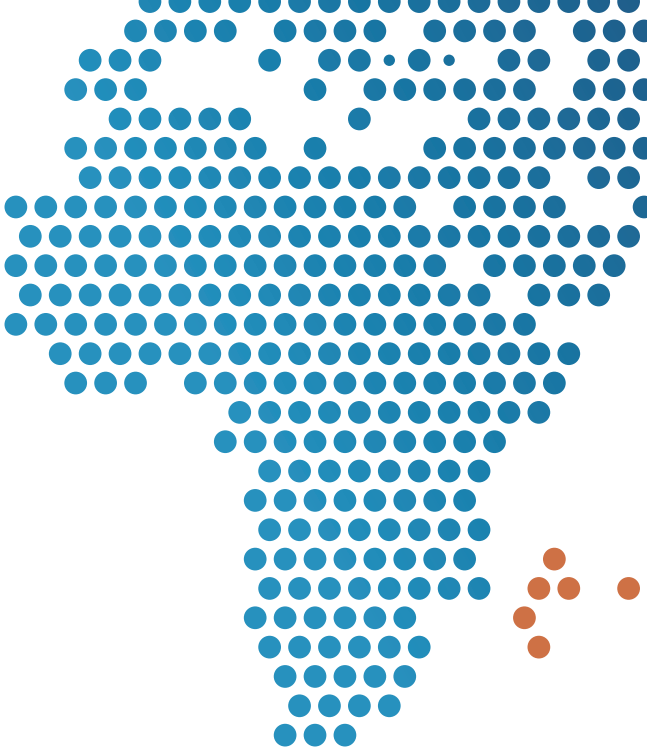
// Amreesh Phokeer (AFRINIC)
// Kevin Chege (Internet Society)
// Josiah Chavula (University of Cape Town)
// Ahmed Elmokashfi (Simula Research Lab)
// Assane Gueye (CMU-Africa)



Avril 2021 (v1.0)

Mesurer la résilience d'Internet en Afrique (MIRA)

Vue d'ensemble du projet

Internet Society

AFRINIC
The Internet Numbers Registry for Africa

Résumé

Internet joue un rôle essentiel dans la société actuelle. La pandémie de Covid-19 a encore souligné l'importance d'une connexion à Internet fiable pour tous. Malheureusement, tous les pays n'ont pas atteint une maturité suffisante en termes de fiabilité de l'infrastructure Internet. En particulier, les pays à faible revenu s'appuient généralement sur des réseaux sous-dimensionnés et ne disposent pas d'un réseau de câbles ou de systèmes d'interconnexion redondants adéquats. Dans ces pays (ou régions), d'importantes coupures d'Internet se produisent en cas de rupture de câble ou de panne de courant. Ces perturbations ont un impact sur l'ensemble de l'écosystème Internet et peuvent entraîner d'importantes pertes de revenus pour l'économie numérique. En outre, de nombreux pays à faible revenu n'ont pas la capacité de réaliser un audit approfondi de leur infrastructure Internet et, dans de nombreux cas, ils n'ont pas élaboré ou adopté de bonnes pratiques pour développer une infrastructure Internet résiliente. Le projet MIRA (Measuring Internet Resilience in Africa) est une initiative conjointe d'AFRINIC (African Network Information Centre, soit, le Registre Internet régional pour l'Afrique) et de l'Internet Society, dont l'objectif est d'évaluer la capacité d'un pays à fournir un moyen stable et fiable de connexion à Internet à tout moment. Sur la base des résultats, nous émettrons des recommandations sous forme de meilleures pratiques qui pourraient aider les réseaux ou les pays à se doter d'un accès à Internet plus résiliant.

1 Introduction

L'un des 13 principes de la Déclaration africaine des droits et libertés de l'Internet[1] est la Sécurité, stabilité et résilience de l'Internet. Ce principe implique que toute personne a le droit de jouir d'une connexion sûre et fiable à Internet, quelles que soient la taille et la localisation de son réseau. La pandémie de Covid-19 a démontré l'importance d'Internet et des services qui en dépendent pour la société et à quel point il est essentiel d'édifier des réseaux résilients. Cependant, de nombreux réseaux africains sont fréquemment soumis à diverses formes de perturbations telles que des pannes de courant, des ruptures de câbles, des arrêts intentionnels ou non et autres incidents de sécurité [1]. Les pannes peuvent être accidentelles, soit en raison d'une mauvaise ingénierie, pour cause de manque d'une infrastructure redondante. Dans certains cas, les perturbations sont dues à des interruptions commanditées par l'État, notamment en période électorale [2]. Dans d'autres cas, les interruptions se produisent car les opérateurs ne sont pas tenus responsables et, par conséquent, n'ont pas d'incitation à investir dans l'amélioration de la résilience de leur infrastructure. Qu'elles soient intentionnelles ou non, les perturbations d'Internet peuvent avoir un impact considérable sur la société et l'économie [3].

De récentes études ont mis en évidence les disparités en termes de qualité de la connexion à Internet entre les pays africains et au sein de ces mêmes pays. [4]–[6]

Cependant, de nombreux problèmes liés à Internet en Afrique n'ont toujours pas fait l'objet d'études. Les affirmations à cet égard reposent principalement sur des connaissances anecdotiques non écrites, partagées de manière informelle entre les acteurs concernés, comme lors de l'Africa Internet Summit (AIS) et du Forum africain sur le peering et l'interconnexion (AfPIF). Cette lacune rend difficile l'élaboration

[1] https://africaninternetrights.org

de solutions fondées sur des preuves ou l'évaluation du succès des interconnexions et des programmes d'investissement nouvellement déployés. Une enquête réalisée par AFRINIC en 2019 [7] a montré que l'évaluation d'Internet n'est pas une pratique courante en Afrique. L'absence d'évaluations efficaces dans les pays africains fait qu'il est très difficile de déterminer avec précision les domaines problématiques devant être traités afin d'améliorer la fiabilité et la résilience d'Internet en Afrique.

Le projet MIRA établira un « cadre de résilience d'Internet » qui évaluera la capacité d'un réseau (et par agrégation, d'un pays) à fournir des moyens stables et fiables de connexion à Internet. Ce cadre sera fondé sur l'analyse de données empiriques (primaires et secondaires) recueillies auprès de divers réseaux et pays en Afrique. Sur la base de ces résultats, nous prévoyons d'identifier et de promouvoir les bonnes pratiques nécessaires à la création d'un système d'interconnexion national et régional plus résilient qui, s'il est mis en œuvre par les fournisseurs d'accès à Internet (FAI) et les opérateurs de réseau, pourra renforcer l'infrastructure Internet et la protéger des perturbations.

1.1 // Contexte

Ce projet est une initiative conjointe de l'African Network Information Centre (AFRINIC) et de l'Internet Society. Il s'inscrit dans le cadre du programme AIM (Africa Internet Measurement) de l'AFRINIC[2] et du projet « Mesurer Internet »[3] de l'Internet Society. AFRINIC et l'Internet Society collaboreront avec d'autres chercheurs, comme décrit dans la section 6.4, pour mesurer la résilience d'Internet en Afrique (Measure Internet Resilience in Africa - MIRA). En résumé, voici nos objectifs :

1. Recueillir et analyser des données empiriques afin de déterminer le niveau actuel de résilience d'Internet dans les pays africains.
2. Accélérer le développement de l'infrastructure de mesure d'Internet en Afrique en augmentant le nombre de points d'observation actifs en Afrique.
3. Présenter les données aux utilisateurs à tous les niveaux (responsables politiques, ingénieurs, opérateurs de réseau, décideurs, internautes, etc.)

1.2 // Public ciblé

Les résultats de ce projet seront utilisés pour informer deux catégories de décideurs :

- Les opérateurs de réseaux et les fournisseurs d'accès à Internet (FAI) cherchant à améliorer la résilience de leur infrastructure.
- Les autorités règlementaires nationales (ARN) qui définissent les environnements juridiques et opérationnels de l'écosystème Internet dans leurs pays respectifs.

Ce projet et ses résultats pourront intéresser un public plus large, notamment les associations de consommateurs et les groupes industriels, les laboratoires de recherche universitaires et privés, ainsi que les organismes de normalisation.

1.3 // Définition et portée

Nous souhaitons étudier, tout au long de ce projet, les menaces qui pèsent sur l'infrastructure Internet et les obstacles auxquels elle est confrontée, ainsi que les mécanismes permettant d'augmenter la résilience des services Internet. En d'autres termes, la capacité d'un réseau à maintenir un niveau de service acceptable en

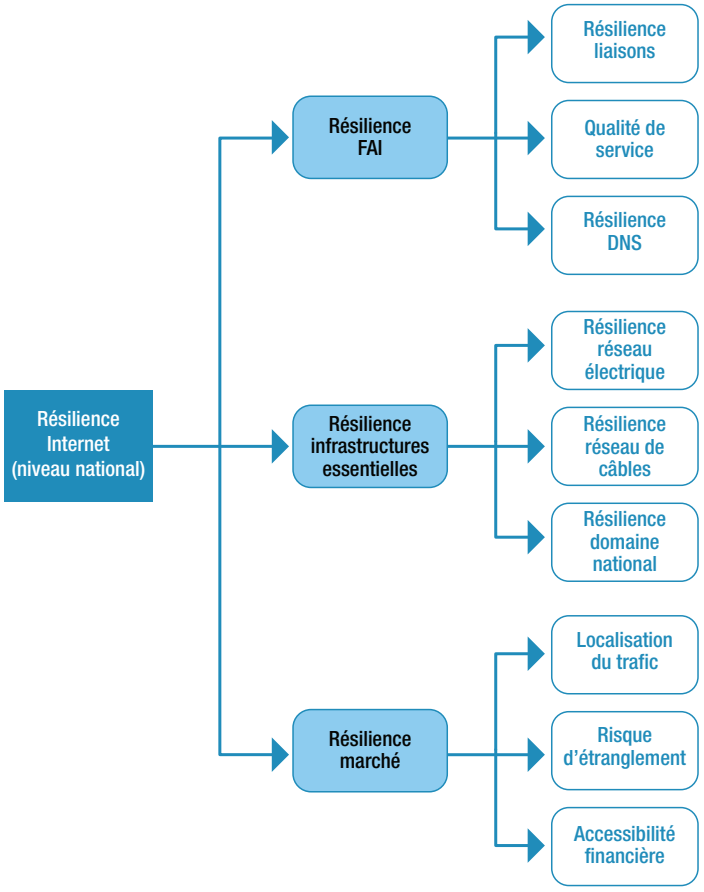


Figure 1: *Taxinomie des composantes de la résilience*

[2] https://afrinic.net/research/programmes/aim
[3] https://www.internetsociety.org/issues/measurement

cas de panne ou de crise [8]–[13]. Ce projet évaluera également la capacité de chaque pays à continuer à fournir le meilleur service possible en cas de crise.

Comme le montre la figure 1, la « résilience d'Internet » englobe de nombreuses composantes[4], allant de la résilience de l'infrastructure physique d'Internet et du réseau électrique à la résilience du marché et à la qualité de service, c'est-à-dire les performances, le temps de fonctionnement, la bande passante disponible, etc.

Définitions :

- Résilience d'Internet au niveau national : la capacité de l'écosystème Internet d'un pays (FAI, règlementations, infrastructure physique, structure du marché) à fournir des services Internet à ses citoyens à un niveau de service acceptable en cas de défaillances ou problèmes entravant le fonctionnement normal.
- Résilience des infrastructures essentielles : la résilience du réseau électrique, du réseau de câbles de télécommunications (terrestres et sous-marins) ainsi que de l'infrastructure des noms de domaine nationaux (ccTLD).
- Résilience du marché : la disponibilité et l'efficacité des points d'échange Internet (IXP) et la capacité à maintenir la proximité du trafic local, la capacité du marché à s'autoréguler et à proposer des tarifs abordables aux utilisateurs finaux sur un marché diversifié et concurrentiel.
- Résilience du réseau et des FAI : capacité d'un réseau à continuer à fournir un niveau de service acceptable en cas de panne ou de crise. Cette composante de la résilience est constituée de divers éléments tels que la résilience des liens physiques, des liens logiques/de peering, des performances/de la qualité de service et du DNS.

Portée et objectifs :

Dans le cadre de notre évaluation, nous tiendrons compte des aspects suivants :

1. La disponibilité et la stabilité de l'infrastructure physique, qui comprend les centrales électriques, la fibre sous-marine ou terrestre, les stations terrestres et les réseaux d'accès du dernier kilomètre.
2. La qualité de service du réseau du point de vue de l'utilisateur final et la stabilité du réseau en termes d'accessibilité, de débit et de latence vers les serveurs cibles sélectionnés.
3. La disponibilité et la performance du système de noms de domaine (DNS).
4. La disponibilité et l'efficacité de la structure de peering locale ainsi que la capacité du pays à conserver le trafic local.
5. La résilience du marché des FAI, c'est-à-dire le niveau de concentration vers des systèmes autonomes (AS) spécifiques et l'accessibilité financière.

2 Approche Et Objectifs

Dans le cadre de ce projet, nous recueillerons des données d'interconnectivité pour les ASN (Autonomous System Numbers) en Afrique et utiliserons ces données pour analyser les indicateurs de résilience, de fiabilité et de performance des réseaux pour la communication entre les ASN. Notre définition principale de la résilience sera axée sur la capacité d'un réseau à tolérer les incidents, tels que ceux causés par des défaillances de dispositifs et des coupures de fibre [10], [14], y remédier et rétablir le service. En tenant compte de la topologie physique, nous étudierons la résilience géographique à la fois du point de vue du réseau de bout en bout et du point de vue du FAI (ASN). En outre, deux autres indicateurs connexes seront analysés : les performances et la fiabilité. Tous les paramètres considérés dans le cadre de ce projet seront évalués au niveau des ASN ainsi qu'au niveau des villes et des pays. Sur le plan géographique, nous regrouperons les routeurs selon différents niveaux de proximité tels que la ville, le pays et la région. Cette analyse sera menée indépendamment de la topologie au niveau des ASN.

[4] Le diagramme illustre la portée initiale du projet et ne constitue pas une liste exhaustive de tous les aspects possibles de la résilience.

2.1 // Aperçu de la conception

Comme l'illustre la figure n° 2, la plate-forme MIRA se compose de plusieurs éléments. Le tableau de bord d'Internet Society Pulse permettra aux utilisateurs finaux de visualiser les données recueillies dans le cadre du projet MIRA. Les utilisateurs pourront concevoir des tableaux de bord personnalisés en fonction de leurs besoins. Les utilisateurs pourront, par exemple, choisir leurs indices et concevoir leur propre indice final. Le tableau de bord Internet Society Pulse recueillera des données à l'aide de l'interface de programmation (API) de MIRA, laquelle peut également être utilisée par les programmeurs pour récupérer des données de MIRA sans utiliser l'interface graphique. L'Outil d'analyse est chargé de générer les indices sur la base des données recueillies (primaires et/ou secondaires).

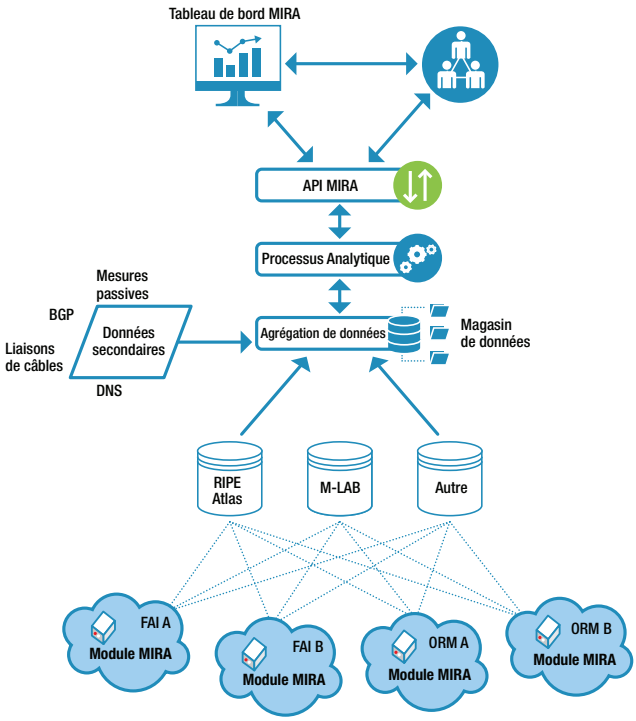


Figure 2 : *Flux de collecte et de visualisation des données MIRA*

Le cadre de résilience d'Internet (4.2 WP2 : Cadre de résilience d'Internet) fournira les caractéristiques de la méthode de traitement des données. Les données proviendront de l'Outil de données, qui stockera et regroupera les ensembles de données primaires et secondaires. Les données primaires seront recueillies par des nœuds de mesure fixes et mobiles basés sur des Raspberry Pi qui utilisent des outils de mesure, à savoir les sondes de RIPE Atlas[5] et l'outil de diagnostic réseau (NDT) de M-Lab[6]. Les scripts de mesure du réseau sont basés sur des outils standards existants et seront installés et orchestrés par le responsable des mesures de MIRA. Les données secondaires proviendront de plusieurs sources de données ouvertes telles que les données de routage des IXP, les informations d'allocation des RIR et les tables de routage BGP (Border Gateway Protocol).

2.2 // Paramètres

2.2.1 Infrastructures essentielles + diversité des chemins

Une des stratégies importantes pour garantir la résilience d'Internet consiste à accroître la diversité des chemins de réseau entre une paire donnée d'hôtes Internet [10], [15]. Dans ce contexte, la diversité est le degré auquel les chemins alternatifs partagent les mêmes nœuds et liens [15]. Pour être plus résilient face aux défaillances, il faut qu'il existe plusieurs chemins disjoints au niveau des liens et des nœuds entre les réseaux [16]. Il est important de noter que la diversité des chemins entre les hôtes connectés à différents réseaux est déterminée par l'infrastructure physique (topologie physique) ainsi que par les politiques en matière de routage (au sein des domaines et inter-domaines) et de peering. La diversité des chemins est intrinsèquement renforcée par le multihoming des AS et des hôtes. Il est donc important d'étudier la diversité des chemins physiques et logiques au travers de plusieurs réseaux.

2.2.2 Performances/Qualité de service

Les opérateurs de réseau mesurent généralement les performances du réseau en termes de métriques standard de qualité de service telles que le débit, la latence, l'instabilité du réseau et la perte de paquets. Les opérateurs peuvent, par exemple, être intéressés par la surveillance de l'encombrement et de la perte de paquets sur les liens au sein des réseaux ou entre ceux-ci. Pour les internautes, les indicateurs de qualité de service ne sont utiles que dans la mesure où ils ont une incidence sur la communication de bout en bout et sur la qualité de leur expérience. Dans ce cas, la qualité d'expérience décrit l'évaluation subjective par l'utilisateur de son expérience lors de l'utilisation d'un service réseau en particulier [20]. Par exemple, en ce qui concerne l'encombrement et la perte de paquets, un utilisateur ne s'intéresse généralement qu'au débit effectif pour

[5] https://atlas.ripe.net/probes
[6] https://pypi.org/project/murakami

ses applications, notamment en ce qui concerne la capacité et la qualité de son expérience lors de l'utilisation de médias enrichis sur un service réseau donné. Une forte dégradation des performances d'un réseau, par exemple en cas d'encombrement ou de défaillance d'un dispositif, peut engendrer une interruption de la transmission des paquets et provoquer des trous dans le réseau, entraînant une indisponibilité du service. Et ceci est lié à un autre aspect de ce projet : la fiabilité du réseau.

2.2.3 Fiabilité du réseau

La fiabilité des réseaux est une notion qui englobe divers indicateurs de stabilité importants pour la disponibilité et la facilité d'utilisation durables des services réseau. L'un des principaux paramètres de la fiabilité des réseaux est le temps de disponibilité, qui correspond au pourcentage de temps pendant lequel un service réseau est disponible. Le niveau de disponibilité du réseau détermine le fait si un utilisateur est en mesure d'accéder aux services Internet en permanence. Ainsi, du point de vue de l'utilisateur, nous pouvons mesurer la fiabilité d'Internet en termes de temps de disponibilité et d'accessibilité, c'est-à-dire la possibilité d'accéder à n'importe quel réseau et service Internet à tout moment [17].

2.3 // Mesure de la diversité des chemins

Pour mesurer et évaluer la résilience d'Internet en ce qui concerne la diversité des chemins, nous mettrons en œuvre un système de mesure afin d'identifier les sauts géographiquement équivalents dans les données traceroute, puis nous calculerons les métriques de la géodiversité pour des paires de points d'extrémité.

2.3.1 Paris Traceroute

Grâce aux mesures de traceroute, nous recueillerons les chemins au niveau IP entre les points d'extrémité sélectionnés, à la fois au sein des zones géographiques (diversité interne) et entre les différentes zones (diversité externe). Un des aspects importants de la mesure de la diversité des chemins consiste à identifier autant de chemins alternatifs que possible entre une paire de réseaux ou de points d'extrémité. Pour ce faire, notre système utilisera Paris Traceroute[7] et effectuera des mesures répétées entre chaque paire de points d'extrémité.

2.3.2 Géo-groupage

Tout d'abord, nous utiliserons plusieurs bases de données de géolocalisation, telles que RIPE IPmap[8], MaxMind[9] et IPInfo[10], ainsi que des mesures actives pour déterminer les emplacements géographiques (au niveau des villes et des pays) des sauts IP traceroute. Nous serons alors en mesure de regrouper les sauts en fonction des zones géographiques à plusieurs niveaux de granularité, ce qui nous permettra d'identifier les chemins géographiquement équivalents. Nous déterminerons ensuite l'équivalence géographique des chemins et nous calculerons les indices de géodiversité entre les emplacements et les points d'extrémité sélectionnés [18].

2.3.3 Mise en correspondance de la topologie physique et logique

Pour mieux comprendre la résilience d'Internet en ce qui concerne la géodiversité des chemins, nous étudierons le problème de la mise en correspondance de la topologie logique sur l'infrastructure du réseau physique [22]. Dans ce contexte, la topologie logique comprend des ensembles de nœuds IP ou ASN, avec des bords indiquant la relation entre les réseaux, comme les relations client-fournisseur ou les relations de peering. D'autre part, un réseau physique désigne un ensemble de nœuds physiques (par exemple, des routeurs frontaliers et des IXP), avec des bords qui représentent des liens de communication physiques, principalement des réseaux de câbles. L'objectif est d'évaluer et de comparer la diversité des chemins physiques et logiques entre les réseaux.

2.4 // Mesure de la fiabilité et des performances des réseaux

Nous effectuerons des mesures actives à long terme, de bout en bout, afin d'évaluer la fiabilité (temps de disponibilité et accessibilité) ainsi que les performances des réseaux en Afrique. Les mesures actives consistent à envoyer des paquets de sondes d'une source (point d'observation) à une destination. Ces mesures actives nous permettront d'analyser les mises en file d'attente, les pertes, les latences, le débit,

[7] Paris traceroute est une autre version d'un outil de diagnostic réseau bien connu (traceroute). Elle traite les problèmes causés par les équilibreurs de charge avec l'implémentation initiale de traceroute. Pour en savoir plus: https://paris-traceroute.net
[8] https://ipmap.ripe.net
[9] https://www.maxmind.com
[10] https://ipinfo.io

les comportements de routage et les temps de propagation du réseau. Pour obtenir des résultats fiables et exhaustifs, les mesures devront être effectuées entre un grand nombre de points d'observation répartis sur divers emplacements géographiques.

Il existe déjà de nombreuses plateformes de mesure d'Internet dotées de sondes qui peuvent être utilisées pour effectuer des mesures répétées du réseau. Certaines des plus connues sont SamKnows[11], Speedchecker[12], Archipelago[13], RIPE Atlas[14] et M-Lab[15]. RIPE Atlas dispose d'environ 12 000 sondes matérielles à travers le monde. Cependant, en 2018, il n'existait que 229 sondes RIPE Atlas actives en Afrique. En février 2021, seules 194 d'entre elles étaient connectées et actives. La plupart de ces sondes sont déployées par des opérateurs de réseau au sein de leurs réseaux internes et un petit nombre de sondes sont hébergées chez des particuliers.

Speedchecker est une plateforme de mesure active dont le nombre de points d'observation est relativement plus élevé en Afrique. En 2018, Speedchecker comptait jusqu'à 850 sondes dans 52 pays africains. Tout comme RIPE Atlas, Speedchecker prend en charge un large éventail de tests réseau, notamment Ping (TCP/ICMP), DNS, Traceroute et HTTP. La plateforme Archipelago du CAIDA compte actuellement 10 moniteurs actifs en Afrique, et ceux-ci fonctionnent comme des sondes dédiées qui exécutent de manière répétée des tests de mesure du réseau visant à découvrir la topologie d'Internet et à mesurer les performances du réseau.

M-Lab est une autre plateforme qui permet aux internautes d'effectuer des tests de débit à partir de leurs navigateurs. Cependant, cette plateforme ne dispose que de sept serveurs en Afrique faisant office de points d'observation pour les mesures de débit, ce qui limite la fiabilité des résultats à partir de nombreux points d'observation. Heureusement, M-Lab possède actuellement une vaste gamme d'outils, et certains d'entre eux peuvent être personnalisés en tant que clients et serveurs pour différentes campagnes de mesure. Par exemple, Network Diagnostic Tool[16] (NDT) fournit des informations détaillées au niveau des paquets ainsi que des statistiques au niveau du noyau sur la façon dont une connexion TCP se comporte sur un chemin donné. NDT peut donc être utilisé pour déterminer les causes des ralentissements, ainsi que pour vérifier les serveurs mandataires, les dispositifs NAT entre la machine qui effectue les tests et le serveur M-Lab. Pour ce projet, un client NDT personnalisé sera développé et déployé en utilisant des Raspberry Pi (Modules MIRA) et effectuera des tests de nos serveurs personnalisés.

Au départ, le projet MIRA donnera la priorité aux sondes logicielles M-Lab et RIPE Atlas.

2.5 // Recoupement des indicateurs

La mesure des caractéristiques spécifiques du réseau (qualité de service, latence, gigue, qualité d'expérience, perte de paquets, débit, diversité des chemins, etc.) est devenue monnaie courante et une approche largement acceptée pour évaluer les performances et/ou la résilience d'un réseau. Ces informations sont censées aider les ingénieurs, les organismes de réglementation et les décideurs, ainsi que les utilisateurs finaux, à prendre des mesures actives pour ajuster et améliorer les performances et la résilience du réseau. Cependant, pour quantifier efficacement l'effet de nos actions, nous devons agréger ces mesures individuelles. Les ingénieurs ont besoin de mesures agrégées pour concentrer leurs ressources sur l'amélioration des réseaux. Les décideurs ont besoin de ces mesures agrégées afin d'orienter leurs décisions de financement et d'élaborer la réglementation. Les utilisateurs ont besoin de ces mesures agrégées dans leur quête d'une meilleure expérience utilisateur. Malheureusement, agréger plusieurs métriques pour obtenir des résultats significatifs n'est pas une tâche simple. Actuellement, il n'existe pas de moyen systématique d'évaluer les performances ou la résilience d'un réseau à partir d'un vecteur de mesures du réseau.

Le principal problème qui rend presque impossible l'agrégation correcte des mesures de réseau est l'absence de « réalité de terrain ». La réalité de terrain fait normalement référence aux informations recueillies sur place. Par exemple, en physique, la réalité de terrain provient du monde physique. Dans les réseaux informatiques, il est difficile d'obtenir une réalité de terrain pour des mesures telles que la perte de paquets ou le débit. Cependant, nous devons obtenir des réponses afin de prendre des décisions éclairées et d'évaluer si nos actions ont contribué à l'amélioration ou la diminution de la résilience du réseau.

[11] https://www.samknows.com
[12] http://speedchecker.com
[13] https://www.caida.org/projects/ark
[14] https://atlas.ripe.net
[15] https://www.measurementlab.net
[16] https://software.internet2.edu/ndt

Dans le cadre de ce projet, nous proposons de définir (et non de découvrir) une réalité de terrain pour ces mesures. Notre approche s'appuiera sur des avis d'experts et, sur la base de ces derniers, nous définirons les méthodes d'agrégation en attribuant la pondération ou le coefficient approprié aux mesures recueillies.

2.6 // Sources de données

Nous utiliserons, dans le cadre de ce projet, des sources de données primaires et secondaires. Les sources primaires proviendront de campagnes de mesure actives et passives, tandis que les données secondaires seront recueillies à partir d'informations provenant de tiers, telles que la table de routage BGP, les ensembles de données IXP, les informations de domaine national, etc. Pour garantir la durabilité de notre cadre, nous devons nous assurer que nos sources de données sont ouvertes, fiables et à jour et qu'elles continueront à fournir des données sur une longue période. Cela nous permettra d'extraire des informations sur les tendances concernant un sujet particulier. L'annexe 1 présente une liste des sources de données, leur objectif et leur catégorie.

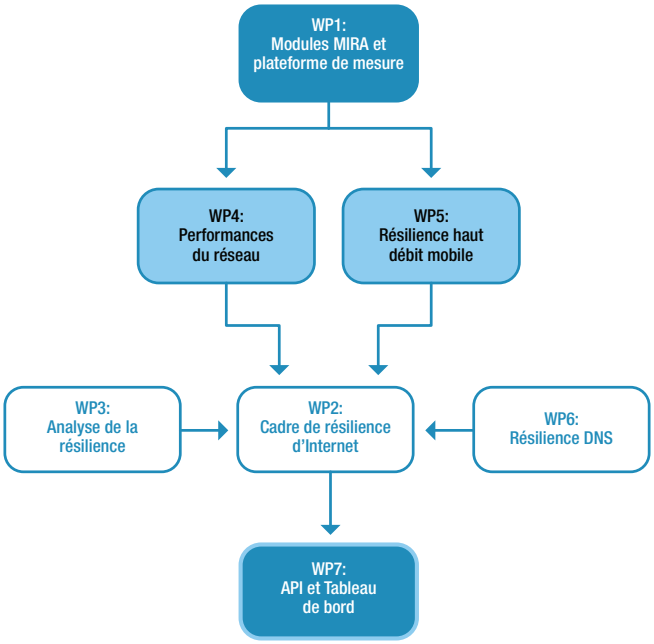


Figure 3 : *Circulation des informations entre les lots de travaux (WP) définis.*

3 Programme de Travail

Le programme de travail est séparé en lots de travaux (WP), à savoir : l'Étape 1, dominée par la mise en œuvre et le banc d'essai et le développement du cadre de résilience d'Internet (WP1, WP2). L'Étape 2 consiste à recueillir et à analyser les mesures du réseau et les autres sources de données secondaires disponibles (WP3, WP4). L'Étape 3 consiste à rassembler toutes les données recueillies, à les agréger, à effectuer des analyses statistiques et à fournir des informations aux utilisateurs finaux (WP7). La figure 3 illustre la manière dont les lots de travaux s'alimentent mutuellement.

Remarque : *les lots de travaux WP5 (Mesures mobiles) et WP6 (Résilience DNS) seront entrepris à un stade ultérieur (à déterminer).*

3.1 // WP1 : Sources de données et infrastructure de mesure

Ce lot de travaux permettra de concevoir et de mettre en œuvre de petits dispositifs appelés Modules MIRA. Les modules sont de petits appareils qui seront dédiés à la réalisation des mesures. A ce stade, les modules sont des Raspberry Pi. Ce projet sera soutenu par AFRINIC et l'Internet Society à travers l'achat des appareils de mesure et la gestion du tableau de bord des mesures sur la plateforme Internet Society Pulse.

Remarque : *ceci sera lié au lot de travaux WP5 : Mesures du haut débit mobile.*

3.1.1 Tâche n° 1 : Modules de mesure

La première tâche consiste à concevoir et à construire une infrastructure appropriée pour lancer les mesures (par exemple, pour les mesures de débit ou de latence). Pour ce faire, nous allons exploiter les outils de mesure existants, notamment RIPE Atlas ou client NDT de M-Lab. Ces dispositifs de mesure seront appelés Modules MIRA. Ils devraient être légers et faciles à connecter à n'importe quel réseau. Les Modules MIRA utiliseront des conteneurs virtualisés légers (par exemple, Docker ou LXD) qui exécuteront les différentes tâches de mesure. Il doit être assez facile de déplacer ou de cloner les tâches de mesure d'un module à l'autre. AFRINIC et l'Internet Society prendront en charge le déploiement des modules dans quelques pays africains avec le soutien des sections locales de l'Internet Society et d'autres bénévoles.

3.1.2 Tâche n° 2 : Orchestration des modules

Un des aspects importants est l'orchestration et la gestion des Modules MIRA. Il doit être facile de lancer et de planifier des mesures à partir d'un système centralisé. L'orchestrateur doit avoir accès aux Modules MIRA et récupérer leur état de santé ainsi que l'état des mesures. L'orchestrateur coordonnera également les

campagnes de mesure et de collecte de données dans divers ensembles de modules. Il sera responsable de la collecte des données des modules. Les contrôles d'accès aux données seront essentiels à cet égard ; elles devront permettre la divulgation de plusieurs abstractions de données à différentes parties.

3.1.3 Tâche n° 3 : Acheminement et stockage des données

Le système doit être capable de traiter les données primaires des modules et les données tierces qui seront utilisées pour compléter les mesures. Les Modules MIRA vont générer une grande quantité de données de mesure au fil du temps. Cela signifie que la tâche « Acheminement et stockage des données » doit : (1) traiter une grande quantité de données, (2) effectuer une agrégation et (3) éliminer les données inutiles. Une API doit permettre un accès facile aux données recueillies. Pour réaliser cette tâche, nous utiliserons les techniques de stockage les plus récentes (par exemple, noSQL, clusters Hadoop, etc.) pour améliorer l'extensibilité et la facilité d'utilisation.

3.2 // WP2 : Cadre de résilience d'Internet

Dans ce lot de travaux, nous concevrons des outils permettant d'agréger les mesures de résilience des réseaux. Cette agrégation nous permettra d'extraire des valeurs sommaires dont on peut dériver rapidement et intuitivement des indications sur la résilience du réseau. Nous définirons d'abord les fondements théoriques de l'agrégation en nous appuyant sur une réalité de terrain que nous prévoyons de définir.

Dans un premier temps, nous élaborerons un cadre simple agrégeant les différents indices à l'aide d'une formule simple. Dans un second temps, nous élaborerons un cadre plus complexe reposant sur les avis d'experts, puis nous utiliserons l'apprentissage automatique pour affiner ce cadre.

La réalité de terrain servira également à valider et re-étalonner en permanence notre outil d'agrégation. Une fois nos méthodes d'agrégation des mesures définies, nous les transmettrons au système d'analyse, qui définit comment les différentes mesures (effectuées à partir de différents points d'observation) seront transmises aux modules d'agrégation. Enfin, grâce à une bonne agrégation des mesures de résilience, les opérateurs de réseau seront en mesure de définir un point de fonctionnement de référence et d'orienter continuellement le réseau vers cette valeur de référence souhaitée.

3.2.1 Tâche n° 1 : Cadre théorique

L'objectif de cette tâche est de développer le fondement théorique de l'agrégation des mesures de résilience des réseaux. Nous commencerons par identifier les mesures qui peuvent être utilisées pour évaluer efficacement le niveau global de résilience des systèmes. Ensuite, ces mesures seront agrégées pour fournir un résumé succinct de la résilience du réseau sous la forme d'un indice, appelé indice de résilience d'Internet. Nous concevrons les outils d'agrégation en répondant à deux questions : (1) comment agréger les mesures de paramètres similaires recueillies à partir de divers points d'observation au sein du réseau et les mesures de différents paramètres recueillies au sein du même réseau ? Et (2) comment agréger des mesures avec un effet de zoom avant/zoom arrière à différents niveaux tels que la ville, la région et le pays ? Les mesures agrégées seront mises en correspondance avec des scores numériques qui seront convertis en un indicateur qualitatif (telle que faible, moyen, élevé et critique) afin d'aider les organisations à évaluer correctement et à hiérarchiser leurs processus décisionnels.

Pour élaborer la base théorique et valider nos théories, nous allons définir une réalité de terrain pour les mesures de résilience du réseau.

3.2.2 Tâche n° 2 : Évaluation des performances/Réalité de terrain

Nous proposons de développer et de documenter une procédure s'appuyant sur des principes scientifiques établis et qui permette d'exploiter les connaissances d'experts pour concevoir une matrice de résilience à partir des paramètres de résilience choisis. En outre, cette procédure permettra la collaboration de plusieurs experts de sorte que la réalité de terrain utilisée aux fins de l'agrégation soit basée sur les connaissances conjointes de ces mêmes experts.

L'Internet Society et AFRINIC disposent de bases de données d'experts dans ce domaine. Nous proposons de leur mettre à disposition notre procédure et les outils associés pour leur permettre d'évaluer l'exactitude de nos scores d'agrégation (en vue de comparer leur avis sur ce que doit être un score avec le score tel qu'il existe). Au fur et à mesure que l'expérience humaine s'accroît et que notre compréhension de la résilience des réseaux évolue, les « vrais » scores évoluent eux-mêmes (en fonction de l'avis des experts). Il en résulte que notre réalité de terrain et nos mesures évolueront au fil du temps. A l'aide de ces nouvelles connaissances, nous allons systématiquement re-étalonner et améliorer nos méthodes d'agrégation.

3.2.3 Tâche n° 3 : Outil d'analyse

L'outil d'analyse hébergera des unités discrètes de calcul appelées Modules d'analyse. Ces modules seront définis par le Cadre de résilience d'Internet. Ils recevront des flux de données des Modules MIRA et d'autres sources, puis les transformeront en une forme traitée (par exemple, en calculant la centralité à partir de cartes topologiques). Cette tâche inclura le développement des API et du cadre permettant d'exécuter ces modules de manière évolutive.

Le fait de disposer de méthodes d'agrégation des mesures permettra aux opérateurs de réseaux et aux fournisseurs d'accès de définir des points de référence et de diriger continuellement le système vers le point souhaité. L'objectif en termes de résilience reflète les exigences des utilisateurs finaux, des organismes de réglementation et des autres parties prenantes quant à un point de fonctionnement acceptable. Le pilotage continu du réseau peut se faire en suivant des cadres d'orientation tels que le cadre de résilience du réseau du NIST [23] et le cadre de résilience de Sterbenz et al. [18]. Cela pourrait prendre la forme suivante (suivant le cadre en cinq étapes du NIST) :

1. Protéger : en prenant des mesures « proactives » pour maintenir le réseau au point de fonctionnement souhaité.
2. Détecter : les indicateurs de dégradation de la résilience du réseau, qui devrait se traduire par une diminution du score.
3. Déterminer : les mesures/paramètres les plus pertinents en termes de dégradation de la résilience.
4. Intervenir : prendre des mesures « réactives » pour rétablir le système au point de fonctionnement souhaité.
5. Remettre en état : malgré une surveillance et une protection permanentes, le système peut éventuellement subir une défaillance désastreuse (intentionnelle ou non). Cela entraînera une dégradation substantielle du score de résilience. Des mesures appropriées doivent être prises pour se remettre d'une telle catastrophe.

3.3 // WP3 : Analyse de la résilience

Ce lot de travaux se concentre sur la quantification de la résilience d'Internet en Afrique à trois niveaux.

3.3.1 Tâche n° 1 : Analyse de la topologie physique

Dans le cadre de cette tâche, nous évaluerons la diversité des câbles sous-marins qui desservent le continent, ainsi que celle des câbles terrestres qui le traversent. Nous nous attacherons également à quantifier les éléments physiques, tels que les stations terrestres et les IXP. Ce lot de travaux fournira (au cadre de résilience - WP2) des mesures de la diversité des câbles et des stations terrestres dans les pays et les villes étudiés. Ces données nous permettront d'évaluer et de comparer, au travers des paramètres quantifiables, la diversité des chemins physiques au sein des pays, des villes et des réseaux et entre eux.

3.3.2 Tâche n° 2 : Analyse de la topologie logique

Cette tâche consistera à déterminer les dépendances en termes de routage entre les FAI à travers le continent, et leur dépendance à l'égard des fournisseurs non africains. Nous nous appuierons pour ce faire sur des mesures effectuées à l'aide de Paris Traceroute pour déterminer les chemins logiques entre certains points d'extrémité dans le but d'identifier des chemins alternatifs. Outre les données Traceroute, nous utiliserons des ensembles de données BGP pour déterminer la diversité des chemins logiques entre les réseaux et les pays.

En particulier, nous communiquerons avec ARDA[17], un système qui synthétise les informations publiques d'échange de trafic et de routage recueillies par les collecteurs d'informations de routage en Afrique, notamment RouteViews[18] et Packet Clearing House[19] (PCH). L'objectif principal de ce lot de travaux est d'obtenir des valeurs d'indice représentant la diversité des chemins logiques au sein des réseaux et des pays.

3.3.3 Tâche n° 3 : Mise en correspondance des topologies physique et logique

Cette tâche consistera à mettre en correspondance la topologie logique avec l'infrastructure physique du réseau. L'objectif est d'identifier les infrastructures physiques (câbles, points d'atterrissement, etc.) utilisées par les différents ASN. L'objectif est d'évaluer et de comparer la diversité des chemins physiques et logiques entre les réseaux. Outre l'identification des câbles, nous signalerons également les installations

[17] African Route-collector Data Analyzer[5]
[18] http://www.routeviews.org
[19] https://www.pch.net

d'interconnexion et les IXP essentiels à la stabilité d'Internet sur le continent. En outre, les flux de trafic en provenance des pays africains seront associés aux câbles respectifs. Il ressortira de cette tâche un indice essentiel, celui de la diversité des chemins physiques internationaux des pays et des réseaux.

3.3.4 Tâche n° 4 : Risque d'étranglement/Hégémonie AS

Internet est composé de plusieurs réseaux qui dépendent les uns des autres pour assurer une connectivité mondiale. Cela signifie que l'accessibilité d'un réseau dépend de sa connectivité avec les autres réseaux. Cette interdépendance reflète généralement les contraintes politiques et économiques d'un pays. Lorsque la dépendance de la connectivité mondiale à l'égard de certains réseaux s'accroît, cette concentration peut représenter un « goulot d'étranglement ». Cette tâche consiste à mesurer le risque d'étranglement [19] ou l'hégémonie AS [20] d'un pays.

3.4 // WP4 : Performance du réseau

3.4.1 Tâche n° 1 : Performances d'accès

L'un des plus grands problèmes lié au déploiement de nouveaux services en Afrique est la mauvaise qualité de la fourniture du haut débit dans certaines régions. La quantification de ce problème est d'une importance capitale pour les organismes de réglementation, ainsi que pour les opérateurs de réseaux (y compris les nouveaux entrants) qui souhaitent cibler au mieux leurs investissements. MIRA permettra d'évaluer la qualité d'expérience des utilisateurs en ce qui concerne la fourniture du haut débit à domicile, les points d'accès Wi-Fi publics et les services mobiles. Il s'agira d'aller au-delà des simples tests de débit et de se concentrer sur le recueil des expériences des utilisateurs finaux dans un ensemble diversifié de services. Le principal indicateur résultant de cette tâche sera l'indice de qualité d'expérience dans les réseaux et les pays.

3.4.2 Tâche n° 2 : Peering des infrastructures

Prendre des décisions concernant le déploiement et l'interconnexion d'infrastructures (réseaux, serveurs de contenu, etc.) peut s'avérer difficile, en particulier dans les environnements en développement et très dynamiques que l'on trouve en Afrique. Il a été largement documenté que le peering a un effet positif sur la plupart des mesures de performance d'Internet. Il est également bien connu que l'Afrique accuse un retard important par rapport à l'Europe en termes d'infrastructure de peering. Pour effectuer cette tâche, nous utiliserons les données MIRA du tableau de bord Internet Society Pulse pour extraire les mesures pertinentes afin de conseiller les fournisseurs de réseau et de contenu, qui souhaitent savoir s'ils doivent s'échanger des informations, avec qui ils doivent le faire et où cela doit se produire. L'accent sera mis sur les IXP en cours de déploiement dans la région, un objectif stratégique majeur de l'Union africaine. Les opérateurs de réseaux et les fournisseurs de contenu pourront recueillir des données statistiques sur leur trafic et leurs besoins, qui seront ensuite fusionnées avec les données provenant de MIRA (chemins connus, emplacements et disponibilité des points de présence, etc.), afin de recommander des réseaux et des emplacements pour le peering. Le principal indicateur résultant de cette tâche sera l'indice de potentiel de peering des réseaux. Le système ARDA constituera l'une des sources d'information utilisées pour cette tâche.

3.4.3 Tâche n° 3 : Maintenir la proximité du trafic local

Maintenir les services et le contenu aussi près que possible des utilisateurs finaux contribue à faire d'Internet un écosystème plus sûr et plus robuste. Les IXP jouent un rôle important en établissant des relations de peering (échange de trafic) entre les FAI, les fournisseurs de contenu et les opérateurs de réseaux de diffusion de contenu (CDN), leur permettant ainsi d'échanger du trafic au niveau local. Cette tâche consistera à analyser dans quelle mesure le contenu local populaire est hébergé et distribué dans un pays et quel est l'impact relatif sur la qualité d'expérience du point de vue des utilisateurs finaux. Pour ce faire, des mesures seront effectuées à partir des Modules MIRA.

3.4.4 Tâche n° 4 : Interférences avec le réseau et le Web

La confidentialité, l'interception (par exemple, l'injection d'entêtes HTTP) et la limitation du débit sont des préoccupations croissantes. Cette tâche utilisera des outils existants tels que l'OONI[20], qui s'appuie sur des indicateurs actifs permettant de détecter les interférences de trafic de site Web, ainsi que les technologies qui sous-tendent les interférences de trafic. Pour ce faire, nous aurons recours à des mesures actives de TCP, DNS, HTTP et TLS. Nous exploiterons également les données provenant d'autres services de surveillance de la censure afin d'en extraire des tendances.

[20] https://ooni.org

3.5 // WP5 : Résilience des réseaux mobiles

Dans ce lot de travaux, nous chercherons à évaluer la facilité d'utilisation de l'Internet mobile dans la région, à partir d'une multitude de points d'observation.

3.5.1 Tâche n° 1 : Adapter les outils de mesure des réseaux mobiles existants

Cette tâche s'appuie sur les travaux réalisés précédemment visant à mesurer et cataloguer les problèmes liés à l'utilisation de l'Internet mobile dans certains pays de l'UE. Nous allons (a) adapter une application de mesure des réseaux mobiles existante au contexte africain, notamment en intégrant une liste de services d'information essentiels en Afrique, (b) étudier la facilité d'utilisation et la qualité de la connectivité Internet dans la région et (c) travailler avec des chercheurs locaux pour effectuer des mesures sur le terrain dans leurs pays.

3.5.2 Tâche n° 2 : Facilité d'utilisation du haut débit mobile

Dans le cadre de cette tâche, nous allons analyser la facilité d'utilisation des réseaux mobiles en Afrique à partir d'une multitude de points d'observation. Cela fournira, pour la première fois, une représentation complète de l'état de la connectivité Internet dans la région.

3.5.3 Tâche n° 3 : Liste des services essentiels

Cette tâche consistera à effectuer des mesures de qualité d'expérience à partir d'une liste de différents sites Web qui fournissent des « services d'information essentiels » dans la région. Cette liste fournira une taxonomie et une catégorisation claires de la myriade de sources d'information publiques et commerciales dans la région. Nous mesurerons et cataloguerons les problèmes d'accès aux services essentiels dans la région, ce qui permettra aux décideurs politiques de savoir sur quels domaines se concentrer pour réduire la fracture numérique sur le continent.

3.6 // WP6 : Résilience de l'infrastructure DNS

A l'aide de plusieurs sources de données, ce lot de travaux consistera à plonger en profondeur dans le système de noms de domaine africain. À cette fin, nous examinerons la fiabilité de l'infrastructure DNS sur le continent, tant pour la résolution de contenus provenant de l'extérieur du continent que de l'intérieur. Pour ce faire, nous examinerons l'hébergement, la fiabilité et les performances des domaines nationaux africains et de tous les services DNS mondiaux présents en Afrique. Deux études récentes d'AFRINIC ont mis en évidence un certain nombre de problèmes susceptibles d'affecter la résilience de l'infrastructure DNS.[21] [22]

3.6.1 Tâche n° 1 : Résilience des domaines nationaux

De nombreux domaines nationaux africains ne respectent pas les recommandations du BCP-16[23] en plaçant les serveurs de noms à des endroits topologiquement et géographiquement différents afin de minimiser la probabilité qu'une seule défaillance les mette tous hors service. Nous allons déterminer si les domaines nationaux africains répondent à l'exigence minimale du BCP-16, à savoir disposer d'au moins deux adresses IP pour desservir leurs zones.

3.6.2 Tâche n° 2 : Adoption et utilisation des DNSSEC

Nous cherchons à savoir quels sont les domaines nationaux africains ayant adopté les DNSSEC. En outre, sur la base des données provenant de l'APNIC[24], nous pouvons savoir qui effectue la validation au moyen d'une DNSSEC.

3.6.3 Tâche n° 3 : Performances Do53/DoH/DoT

Nous comparerons les performances de Do53 (DNS traditionnel), DNS sur TLS (DoT) et DNS sur HTTPS (DoH) dans différentes conditions de réseau (mobile et fixe) Nous rechercherons les causes de la latence et des chemins de résolution DNS détournés qui amplifient l'incidence des protocoles DNS sécurisés sur le temps de résolution DNS et le temps de chargement des pages.

3.7 // WP7 : Tableau de bord MIRA

Ce lot de travaux traite principalement de la diffusion des données (après traitement) par le biais d'un tableau de bord de visualisation hébergé sur la plateforme Internet Society Pulse et d'une API permettant de récupérer facilement les données.

[21] https://afrinic.net/research/african-cctlds-technical-environment
[22] https://afrinic.net/research/african-dns-authoritative-nameservers
[23] https://tools.ietf.org/html/bcp16
[24] https://stats.labs.apnic.net/dnssec

3.7.1 Tâche n° 1 : API pour usage externe

Une API permettra d'accéder facilement aux différents indices et données recueillis pour calculer l'indice. Les données doivent être mises à disposition pendant un laps de temps suffisant pour permettre une analyse longitudinale.

3.7.2 Tâche n° 2 : Tableau de bord de visualisation

MIRA présentera les données en utilisant la plateforme Internet Society Pulse qui sera personnalisable en fonction des besoins des utilisateurs finaux (organismes de réglementation, FAI, etc.). L'utilisateur accèdera d'abord à une carte thermique de l'Afrique sur laquelle les pays seront colorés en fonction de l'« indice de résilience d'Internet » calculé dans le WP2. Il sera possible de comparer plusieurs pays côte à côte. L'utilisateur pourra ensuite accéder à des indices plus détaillés qui, ensemble, auront contribué à calculer l'Indice de résilience d'Internet. Les participants qui hébergent des sondes de mesure pourront avoir accès à d'autres données de base non accessibles aux utilisateurs normaux.

4 Diffusion

La diffusion des résultats du projet se fera par le biais d'un portail de la plateforme Internet Society Pulse qui sera accessible à tous les internautes. Les participants au processus de mesure qui hébergent des sondes ou des infrastructures de mesure pourront obtenir des données plus techniques du projet MIRA.

4.1 // Recrutement des hôtes de Module MIRA

La durabilité et la précision du projet MIRA dépendront du nombre de Modules MIRA effectuant des mesures actives en Afrique. Il est donc important de recruter et de conserver un nombre important d'hôtes de Modules.

AFRINIC et l'Internet Society, grâce à leurs relations avec les chercheurs, les techniciens et les sections locales de l'Internet Society, tiennent à jour une liste d'hôtes volontaires. Au fur et à mesure de l'évolution du projet, nous continuerons à recruter de nouveaux hôtes.

4.2 // Implication et renforcement des capacités

Par le biais du groupe de travail sur les mesures d'AFRINIC, nous avons l'intention d'organiser une série d'ateliers autour du vaste sujet des mesures d'Internet. Nous avons l'intention de couvrir des sujets tels que la mesure des performances du réseau, la surveillance de la qualité d'expérience et la censure d'Internet. Nous inviterons les opérateurs d'infrastructure de mesure tels que M-Lab, OONI, RIPE Atlas à participer à nos ateliers. Nous avons l'intention d'organiser les ateliers suivants :

1. Atelier n° 1 : AIS 2021, juin 2021
2. Atelier n° 2 : AfPIF2021, août 2021
3. Atelier n° 3 : SAFNOG 2021, novembre 2021

En outre, chaque lot de travaux sera divisé en plusieurs études scientifiques. Les résultats seront diffusés sous la forme de publications scientifiques (articles de conférence ou publications dans des revues), d'articles de blog et de rapports techniques. L'idée générale est de rendre nos résultats facilement accessibles à différents publics (techniques et moins techniques).

5 Exécution et Feuille de Route

L'annexe 2 donne un aperçu des tâches et du moment où elles seront exécutées.

5.1 // Infrastructure de mesure

Dans le cadre du projet MIRA, des mesures seront effectuées à l'aide, dans un premier temps, de l'outil Murakami de M-Lab, lequel sera complété par RIPE Atlas (RIPE NCC) dans les mois à venir. Nous avons l'intention d'ajouter d'autres outils en fonction des besoins futurs. Ces deux outils s'appuient sur des logiciels qui peuvent être installés sur différents systèmes d'exploitation et peuvent effectuer diverses mesures Web. Les logiciels seront installés sur de petits Raspberry PI que nous appelons des Modules MIRA. Nous avons opté pour cette technologie car elle permet d'effectuer des mesures continues et dédiées sur du matériel léger et de faible puissance facilement disponible dans de nombreux pays africains.

5.2 // Participation de la communauté

Plusieurs sections locales de l'Internet Society participent actuellement à ce projet en hébergeant des sondes, ce qui permet d'augmenter le nombre de points d'observation en Afrique. Actuellement, les sections de Madagascar, du Bénin, de Tunisie et d'Éthiopie sont pleinement impliquées dans la mise en place de sondes de mesure et disposent d'une infrastructure active. Nous recueillons déjà des données au Kenya et à l'île Maurice sur des infrastructures qui ont été déployées par le personnel de l'Internet Society (Kenya) et d'AFRINIC (île Maurice).

5.3 // Phase pilote

Nous avons déjà commencé à augmenter le nombre de points d'observation de mesure d'Internet (Modules MIRA) en Afrique en fournissant l'infrastructure de mesure et en soutenant le déploiement. Nous recueillons déjà, ou nous nous préparons à recueillir, des mesures de débit, de temps de transmission aller-retour (RTT) et de latence au Bénin, au Burkina Faso, en RDC, au Kenya, à Madagascar, au Nigéria, en Tunisie, au Rwanda et en Afrique du Sud.

D'autres pays seront ajoutés dès que des points d'observation appropriés seront identifiés.

5.4 // Partenaires

Ce projet sera réalisé en partenariat avec différents instituts universitaires. Vous trouverez ci-dessous une liste des principaux chercheurs et instituts impliqués dans les différents lots de travaux.

1. Amreesh Phokeer (AFRINIC) et Kevin G. Chege (Internet Society) seront responsables de la coordination générale des activités mentionnées dans les différents lots de travaux (WP).
2. Assane Gueye, CMU-Rwanda, sera chargé de la modélisation du cadre de résilience des infrastructures dans le cadre du WP2.
3. Ahmed Elmokashfi (Simula Research Lab) sera chargé de la mesure et de la cartographie de la topologie physique et logique dans le cadre du WP3.
4. Josiah Chavula (Université du Cap) sera responsable des WP3 et WP4, qui consisteront à mesurer la résilience du réseau en termes de points d'étranglement physiques et logiques, ainsi que la qualité de service au niveau du réseau et des applications.

Remarque : *AFRINIC et l'Internet Society assureront la gestion du projet MIRA et superviseront donc conjointement l'ensemble des lots de travaux définis ci-dessus, en s'assurant que les différents collaborateurs répondent aux exigences définies en termes de prestations prévues et de délais.*

6 Déontologie

Les membres du projet prendront toutes les précautions nécessaires pour s'assurer qu'aucune donnée à caractère personnel et identifiable ne soit rendue publique. Toutes les données seront rendues anonymes avant leur traitement afin d'éviter toute fuite d'informations confidentielles. Ne seront recueillies que les données nécessaires. Les méta-informations relatives aux sources (telles que l'adresse IP et la localisation géographique) ne seront pas conservées et ne feront l'objet d'aucun traitement. Nous agrègerons les données au niveau de l'ASN et au niveau du pays.

Les ensembles de données contenant des données à caractère personnel seront utilisés uniquement aux fins de ce projet, ne seront transférés à aucune tierce partie et seront éliminés dès l'achèvement du projet.

En outre, les Modules MIRA stockent des données au format JSON qui ne contiennent que les données de mesure et aucune donnée d'identification. Ces données seront traitées et affichées sur le tableau de bord MIRA d'Internet Society Pulse à des fins de visualisation.

7 Résumé

L'évaluation de la résilience d'Internet est une activité importante dans la détermination des moyens d'amélioration de l'accès à Internet et de son utilisation. Les coordonnées et les informations relatives au projet seront disponibles sur les sites Web de l'Internet Society[25] et d'AFRINIC[26] ainsi que sur Internet Society Pulse[27]. Pour en savoir plus sur le projet MIRA et l'infrastructure de mesure, visitez le site https://github.com/mira-project/mira/wiki.

[25] https://internetsociety.org
[26] https://afrinic.net/research/studies/mira
[27] https://pulse.internetsociety.org

Sources

[1] J. Rydzak, M. Karanja et N. Opiyo, “Internet Shutdowns in Africa| Dissent Does Not Die in Darkness: Network Shutdowns and Collective Action in African Countries” [Coupures d’Internet en Afrique - La dissidence ne meurt pas dans l’obscurité : Fermetures de réseaux et action collective dans les pays africains], Int. J. Commun., vol. 14, p. 24, 2020.

[2] T. Freyburg et L. Garbe, “Blocking the bottleneck: Internet shutdowns and ownership at election times in sub-Saharan Africa” [Empêcher le goulot d’étranglement : Coupure de l’Internet et appropriation en période électorale en Afrique sub-saharienne], Int. J. Commun., vol. 12, pp. 3896–3916, 2018.

[3] R. Kathuria, M. Kedia, G. Varma, K. Bagchi et R. Sekhani, “The anatomy of an Internet blackout: measuring the economic impact of Internet shutdowns in India” [Anatomie d’une panne d’Internet : mesurer l’impact économique des coupures d’Internet en Inde], 2018.

[4] R. Fanou, F. Valera et A. Dhamdhere, “Investigating the Causes of Congestion on the African IXP substrate” [Enquête sur les causes de la congestion des points d’échange Internet en Afrique] in Proceedings of the 2017 Internet Measurement Conference, 2017, pp. 57–63.

[5] A. Formoso, J. Chavula, A. Phokeer, A. Sathiaseelan et G. Tyson, “Deep diving into africa’s inter-country latencies” [Analyse des latences entre pays africains] in IEEE INFOCOM 2018-IEEE Conference on Computer Communications, 2018, pp. 2231–2239.

[6] A. Gupta, M. Calder, N. Feamster, M. Chetty, E. Calandro et E. Katz-Bassett, “Peering at the Internet’s frontier: A first look at isp interconnectivity in Africa” [Le peering à la frontière de l’Internet : Un premier regard sur l’interconnexion des FAI en Afrique], Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 8362 LNCS, pp. 204–213, 2014.

[7] M. Isah, A. Phokeer, J. Chavula, A. Elmokashfi et A. S. Asrese, “State of Internet measurement in Africa-A survey” [Enquête sur l’état de la mesure de l’Internet en Afrique], in International Conference on e-Infrastructure and e-Services for Developing Countries, 2019, pp. 121–139.

[8] R. Cohen, K. Erez, D. Ben-Avraham et S. Havlin, “Resilience of the Internet to random breakdowns” [Résilience de l’internet aux pannes aléatoires], Phys. Rev. Lett., vol. 85, n° 21, p. 4626, 2000.

[9] M. Omer, R. Nilchiani et A. Mostashari, “Measuring the resilience of the global Internet infrastructure system” [Mesurer la résilience de l’infrastructure Internet mondiale], in 2009 3rd Annual IEEE Systems Conference, 2009, pp. 156–162.

[10] J. P. Rohrer, A. Jabbar et J. P. G. Sterbenz, “Path diversification for future Internet end-to-end resilience and survivability” [Diversification des chemins pour la capacité de survie et la résilience de bout en bout de l’Internet du futur], Telecommun. Syst., vol. 56, n° 1, pp. 49–67, 2014.

[11] J. P. G. Sterbenz, E. K. Çetinkaya, M. A. Hameed, A. Jabbar, S. Qian et J. P. Rohrer, “Evaluation of network resilience, survivability, and disruption tolerance: analysis, topology generation, simulation, and experimentation” [Évaluation de la résilience, de la capacité de survie et de la tolérance aux perturbations des réseaux : analyse, génération de topologies, simulation et expérimentation], Telecommun. Syst., vol. 52, n° 2, pp. 705–736, 2013.

[12] J. P. G. Sterbenz et al., “Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines” [Résilience et capacité de survie des réseaux de télécommunication : stratégies, principes et aperçu des disciplines], Comput. Networks, vol. 54, n° 8, pp. 1245–1265, 2010.

[13] J. Wu, Y. Zhang, Z. M. Mao et K. G. Shin, “Internet routing resilience to failures: analysis and implications” [Résilience du routage Internet aux défaillances : analyse et implications], in Proceedings of the 2007 ACM CoNEXT conference, 2007, pp. 1-12.

[14] J. P. G. Sterbenz et al., “Resilience and Survivability in Communication Networks: Strategies, Principles, and Survey of Disciplines” [Résilience et capacité de survie des réseaux de télécommunication : stratégies, principes et aperçu des disciplines], Comput. Networks Spec. Issue Resilient Surviv. Networks, vol. 54, n° 8, pp. 1245–1265, 2010.

[15] J. P. Rohrer et J. P. G. Sterbenz, “Predicting topology survivability using path diversity” [Prévision de la capacité de survie d’une topologie à l’aide de la diversité des chemins], in 2011 3rd International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2011, pp. 1–7.

[16] R. Teixeira, K. Marzullo, S. Savage et G. M. Voelker, “Characterizing and measuring path diversity of Internet topologies” [Caractérisation et mesure de la diversité des chemins dans les topologies Internet], ACM SIGMETRICS Perform. Eval. Rev., vol. 31, n° 1, pp. 304-305, 2003.

[17] D. Baltrunas, A. Elmokashfi, and A. Kvalbein, “Measuring the reliability of mobile broadband networks” [Mesurer la fiabilité des réseaux mobiles à large bande], in Proceedings of the 2014 conference on Internet measurement conference, 2014, pp. 45–58.

[18] A. Csoma, A. Gulyás et L. Toka, “On measuring the geographic diversity of Internet routes” [Mesure de la diversité géographique des chemins Internet], IEEE Commun. Mag., vol. 55, n° 5, pp. 192-197, 2017.

[19] K. G. Leyba, B. Edwards, C. Freeman, J. R. Crandall et S. Forrest, “Borders and gateways: measuring and analyzing national as chokepoints” [Frontières et passerelles : mesurer et analyser les points d’étranglement nationaux], in Proceedings of the 2nd ACM SIGCAS Conference on Computing and Sustainable Societies, 2019, pp. 184-194.

[20] R. Fontugne, A. Shah et E. Aben, “As hegemony: A robust metric for as centrality” [Hégémonie AS : un indicateur essentiel de la centralité des systèmes autonomes], in Proceedings of the SIGCOMM Posters and Demos, 2017, pp. 48–50.

Annexe 1

Catégorie	Indicateur	Type de données	Objet/Questions	Source
FAI Résilience	Résilience des liens	Secondaire	• Quelle est la résilience d'un FAI en termes de liaison en amont ?	BGP, Registres de routage, CAIDA
-	Qualité de service/ d'expérience	Primaire	• Quelle est la qualité du lien (performances, temps de fonctionnement, fiabilité) ? • La qualité d'expérience est-elle identique pour tous les utilisateurs ?	M-Lab (RIPE Atlas)
	DNS Résilience	Primaire	• Les FAI fournissent-ils un service de résolveur DNS résilient ?	Informations publiques sur le DNS
Résilience des infrastructures essentielles	Réseau de câbles	Secondaire	• Existe-t-il des goulots d'étranglement physiques dans la connectivité ? • Existe-t-il une concentration (commerciale ou géographique) des ports de destination ? • Existe-t-il une concentration des sociétés de services par câble ?	Telegeography ITU Transmission Map Africa Bandwidth Map
	Réseau électrique	Secondaire	• Quelle est la résilience du réseau électrique national ?	
	Domaine national (ccTLD)	Primaire	• Nombre de serveurs DNS ? • Emplacement des serveurs DNS ? • DNSSEC	Boîte à outils ISC
Marché résilience	Risque d'étranglement	Secondaire Primaire	• Constate-t-on une concentration vers un petit groupe en amont ?	Route Views Traceroute
	Localisation du trafic	Primaire Secondaire	• % d'AS en peering avec l'IXP ? - % d'AS échangeant du trafic ? Nombre d'IXP dans le pays • Proportion du contenu populaire local hébergé dans le pays	PeeringDB PCH IXP Data Traceroute à l'aide de RIPE Atlas
	Accessibilité financière	Secondaire	• L'accès à Internet est-il abordable ?	A4AI

Annexe 2—Plan 2021

Lot de travaux (WP)/Tâche	Acteurs	Janv.	Fév.	Mars	Avr.	Mai	Juin	Juill.	Août	Sept.	Oct.	Nov.	Déc.
WP 1. Infrastructure de mesure													
1.1 Modules de mesure	AFRINIC/ISOC	//	//	//									
1.2 Orchestration des modules	AFRINIC/ISOC	//	//	//									
1.3 Acheminement et stockage des données	AFRINIC/ISOC		//	//									
WP 2. Cadre de résilience d'Internet													
2.1 Cadre théorique	CMU/AFRINIC/ISOC		//	//									
2.2 Évaluation des performances/ Réalité de terrain	CMU/AFRINIC/ISOC			//	//								
2.3 Analyse	CMU/AFRINIC/ISOC			//	//	//							
WP 3. Analyse de la résilience													
3.1 Analyse de la topologie physique	Université du Cap, Simula/AFRINIC/ISOC	//	//										
3.2 Analyse de la topologie logique	UUniversité du Cap, Simula/AFRINIC/ISOC		//	//									
3.3 Mise en correspondance de la topologie physique et logique	UUniversité du Cap, Simula/AFRINIC/ISOC			//	//								
3.4 Risque d'étranglement/Hégémonie AS.	AFRINIC/ISOC				//	//							
WP 4. Performances du réseau													
4.1 Performances d'accès	Université du Cap, AFRINIC/ISOC					//	//	//					
4.2 Peering des infrastructures	Université du Cap AFRINIC/ISOC						//	//	//				
4.3 Comprendre l'utilisation du Web	Université du Cap AFRINIC/ISOC							//	//	//			
4.4 Interférences avec le réseau et le Web	Université du Cap AFRINIC/ISOC								//	//	//		
WP 5. Résilience des réseaux mobiles													
5.1 Développement des outils de mesure des réseaux mobiles	À déterminer												
5.2 Facilité d'utilisation du haut débit mobile	À déterminer												
5.3 Services essentiels (Qualité d'expérience)	À déterminer												
WP 6. Résilience de l'infrastructure DNS													
6.1 Robustesse du domaine national	AfTLD/ISOC												
6.2 Performances du DNS	AfTLD/ISOC												
WP 7. Tableau de bord MIRA													
7.1 API pour usage externe	AFRINIC/ISOC			//	//	//	//						
7.2 Tableau de bord de visualisation	AFRINIC/ISOC					//	//	//					