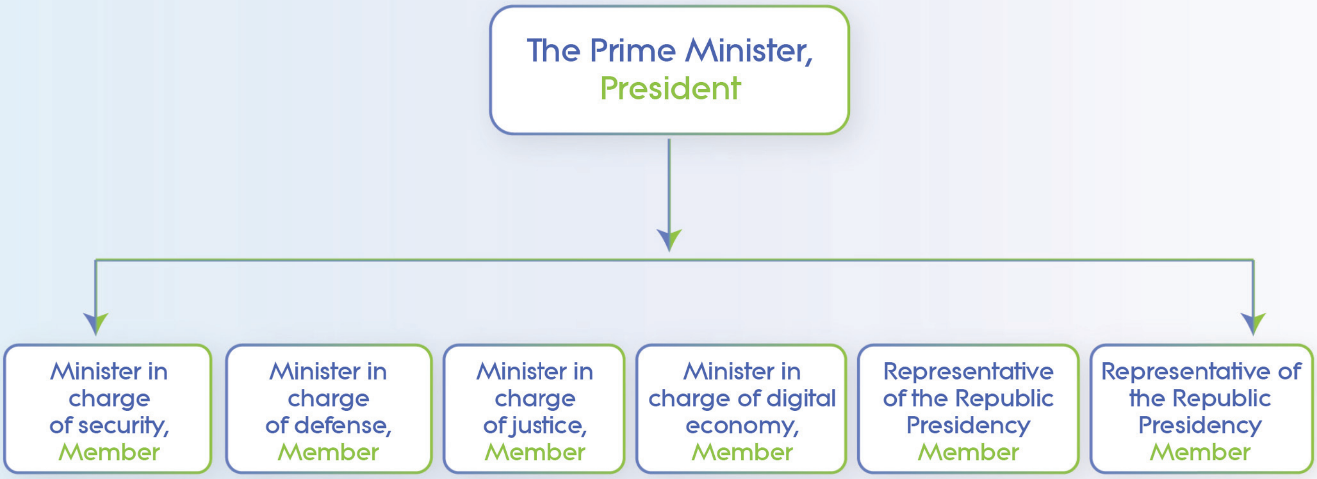
The result of hard work and broad coordination with the stakeholders involved in cyber security, our NCS is both, ambitious and realistic.

It draws on international best practices in the field and is adapted to our unique national context. I therefore invite you to fully commit yourselves to the implementation of this strategy, which is a reference document for our collective action on cybersecurity.

Thank you.

Gbota GWALIBA,
General Director of NCA

Organizational chart of the strategic committee



The Prime Minister, President

Minister in charge of security, Member

Minister in charge of defense, Member

Minister in charge of justice, Member

Minister in charge of digital economy, Member

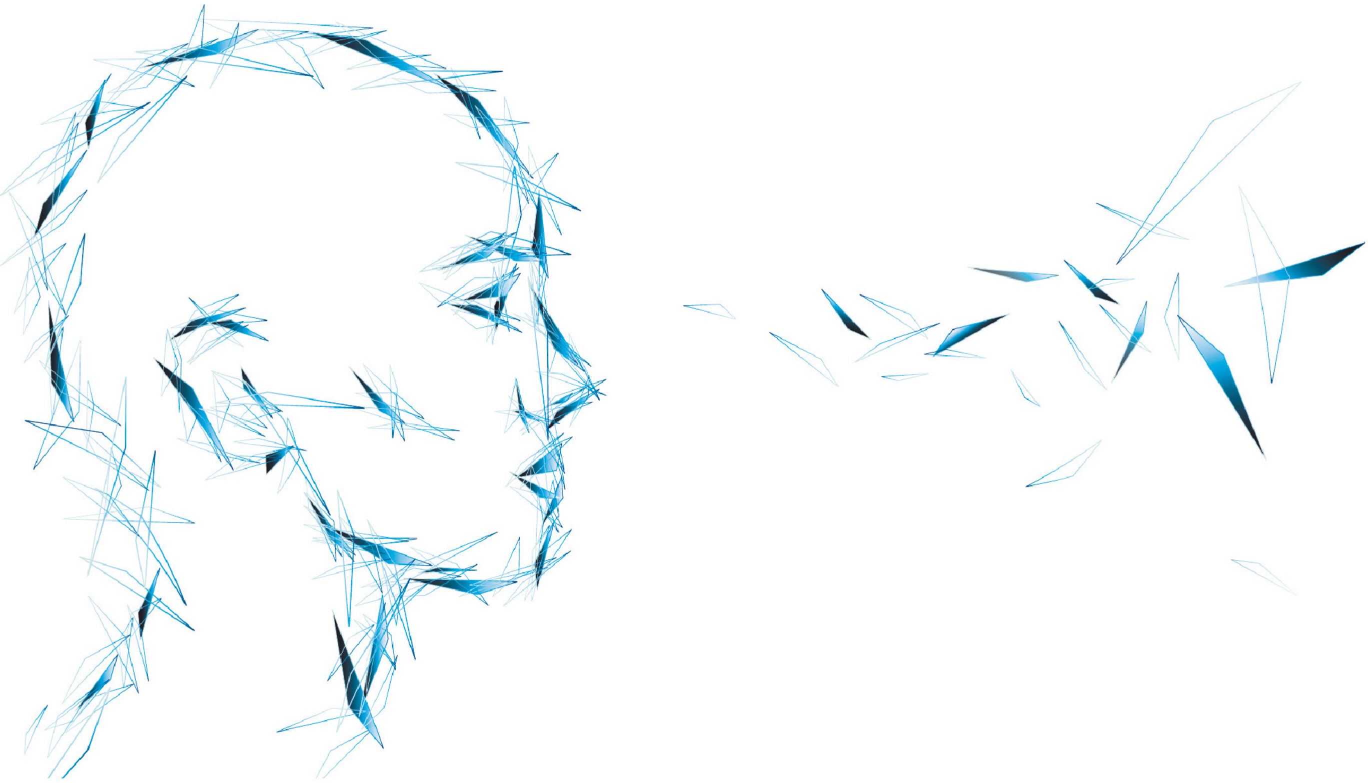
Representative of the Republic Presidency Member

Representative of the Republic Presidency Member

Contents

Glossary

ADS	Asseco Data Systems
AfricaCERT	Africa Computer Emergency Response Team
AFRIPOL	African Union Mechanism for Police Cooperation
GEIA	Gnassingbé Eyadema International Airport
NCA	National Cybersecurity Agency
APT	Advanced Persistent Threat
ECPRA	Electronic Communication and Posts Regulation Authority
TDA	Togo Digital Agency
CDA	Cyber Defence Africa
ECOWAS	Economic Community of West African States
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
ENISA	European Union Agency for Cybersecurity
SWOT	Strength Weakness Opportunities Threats
FIRST	Forum of incident Response and Security Teams
GFCE	Global Forum on Cyber Expertise
PDPA	Personal Data Protection Agency
ISOC	Information Security Operations Center
LEC	Law on Electronic Communications
MDEDT	Ministry of Digital Economy and Digital Transformation
NIST	National Institute of Standards and Technology
OCWAR-C	West African Response on Cybersecurity and fight against Cybercrime
OES	Operator of Essential Services
OT	Operational Technologies
APL	Autonomous Port of Lomé
PPP	Public-Private Partnership
OSP	Operator Security Plan
IS	Information Systems
SOC	Security Operation Center
TF-CSIRT	Task Force-Computer Security Incident Response Team
IT	Information Technologies
ICT	Information and Communication Technologies
AU	African Union
WAEMU	West African Economic and Monetary Union
NCS	National Cybersecurity Strategy



Objective and vision

Togo is in the midst of a transition, with a marked growth in the use of digital technology in administrations, the economy and people's daily lives. In turn, this growth is exposing the country to a multitude of risks and threats from cybercrime, which is also increasing (fraud, data theft, blackmail, ransomware). Given this situation, the protection and security of the State's information systems and critical infrastructures are becoming a national requirement, hence the need to develop a national strategy to protect Togo's cyberspace.

The aim of this national cybersecurity strategy is to make Togo a regional leader in cyber security, recognised as such on a global scale and contributing actively and positively to the international cyber security community.

This cyber security strategy aims to build confidence in the use of digital technology in order to stimulate growth and foster the emergence of new markets for the benefit of citizens and national and international investors. Its aim is to guarantee the security, stability, continuity, resilience of essential digital infrastructures and services, and to promote the development of knowhow and skilled jobs in Togo in the field of cyber security. Finally, it should enable citizens to take advantage of the opportunities offered by the virtual world in full knowledge of the dangers and risks to which they are exposed.

Analytical summary

The digital economy is growing quickly in Togo. Mobile penetration rates are on the rise: 77,6% in the second quarter of 2021, internet access is improving, with a fixed and mobile data penetration rate of 66.86% in the second quarter of 2021, and mobile payments are gaining in popularity. This growth has been boosted by the government's commitment to stimulating the rapid expansion of mobile broadband and fixed networks across the country, notably with the reception of Google's Equinox submarine cable, which increases the number of submarine cables to three (03). Thanks to these innovations, Togolese citizens are benefiting from more opportunities offered by the digital economy, such as better communications, better access to online information and new opportunities for e-commerce, and an increase in the digital services offered to the Togolese population through social or health programmes such as Novissi or the traveller management platform and the vaccination monitoring platform to combat COVID 19.

Paradoxically, throughout the world, the growth of the digital economy has led to an increase in cybercrime. Togo, like other countries around the world, must therefore be prepared to deal with cyber threats in order to promote stability and confidence in digital services on the part of its citizens, as well as national and international investors.

Aware of this urgency, the Togolese government has been fully committed since 2018 to securing its cyberspace in order to protect citizens, businesses, public institutions and critical infrastructures against cybercrime, by strengthening regulatory and operational frameworks, thus guaranteeing national digital sovereignty and the protection of citizens' data.

The Togolese government's target is to make Togo a regional leader in cyber security, recognised as such on a global scale and contributing actively and positively to the international cybersecurity community.

With this in mind, the four (04) strategic objectives developed in this national cyber security strategy document aim to develop a high-performance cyber security and anti-cybercrime ecosystem based on local skills.

By applying the strategy described in this document, the vision of the competent national authorities is to promote the economic development of skilled jobs and the positioning of Togo at the forefront of the knowledge economy by ensuring the security of its cyberspace, the stability and continuity of essential digital services and the confidence of citizens and national and foreign investors in the country's ability to deal effectively with cyber threats.

[1] Novissi: Monetary transfer program implemented by the Togolese Government that aims to help the most vulnerable individuals and families that lost their income because of the adoption of measures against Coronavirus

Introduction

Rapid access to reliable and usable information in the production and management of services, in both the public and private sectors, contributes to economic and social development and to the preservation of national security and stability. As part of the accelerated modernisation and digitisation of public services and the economy, cybersecurity is now a national priority.

The General Policy Statement presented by the Prime Minister confirms the priority given to digitisation, since out of the 42 major projects and reforms in the government's 2020-2025 roadmap, % relate to digital issues, including digital identity, digitisation of the administration, the use of biometrics and the creation of a digital database for all layers of Togolese society.

Dynamic social and technological changes require greater protection of digital resources, which should encourage investment in new digital technologies and accelerate the country's social and economic development. Digital technologies are shaping social relations. Internet services have become a tool for influencing the behaviour of social groups and the political sphere. Any significant disruption to the functioning of digital technologies, whether global or local, will affect the security of economic transactions, citizens' sense of security, the effectiveness of public sector institutions, production and service processes and, consequently, national security in general.

As threats to cyberspace have no geographical barriers, cybersecurity activities require strong international cooperation. Togo is aware of this need, and its presence in both regional and international bodies is highly visible, such as ECOWAS and its initiative Organised Crime: West African Response on cybersecurity and fight against cybercrime (OCWAR-C) initiative, as well as its ratification of the African Union convention on Cybersecurity and the Protection of Personal Data, known as the Malabo convention.

The national protection of information systems and processed data is a major challenge for all the national involved actors, such as public authorities, national security authorities, specialised entities dedicated to dealing with cybersecurity, in this case the National Cybersecurity Agency (NCA) and Cyber Defence Africa (CDA), as well as all public or private operators who provide essential services via information systems.

The COVID-19 pandemic has led to an increase in the use of remote, digital services, reinforcing the need to secure information systems, digital transactions and personal data. Finally, cybersecurity is a new dimension of national security and sovereignty, whether it involves organising elections securely and without interference, protecting the country's essential infrastructure from malicious attacks, or other destabilising factors made possible by information and communication technologies.

The aim of this document is to define and guide the strategies and adopt the political, regulatory and operational measures needed to protect citizens and provide optimum security for the information systems in the national digital ecosystem, namely:

- public administrations and departments of the State;
- operators of essential services;
- operators of essential infrastructures;
- other key actors in sensitive sectors.

1.

Assessment of the national strategy context

1.1

Togo, regional logistics and financial hub

Located along the Gulf of Guinea in West Africa, Togo covers an area of 56,785 km2 and is bordered to the north by Burkina Faso, to the east by Benin, to the south by the Atlantic Ocean and to the west by Ghana.

Togo has a population of 8.3 million, of which 1.9 million live in Lomé, the capital, and 43% in other urban areas. Togo's population is young: The median age is 20 and 70% of the population is under 35. The country has 6.5 million mobile phone subscribers (penetration rate of 77%) and around 3 million mobile and fixed internet subscribers (penetration rate of 43%).

Togo's strategic location and its membership of the ECOWAS and WAEMU economic zones make it an ideal gateway to the booming West African market, with a rapidly growing population of over 350 million and rising incomes.

Over the past ten years, Togo has made considerable investments to develop first-class infrastructure. It has also undertaken structural reforms to support the development of a prosperous private sector, and has thus become a preferred destination for investment. These efforts have resulted in sustained growth in its port activities and progress in improving the business climate, which has earned it 3rd place among the top 10 most reform-minded countries in the world and 1st place in Africa in the annual 2020 Doing Business ranking published by the World Bank. To achieve the goal of becoming a middle-income country, Togo is accelerating its economic transformation by facilitating foreign direct investment in priority sectors, with the main ambition of strengthening its position as a logistics hub in West Africa in order to become a major agricultural and industrial centre.

In 2019, services centred on trade, port, airport and banking activities contributed half of its GDP, i.e. 49.9%.

The autonomous Port of Lomé is the only deep-water port on the West African coast capable of accommodating 3rd generation vessels, with a natural depth of 16.60 metres. This puts it ahead of its competitors in the sub-region, with a volume of container traffic of 1.2 million Twenty-feet Equivalent Units (TEUs) recorded.

The International Airport of Lomé has already reached half of its capacity, with 1 million passengers per year (before COVID-19), and connects several cities around the world. It serves as a hub for West Africa's regional airline, to Asky, and its partner Ethiopian Airlines, which serve 26 cities directly from Lomé.

In addition of being a regional logistics hub, Togo is also a commercial hub (the Lomé market has an international reputation) and a financial hub, with a number of leading regional financial institutions having chosen Togo as the location for their head offices, including Ecobank, Oragroup.

[2] Source ECPRA: evolution of regulated markets : posts and electronic communications – 2019 report

[3] https.//www.tresoreconomie.gouv.fr/Pays/TG/conjoncture

[4] https.//www.togo-port.net/presentation-pal/atouts-port-lome/

1.2
Togo digital or the momentum of the country's digitalization

The Togolese Government's ambition is to make the digitalization of the Togolese society one of its priorities, with nationwide projects such as providing identity for all, setting up a single social register of individuals and households, digitalizing public services, and creating a digital bank for all.

This digital momentum, the strategic objective of which is to offer the country inclusive development of society and the economy, involves democratising access to the internet. To support this digitalization, Togo can rely on solid telecoms operators and a major infrastructure that has yet to be deployed throughout the country. This digitisation will affect all Togolese citizens, giving wider access to individuals and businesses, It will require new tools and new ways of working, and will involve sensitive information on the entire population. It is now imperative that this data should be secure, accessible and filtered only to those who have the right to access it according to the strict requirement of their position. Confidentiality, integrity and credibility are essential.

The creation of the Togo Digital Agency, the National Agency for Identification and Digital Infrastructures Society reinforces this momentum towards digitalisation.

1.3
Cyber threat landscape in Togo

Togo has six (06) electronic communications operators: two (02) mobile Internet access service providers (Togocom and Moov Africa Togo) and four (04) fixed Internet access service providers (Togocom, CAFE Informatique & Télécommunication, Téolis and Vivendi Group Africa Togo VGA). Internet take-up is faster via mobile, with more than 5 million subscribers in 2021, compared with just over 54,000 for fixed-line Internet.

It is therefore no surprise, that viruses and trojans for mobile devices are the most detected in Togo, particularly malwares targeting devices running the Android operating system, such as Hummer, Backdoor prizmes and Rootnik. These malwares take total control of the device, mainly to disrupt the owner's use of it by displaying untimely advertisements or installing unwanted applications. It is also used to collect information about the infected device (screenshots, keyboard entries, etc.).

Other types of cyber-attack such as phishing, ransomware, minor wedges, rebound attacks, DDoS attacks and spam campaigns are also detected on vulnerable equipment. In Togo, devices are either attacked directly, or used as a vector for attacks on other destinations. As a result, the reputation of IP addresses originating in Togo is tarnished on the Internet. The non-application of minimum security measures, the use of pirated software carrying viruses and malicious codes, and the lack of knowledge of the pitfalls associated with the use of digital media, make easier the installation and persistence of this malware. Operators of Essential Services (OES), public administrations, state's departments and large togolese companies are the first victims of these attacks.

The use of digital means to commit fraud, particularly against financial institutions, is on the increase. In this respect, the creation of fake banking websites to lure users and collect their login details, and fraud affecting payment methods are attacks that users' negligence makes easier and more lucrative. These attacks have direct financial consequences, affecting the reputation of banks and causing a loss of customer confidence, with a real potential impact on the country's economic growth in the medium term.

[5] Source ARCEP: electronic communications market observatory, chart at the second quarter of 2021

The most used social networks by Togolese people are being used as a medium for widespread online fraud campaigns by falsifying the accounts of political figures and members of government, false promises of scholarships, visas, employments, spread of fake news, etc. These new information channels facilitate online fraud by targeting togolese people who are least aware of cyber threats and most vulnerable to cyber-attacks.These threats are exacerbated by the global nature of cyberspace and the internationalisation of mobile money payments. Fraudsters are positioning themselves geographically in neighbouring countries to perpetrate attacks targeting togolese people, while ensuring that they collect the data via international mobile money. Conversely, other groups of cybercriminals based in Togo are engaging in online scams in neighbouring countries.

1.4
The strategic context of cybersecurity

Given the national strategic context of the digitisation of Togolese society, and the permanent presence of cyber-threats, cybersecurity is a national priority.

Effective cybersecurity needs to be based on a number of pillars that need to be continually strengthened, with a level of quality that is systematically improved. These pillars are:

1. The protection and defence of information systems;
2. The resilience of information systems in front of cyber threats;
3. The effectiveness of cybercrime detection and repression services and hybrid activities (including terrorism) and spying, and strengthening the maturity of the judicial system in relation to new digital offences and crimes.

The Togolese Republic is an active member of many international organisations, including African organisations such as:

- the African Union (AU);
- the Economic Community of West African States (ECOWAS);
- the West African Economic and Monetary Union (WAEMU);
- SMART Arica.

The Togolese Republic is also an active member of several regional initiatives to promote cybersecurity and regional and African cooperation in this area.

a. At the level of the Economic Community of West African States (ECOWAS), an initiative called "West African Response on Cybersecurity and fight against Cybercrime (OCWAR-C)" has led to the adoption of the regional strategy for cyber security and the fight against cybercrime, as well as the adoption of the regional strategy for the protection of critical infrastructures.

b. at the level of the African Union (AU), Togo has ratified the Malabo Convention on cybersecurity and the protection of personal data, which has enabled it to take part in numerous international cooperation initiatives.

1.5
Legal and regulatory framework for cybersecurity

Togolese government has improved and consolidated the legislative and regulatory framework in the field of Information and Communication Technologies (ICT), in particular by adopting several laws enabling:

- the implementation of the sectorial strategy for the digital economy;
- the establishment of the necessary governance structures;
- the protection of citizens from the new security risks and threats posed by cyberspace and access to new information technologies.

These laws, decrees and orders are the following:

- law n° 2016 - 006 of 30 March 2016 on freedom of access to information and public documentation;
- law n° 2017-007 of 22 June 2017 on electronic transactions;
- law n° 2018-026 of 7 December 2018 amended by law n° 2022-009 of 22 June 2022 on cybersecurity and the fight against cybercrime;
- law n° 2019-014 of 29 October 2019 on the protection of personal data;
- decree n° 2017-104 of 30 October 2019 on the implementation of Law n° 2016-06 of 30 March 2016 on freedom of access to public information and documentation;
- decree n° 2018-062/PR of 21 March 2018 regulating electronic transactions and services in Togo;
- decree n° 2019-022/PR of 13 February 2019 on the remit, organisation and operation of the National Cybersecurity Agency (NCA);
- decree n° 2019-095/PR of 08 July 2019 on Operators of Essential Service (OES), essential infrastructure and related obligations;
- order n° 2022-040 /PMRT of 29 June 2022 adopting cybersecurity rules in the Togolese Republic;
- decree n° 2022-090/PR of 25 August 2022 201 relating to the qualification of providers of cybersecurity trust services and cybersecurity products and to the approval of assessment centers.

[6] Detailed information in Annex 1

1.6
The National Cybersecurity Agency (NCA)

According to Article 4 of Decree 2019-022/PR of 13 February 2019 on the attributions, organisation and operation of the National Cybersecurity Agency (NCA), its main missions are as follows:

- It provides assistance to the services of the Togolese Republic in matters of defence and national security.

- It is responsible for raising awareness among users of IT equipment, services and facilities, preventing intrusions, and securing and defending all information systems.

- The National Cybersecurity Agency is also responsible for coordinating the response to cyber-attacks.

- It examines requests for qualification and qualifies cybersecurity products and trusted service providers for the purposes of information systems security, in accordance with the procedures laid down by regulation.

A NATIONAL STRATEGY...

...FOR A GLOBAL RESPONSE TO CYBER THREATS

1.7
Cyber Defense Africa (CDA)

Aware of national limitations in terms of human resources and funding, the government has opted for the quick establishment of an operational and technical arm of the NCA responsible for the analysis, response and remediation of cyber-attacks. Indeed, in 2019, the Republic of Togo entered into a Public-Private Partnership (PPP) with Asseco Data Systems (ADS), a leading Polish IT company and Europe's sixth largest software producer, creating a joint venture called Cyber Defense Africa whose mission is to provide the operational expertise needed for maximum protection of Togolese cyberspace.

The creation of CDA was a direct response to the urgent need to put in place a technical framework to serve essential service operators and the NCA.

The partnership with Asseco has enabled Togo to establish a centre of excellence combining a national CERT (Computer Emergency Response Team) and a SOC (Security Operations Centre), creating economies of scale and synergies. This partnership not only solves the problem of the shortage of local expertise to operate cyberspace security, but also develops local capacity to manage cybersecurity infrastructures over the long term.

This PPP is structured in such a way that CERT is offered as a mainly free service to the public. The CERT alerts the public about vulnerabilities and raises awareness of how to protect themselves against attacks. The CERT also publishes patches on identified vulnerabilities. The SOC, for its part, is a paying service that provides cybersecurity as a tailor-made service for Operator of Essential Services (OES), businesses, public institutions and other parties interested in protecting their computer networks.

Thus, this model enables national cybersecurity capabilities to be strengthened quickly, on a large scale and at a reasonable cost.

Thanks to the current partnership with CDA, cybersecurity professionals are being trained in Togo and will eventually be able to work within national, regional, African and international organisations, in line with Togo's desire to be a "hub" of cybersecurity expertise in the sub-region.

It is only a matter of time before demand and research for cybersecurity skills are very high, so Togo wants to be ready to provide this expertise when the time comes.

1.8
Distribution of roles between NCA and CDA for effective national cybersecurity

The NCA, as the national authority for information systems security, regulates the togolese cyberspace. The NCA coordinates activities and relations between the various actors in the sector, pilots national cybersecurity programmes and monitors the application of laws and various texts in the sector.

The NCA monitors and controls the services it delegates to CDA under a service delegation contract containing clear and measurable performance measurement criteria.

As the operational arm of the ANCY, CDA is responsible for:

- operating the National CERT, the CERT.tg;
- operating the National SOC to monitor and support the security of Essential Service Operators;
- raising awareness among users of IT equipment, services and facilities;
- preventing intrusions, securing and defending all information systems;
- coordinating the response to IT attacks;
- providing technical support on behalf of the NCA.

CERT
SOC

1.9
CERT.tg and National SOC services

The National CERT is responsible for the general function of monitoring risks in Togo associated with cyberspace, protecting civil society against malicious use of Internet tools or services, and responding to any attacks that may occur. The CERT team provides these services free of charge 24 hours a day, 7 days a week to the Togolese government, the general public and any other organisation in Togo. In particular, it is responsible for:

- analysing data on threats in Togolese cyberspace based on information gathered from the Togolese population, Togolese companies, administrations and other organisations; as well as the global CERT and CSIRT community;
- processing, responding to and coordinating national cybersecurity incidents;
- receiving threats detected and communicated by Togolese citizens to the call centre; by email and on the website;
- announcing intrusions and vulnerabilities and publish security bulletins;
- carrying out advanced analysis of malicious software at national and/or international level;
- writing reports on trends in cyber-attacks and their potential impact on the country;
- organising cyber-security training and awareness campaigns aimed at the general public, schools, universities, etc. ;
- carrying out security audits and issue certificates under the supervision of NCA;
- participating in and contribute to specific technical studies or research and development projects on cybersecurity;
- participating in the development of cybersecurity standards throughout the country.

The SOC team, on the other hand, provides fee-based services to essential service operators and to any other organisations wishing to benefit from proactive cybersecurity protection services. It is dedicated to the security of the businesses it protects and uses the support and services of the CERT team when required. The SOC operates as a cybersecurity services company, providing managed services "SOC as a Service".

These include:

- the administration and maintenance of the national SIEM infrastructure (Security Information & Event Management) or the site of each organisation benefiting from SOC services;
- the bespoke monitoring of security events 24 hours a day, 7 days a week;
- the detection and identification of threats and targeted attacks;
- the response to threats and corrective measures (in collaboration with the CER team);
- the assistance in the process of coercion and recovery of the information system (in collaboration with the CERT team);
- the targeted analysis of malicious software (in collaboration with the CER team);
- the analysis and management of vulnerabilities inherent in the protected organisation;
- the preparation of periodic reports.

The SOC team also provides other services needed to secure the information systems of protected organisations, such as:

- Cybersecurity consulting (drafting of information system security policies, mapping, etc.);
- Advanced cybersecurity training;
- Integration of cybersecurity solutions;
- Audits and intrusion tests.

2. Strengths, Weaknesses, Opportunities, Threats (SWOT)

As the aim of Togo's cybersecurity development strategy is to implement the needed resources to control the risks to the security of information systems in Togo, it is necessary to carry out a diagnosis of the strengths and weaknesses, opportunities and threats of the national cyber environment in order to give a real chance of success to the ambition of implementing effective high-level cybersecurity that is capable of meeting its desire to become a regional leader in cybersecurity, recognised as such on a global scale and contributing actively and positively to the international cybersecurity community.

STRENGTHS

1. Strong involvement of the highest authorities of the State
2. Relevant legal and regulatory framework
3. Innovative operational framework commensurate with the issues at stake
4. Funding for cybersecurity activities
5. Collaboration between all national actors
6. International cooperation
7. Public-private partnership for operational cybersecurity.

OPPORTUNITIES

1. Togo's digitalization momentum
2. African and global response to cyber threats
3. Young population with an appetite for learning
4. Growing economy

WEAKNESSES

1. Low level of maturity in cybersecurity
2. Shortage of cybersecurity skills
3. Insufficiently secure essential services
4. Vulnerability of deployed applications
5. Poor prosecution of cybersecurity crimes and offences
6. Budget still limited

THREATS

1. Cyberspace: a space without borders
2. A constantly changing world
3. Regional cybercrime
4. Difficulties in mobilising internal and external resources linked to security crises and conflicts

The Togolese government, aware of the various external constraints that may affect the achievement of strategic cybersecurity objectives and of the need to take strong, rapid and concerted action, is determined to implement a reliable environment of trust that will make it possible to disseminate good cybersecurity practices to all the actors concerned, whether the various public administrations among themselves or between them and players in the commercial sector, in particular operators of essential services.

2.1
Togo's main strengths in favour of the cybersecurity strategy

2.1.1.
Involvement of the highest State authorities

The involvement and leadership of the President of the Republic, the Prime Minister and the Ministers involved in the digital transformation of Togolese society, taking account of the accompanying national cybersecurity, is the main guarantee of the success of the national strategy for digitising society and its economy.

This strong political will has enabled the national cybersecurity regulations and the Public-Private Partnership agreement between the Togolese Republic and Asseco Data Systems to be implemented in record time, along with the operational cybersecurity framework.
The following are now operational:

- The National Cybersecurity Agency (NCA);
- Cyber Defense Africa SAS (CDA);
- The national CERT (CERT.tg);
- The national SOC;
- A team of Togolese specialists to assist the OES.

The commitment of all the actors involved in national cybersecurity under the leadership of the Head of State allows an optimal operational action and strict control.

2.1.2.
The legal and regulatory framework

The legal and regulatory framework put in place in Togo encourages stakeholders to strengthen their cybersecurity and personal data protection posture, and provides for a set of sanctions likely to discourage behaviour that destabilises confidence in society and the digital economy. This factor encourages citizens, businesses and society as a whole to comply with the regulations.

It establishes a framework that encourages public awareness and draws the public's attention to risky behaviour that exposes them to cyber threats on a daily basis. All these mechanisms contribute to a change in social behaviour, with a continual reduction in the number, severity and impact of cyber-attacks that take place in Togo.

The establishment of regulations and social norms, as well as law enforcement, are an important factor in the implementation of successful cyber security.

2.1.3.
An innovative operational framework commensurate with challenges

The National cybersecurity is subdivided into two levels of functions:

1. The regulatory functions, monitoring the national cyber security strategy, and controlling the application of operational cyber security in accordance with national regulations;
2. The operational functions for implementing national cyber security.

Separating these two levels of functions ensures that national cyber security is more successful. This is the decision taken by the Togolese government when it decided to entrust the implementation of the national cybersecurity policy to two different organisational structures: the NCA and CDA.

The NCA, as a national authority, has the institutional anchoring necessary to carry out its missions of regulation and control of the cybersecurity sector CDA, which is the result of a public-private partnership, in addition to its role as the technical and operational arm of the NCA, has the skills and operations more in line with the private sector, which enables it to provide this sector with the operational service it needs.

2.1.4.
Financing cybersecurity activities

Setting up an SAS as a Public-Private Partnership in charge of the proactive protection of the administration, State institutions, operators of essential services and citizens makes it possible to optimise the funding and expenditure linked to cyber security.

CDA operates both the national CERT and the national SOC, creating synergies between CERT and SOC resources and generating cost savings.

Through the national SOC, CDA offers managed security services (also known as facilities management) to Togolese businesses. This enables companies to entrust all or part of the security of their information systems to the national SOC. Companies save on costs, time and reliability. The implementation of an in-house security system capable of dealing with the most serious attacks requires significant investment in both hardware and personnel. With the managed services offered by CDA, Togolese companies can benefit from higher quality security at a lower cost. They also benefit from the guarantee that their information systems will be secured by a national company audited and controlled by the NCA.

The revenue generated by these services for businesses makes it possible to minimise State funding of public utility activities such as the national CERT, the SOC for public administrations, training for civil servants, awareness campaigns and other related activities.

2.1.5.
Collaboration between all national actors

Too often, business and national leaders wrongly believe that cybersecurity is the exclusive domain of IT specialists or cybersecurity experts. This simplistic understanding of cybersecurity provides an ideal breeding ground for cyber criminality.

The organisation of a cyber-attack exploits IT vulnerabilities or failures as well as human or organisational vulnerabilities. Cybersecurity concerns everyone, users, communication specialists, lawyers, security service staff, managers, IT specialists, etc.

The Togolese authorities have understood this, by placing the National Cybersecurity Agency under the technical and administrative supervision of the Ministry of Security and the Ministry of the Digital Economy. Moreover, the agency is administered by a strategic committee chaired by the Prime Minister, composed of the Minister in charge of Security, the Minister in charge of the Armed Forces, the Minister in charge of Justice, the Minister in charge of the Digital Economy and two representatives of the Presidency of the Republic.

CDA, the body responsible for national operational cybersecurity is under the supervision of the Ministry of Security and Civil Protection, the Ministry of the Armed Forces, the Ministry of the Digital Economy and Digital Transformation and the Ministry of the Economy and Finance.

2.1.6.
The international cooperation

The international cooperation for cybersecurity is a vital element in the securing the national cyberspace successfully. It is based on exchanges of data, information and experience concerning threats and responses, and best practices. It also involves raising collective awareness on cybersecurity issues and aligning countries on common norms and standards. In this respect, Togo has ratified the African Union Convention on cybersecurity and the protection of personal data and, as part of the project "Organised Crime: West African Response on Cybersecurity and fight against Cybercrime (OCWAR-C)" the regional cybersecurity and fight against cybercrime strategy and the regional critical infrastructure protection strategy.

On the operational plan, international cooperation enables Togo to be continually enriched with information, particularly on trends in the sector. Moreover, cyberspace is the centre for the exchange of data and information between humans, which means that international cooperation in cybersecurity concerns all human security activities, such as civil society security services, including computer and police investigations in the field, legal services and control mechanisms.

The NCA, CDA and CERT.tg teams representing Togo actively participate in international cooperation in order to benefit from information received from abroad, and to disseminate useful information and solutions to concrete problems that arise.

Togo's involvement in international cooperation for the success of its national cybersecurity has gained considerable momentum since CDA has came into operation, and CERT.tg is a member of the international CERT networks as AfricaCERT, TF-CSIRT and FIRST. It also has a privileged partnership with ComCERT, the CERT of the Asseco group.

As part of their partnership, the ANCy and CDA will have to step up this international cooperation activity by strengthening its collaboration and its contribution on cybersecurity issues and by asserting its place in the global cyber ecosystem.

2.1.7 Public-Private Partnership for operational cybersecurity

The Public-Private Partnership (PPP) approach adopted by the Togolese Republic for the creation of CDA has enabled effective and efficient capacity building. Benefiting from the expertise of its partner Asseco Data Systems, Togo has ensured a successful transfer of skills and technologies, enabling it to assist the NCA with a competent operational entity.

This partnership not only makes it possible to make up immediately for the shortage of expertise to operate the technical framework for proactive defence against cyber threats, but also to develop in the medium term local capacity to manage cybersecurity infrastructures. This approach means that Togo now has an entity capable of delivering high-quality cybersecurity services to public bodies and private companies CDA has provided cybersecurity training at national level for the RSSI of several OES and at regional level for Interpol and OCWAR-C.

2.2
The main weaknesses of the national cybersecurity strategy

2.2.1.
Low level of maturity in cybersecurity

Cyber threats are developing quickly, cyber attackers have reached a high level of maturity and are organising themselves into groups to combine their skills. Their actions are increasingly sophisticated, persistent and targeted against organisations and governments.

The issue of cybersecurity is relatively recent in Togo for the majority of local institutions and businesses. The lack of awareness among managers and the togolese population in general, and the lack of specialised cybersecurity training, represent a weakness when it comes to ramping up cybersecurity programmes in the country.

To reach a sufficient level of maturity, teams need to be brought up to speed quickly, actions need to be optimised, and the whole process needs to be supported by sufficient budgets.

2.2.2.
Shortage of cybersecurity skills

An operational and effective cybersecurity service requires the organisation of teams of specialists who know how to adapt to a fast-changing environment and have many years of experience in a variety of skills.

The number of experts in the field is very insufficient in Togo as well as in Africa.

In Togo, this shortage is reflected in a permanent difficulty in recruiting skills. Recruitment in the field most often involves employing IT specialists who need to be trained and converted to cybersecurity professions, which requires some time and support resources.

2.2.3.
Insufficiently secure essential services

In view of the country's ambitious digitalization plan, more and more so-called essential services for public safety, economic stability, national security and international stability are based on digital infrastructures. The operators of these services must be aware of the impact of a cyber-attack on these essential infrastructures and deploy a global cybersecurity strategy based on the legal obligations and risks inherent in their sector. This strategy must be accompanied by operational deployment that is consistent over time. Beyond these technical aspects, users' reluctance to change is a sociological factor that needs to be taken into account.

2.2.4.
The lack of effective prosecution of cybersecurity crimes and offences

Cyberspace has no borders and cyber attackers can hide effectively by covering their tracks. It is therefore difficult to determine who is behind a cyber-attack. However, criminalising hackers is fundamental to securing cyberspace.

Therefore, the legal and regulatory framework put in place in Togo and international cooperation are key elements in the prosecution of cybercriminals. However, the capacities of those involved in the fight against cybercrime need to be strengthened by training judges and law enforcement officers in the detection and effective prosecution of these crimes and offences.

2.2.5.
A still limited budget

Togo has decided to call on all its national forces, both public and private, to establish a substantial budget dedicated to cybersecurity, in order to be able both to deploy the necessary hardware and software infrastructure, and to ensure the rapid increase in the skills of the teams and implement, in the best possible conditions, security actions in Togolese cyberspace. Despite the efforts made, budgets remain limited, hence the need to increase the financial envelope devoted to this purpose.

2.3
The main opportunities for the national cybersecurity strategy

2.3.1.
The momentum of Togo's digitalization

In the national strategic context, the momentum of Togo's digitalization developed in section 3.2 represents an opportunity for the country's cybersecurity. The legal, structural and organisational bases that have been put in place represent a strong asset for its success. Implementing digitisation at the same time as security is a tremendous opportunity that will enable Togo to build a secure digital environment.

2.3.2.
The African and global response to cyber threats

With the awareness that cyberspace has no borders, cybersecurity is being organised at both African and global level. Major structures are being set up to ensure coordination and collaboration between countries in order to deploy common measures and harmonise the texts governing the sector worldwide.

The following works and initiatives are the perfect illustration:

- The work carried out by the United Nations, particularly in the context of Resolution no. 74/247 on combating the criminal misuse of information and communication technologies, adopted by its General Assembly on 27 December 2019, which decided to establish an ad hoc intergovernmental committee of experts with the task of drafting a comprehensive international convention on combating the criminal misuse of information and communication technologies;

- The work carried out by the International Telecommunication Union, including the launch in 2007 of an international cooperation framework designed to increase confidence and security in the information society, the "Global Cybersecurity Agenda", and the drafting in 2021 of the "Draft Guidelines" for its implementation;

- The proliferation of African initiatives on cybersecurity and the fight against cybercrime, in particular the drafting by the African Union Commission and the Internet Society (ISOC) of the Internet Infrastructure Security Guidelines for Africa on 30 May 2017 and the definition by AFRIPOL (African Union Mechanisrn for Police Cooperation) of a Cybercrime Strategy;

- The African Union Convention on cybersecurity and the protection of personal data - known as the "Malabo Convention" adopted on 27 June 2014 by the twenty-third ordinary session of the Conference of the African Union in Malabo, Equatorial Guinea, to enable the development of a safe African cyberspace;

- The work of the project "Organised Crime: West Africa's response to Cybersecurity and the fight against Cybercrime" (OCWAR-C), which aims to assess the state of readiness in terms of cybersecurity and determine the level of maturity of each ECOWAS Member State and Mauritania. And this in order to establish an action plan for each State. These works helped to set up a regional cybersecurity strategy and a regional protection of critical information infrastructures policy;

- The work of the Global Forum on Cyber Expertise (GFCE), a multi-stakeholder community of more than 140 members and partners from all regions of the world, aimed at strengthening cyber capabilities and expertise on a global scale.

To fight efficiently against cyber-attacks perpetrated by individuals and organised groups with different motivations, it is important to continually increase international initiatives aimed at raising the level of cyber security of organisations and countries to ensure continued global stability.

This shared commitment to the fight against cybercrime continually reinforces mutual assistance, partnership and good technical, behavioural, organisational and legal coordination between the various actors involved in cybersecurity.

2.3.3.
A young population with an appetite for learning

Togo has around 8.3 million inhabitants and 70% of the population is under 35. This young population is one of the pillars for structurally transforming the economy and developing strong, sustainable, resilient and inclusive growth. These young people use information technologies and are eager to learn. This represents an opportunity for Togo when national training programmes in digitalization and cybersecurity become effective.

2.3.4.
A growing economy

According to the main macroeconomic indicators published by the IMF, real GDP per capita growth in 2021 was +2.6%, and for 2022 it will be +3% for a population of around 8.6 million. This growth has increased after lowering due to the negative impacts of COVID 19.

This growth has been sustained by reforms, including those in logistics and transport around the Autonomous Port of Lomé (APL) and the Gnassingbé Eyadema International Airport (GEIA), telecommunications, finance and banking, which have made it possible to maintain a stable macroeconomic framework and to motivate technical and financial partners to continue to support Togo through development programmes and projects.

The good health of the Togolese economy represents an opportunity to pool all financial and human resources to strengthen the security of the country’s cyberspace.

[7] IMF Services Report N° 20/107 of May 2020

2.4 The main threats to cybersecurity strategy

2.4.1. The cyberspace: a space without borders

The cyberspace is often presented as a virtual territory, a space apart, without borders, free from the constraints of the physical world, whose intangible nature is reinforced by the advent of the Cloud.

This situation is forcing us to rethink the principle of sovereignty because of the multiplicity of actors and the intertwined nature of the issues and risks involved. New online services are upsetting the economic balance and threatening entire sectors; cyber-attacks are increasingly numerous, targeted and sophisticated, threatening the security of vital infrastructures and citizens; companies can see their data stolen, disclosed, destroyed or their installations sabotaged remotely; individuals are exposed to the exploitation of their personal data and privacy by governments or companies; police officers and judges face the challenge of encryption of online communications by terrorists and criminals; military personnel risk having their operational capabilities affected by sabotage, manipulation of information or influence.

To handle this situation, it is necessary to rebuild a new approach with new legislation, rethinking sovereignty and modes of governance

2.4.2.
A constantly changing world

The world of information technologies is constantly evolving. Cyber threats are evolving at the same pace as societies are digitalising and citizens are adopting technologies States, public administrations, private companies and certain individuals are now the target of advanced persistent threats APTs (Advanced Persistent Threats) are threats that are much more subtle, intelligent, sophisticated and dangerous than previous ones They are stealthy and continuous over time and take advantage of human failings or vulnerabilities present even in the latest versions of software or equipment

Cybercriminals are constantly adapting their techniques and methodologies to circumvent the security measures in place. In the face of these constantly evolving threats, cybersecurity experts also need to keep abreast of all these developments in their role as guarantors of the security of the information systems for which they are responsible.

2.4.3.
Regional cybercrime

The West African region is full of cyber crooks who regularly hit the headlines, such as the «Yahoo boys», the «Sakawa boys», the "Brouteurs" and the «gayman», who are being combated by Nigeria, Ghana, Ivory Coast and Benin respectively. Because of Togo's geographical proximity to these countries and the significant strides they have made in the fight against cybercrime, the togolese territory is becoming a haven for these cybercriminals. As with the physical security of a country, effective cybersecurity and the fight against cybercrime require a detailed understanding of people's socio-cultural beliefs and habits.

To guide the cybersecurity approaches to be implemented, an in-depth analysis will have to be carried out on the origin of national threats, knowledge of organised attack methods in the region, the types of action taken by known groups, recognised forensic approaches, and so on. Similarly, an analysis must be carried out of vulnerabilities based on lifestyle, beliefs, political convictions and links with the populations of neighbouring countries.

In other words, cooperation and exchanges of information with countries in the sub-region are important, as is their level of investment in operational cybersecurity.

2.4.4.
A reduced or weak budget

In Togo, the funding of cybersecurity activities represents a new line of thinking that political and business leaders must now take into account. The main reason for this is to implement operations to reduce the potential costs associated with large-scale incidents on the essential digital infrastructures needed, as the case may be, for the activity of the country's business or government. For a director whose objective is to maximise profits or demonstrate good management by reducing costs as much as possible, cybersecurity-related costs are not a priority. It often takes a great deal of courage to incur costs which usefulness is not sufficiently obvious to decision-makers.

What's more, the implementation of budgetary changes at administrative and legislative level is often out of step with the dynamism of cybercrime.

Cybersecurity must no longer take second place to digital transformation and must be at the centre of the concerns of private or public businesses like governments.

The current period has thus highlighted the importance of allocating more substantial budgets dedicated to cybersecurity.

Moreover, opinion polls show that governments in developed countries have substantially increased their budgets for cybersecurity, in recognition of the high risks and threats involved.

Consequently, it is becoming urgent for developing countries to increase the financial envelope dedicated to cyber security, so as not to remain on the side lines of the revolution in the fight against cyber threats that threaten the ongoing digital transition.

This increase in the budget envelope requires an increase in the internal resources mobilised and also in external resources. But, in the event of an economic crisis, the capacity for internal mobilisation is reduced because companies are doing badly (the tax resources mobilised are no longer equal to the ambitions) and the resources that can be mobilised become scarce.

3.
The national cybersecurity strategy

In this chapter, we set out to define the national cybersecurity strategy with actions to be deployed until the end of 2028. A mid-term review will be carried out on the basis of a new analysis of achievements and changes in strengths, weaknesses, opportunities and threats.

We rely on the SWOT analysis of the previous chapter, with the priority of consolidating the strengths developed in previous years, with the aim of reducing the potential for threats to take hold of existing weaknesses, while building on the opportunities available in Togo.

The role of all the actions defined is to protect the economy and society against disruptions linked, among other things, to information and communication technologies (IT/ICT) and operational technologies (OT).

The national cybersecurity strategy is based on the following four (04) strategic objectives:

1. Promote a culture of cybersecurity and develop national technical skills;
2. Ensure the continued security of essential services and the digital economy;
3. Strengthen the cybersecurity incident response system;
4. Ensure effective prosecution of cybersecurity crime.

In order to achieve the strategic objectives listed above, it is necessary to determine the following for each of these strategic objectives:

1. The objectives and priorities;
2. The measures and actions to be implemented;
3. The key actors involved in the implementation of the national cybersecurity strategy.

The cybersecurity strategy is aimed directly at public administration entities, operators of essential services and indirectly at other public authorities, entrepreneurs and citizens.

The National Cybersecurity Strategy NCS 2024-2028 is therefore based on four (04) pillars:

- Pillar 1 : Promotion of a cybersecurity culture and development of national technical skills;

- Pillar 2 : Ongoing promotion of the security of essential services and the digital economy;

- Pillar 3 : Strengthening the cybersecurity incident response system;

- Pillar 4 : Strengthening the framework for the effective prosecution of cybersecurity crimes and misdemeanors.

1. Promoting a culture of cybersecurity and developing national technical skills;

2. Ensuring the security of essential services and the digital economy;

3. Strengthen the cybersecurity incident response system;

4. Ensure effective prosecution of cybersecurity crimes and offences.

4. Orientations of the cybersecurity strategy

4.1 Pillar 1: promoting a culture of cybersecurity of the populations and developing national technical skills

As the human factor is a major cause in 95% of cyber-attacks, there is no doubt that awareness and training are a very important part of a solid cybersecurity strategy. Indeed, when the majority of attacks specifically target users, seeking to encourage them to click on a malicious link, disclose login credentials, open an attachment or simply pay a fake bill, creating a culture of cybersecurity to detect and repel these attacks seems an obvious choice.

To implement this culture of cybersecurity, both in companies and among the population, it is necessary to train people to use digital tools responsibly and securely. But to be more effective, this training would be better targeted at younger people, right from the start of their school careers.

Aware of this reality, the national strategy has decided to pay a particular attention to the following aspects:

1. Teaching in primary and secondary schools
2. Teaching in higher vocational education
3. Public awareness programme

Ultimately, the implementation of these reforms will make it possible to bridge the skills gap that the digital economy needs for its development and to improve people's skills so that they can make greater and more responsible use of digital technologies.

4.1.1. Integrate cybersecurity teaching into primary and secondary education

The Togolese government's objective is to focus on opening up young people to new technologies by modernising existing equipment and connecting schools to the Internet using a PPP model that mobilises national savings.

But more than that, there is a real desire to set up training programmes in the education system to ensure that pupils are integrated into the digital society and learn about digital media, because the objective of schools remains the training of citizens, and the digital dimension cannot be neglected today, because investing in Cybersecurity should no longer be seen as a cost, but as an investment.
As primary and secondary education is a key channel for transmitting a culture on the potential of information technologies and the risks associated with them, it is important to prepare a teaching programme and incorporate cybersecurity into the training of teaching staff with a view to transmit.

- Knowledge and understanding of how the technology works and its limitations;
- The risks and threats associated with this source of information;
- Best practice in its use;
- Ways of finding and verifying information using a variety of sources.

Teaching of information technology and cybersecurity at primary and secondary level will help prepare young people for university studies in the fields of technology and cybersecurity. The most talented students could be guaranteed the chance to continue their studies (scholarships) or even find employment in this sector.

It is for this reason that digital technology should be introduced very early on as an object of learning in training curricula and extended to the higher education cycle I encourages and promotes the use of technology in teaching, with a view to providing a digital solution to the challenges of capacity in teaching and education establishments and institutions.

RESPONSIBILITY

- MINISTRY OF DIGITAL ECONOMY AND DIGITAL TRANSFORMATION
- NATIONAL CYBERSECURITY AGENCY

PARTICIPANTS

Ministry of Primary, Secondary, Technical and Crafts Education

INTERVENTIONS

1. Prepare a training programme on new technologies, starting in the first primary classes and including practical exercises:

   a. The basics in computer science;
   b. Use of Internet;
   c. A good knowledge of all terminals, including mobile phones and smartphones;
   d. Searching for information;
   e. The security of online transactions;
   f. Online identification and authentication;
   g. Social networks.

2. Involve security experts to support teachers in the scope of the training courses and application exercises to be implemented, so that the programmes can evolve and be adapted to the pupils' ability to understand and integrate the knowledge. To ensure greater success, it is important that these training programmes are close to the usage habits of the pupils who will be taught.

[9] Ministry of Primary, Secondary, Technical and CraftS Education (https://education.gouv.tg/)

INTERVENTIONS

3. Depending on opportunities and capacities, facilitate and motivate e-learning activities - particularly in rural areas. It is important to choose the strengths and resources that will enable real education to be offered in less digitised areas. The experience of the COVID-19 pandemic can provide new concepts in this aspect to reach rural areas with educational information - not necessarily with the use of computers.

4. Organise cybersecurity competitions (hackaton, CTF) to identify, recruit and coach talents.

4.1.2. Integrate cybersecurity teaching into higher vocational education.

The development of the digital economy and the provision of cybersecurity require a highly qualified staff. Vocational training is a multi-year process that requires an analysis of the foreseeable needs of the future labour market in order to plan the education programmes to be implemented accordingly. It is a continuous process managed by the Ministry of Higher Education and Research, the Ministry of Technical Education and Vocational Training and the Ministry of the Digital Economy and Transformation, based on forecasts of the development of the established labour market.

The Togolese government will endeavour to strengthen international cooperation in higher vocational intelligence through exchanges of university staff, study programmes and students.

In order to guarantee its sovereignty in the field of vocational training thanks to a highly qualified workforce, the Togolese Republic is determined, as far as possible, to ensure its independence from foreign suppliers of technologies and solutions, in order to have at its disposal, within its labour market, appropriately qualified personnel for national control of the development and maintenance of highly qualified skills.

RESPONSIBILITY

NATIONAL CYBERSECURITY AGENCY

PARTICIPANTS

1. Ministry of Higher Education and Research;
2. Ministry of Technical Education and Crafts;
3. Ministry of the Digital Economy and Digital Transformation;
4. University of Lomé;
5. University of Kara.

INTERVENTIONS

1. Preparation of postgraduate cybersecurity courses, in particular for :

   1.1. Management and production engineering;
   1.2. Software development;
   1.3. Telecommunications - computer networks;
   1.4. Computer science - system architecture;
   1.5. Information security management.

The preparation of an effective training programme must be preceded by a review of the existing training programme. Next, it is necessary to plan the possibilities of new directions, taking cybersecurity into account, by checking the skills required of university staff, the infrastructure (e.g. laboratories) needed to run the courses, and the scope of the programme itself.

2. Including companies in the preparation of training programmes:

Close collaboration with business representatives regarding the expectations of the labour market is necessary to achieve the desired goal. In this respect, companies will be involved in identifying the expectations of the labour market with regard to graduates, and will be key players in setting up training programmes that will provide the skilled employees expected.

[10] Ministry of Higher Education and Research (https://edusup.gouv.tg/)

[11] Ministry of Technical Education and Crafts (https://edutech.gouv.tg/)

[12] Ministry of the Digital Economy and Digital Transformation (https://numerique.gouv.tg/)

INTERVENTIONS

3. Mobilising grants in the field of cybersecurity

4. Online training

It will also be necessary to facilitate online learning activities and access to knowledge.

When preparing these courses, it is important to ensure:

- The choice of e-learning platform;
- The planning and content of the courses;
- Monitoring the delivery of training courses and evaluating their effectiveness.

The COVID-19 pandemic has provided a wealth of experience in distance learning that could be put to good use.

4.1.3. Implementing an awareness programme

The aim of awareness-raising is to motivate citizens to use cyberspace services and information responsibly, by continually drawing their attention to the associated risks and threats.

The development of national digital security necessarily involves a change in the habits of citizens, who are in the front line when it comes to cyber threats. However, it has been noted that, as things stand, awareness is still very low, or even non-existent in some places, despite the many efforts made by the government in this area. It is therefore urgent to develop a national cybersecurity awareness programme, encompassing all social strata in the country, the State, businesses, civil society, the media, universities, schools and, above all, rural populations.

With this in mind, communication methods and media should be adapted to the perceptive capacities of the beneficiaries. To this end, messages should be short, simple to understand and adapted to the circumstances.

An effective awareness-raising campaign is permanent and dynamic. A co-ordination team is in contact with as many local, regional and national sources of communication as possible, such as the government, the various regional administrations, the various sectors of activity (telecommunications, banks, water and electricity services), etc. The most accessible media are television, radio, advertisers' websites, social networks and other media. While basing on the established awareness programme, the coordination team will use all communications from the various partners to include up-to-date awareness and security messages about the most dangerous and emerging threats and vulnerabilities.

RESPONSIBILITY

- NATIONAL CYBERSECURITY AGENCY (NCA);
- CERT.TG WITH POSSIBLE OTHER SECTORAL CSIRT/CERT.

PARTICIPANTS

1. The Ministry of Primary, Secondary, Technical and Crafts Education;
2. Ministry of Higher Education and Research;
3. Ministry of the Civil Service, Labour, Administrative Reform and Social Protection;
4. Ministry of the Digital Economy and Digital Transformation;
5. Ministry of Human Rights, Citizenship Training and Relations with the Institutions of the Republic;
6. Ministry of Security and Civil Protection;
7. Ministry of Communication and Media;
8. Personal Data Protection Agency (PDPA);
9. Electronic Communication and Posts Regulation Authority (ECPRA);
10. Telecommunications providers (companies);
11. Central Bank of West African States (CBWAS);
12. Banks (companies).

INTERVENTIONS

1. Preparing an awareness programme - Information (posters/web), trainings and events

   The social awareness programme should be planned in several ways. Firstly, define one month of the calendar year as Cybersecurity Month. Cybersecurity month could be characterised by well-targeted educational activities using web-based messages (social media) or media announcements. Messages could focus on positive online behaviour by users or warnings about threats.

2. The second pillar of awareness is the launch of an alert programme on emerging threats on the Internet through the following measures:

   - Telecommunications' operators via SMS alerts;
   - Banks via Online Banking messages.

[13] Ministry of Civil Service, Labour, Administrative Reform and Social Protection (https://fonctionpublique.gouv.tg/)

[14] Ministry of Digital Economy and Digital Transformation ((https://numerique.gouv.tg/)

[15] Ministry of Human Rights, Citizenship Training and Relations with the Institutions of the Republic. (https://droitsdelhomme.gouv.tg/)

4.2

Pillar 2: Continuous promotion of the security of information systems of the public sector, operators of essential services and the digital economy

Information systems security (ISS) is a major issue for the operators of essential services (OES), public administrations and the digital economy. These actors are exposed to growing risks of cyber-attacks that can compromise the ongoing of their activities, the protection of personal data and the trust of users. To strengthen the resilience of these strategic sectors, it is necessary to promote an IS culture and to implement measures adapted to their level of criticality.

4.2.1.

Legislative and regulatory provisions, and determination of the institutional framework

The law 2018-026 of 07 December 2018 on cybersecurity and the fight against cybercrime is the legal basis for cybersecurity and establishes the framework for the fight against cybercrime

The National Cybersecurity Agency (NCA) is responsible for the effective implementation of the strategic guidelines and measures, as well as the national sovereignty fund, which contributes in particular to financing the implementation of the national cybersecurity strategy and the actions of the NCA.

Following on from this law, the Decree 2019-095/PR of 08 July 2019 on operators of essential services, essential infrastructure and related obligations determines, among other things, the method for designating operators of essential services (OES) based on the list of essential services by sector of activity structuring Togolese society as well as cybersecurity rules that the OES must respect. In this context, they must have an Operator Security Plan (OSP) in compliance with the "cybersecurity rules" set by the NCA and a "Security Operations Centre" (SOC) to protect their essential IT infrastructures and react in the event of an incident.

The development and application of the national cybersecurity strategy requires the establishment of indicators to evaluate and progress the levels of security achieved.

RESPONSIBILITY

- NATIONAL CYBERSECURITY AGENCY (NCA);
- CERT.TG WITH POSSIBLY OTHER SECTORAL CSIRT/CERT.

PARTICIPANTS

Ministry Of Digital Economy and Digital Transformation

INTERVENTONS

1. Monitoring and optimising the effective implementation of legislation

With the law on cybersecurity, the decrees relating to OES and the creation of NCA as well as CDA and the cybersecurity rules, the Togolese Republic has put in place a legislative and regulatory basis for the security of national cyberspace and the institutions responsible for its application. This is the reference point for setting up the national cybersecurity system. The application of the regulations requires monitoring to ensure that the effects are those expected in order to determine the adjustments to be implemented where necessary. The proper functioning of the supervisory authority (NCA) is essential to the effectiveness of the application of the law. Its action is decisive and should take the form of sanctions against entities that do not comply with the legislation, as well as reports on the development of indicators to measure the effects of the regulations and their application, and rational and justified proposals on possible changes to the legislation.

2. Keep the list of OES up to date

An evolving list of operators of essential services by sector and sub-sector of activity is kept up to date.

3. Supervise the operators of essential services

The decree on operators of essential services precisely sets out their obligations, which are set out in the cybersecurity rules, subject to fines. An annual audit is planned to ensure that the OES comply with Togolese legislation and the security plan accepted by the regulator, which ensures a respectable level of security for their essential IT infrastructures.

The operator's security plan must, among other things, draw up audits, surveys, reports on the exploitations of essential services and incident reports, in order to monitor the indicators measuring their level of security in relation to the objectives set out in their operator's security plan.

4.2.2. Defining security standards and rules

The definition of norms and rules for the security of IT infrastructures supporting essential services is an important element in the implementation of cybersecurity. These elements specify how the requirements and general intentions set out in the regulations are to be implemented in practice.

RESPONSIBILITY

- NATIONAL CYBERSECURITY AGENCY (NCA);
- CERT.TG WITH POSSIBLY OTHER SECTORAL CSIRT/CERT.

INTERVENTIONS

1. Draw up guidelines for the implementation of cybersecurity legislation.

To ensure correct and effective implementation of the cybersecurity legislation, it is necessary to develop or use existing international guidelines for operators of essential services in this area. These guidelines identify each stage of the implementation of the legislation, taking into account all the measures to be taken by the entities required to implement the requirements.

2. Develop and maintain a comparable methodology for assessing the level of security (risks-based)

The methodology is developed by a group of experts. The assumptions of the methodology take into account the fact that it is understandable, simple and at the same time reflects the actual state of information security in a given entity.

INTERVENTIONS

The risk management method covers the following aspects:

- Identification of threats;
- Identification of vulnerabilities;
- Risks assessment;
- Assessment of security controls;
- Risks treatment.

The methodology ensures that the results of the risk assessment provide objective and comparable results. This assessment is carried out on a cyclical basis (it means every year) in order to maximise its effectiveness.

3. Drawing up and updating security assessment reports (Verification)

The development of the audit procedure is based on internationally recognised best practices, such as the guidelines of ENISA (European Union Agency for Cybersecurity) or NIST (National Institute of Standards and Technology). These types of guidelines for implementing audits make it possible to draw on worldwide experience to develop an audit methodology.

4. Carry out an annual survey of the state of cybersecurity in Togo for OES and administrations:

This will involve questioning essential service operators, administrations, civil servants and members of government who work in or are familiar with the field. The aim will be to take stock of the situation, assess the results of the strategy and understand the trends and prospects. The aim is namely to:

- determine the level of protection against cyber threats provided by the country's companies and institutions;
- determine the level of threats faced by these structures;
- assess their level of knowledge in the field;
- assess their practices and customs in this area.

INTERVENTIONS

- assess the level of commitment of decision-makers to cybersecurity issues;
- anticipate market prospects.

5. Conduct an annual survey of the state of cybersecurity in Togo among citizens:

This will involve assessing the results of the strategy on the Togolese population, in particular:

- determining the general public's level of awareness of cybersecurity issues and their interest in the subject;
- assessing the general public's perception of these issues.

6. Maintain a cybersecurity discussion forum to exchange on best practices

A discussion forum is a mean of improving current knowledge among specialists responsible for cyberspace security. For its effectiveness, it must take account of the participation of a wide range of experts from different sectors that are important for the operation of the national cybersecurity system. The forum should also be preceded by an analysis of threat trends and focus on well-defined issues requiring debate. Mechanisms will be put in place to ensure that the conclusions of these debates are communicated to interested parties. In order to ensure that the discussion forums are highly effective, it is important to define their timetable and (if possible) their agenda in advance.

4.2.3. Encouraging investment in cybersecurity

Investment in cyber security does not always yield a measurable return on investment, especially in the short term. How do you put a figure on a risk that has been avoided or pre-empted? However, business leaders have become much more aware of cyber risks in recent years, not least because of the high media profile of attacks, the frequency of which and the costs to the companies and public authorities that fall victim to them are on the increase.

Some studies of risk perception by company directors, such as the one carried out each year by the Allianz insurance company, show that they perceive cyber risk as one of the 3 biggest risks to their companies. Today, the majority of business leaders agree to accord a budget to strengthen the security of their companies' information systems.

Company leaders are then faced with the dilemma of having to allocate an annual budget, which is very difficult to redistribute on the prices of the offered services and which affects the results of the company they manage.

This situation forces boards of directors to limit their attention to these investments. In the face of increasing risks and threats, all initiatives that could provide additional funds should be studied. The interests of businesses and governments converge in the need for security in cyberspace. The government's initiatives to encourage, facilitate and support business investment in cybersecurity should be analysed. Among others indirect aid, such as tax reductions or debt forgiveness to the state, could be considered, with amounts and conditions defined annually in the State budget.

RESPONSIBILITY

NATIONAL CYBERSECURITY AGENCY

PARTICIPANTS

- Ministry of Economy and Finance;
- Ministry for the Digital Economy and Digital Transformation.

INTERVENTIONS

1. Develop an incentive programme for investment in cybersecurity.

Given the specificity of each sector and company, a fair incentive plan for cybersecurity will be drawn up. The plan will define the areas in which investment is necessary and identify companies of mutual interest. Because of the dynamic evolution in the technological and business environment, the programme will be updated annually. This will ensure the inclusion of incentive plans into the State's annual budget plans.

[16] Ministry of Economy and Finance (https://finances.gouv.tg/)

[17] Ministry of the Digital Economy and Transformation (https://numerique.gouv.tg/)

INTERVENTIONS

2. Organise a round table to mobilise resources to implement the programme

A round table of donors should be organised around the elaborated investment plan. The various information security projects in the various areas in which investments are needed.

3. Monitor the implementation of the elaborated investment plan.

An annual report on the implementation of the investment plan must be drawn up. This will make it possible to assess the status of the implementation of the plan, identify bottlenecks and make proposals to improve its implementation in all the sectors involved.

4.3
Strengthening the response system to cybersecurity incidents

Strengthening the national response system for cybersecurity incidents is a strategic priority to ensure the protection of critical infrastructures and sensitive data. This means setting up mechanisms for coordination, information sharing, risk analysis, prevention and reaction to computer threats and attacks. The national response system for cybersecurity incidents must be capable of detecting, identifying, containing, eradicating and restoring cybersecurity systems affected by cybersecurity incidents.

4.3.1.
Establish an effective national system for responding to cybersecurity incidents

No information system can be l00% secure, and security incidents are an integral part of it. Making an information system secure is a constantly improving process, and the detection of an incident must be seen as a potential for improvement, with the aim of preventing information system from this type of incident in the future. This is one of the activities of CSIRT (Computer Security Incident Response Team) or CERT (Computer Emergency Response Team), one of whose main tasks is to provide responses to computer incidents and to the risks and threats to information systems.

These incident response teams rely in their work on information exchange within the international CSIRT / CERT networks in order to develop skills in threat management and prevention and defence methods against them. They provide their services to administrations, businesses and citizens affected by security incidents and to provide new protection and defence scenarios for the latter.

Togo's national CERT, CERT.tg, has been operational since 01 February 2021 and is operated by Cyber Defense Africa (CDA) as a service delegated by the National Cybersecurity Agency (NCA). CERT.tg handles, coordinates and responds to incidents involving the IT security of togolese administrations, businesses and citizens. It publishes reports on intrusions, vulnerabilities and security bulletins via its website https://cert.tg. This website also contains cybersecurity awareness information for families, small and medium-sized enterprises, large businesses, administrations and Operators of Essential Services.

RESPONSIBILITY

- NATIONAL CYBERSECURITY AGENCY (NCA);
- CYBER DEFENSE AFRICA (CDA).

INTERVENTIONS

1. Continuously improve the services offered by CERT.tg

As part of a continuous improvement process, CERT.tg must constantly seek ways to improve in order to guarantee the best quality of service to its constituents and effectively counter the evolving cyber threats.

The main objectives of CERT.tg are to recognise, prevent and detect threats to the security of the information systems of operators of essential public, semi-public and private services in Togo.

CERT.tg will add to its arsenal of current services, research on new techniques and trends in the sector, so as to be constantly up to date.

The national CERT is also responsible for recording and processing network security incidents and responding to direct threats against users. In this respect, clear procedures to be followed, by companies and citizens, have been drawn up in the case of the detection of an incident.

2. Ensuring that the national CERT meets the needs of all the stakeholders

The national CERT is focused on a proactive approach, targeting different constituent groups (telecommunications, banking, government, etc). To this end, it is recommended to develop within the national CERT in order to provide a targeted public service for incident management service with working methods, terminology and an understanding of the particular needs and risks of each constituent.

3. Organise regular national and inter-national cyber security exercises to regular intervals.

With the aim of carrying out security tests for OES, as well as simulations to test the behaviour and resilience of systems to real-life conditions caused by a security incident,

INTERVENTIONS

exercise programmes involving various interveners from the national cybersecurity system will be organised.

4. Draft the national plan for responding to cybersecurity incidents

With the increasing frequency and severity of cybersecurity incidents, it is crucial to provide Togo with a national response plan to prepare for threats that could impact public security, economic stability, national security or international stability. This plan will help Togo to minimise the consequences of a large-scale attack for the nation and assist stakeholders in taking the right decisions in the event of an attack to regain control of the affected information system.

The plan enables:

- to establish the roles and responsibilities of stakeholders during a crisis situation;
- to design means of resolving incidents;
- to ensure that information is properly shared between the various stakeholders;
- to serve as a basis for improving the management and coordination of cybersecurity incidents at institutional level;
- to define an effective communication channel for the transmission of incident-related messages.

4.3.2. Set up an effective response system to cybersecurity incidents at international level

The cyberspace tends to escape the rules governing the physical borders of states because the legal framework governing this area is still very incomplete. As proof of this, the hardware and software tools that make up the information systems are international and interconnected and, as a result, vulnerabilities and loopholes can be exploited from anywhere on the planet. So, it is vital to write down all the components of an information system and to be able to exchange information at a high level on these elements and on provided equivalent services (such as banking, telecommunications, etc.) between specialists, information and experience on current cyber threats as well as on practices in the field of information security.

These exchanges on cybersecurity enable to benefit from the knowledge and experience acquired elsewhere in the world for a quick and coherent response to a threat or an existing local security incident. The national CSIRT / CERT networks support international cooperation in the world of cybersecurity. Conscious of this fact, the CERT.tg represents Togo at the international level and establishes these exchange channels with other international bodies.

To this end, CERT.tg is already a member of AfricaCERT and a listed member of TF-CSIRT. The CERT.tg and NCA collaborators regularly take part in conferences, symposia and other activities organised by CERT communities such as the FIRST.

RESPONSIBILITY

- NATIONAL CYBERSECURITY AGENCY (NCA);
- CYBER DEFENSE AFRICA (CDA).

INTERVENTIONS

Participate in and/or organise international exchanges of experience in the field of cybersecurity at regular intervals.

In the field of international cooperation, it is possible to take part in actively in research workshops, forums, to the creation of a common body of knowledge or exercises. This strategy paper will be to launch procedures to start using external experience and sharing observations in the field of cybersecurity.

4.4
Plier 4: Strengthening mechanisms for the effective prosecution of Cybersecurity crimes and offenses

Cybersecurity is a major challenge for the protection of citizens' rights and freedoms, as well as for the defence of national interests. Given the diversification of online threats, it is necessary to strengthen the national mechanism for prosecuting cybercrime. This mechanism aims to ensure an effective and proportionate criminal response to infraction in the cyberspace, taking account of their seriousness, impact and transnational nature. It involves close cooperation between the judicial judicial authorities, police and intelligence services, private-sector actors and international partner.

4.4.1.
Rules for collecting digital evidence

Digital evidence is quite different from other physical evidence. Digital evidences are easy to collect, but it may be difficult to assess its authenticity and protect it from tampering. Digital evidence can be accessed from anywhere in the world, so it is essential to define rules concerning:

- their storage location;
- the control access to their content;
- the duration of storage;
- the means of protecting them against any modification;
- the mechanisms for transmitting digital evidence.

The transfer of digital evidence between two authorised parties can take a long time. The transfer path may be several thousands of kilometres long and thousands of computer exchange stations located in dozens of countries. The definition of the rules will require close cooperation with local and international telecommunications companies

RESPONSIBILITY

- NATIONAL CYBERSECURITY AGENCY (NCA)

PARTICIPANTS

1. MINISTRY OF JUSTICE AND LEGISIATION;
2. NATIONAL POLICE;
3. NATIONAL GENDARMERIE.

INTERVENTIONS

1. Establish a set of technical rules for the collection of digital evidence

   To this end, it is necessary to define: the types of data that can be considered as evidence to be collected, the types of data source and the basic security mechanisms to ensure the integrity and confidentiality of the data. Rules for evidences should cover the management of data throughout the processing cycle (collection, processing, backup, storage, deletion) while maintaining the responsability of the operation, which is the most important factor in ensuring that the data collected is ultimately considered as evidence in court.

Developing a process approach means:

- the collection of resources - taking evidence samples (telecommunications operators records);
- processing means - examining the material and assessing whether the material can be considered as an element of evidence;
- backup techniques - recording the evidence in an appropriate format to prevent unauthorised modification;
- means of storage - placing evidence in a safe place to prevent unauthorised access;
- the effective deletion of data from the system where this is legally permitted.

The above steps will be detailed in the technical part of the set of rules relating to the collection of digital evidence.

2. Define and implement a harmonised framework for data retention with key actors in the sector.

4.4.2. Create a single entity responsible for combating cybercrime

The fight against cybercrime in Togo is organised around three main entities, the National Police, the National Gendarmerie and the National cybersecurity Agency (NCA) via its operational arm, Cyber Defense Africa (CDA).

This silo approach limits cooperation, slows down investigations and increases costs of the fight against cybercrime. These three (3) entities use the same technologies, the same skills and the same procedures for their investigation missions, but do not create synergies nor economy of scale.

This distribution in Togo also makes it impossible to have a global view of the problem, an effective strategy for combating cybercrime and a single point of contact for all the stakeholders, including telecommunications operators.

The fight against cybercrime also requires the effective collection of digital evidence which is different from other physical evidence. Digital evidence is very difficult to collect and to protect against tampering. Some types of digital evidence do not occur at the "crime scene" and must be protected on the network linking the offender and the victim. This network can be several miles long and linked by thousands of computer equipment located in dozens of countries. This requires close cooperation with local and international telecommunications companies and the strengthening of the capacities of digital forensic laboratories, which will make it possible to carry out work to restore the usefulness of evidences.

RESPONSIBILITY

NATIONAL CYBERSECURITY AGENCY

PARTICIPANTS

1. MINISTRY OF SECURITY AND CIVIL PROTECTION;
2. MINISTRY OF THE ARMED FORCES;
3. MINISTRY OF JUSTICE AND LEGISLATON;
4. NATIONAL POLICE;
5. NATIONAL GENDARMERIE;
6. NATIONAL CYBERSECURITY AGENCY (NCA).

INTERVENTIONS

Create a unit to fight against cybercrime.

The primary aim is to gather the digital skills currently scattered across several police and gendarmerie units into a single one. This, to create synergies, pool resources and make the fight against cybercrime more efficient.

This unit, made up of digital and cybersecurity experts, will be able to design, implement, maintain and operate all projects to combat cybercrime.

Its overall tasks will be:

1. to be the focal point for the fight against cybercrime and for digital and security-related projects;
2. to set up and operate the national laboratory of digital criminalistics;
3. to train staff and support them through the change process;
4. to collect, process, analyse and publish statistics, including on cybercrime in Togo.

This unit, made up of officers from the Police, Gendarmerie and civilians will be the core of a large operational entity dedicated to public, with tools for combating cybercrime, escalation of information (police rescue-type call centre), the fight against fake news, etc.

This entity will operate a digital forensics laboratory on the basis of precise guidelines. The laboratory's activities should focus on scientific research development work in the field of forensic science, particularly the criminalist techniques used in the process of preventing, detecting and combating of cybercrime, as well as expertise, analysis and training. It will also develop methods, standards and rules applicable to the work of digital investigators in police and gendarmerie units.

It will support the nation's other security forces (Police, gendarmerie, TAF, fire brigades, forest rangers, customs, border protection, etc...).

4.4.3
Implement the criminal law of cybersecurity

It is important to clearly indicate the specific procedure and regulations in the fight against cybercrime. In order to ensure that judges are highly competent in the field of cybersecurity and the fight against cybercrime, it is necessary to increase their knowledge. This requires judges to take part in regular training sessions.

RESPONSIBILITY

NATIONAL CYBERSECURITY AGENCY

PARTICIPANTS

1. MINISTRY OF JUSTICE AND LEGISLATION;
2. MINISTRY OF SECURITY AND CIVIL PROTECTION.

PARTICIPANTS

1. Define regulations and procedures relating to cybercrime.

Police and judicial authorities are faced with multiple obstacles and incertitude concerning procedures related to cybercrime especially when collecting digital evidence of cross-border nature.

It is therefore necessary to adapt regulations and criminal procedures to cope with the intangibility and volatility of digital evidence without creating legal uncertainty.

Procedures and regulations should also set limits on the activities of police and forensic laboratories, and provide legal tools for detecting and prosecuting criminal infractions.

[18] Ministry of Justice and Legislation (https://justice.gouv.tg/)
[19] Ministry of Security and Civil Protection (https://securite.gouv.tg/)

ACTIVITIES (CONTINUATION)

2. Train judges on cybersecurity procedures and regulations for cybersecurity.

A training programme for judges who will be responsible for adjudicating on cybercrime will be drawn up and implemented. The training programme will provide an introduction to the field of information security and the national cybersecurity system, discuss the threats and challenges and provide information on the potential effects of criminal activities. The programme for judges aims to make decision-making efficient and effective in judicial proceedings.

5.
Management of the national cybersecurity strategy

5.1.
Monitoring and evaluation of the strategy via the results of the National SOC and CERT.tg

The national cybersecurity strategy covers the period from 2024 to 2028.

The strategy is linked to the NDP and the government roadmap. Its implementation involves all development actors, including ministries, technical and financial partners, the private sector, international NGOs and Civil Society Organisations (CSO), each in its own field of competence. The strategy is overseen by the Prime ministership.In this respect will provide the necessary facilities for the successful implementation of the implementation of the strategy.

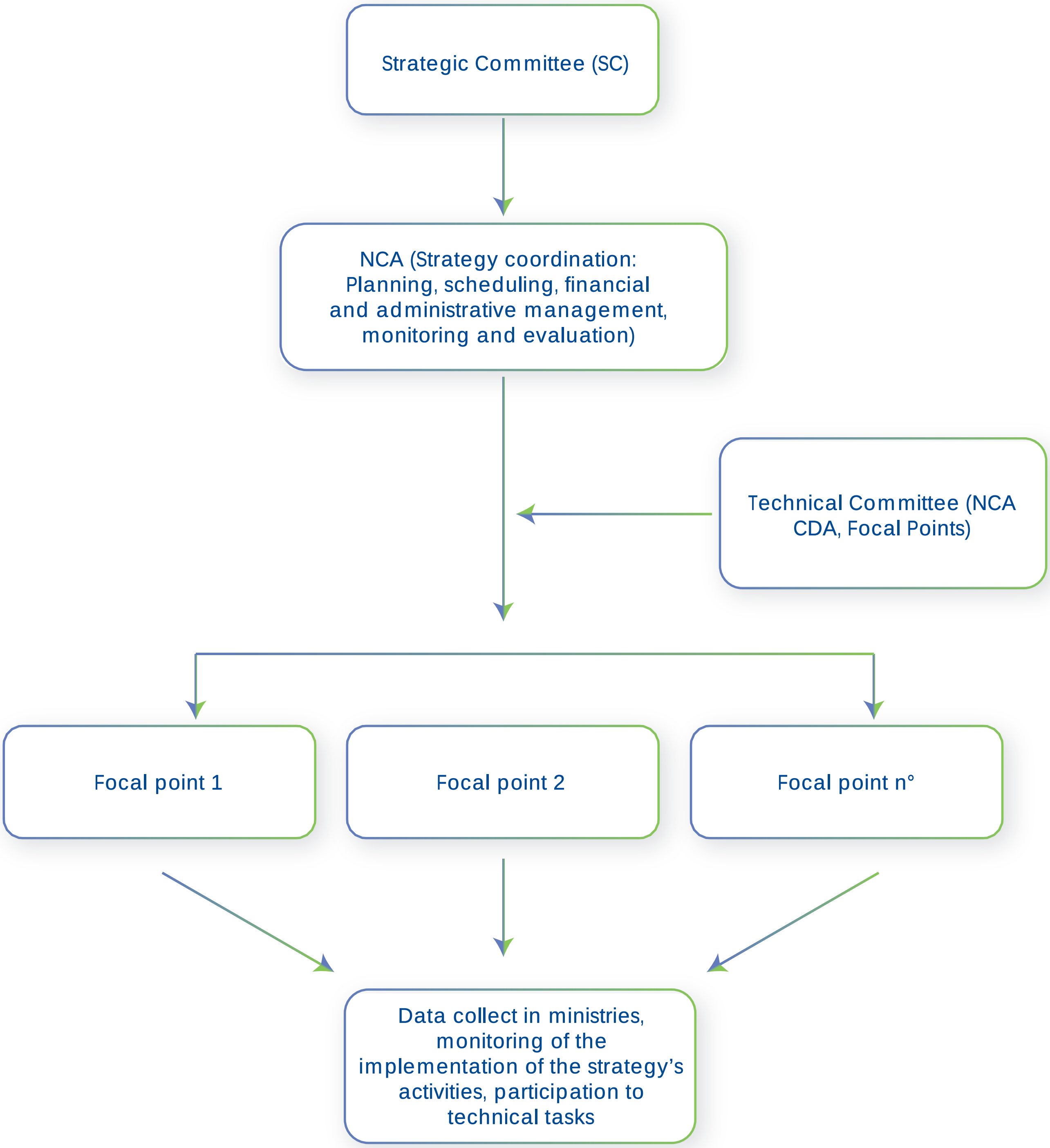
The strategy will be overseen by the Strategic Committee chaired by the Prime Minister. The implementation of the programme will be coordinated by the national cybersecurity agency (NCA). The coordinator for the implementation of the cybersecurity strategy is therefore the Director General of the National Cybersecurity Agency. In coordinating the implementation and monitoring of the strategy, NCA will be supported by a Technical Committee whose members will be the focal points designated by each ministry involved in the implementation of the strategy.

FACE RECOGNITION SYSTEM
HAND RECOGNITION SYSTEM
SERIAL : 124366576796870845
100% MATCH
VOICE IDENTIFICATION SYSTEM
SERIAL : 124366576796870867
50
100
200
400
600
800
1000
1200
1400
1600
200
100
50
0
OBJECT : A-2107/5
MODE : SEARCH
PROGRESS : 87%
STATUS : IN PROGRESS...
IDENTIFICATION
FINGERPRINT RECOGNITION SYSTEM
SERIAL : 124366576796870867
CURL-SHAPED
OBJECT : A-2107/2
MODE : SEARCH
STATUS : COMPLETE
WAVY-SHAPED
OBJECT : A-2107/3
MODE : SCANNING
PROGRESS : 45%
STATUS : IN PROGRESS...
ARCH-SHAPED LOOK
OBJECT : A-2107/1
MODE : SCANNING
PROGRESS : 57%
STATUS : IN PROGRESS...
EAR IDENTIFICATION SYSTEM
SERIAL : 124366576796870867
Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat.
A
39%
B
61%
C
D
A
B
C
D
EYES SCANNER
DNA RECOGNITION SIYTEM
CH3
P(5')
dRib
T
A
H-C
P(3')

Table 1: Coordination framework of the strategy

BODIES	ROLES AND MISSIONS	MEMBERS
Strategic Committee (SC)	The SC will coordinate the strategy. The SC is created by decree of the Council of Ministers. It is chaired by the Prime Minister. The role of the SC is to: ✓ define the political guidelines and directives for the implementation of the strategy; ✓ ensure effective cross-sectorial communication and information ; ✓ mobilise internal and external resources to implement the strategy; ✓ validate the annual reports on implementation of the strategy; ✓ approve the annual budgets and programmes for implementing the strategy. They meet once every three months	The members of the SC are appointed by the Council of Ministers and are composed of: ○ the prime minister; ○ the minister of digital economy; ○ the minister of security; ○ the keeper of seals, minister of justice and legislation; ○ the minister of Army; ○ two personalities of the Presidency
NCA	The NCA will ensure the coordination of the national cybersecurity strategy and will be have for mission: ✓ to prepare and adopt the management and monitoring and evaluation tools for the strategy; ✓ to prepare the documents to be submitted to the committee for approval; ✓ to monitor the implementation of interventions; ✓ to draw up and submit periodic reports on the implementation of strategy activities to the SC; ✓ to prepare the mid-term and final reviews of the strategy; ✓ to hold regular meetings to monitor the implementation of planned activities with all the Focal Points of all the stakeholders to ensure progress on activities; ✓ to take part in SC meetings as part of the implementation and monitoring of the national cybersecurity strategy.	NCA is created by the decree n° – The director general of NCA is the national coordinator of the strategy.
Technical Committee	The Technical Committee is NCA's operational structure for coordinating and implementing the strategy. Its role is to support the NCA in drawing up some documents that will be submitted to the strategic Committee for approval and in the technical validation of some documents/tools	The committee is chaired by the Director general of NCA and is composed of focal points appointed by each ministry involved in the implementation of the strategy. They will meet periodically and whenever the need arises. The Focal Points are responsible for regularly transmitting the progress status of the implementation of activities within their ministries to NCA

Figure 1: Institutional mechanism for coordinating the national cybersecurity strategy


Strategic Committee (SC)
NCA (Strategy coordination: Planning, scheduling, financial and administrative management, monitoring and evaluation)
Technical Committee (NCA CDA, Focal Points)
Focal point 1
Focal point 2
Focal point n°
Data collect in ministries, monitoring of the implementation of the strategy's activities, participation to technical tasks

*Focal points are assigned to each ministry

5.2.
Instruments for planning and implementing the national cybersecurity strategy 2024-2028

The implementation of the strategy is based on the establishment of the action plan, which sets out the activities to be implemented in order to achieve its objectives. A framework for measuring performance and monitoring evaluation indicators is also defined.

Within six months after the adoption of the cybersecurity strategy, the coordinator shall draw up and submit to the Council of Ministers for approval an action plan for the implementation of the cybersecurity strategy. At the time of drawing up the action plan, the above-mentioned authorities shall take account of cybersecurity issues within the limits of their statutory competences.

The action plan will namely include:

1) The name of the specific objective;
2) The name of the task;
3) The name of the action used to carry out the task;
4) The type of action: legislative, organisational, technological, educational, information, promotional and other;
5) The timetable: start date and end date of the undergoing initiative;
6) The organisation or organisations: the lead organisation and the organisations cooperating in the execution of the task (where applicable);
7) The KPIs
8) The expected effects of implementing the action;
9) The estimated cost of implementing the action.

The action plan includes project-type activities, characterised by the beginning and end of the implementation period and by the outputs resulting from the implementation of the activity. An annual review of the action plan will be carried out in order to assess the progress of the activities.

The instruments below will enable a better planning and an effective implementation of the strategy. They are as follows:

- State budget: all the ministries involved in the implementation of the strategy must include the actions that concern them in their budget allocation. In addition, the NCA's budgetary envelope must enable it to carry out, year by year over the five years of the strategy's implementation, the activities for which it is responsible;

- Work Plan and Annual Budget (WPAB): the activities to be carried out in the course of a year must be included in the WPAB of each ministry involved. However, a consolidated annual work plan for the strategy will have to be drawn up by NCA and submitted to the Strategic Committee for approval.

5.3.
Risk factors of the 2024-2028 national cybersecurity strategy

- **Risk related to socio-political instability**: social peace is an important factor in promoting respect for human rights and individual freedoms, thereby guaranteeing the good execution of the strategy.

- **Risk related to security**: the threat of terrorism poses security risks to countries, which could compromise all the development efforts made. Togo must therefore focus its priorities on the fight against terrorism and organised crime in order to ensure that the strategy is implemented efficiently and effectively.

- **Risk related to funding**: the strategy's funding scheme is based mainly on internal resources. However Togo's capacity to mobilise internal resources is still low. In addition, the procedures for mobilising external resources remain fairly cumbersome, despite the efforts made in the context of mutual search for aid effectiveness. All these factors constitute a real risk to the availability of financial resources and, by extension, a risk of failure of the strategy.

This risk of insufficient mobilisation of the funds needed to implement the strategy can only be reduced if greater efforts are made to mobilise internal resources and a redeployment of external economic cooperation in order to diversify development partnerships, etc.

- **Risk related to insufficient capacities**: the success of the strategy will depend on a large extent on the steering framework. New ways of involving development actors (public, private actors and CSO) is necessary. The novelty of these approaches entails a risk that must be minimised by strengthening the capacity of state actors to supervise and monitor the implementation of activities on the field. The success of the strategy also supposes that the necessary resources are available in time.

In addition, if the strategy is to succeed, community actors must be motivated and dedicated, and must have adequate resources to support the implementation of the strategy's activities.

- **Risk related to natural disasters and health crises**: natural disasters and natural crises create instability and displace people, this is not conducive to the implementation of development activities. Periods of crisis often lead to a reorientation of development priorities, which could affect the resources needed to implement the strategy.

6. Financing the national cybersecurity strategy

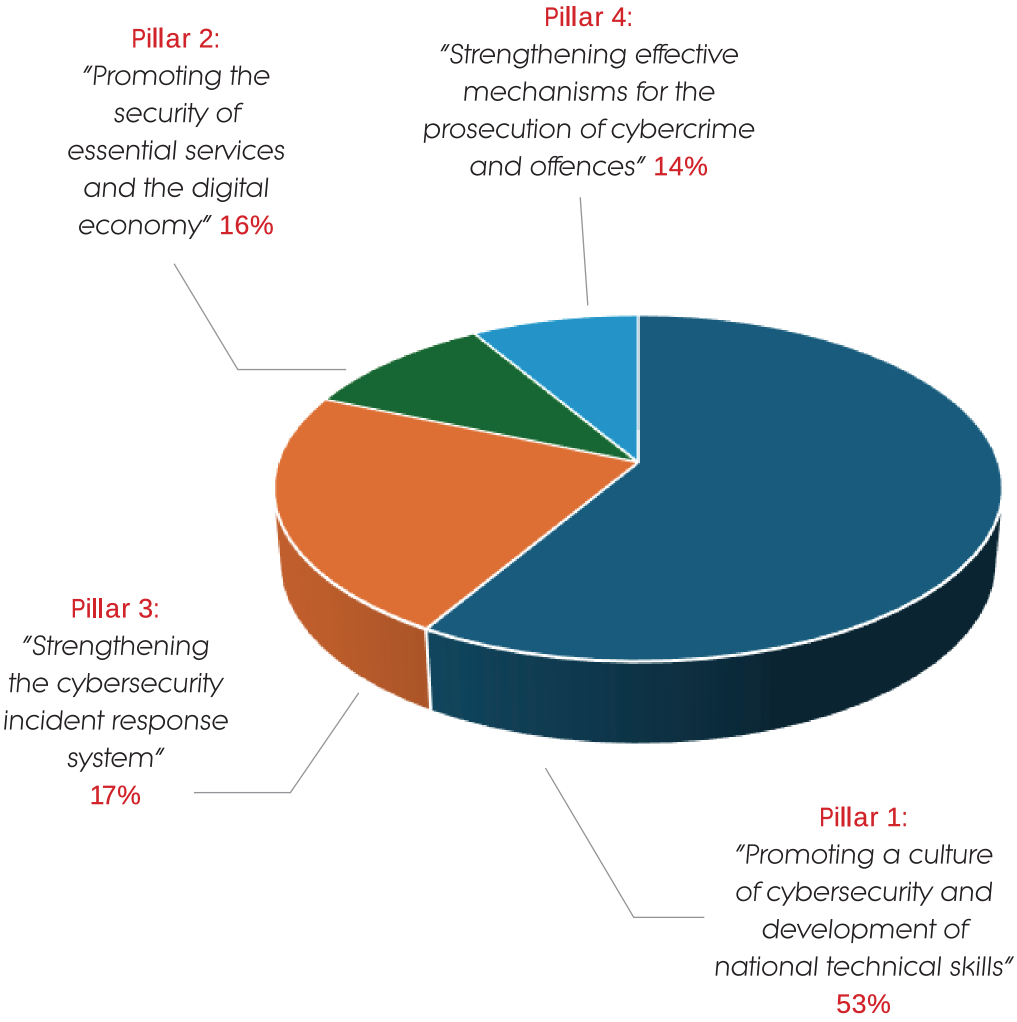
Under current legislation, public mission entities are required to include cybersecurity expenditure in their financial plans.

The sources of funding for the implementation of the activities described in the document will be specified in the financial plans of the various entities involved in implementing the cybersecurity strategy.

Public-private partnerships (PPP) are encouraged in order to minimise expenditure on public funds, implementation times and maximise service quality. The Minister of the Digital Economy and Digital Transformation (MDEDT) is authorising officer for the digital sovereignty Fund, whose purpose is to finance all actions to protect and guarantee Togo's digital sovereignty. These actions include setting up a national CERT, providing SOC services to public administrations, cybersecurity training for civil servants and other related activities.

Other funding mechanisms will be put in place as the Togolese cybersecurity market develops.

Figure 2: Breakdown of the overall cost of the strategy by pillar



7.
Monitoring and evaluation framework for the national cybersecurity strategy

7.1.
Mechanisms for monitoring the 2024-2028 national cybersecurity strategy

In order to ensure that the objectives pursued are achieved, the strategy must be accompanied by a monitoring and evaluation system. This monitoring and evaluation system will be provided by NCA.

The monitoring and evaluation of the strategy will ensure that the planned activities:

- are implemented in accordance with the schedule of activities and that there is coherence/harmony between interventions;
- enable the expected results to be achieved;
- are effective, owned by stakeholders and managed sustainably;
- are relevant to development needs and priorities;
- are monitored so that bottlenecks and risk factors can be identified in time.

To achieve this, NCA will develop data collection tools, report templates, data and report transmission, and plans for data analysis and processing adapted to the needs of the target, which will be validated by all the actors involved in the technical committee made up of the focal points.

To ensure that information flows smoothly and that the reports are validated at each level of intervention, all the stakeholders, in particular the focal points, are responsible for the monitoring and evaluation framework and will therefore have to produce quarterly reports and send them to NCA.

The NCA, check, summarise and prepare the annual progress report on the implementation of the strategy and sends it to the Technical Committee.

The strategy's technical committee verifies, reviews and technically validates the annual reports drawn up by NCA. The reports validated by the technical committee are forwarded to the strategy committee for approval.

7.2. Mechanisms for evaluating the 2024-2028 national cybersecurity strategy

The national cybersecurity strategy provides for two evaluations:

- Mid-term evaluation in 2026

Two years after the start of its implementation, the strategy document will be the subject of a mid-term evaluation. The results of the evaluation will be presented to the strategic committee of the national cybersecurity agency. The procedures and modalities of this evaluation will be determined by the NCA. The validated results will be shared will be shared with all actors.

Following this review, the national cybersecurity Agency will draw up a proposal for corrective measures, which will be submitted for approval to the strategic Committee.

- Final assessment in 2028

At the end of 2028, a final evaluation will be organised. The reference terms for this evaluation will be drawn up by NCA and submitted to the strategic committee for approval. The procedures and modalities of this evaluation will be determined by the strategic committee. The results of the final evaluation will be submitted for validation and shared.

The results of this final evaluation will be used to draw up the second generation of national cybersecurity strategy for the next five years.

Appendixes

Appendix 1
Legal and regulatory framework on cybersecurity in Togo

1. Electronic communications

Law:

- Law n° 2012-18 of 17 December 2012 on electronic communications amended by Law No 2013-003 of 19 February 2013.

This law organises the electronic communications sector and defines the roles of each stakeholder and their relationships.

2. Electronic transactions

Laws and regulations:

- Law n° 2017-007 of 12 June 2017 on electronic transactions;
- Decree n° 2018-062 of 21 March 2018 regulating electronic transactions and services in Togo;
- Decree n° O16/MPEN/CAB du 17 December 2018 on the recognition conditions of electronic certificates and signatures in Togo delivered by the reliable service providers out of the national territory.

The electronic transactions law applies to transactions and services by electronic means and deals with:

- Electronic certificates/signatures and their legal recognition;
- Information to be made available to customers about persons engaged in electronic commerce;
- Information that must be made available to the public by online publishers of public communication services;
- Data enabling the identification of any person who has contributed to the creation of the content or fun of elements of the content of the providers' services;
- The certification authority.

3. Information society

Law:

- Law n° 2017-006 of 22 June 2017 orientation on the information society in Togo (LOSITO).

This law defines the objectives and main orientations of the information society in Togo.

4. Cybersecurity

Laws and regulations:

- Law n° 2016-006 of 30 march 2016 on liberty of access to information and to public documentation;
- law n° 2017-007 of 22 June 2017 on electronic transactions;
- law n° 2018- 026 of 7 December 2018 amended by law no 2022-009 of 22 June 2022 on cybersecurity and the fight against cybercrime;
- law n° 2019-014 of 29 October 2019 on the protection of personal data;
- decree n° 2017-104 of 30 October 2019 relating to the terms of application of the law no. 2016-06 of 30 March 2016 on freedom of access to public information and documentation;
- decree n° 2018-062/PR of 21 March 2018 regulating electronic transactions and services in Togo;
- decree n° 2019-022/PR du 13 February 2019 on attributions, organisation and operation of the National Cybersecurity Agency (NCA);
- decree n° 2019-095/PR of 08 July 2019 on operators of essential services (OES), essential infrastructures and related obligations;
- decree n° 2022-040 /PMRT of 29 June 2022 on the adoption of cybersecurity regulations in the togolese Republic;
- decree n° 2022-090/PR of 25 August 2022 relating to the qualification of reliable providers of cybersecurity services and cybersecurity products and the approval of assessment centres.

The cybersecurity law defines the mechanisms for promoting cybersecurity and establishes the framework for fighting against cybercrime, as well as penalties for digital crimes and offences.

The law on cybersecurity provides for the creation of National Cybersecurity Agency (NCA), in charge of the effective implementation of orientations and measures, and the digital sovereignty Funds, which will contribute to financing the implementation of national cybersecurity strategies and supports the actions of NCA.

5. Personal data protection

Law:

- Law n° 2019-014 of 29 October 2019 on the protection of personal data.
- Decree n° 2020-111/PR of 9 December 2020 on the organisation and operation of the personal data protection authority.

The purpose of this law is to establish a legal and institutional framework to protect efficiently people's fundamental rights and freedoms with regard to the processing of personal data.

The texts also provide for the creation of Personal Data Protection Agency (PDPA).

ANCy
Agence Nationale
de la Cybersécurité

National Cybersecurity Strategy

2024-2028

RÉPUBLIQUE TOGOLAISE

ANCy
Agence Nationale
de la Cybersécurité

National Cybersecurity Strategy
2024-2028

National Cybersecurity Agency (NCA)
Address: 63 Bd du 13 Janvier
Nyékonakpoè, Lomé-TOGO
07 BP 7878
+228 97 52 58 58
+228 70 60 60 83

AncyTG ancytg AncyTogo ANCyTG https://www.ancy.gouv.tg