Rapport d'activité 2022 du réseau Fratel

À propos de Fratel

Lancé en 2002 à Paris à l'occasion d'un symposium des régulateurs francophones organisé à l'initiative de l'Autorité française de régulation des télécommunications (devenue l'Arcep en 2005) et en présence de représentants de l'Union Internationale des Télécommunications (UIT), de l'Organisation Internationale de la Francophonie (OIF), de la Banque mondiale et de la Commission européenne, le réseau francophone de la régulation des télécommunications (Fratel) compte une cinquantaine de membres répartis sur cinq continents.

Le réseau s'est fixé comme objectif, d'une part, de créer des liens privilégiés et faciliter les échanges d'information et d'expérience entre les régulateurs ayant la langue française en partage et, d'autre part, de mettre en œuvre des actions de formation sur des thèmes d'intérêt commun.

Organisation de Fratel en 2022

Une charte, adoptée à Bamako en 2003 et mise à jour en 2019 à Bucarest, définit les objectifs du réseau et son mode de fonctionnement. En particulier, un Comité de coordination, composé d'un président et de deux vice-présidents, est renouvelé chaque année. En outre, un secrétariat exécutif permanent assuré par l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (Arcep) de France est chargé, notamment, de mettre en œuvre le plan d'action annuel.

En raison de la situation sanitaire (COVID-19) en 2022, le Comité de coordination de Fratel a pris la décision d'organiser le séminaire et la réunion annuelle en présentiel et en ligne. Cette configuration hybride pourrait devenir la norme pour les prochaines réunions, même si une participation sur place est privilégiée.

Le comité de coordination 2022, composé de trois dirigeants d'autorités de régulation membres du réseau

Le Président

M. Luc TAPELLA, Directeur de l'Institut luxembourgeois de régulation (ILR)

Les Vice-présidents

M. Abdoul LY, Directeur général de l'Autorité de régulation des télécommunications et des postes (ARTP) du Sénégal

M. Az-El-Arabe HASSIBI, Directeur général de l'Agence nationale de réglementation des télécommunications (ANRT) du Maroc

Le mot du président de Fratel

L'année 2022 s'achève, riche en événements et en échanges sur la sécurité et la résilience des réseaux. Nous avons eu la chance, cette année, de participer à des réunions en présentiel tout en facilitant la participation de tous, grâce aux moyens techniques permettant des réunions hybrides, déployés par nos hôtes de la République du Congo et de la République de Maurice que je remercie chaleureusement pour leur accueil.

La numérisation et l'explosion de la quantité de données ont conduit les membres de Fratel à se pencher cette année sur les sujets de la résilience et de la sécurité des réseaux.

Les cybermenaces ne sont pas de la science-fiction : régulateurs, opérateurs, entreprises, services publics y sont tous confrontés. Se protéger contre les vulnérabilités est l'affaire de tous. Lors de nos réunions riches en enseignements, nous avons été sensibilisés à ces nouvelles menaces et identifié des solutions et des outils pour réduire les potentiels risques des réseaux.

Je souhaite mentionner les échanges organisés en marge de grands évènements internationaux tels que le Mobile World Congress à Barcelone, la Conférence de plénipotentiaires de l'UIT en Roumanie ou l'IIC au Canada. Ces nouveaux évènements en marge d'autres réunions auxquelles des membres de Fratel participent, ont permis de renforcer le dialogue pour davantage d'échanges d'expériences. Ils nous ont également permis de nouer des liens avec le réseau REFRAM, le groupe des régulateurs francophones de l'audiovisuel en particulier lors de l'atelier de l'IIC relatif au développement des compétences en matière de données pour les régulateurs.

La formation est justement un des moyens de répondre aux attentes des régulateurs membres de notre réseau en matière de compétences. Aussi, un partenariat avec le régulateur suédois PTS a été initié pour promouvoir auprès des membres un programme en langue française intitulé « Team Europe Initiative » visant le renforcement des capacités réglementaires en Afrique subsaharienne. Ce programme vient complémenter la formation qualifiante en régulation du numérique de Télécom Paris soutenue par Fratel.

Je passe la main à l'ANRT du Maroc sur un thème d'importance dans la régulation : les consommateurs. Il est essentiel de leur redonner du pouvoir compte tenu de la maturité des marchés des communications électroniques.

L'outil de mesure de la qualité de service des réseaux mobiles dont est en train de se doter Fratel en est l'illustration. Cette année a permis d'accélérer le projet de mise en

place d'un outil de mesure de la qualité de service des réseaux mobiles financé par l'agence française de développement et piloté par l'ARCEP du Burkina Faso avec le choix d'un prestataire.

2023 s'annonce passionnante et marquera les 20 ans de l'existence officielle de Fratel.

Ce réseau unique représentant 960 millions de personnes partout dans le monde est précieux et nous permet d'enrichir nos pratiques de régulation. Je vous remercie pour votre confiance, j'ai été très heureux et très honoré de présider notre réseau francophone cette année.

Luc TAPELLA, directeur de l'ILR du Grand-Duché de Luxembourg et président 2022 de Fratel

Résumé

L'année 2022 du réseau Fratel a été placée sous le thème de la résilience et la sécurité des réseaux avec :

- un séminaire d'information et d'échange à Brazzaville, en République du Congo, les 23 et 24 mai sur « Quels défis pour la sécurité des réseaux de nouvelle génération » ;
- une réunion annuelle les 10 et 11 novembre à Balaclava, en République de Maurice, sur « Enjeux et moyens d'améliorer la résilience et la sécurité des réseaux de télécommunications ».

Pour préparer ce thème, un questionnaire sur la résilience et la sécurité des réseaux a été envoyé en début d'année aux autorités membres de Fratel. Une synthèse de ces contributions a été présentée par le Secrétariat exécutif lors du séminaire.

En outre, des travaux pour développer un outil sur la couverture et la qualité de service mobiles se sont poursuivis en 2022 avec le lancement d'un appel d'offre par l'Agence française de développement (AFD), qui soutient Fratel sur ce projet, le choix du prestataire ainsi que les premiers tests avant une mise en ligne de l'outil prévue en 2023.

Les cinq parties qui composent le présent rapport d'activité évoquent les principaux travaux en lien avec le thème de l'année, les travaux sur la couverture et qualité de service mobiles, la promotion de la formation des membres du réseau en particulier la formation RegNum organisée par Telecom Paris ainsi que les autres activités du réseau.

1. 19e séminaire d'échange d'information et d'expérience sur « Quels défis pour la sécurité des réseaux de nouvelle génération »

À l'invitation de l'Agence de Régulation des Postes et des Communications électroniques (ARPCE) de la République du Congo et de l'Institut Luxembourgeois de Régulation (ILR), président de Fratel en 2022, Fratel a tenu, à Brazzaville et en ligne, son 19e séminaire, les 23 et 24 mai 2022 sur le thème « Quels défis pour la sécurité des réseaux de nouvelle génération ».

Plus de 150 personnes ont participé en présentiel ou virtuellement au séminaire représentant notamment 29 autorités de régulation membres du réseau Fratel, mais aussi des institutions internationales (UIT, OIF, Banque mondiale), des agences en charge de la cybersécurité, des administrations, des associations de consommateurs, des universitaires et des acteurs du secteur.

La cérémonie d'ouverture incluait les discours de MM. Louis-Marc SAKALA, Directeur général de l'ARPCE, Luc TAPELLA, Directeur de l'ILR et Léon Juste IBOMBO, Ministre des postes, télécommunications et de l'économie numérique.

Le secrétariat exécutif a présenté, en introduction des travaux, un état des lieux sur la résilience et la sécurité des réseaux dans les pays membres de Fratel sur la base des réponses au questionnaire envoyé aux autorités en début d'année.

Ensuite, se sont tenues deux tables rondes et un atelier pratique. Le séminaire fut l'occasion de faire un point d'étape sur le processus de mise en ligne d'un outil de représentation de la couverture et qualité de service mobiles ouvert aux membres du

réseau ainsi que, pour l'UIT, de présenter l'initiative de politique et de régulation pour l'Afrique numérique (PRIDA).

Première table ronde sur « Quels sont les grands enjeux liés à la sécurité pour les réseaux de télécommunications ? »

La première table ronde, présidée par M. Louis Marc SAKALA, Directeur général de l'ARPCE (République du Congo), a été introduite par M. Jean-Jacques MASSIMA-LANDJI, Représentant de l'UIT pour l'Afrique centrale et Madagascar. Ont ensuite témoigné M. Claver MANAMOU, Directeur technique d'Airtel Congo, M. Jacques BEUGRE, Chef du département audit de sécurité des systèmes d'information à l'ARTCI (Côte d'Ivoire), M Saâd EL KHADIRI, Directeur de la Stratégie et de la Réglementation au sein de la Direction Générale de la Sécurité des Systèmes d'Information (Maroc), M. Pascal STEICHEN, Directeur de Security made in Luxembourg et Président du Centre de compétences européen en matière de sécurité (ECCC) et M. Alfred ZONGO NONGOBZANGA, Chef du département réseaux fixe et mobile de l'ARCEP (Burkina Faso).

M. MASSIMA-LANDJI a encouragé la participation des régulateurs francophones, en particulier africains, à la Commission d'études 17 de l'UIT-T sur la sécurité afin de se tenir informés des nouvelles normes de sécurité et d'échanger entre experts. Il a également milité pour la création de CERT (Computer Emergency Response Team) dans tous les pays en développement pour éviter que les efforts de numérisation de la société ne deviennent vains en cas de cyberattaque.

Après avoir détaillé les objectifs de sécurité pour un opérateur de réseau, M. CLAVER a insisté sur l'importance d'identifier les équipements, applications et ressources nécessitant un grand degré de sécurité et, en particulier, leurs faiblesses et vulnérabilités. Il a précisé que le risque zéro n'existait pas mais que les opérateurs se devaient de les réduire avec une bonne connaissance des menaces et une maitrise

des applications et outils de défense et de réaction. Il a également souligné qu'il n'existait pas, au Congo, d'agence de sécurité qui imposait des mesures et protocoles de sécurité et que seule une charte interne à Airtel était actuellement appliquée.

Pour sa part, M. BEUGRE a présenté le cadre réglementaire en Côte d'Ivoire et le rôle de l'ARTCI en tant qu'autorité en charge de la cybersécurité. Il est d'abord revenu sur l'importance de la mise en place d'un plan national de télécommunications en cas d'urgence et de catastrophes naturelles pour améliorer la résilience des réseaux et assurer la continuité de service. Ensuite, ont été évoquées les obligations des opérateurs inscrits dans leurs cahiers des charges concernant la sécurité, le rôle et prérogatives du régulateur ainsi que les mesures pour réduire les risques de cyberattaques. Lors de la session de questions-réponses, il a insisté sur la nécessité d'un cadre de discussions et de dialogue avec les opérateurs afin de fixer les obligations adaptées compte tenu des évolutions techniques et architectures réseaux, obligations faisant l'objet d'un audit par le régulateur.

M. EL KHADIRI a présenté le cadre réglementaire sur la cybersécurité au Maroc, en particulier les obligations imposées aux opérateurs télécom (conservation des données techniques en cas de cyberattaque et transmission de l'information à la DGSSI, possibilité pour la DGSSI de recueillir et analyser les données techniques, installation d'outils de détection dans les réseaux des opérateurs, mise en œuvre de mesures pour détecter les menaces…) et le rôle que joue le régulateur en charge des télécommunications. L'ANRT est membre du comité national stratégique de la cybersécurité et est partie prenante des décisions. En tant que coordinateur pour le secteur des télécommunications, l'Agence désigne les opérateurs d'importance vitale auxquels s'imposent des mesures de cybersécurité spécifiques, telles que l'audit et le recensement des systèmes d'information et leur homologation.

Lors de son exposé, M. STEICHEN a évoqué l'importance des échanges d'information pour mieux se protéger, améliorer ses connaissances sur les nouveaux types d'attaques et aider les autres entités. Il y a, selon lui, trois grandes étapes. Premièrement, un pays ou un secteur doit se doter d'un CERT (il y a en a 10 au Luxembourg) afin qu'il puisse détecter les attaques et réagir le plus rapidement possible. Deuxièmement, les informations techniques doivent remonter vers les structures en charge de la gestion des crises et des communications aux citoyens. Troisièmement, les informations techniques échangées doivent être rendues compréhensibles pour permettre aux pouvoirs politiques, acteurs étatiques, de mener des politiques stratégiques de cybersécurité. C'est le rôle d'agences comme l'ENISA qui publient des rapports, diffusent des informations, sensibilisent les parties prenantes… Ces échanges sur la connaissance des menaces, alimentés par chaque CERT, sont généralement journaliers et automatisés. Les plateformes de partage sont habituellement des outils open source qui peuvent être installés par les instances

publiques en charge de la cybersécurité. Des règles de partage sont définies entre les différentes plateformes.

Enfin, M. ZONGO a évoqué les risques de sécurité physique auxquels font face les opérateurs, que ce soit sur les infrastructures filaires avec le vol de câble ou les travaux de voirie détériorant le réseau, par manque de coordination entre acteurs sur le terrain ou sur les sites mobiles avec notamment la destruction des antennes par les terroristes. Ces derniers s'attaquent aux installations mobiles ce qui engendre pour la population, une isolation accrue, une interruption des communications d'urgence et des transactions financières mobiles, une perte d'emplois notamment dans le secteur informel. Pour les opérateurs, les conséquences sont également dramatiques avec une perte de revenus, une diminution de la couverture, pas de retour sur investissement et des risques pour le personnel sur le terrain. Si sur les quatre premiers mois de 2022, 106 sites ont été détruits, se sont en réalité plus de 630 sites qui étaient inaccessibles, du fait de la configuration du réseau (site modal touché impactant les sites rattachés). Les solutions ont été mises en œuvre dans le pays pour minimiser les risques et sécuriser les réparations. Il s'agit notamment d'accompagner les opérateurs par les forces de défense et de sécurité pour les relèves et maintenances des sites ou encore de sous-traiter les interventions sur le terrain à des sociétés qui maitrisent mieux les localités à risque.

Atelier pratique sur « Présentation de méthodes de contrôle et de prévention de la sécurité des réseaux »

Animée par Mme Tantely JEANS, économiste à l'ILR, sont intervenus M. Didier SIMBA, Fondateur et Président du Club d'experts de la sécurité de l'information en Afrique, pour les propos introductifs, M. Hervé AHOUANGONOU, Directeur général adjoint en

charge de l'exploitation et des projets chez Congo Telecom, M. Guy MAHOWALD, Ingénieur à l'ILR et M. Jean-Louis PERRIER, Directeur de programme pour Africa Cyber Security.

Lors de l'introduction de l'atelier, M. SIMBA a présenté le baromètre de la cybersécurité en Afrique. Selon un sondage réalisé par le CESIA, plus de 64% des entreprises déclarent avoir subi une cyberattaque en 2022. Le vecteur principal d'attaque reste l'hameçonnage ou « fishing » avec des techniques de plus en plus perfectionnées y compris en langue française. Les messageries sur les réseaux sociaux sont également visées par ces attaques qui deviennent virales. Parmi les solutions de protection, les entreprises sécurisent les accès à distance surtout avec la généralisation du télétravail. En tant que responsable de sécurité des systèmes d'information, il pousse les entreprises à intégrer les aspects de sécurité dès le début d'un projet de numérisation. La surface d'attaque augmentant avec la numérisation des entreprises, il propose de mieux gérer les crises et attaques avec la création de cellules de crise internes et de former et sensibiliser les collaborateurs, y compris chez les opérateurs télécoms.

M. AHOUANGONOU a, quant à lui, souligné l'augmentation du risque d'attaque en Afrique, y compris depuis le continent, avec l'augmentation de la bande passante, la numérisation de l'économie et l'utilisation accrue d'internet. Il est nécessaire pour les opérateurs de se doter d'outils de sécurité avec des correctifs semi-automatiques et de l'intelligence artificielle afin de détecter les failles et circonscrire les attaques. Dans le cadre du déploiement de son réseau fixe ou de projets logiciels, Congo Télécom intègre l'aspect sécuritaire dès le début du projet tout en tenant compte des ressources financières limitées.

De son côté, M. MAHOWALD a d'abord présenté l'outil d'analyse des risques basé sur un tableur Excel, développé en 2016 par le régulateur luxembourgeois et utilisé par les opérateurs nationaux. Il recense les différents risques basés sur les menaces, vulnérabilités, impacts pour chaque actif, service de télécommunication et équipement du réseau. Il a insisté sur l'importance du dialogue préalable avec les acteurs du marché afin d'établir une nomenclature commune pour tous les paramètres de l'outil. Il a ensuite évoqué l'outil d'analyse des mesures de sécurité prises par les opérateurs. Cette série de mesures est issue d'une liste élaborée par l'ENISA. Pour chaque mesure, différents niveaux de sécurité sont définis. Sur la base d'un rapport annuel publié par le régulateur, des discussions peuvent s'engager avec les opérateurs afin qu'ils améliorent leur niveau de sécurité. Il a également précisé que les opérateurs notifient au régulateur les incidents via un formulaire sur le site de l'ILR. Enfin, il a présenté un nouveau projet commun avec le régulateur belge, l'IBPT, et cases.lu, initiative du gouvernement luxembourgeois. Cette plateforme unique disponible pour plusieurs secteurs pour une analyse des risques automatisée est un

outil en ligne en libre accès qui peut être utilisé par toute agence ou autorité en charge de la sécurité[1].

Enfin, M. PERRIER a axé sa présentation sur la cybersécurité dans le secteur financier africain. Il a rappelé, en préambule, l'importance de la collaboration entre les différents acteurs et de la remontée des incidents mais aussi le manque de ressources financières et humaines pour sécuriser le secteur. Il a présenté le consortium public-privé à but non lucratif Cyber4Dev qui a lancé le Centre de ressources sur la cybersécurité en Afrique (ACRC), soutenu par la Banque africaine de développement, qui vise, notamment, à améliorer la cyber-résilience des institutions d'inclusion financière et protéger les clients contre les cyber-attaques. Il a souligné l'intérêt pour une collaboration intersectorielle entre les télécoms et le secteur financier, surtout avec la popularité des paiements mobiles en Afrique. M. PERRIER a terminé son intervention par la présentation du concept de centres d'analyse et de partage de l'information (ISAC) et l'intérêt pour la mise en œuvre de ce modèle en Afrique. Ce sont des organisations à but non lucratif qui fournissent une ressource centrale pour la collecte d'informations sur les cybermenaces, généralement entre acteurs d'un même secteur. Ils permettent également le partage bidirectionnel d'informations entre le secteur privé et le secteur public sur les incidents et les menaces, ainsi que le partage d'expériences, de connaissances et d'analyses.

Deuxième table ronde sur « L'évolution des technologies et des architectures réseaux implique-t-elle des nouvelles problématiques de sécurité ? »

[1] https://www.cases.lu/services/monarc_fr.html

Sous la présidence de M. Serge ABITEBOUL, Membre du Collège de l'Arcep (France), ont témoigné à cette table ronde, M. Benjamin MOUANDZA, Directeur des réseaux et des services de communications électroniques à l'ARPCE (République du Congo), M. Pierre-François VANDENHAUTE, Conseiller sécurité à l'IBPT (Belgique), M. Kinvi FOLLY-NOTSRON, Directeur technique chez MTN Congo et M. Alexandre DE OLIVEIRA, Expert en sécurité des télécoms à Post Luxembourg.

La deuxième table ronde a débuté avec l'exposé de M. MOUANDZA centré sur les vulnérabilités de sécurité des cartes SIM selon les différentes technologies mobiles et la nécessité d'identification de l'utilisateur pour réduire les risques. En effet, en absence de compétence sur la cybersécurité, l'approche utilisée par l'ARPCE pour lutter contre les phénomènes de fraude et de piratage, notamment les intercepteurs d'IMSI (IMSI catchers) est d'ordre pénal avec l'identification de la SIM, l'historique des appels et de potentielles poursuites. Il a terminé son exposé sur les risques liés aux services de messagerie sur IP qui ne nécessitent pas de carte SIM. Comme solution, il propose l'usage de cartes SIM avec une adresse IPV6 fixe pour tout type de terminal, y compris les smartphones afin de garantir une identification de l'utilisateur. Les régulateurs pourraient être associés à l'attribution de ces adresses.

Après une présentation du cadre belge de la cybersécurité et du rôle de l'IBPT qui assurer cette compétence réglementaire au niveau national, pour le secteur télécom et numérique (partage d'information, inspection et audit, mise à disposition d'expertise auprès des autorités, gestion de crise, organisation d'exercices d'analyse de risque), M. VANDENHAUTE a évoqué quelques exemples de pannes qui ont eu des conséquences au niveau national. Ces impacts sont de plus en plus importants avec la numérisation des réseaux et l'utilisation des logiciels. Il existe de plus en plus de points de défaillance unique qui causent ces incidents et les réponses à apporter évoluent avec les nouvelles architectures réseaux.

Avec la dépendance croissante des services de base à la population aux infrastructures numériques, les besoins de sécurité, de résilience et de collaboration entre opérateurs augmentent. Par ailleurs, le régulateur devra également augmenter son niveau de surveillance des réseaux. Enfin, il a insisté sur le besoin d'harmonisation de la taxonomie et du vocabulaire entre les différents acteurs, l'instauration d'une relation de confiance entre le régulateur et les opérateurs et l'utilisation d'outils d'analyse de risque similaires entre secteurs.

M. FOLLY-NOTSRON, après avoir détaillé les évolutions des architectures des réseaux mobiles (accès, transport, cœur, edge et cloud, terminaux) et les risques associés, a précisé les mesures prises par MTN Congo et MTN Groupe pour réduire ces risques, que ce soit en interne pour leurs collaborateurs ou sur la partie réseau pour les clients de l'opérateur.

Enfin, M. DE OLIVEIRA a présenté les évolutions du réseau de Post Luxembourg et l'approche prise par l'opérateur pour reconstruire son réseau de télécommunications de façon sécurisée. En effet, avec la complexité des interactions entre les différentes technologies (de la 2G à la 5G, l'IPTV, les liens satellitaires…) et la virtualisation des équipements, la surface d'attaque devient gigantesque et sécuriser le réseau devient pratiquement mission impossible. Dès lors, l'opérateur a pris la décision de revoir toute son architecture réseau et de migrer toutes les technologies sur ce nouveau réseau nativement hautement sécurisé et basé sur un réseau en nuage souverain. Une revue complète des équipements a été nécessaire et des tests offensifs pour déceler les failles et vulnérabilités des logiciels et équipements sont réalisés régulièrement. Selon lui, un des grands défis pour les opérateurs avec la virtualisation des réseaux et le cycle très court des logiciels (mise à jour toutes les 2 semaines) est d'assurer la maîtrise, la souveraineté et le contrôle en interne du réseau. C'est la raison pour laquelle la formation des ingénieurs télécoms est essentielle.

2. 20e réunion annuelle sur « Enjeux et moyens d'améliorer la résilience et la sécurité des réseaux de télécommunications »

À l'invitation de l'Autorité de régulation des technologies de l'information et de la communication (ICTA) de la République de Maurice et de l'Institut Luxembourgeois de Régulation (ILR), la 20e réunion annuelle du réseau s'est tenue les 10 et 11 novembre à l'hôtel InterContinental Balaclava Fort, en République de Maurice.

Près de 110 participants, représentant 26 autorités de régulation, membres de Fratel, des institutions internationales (UIT, Internet Society), des administrations, des universitaires et des acteurs du secteur ont assisté, soit en présentiel, soit en virtuel, à la réunion qui avait pour thème « Enjeux et moyens d'améliorer la résilience et la sécurité des réseaux de télécommunications ». Cette thématique a été déclinée en trois tables rondes.

La réunion annuelle a été ouverte par MM. Pravind JUGNAUTH, Premier Ministre de la République de Maurice, Dick Christophe NG SUI WA, Président de l'ICTA et Luc TAPELLA, Directeur de l'ILR et Président 2022 de Fratel.

La réunion annuelle fut l'occasion de présenter les travaux du groupe de travail sur l'outil de représentation de la couverture et de la qualité de service mobile et les formations disponibles pour les membres de Fratel, comme le Mastère RegNum

organisé par Télécom Paris et l'initiative de Team Europe soutenue par PTS, le régulateur suédois, pour le renforcement des capacités réglementaires en Afrique subsaharienne.

Le plan d'action 2023 y a été adopté et un nouveau comité de coordination a été nommé. Il sera composé pour 2023 de M. Az-el-Arabe HASSIBI, Directeur général de l'ANRT du Maroc (président), de M. Luc TAPELLA, Directeur de l'ILR du Luxembourg et de Louis-Marc SAKALA, Directeur général de l'ARPCE de la République du Congo (vice-présidents).

Première table ronde sur « Comment éviter les risques de congestion des réseaux ? »

Cette première table ronde a été modérée par Mme Mana AIDARA de l'ARTP du Sénégal. Après une introduction de M. Serge ZONGO de l'UIT (en ligne), sont intervenus Mme Laure DE LA RAUDIERE, Présidente de l'Arcep France, M. Jean-Jacques SAHEL, Responsable de la politique d'information pour l'Asie-Pacifique à Google (en ligne) et M. Avinash CHETTIAR, Directeur technique d'Emtel Maurice.

En introduction, M. ZONGO a notamment évoqué la plateforme de l'UIT « REG4COVID » et l'initiative Connect2Recover. Cette dernière a pour objectif de renforcer l'infrastructure numérique et les écosystèmes numériques des pays bénéficiaires de manière à ce qu'ils s'adaptent à l'après COVID-19 et restent résilients en période de catastrophes naturelles. De son côté, la plateforme recense les initiatives du secteur privé, les mesures politiques et réglementaires et pratiques que les pays ont prises pour s'assurer que les communautés restent connectées et en sécurité pendant la pandémie via les télécommunications. Les membres de l'UIT ont ainsi pu partager et tirer parti des différentes expériences de par le monde.

Mme de LA RAUDIERE et M. CHETTIAR ont présenté les mesures prises pour limiter les risques de congestion des réseaux respectivement en France et à Maurice lors de la crise de COVID-19. La présidente de l'Arcep a ensuite exposé les leçons tirées. Cette crise a en effet révélé, d'une part, l'importance de la connectivité partout, pour tous et de qualité et, d'autre part, les inégalités d'accès des citoyens aux services de télécommunications. Mme de LA RAUDIERE a en outre souligné la nécessité d'une montée en débit des infrastructures au travers du déploiement de la fibre et de la 5G. Cette période a aussi permis de montrer que le règlement européen sur l'internet ouvert pouvait s'appliquer en toutes circonstances.

De son côté, le représentant d'Emtel a mis en avant les partenariats avec les fournisseurs de contenu et d'applications (FCA) afin de livrer les contenus les plus populaires, de la façon la plus efficace qui soit sans congestionner les liens internationaux.

Enfin, M. SAHEL a évoqué le rôle de Google pour éviter les congestions notamment grâce aux partenariats avec les opérateurs télécoms. L'action de Google passe aussi par des investissements dans des infrastructures telles que les câbles sous-marins, les centres de données et les réseaux de diffusion de contenu (CDN). Le groupe américain souhaite ainsi pour réduire les coûts et amener les contenus au plus près des utilisateurs. M. SAHEL a aussi souligné que Google s'appuie aussi sur les innovations et les travaux de normalisation pour améliorer l'encodage et la compression vidéo permettant de réduire la quantité de données utilisées par les consommateurs et d'améliorer leur expérience.

Lors des discussions, les problématiques du financement des réseaux par les fournisseurs de contenus et d'application et de la couverture mobile dans les zones peu denses ont été largement abordées.

Deuxième table ronde sur « Comment améliorer la résilience des réseaux et quelles mesures pour répondre aux évènements extrêmes ? »

La deuxième table ronde présidée par Mme Tantely JEANS de l'ILR, a été introduite par M. Eric VEVE. Au cours de cette table ronde, sont intervenus M. Louis Marc SAKALA, Directeur général de l'ARPCE de la République du Congo, M. Hervé GUEDEGBE, Secrétaire exécutif de l'ARCEP du Bénin (en ligne), M. Gauthier NANOUX, Directeur de l'exploitation chez Axione (en ligne), M. Vincent ROGER-MACHART, Représentant du Cercle CREDO et M. Amreesh PHOKEER, Expert en mesure de l'internet à l'Internet Society.

M. VEVE dans son exposé introductif, est d'abord revenu sur la définition de résilience et son importance pour les gouvernements, l'économie et la société en général qui sont de plus en plus dépendants du bon fonctionnement des réseaux. Il a ensuite exposé les responsabilités des opérateurs, des États et des régulateurs. Il a notamment suggéré que les opérateurs, au-delà des mesures sur la disponibilité et la qualité de service se voient imposer une double obligation de permanence et de sécurité. De son côté, l'État doit, à travers des textes, protéger, inciter à la redondance, coordonner, sanctionner, voire prioriser les trafics en cas de gestion de crise. Enfin, il a exhorté les régulateurs à exercer leurs pouvoirs de contrôle et d'enquête sur la disponibilité des services et si besoin de sanction.

Ensuite, sont intervenus MM. ROGER-MACHART et NANOUX sur les aspects techniques pour améliorer la résilience des réseaux fixes. Après avoir présenté les fiches du CREDO[2] sur la pérennité des réseaux en fibre optique et la méthode AMDEC (analyse des modes de défaillance, de leurs effets et de leur criticité) pour mesurer la résilience des réseaux optiques, M. ROGER-MACHART a posé la question des risques

[2] Association des métiers et expertises pour le très haut débit en France. Fiches du Credo sur la pérennité des réseaux optiques https://www.cercle-credo.com/publications/

de la mutualisation des réseaux et en particulier dans les nœuds de raccordement optique (NRO) et armoires de rue pour la qualité et résilience du réseau. De son côté, M. NANOUX a présenté l'étude d'InfraNum[3] sur la résilience des infrastructures numériques. Cette étude a pour objectif de recenser les aléas pouvant impacter la continuité de service des réseaux de fibre optique jusqu'à l'abonné (FttH), d'évaluer la criticité de ces aléas, d'identifier les moyens d'anticipation et de limitation des risques ex ante et de proposer des axes d'amélioration en matière de gestion de crise. Lors des discussions, il a évoqué les travaux mis en place par Axione en partenariat avec des sociétés spécialisées pour prédire les risques liés aux aléas climatiques (inondations, tempêtes, incendies…) grâce à des algorithmes d'intelligence artificielle et les mesures pour y répondre comme l'élévation ou le déplacement des équipements de réseau.

M. PHOKEER a, quant à lui, présenté l'indice de résilience de l'internet[4] développé par l'Internet Society. Cet indice, actuellement appliqué au niveau des pays africains, permet de mesurer la performance d'un pays par rapport aux principaux piliers d'un écosystème Internet robuste, à savoir les infrastructures, la performance, la sécurité et l'adéquation du marché. Un ensemble de 30 indicateurs permet de classer les pays selon leur niveau de résilience.

Enfin, les régulateurs de la République du Congo et du Bénin ont évoqué les mesures réglementaires prises dans leurs pays respectifs.

M. SAKALA a centré son intervention sur trois points : la nécessité de sensibiliser toutes les parties prenantes y compris les acteurs des autres secteurs au besoin de résilience, l'importance de cartographier les risques et la mise en place de mesures de prévention adéquates. Au Congo, un club des DSI des grandes entreprises publiques et privées a été mis en place pour partager les bonnes pratiques. Sur la cartographie, il a insisté sur les risques liés à l'énergie (délestage, pénuries de carburant), la gestion des infrastructures aériennes très présentes en Afrique et les risques de sabotage terroriste. En termes de prévention, il a été notamment prévu que les fournisseurs satellitaires prennent le relais en cas de coupure dans des zones rurales afin qu'elles restent couvertes.

M. GUEDEGBE est revenu sur le cadre réglementaires béninois en particulier les compétences attribuées à l'ARCEP pour s'assurer de la disponibilité et continuité des services par les opérateurs télécoms et les obligations des opérateurs. Il a ensuite exposé les mesures de régulation prises pour améliorer la résilience telles que la mise

[3] Fédération qui regroupe plus de 220 industriels des infrastructures numériques en France. L'étude https://infranum.fr/wp-content/uploads/2022/06/E%CC%81tude-re%CC%81silience-nume%CC%81rique.pdf

[4] https://pulse.internetsociety.org/fr/resilience

en œuvre des conditions transparentes de partage d'infrastructures, le suivi des accords d'itinérance nationale ou encore l'ouverture du service de vente de capacité aux opérateurs mobiles en cas d'indisponibilité chez l'opérateur titulaire de la licence d'infrastructure fixe. Il a terminé son propos par les futurs travaux au niveau national comme l'adoption de la politique de protection des infrastructures d'information critiques du Bénin, la mise en œuvre de la stratégie nationale de sécurité et la mise en place, par l'ARCEP, du plan de continuité des activités (PCA) en cas de survenance d'événements imprévus.

Troisième table ronde sur « Comment assurer l'intégrité et la confidentialité des réseaux et services ? »

Présidée par M. Louis-Marc SAKALA, et introduite par le Professeur Kavé SALAMATIAN, Professeur à l'université de Savoie, la troisième table ronde était dédiée à l'intégrité et la confidentialité des réseaux et services de télécommunications. Ont témoigné, M. Tomi FRASHERI, Président de l'AKEP d'Albanie (en ligne), M. Jérôme LOUIS, Directeur du département Ingénierie et M. Amrit CHUTTOORGOON, Directeur IT à l'ICTA, le régulateur mauricien et M. Thys KAZAD, Responsable de la politique publique pour l'Afrique, Accès et Connectivité chez Facebook.

Dans son exposé introductif, M. SALAMATIAN a insisté sur les aspects stratégiques, économiques et politiques de la cybersécurité qui n'est pas seulement une problématique technique, notamment en cas d'autorisation d'accessibilité et de disponibilité d'un service ou équipement. Il importe aux pays de se doter d'un cadre

de réflexion stratégique sur la sécurité informatique de leurs infrastructures dont ils sont de plus en plus dépendants. Il est nécessaire de détecter les forces en présence (techniciens, ingénieurs, universités et centres de formation) et les objectifs à protéger mais aussi à atteindre. Il est revenu sur les avancées du cadre européen en la matière et notamment les directives sur la sécurité des réseaux et des systèmes d'information NIS 1 et NIS 2 et l'obligation de moyen désormais imposée à un grand nombre d'acteurs et pas uniquement aux opérateurs d'importance vitale.

Dans son intervention, le président de l'AKEP a insisté sur les impacts de la cyberguerre sur les infrastructures numériques de son pays. Le pays subit depuis le 15 juillet 2022 une agression cybernétique lancée depuis un pays non ami qui a pour conséquence de bloquer et crypter les serveurs de l'administration, des services publics et d'effacer les disques durs. Des défis de nature politique (mise à niveau des agences spécialisées avec des moyens opérationnels renforcés, prise de conscience de la part des Gouvernements sur le bon usage de la souveraineté dans ce domaine, mise en place d'une plateforme d'état-major de la sécurité cybernétique) et réglementaire (adaptation intellectuelle et technique des régulateurs télécom, participation active à l'inventaire des infrastructures critiques suivant des normes élevées, sensibilisation des fabricants et des fournisseurs d'équipements technologiques, intervention par des règlements techniques pour obliger les opérateurs à plus de responsabilité dans le choix des équipements…) sont à relever.

M. LOUIS a présenté le cadre réglementaire de la gestion des infrastructures d'information critiques (IIC) à Maurice avec notamment le rôle et le fonctionnement du Comité National sur la Cybersécurité et celui des différents régulateurs. Le Comité est notamment chargé de conseiller le gouvernement et mettre en œuvre sa politique en matière de cybersécurité et cybercriminalité et de cordonner et faciliter la mise en place d'un cadre de protection pour les infrastructures d'information critiques. L'ICTA et les autres régulateurs sectoriels (eau, énergie, finances…) doivent mettre en place des directives pour les opérateurs d'IIC afin notamment qu'ils procèdent à une évaluation des menaces, vulnérabilités, risques et la probabilité d'une cyberattaque, mettent en œuvre la politique de sécurité de l'information, effectuent une évaluation périodique des risques de sécurité informatique, mettent en œuvre une politique de signalement des incidents ou encore élaborent un programme de sensibilisation à la sécurité. Quant à la présentation de M. CHUTTOORGOON, elle était axée sur la sécurité informatique, y compris au sein de l'ICTA. En tant que responsable informatique, il a insisté sur la nécessité des analyses coûts/bénéfices pour le

lancement de nouveaux services numériques, notamment le coût financier lié à la cybersécurité et celle de faire des tests de vulnérabilité.

Enfin, M. KAZAD a évoqué le projet de câble sous-marin 2Africa qui sera le premier à faire le tour du continent africain. Outre l'augmentation de capacité attendue et le système d'accès ouvert qui caractérisent ce projet, la fiabilité et la sécurité accrues par rapport aux autres câbles ont été mises en avant. En effet, la route choisie a été spécialement conçue pour maximiser la disponibilité, en évitant les endroits où les perturbations sous-marines sont connues en augmentant la profondeur d'enfouissement des câbles de 50 % par rapport aux anciens systèmes.

3. Travaux sur la couverture et qualité de service mobiles

Outil ouvert aux membres sur la représentation de la couverture et la qualité de service mobiles : élaboration d'un cahier des charges

Dans le cadre du plan d'action 2020 du réseau Fratel adopté lors de la réunion annuelle de Bucarest, il a été convenu d'examiner la faisabilité d'un outil ouvert aux membres de Fratel sur la représentation de la couverture et la qualité de service mobiles.

Rappel du Processus

Pour mener à bien ce projet, un groupe de travail composé d'experts de onze autorités de régulation a été créé, présidé par M. Stéphane YAMEOGO de l'ARCEP du Burkina Faso, autorité présidente 2020 du réseau, sous le pilotage du comité de coordination. En 2021, cinq autres autorités ont rejoint le groupe.

Dans un premier temps, le groupe de travail a rédigé un rapport sur la faisabilité d'un tel outil reprenant les besoins des autorités, une description de scénarios, une analyse et des recommandations. Il a été présenté à l'ensemble des membres du réseau en vue de décider de la suite des travaux lors de la réunion annuelle du 3 décembre 2020. Par ailleurs, l'Agence française de développement, qui soutient cette initiative, a recruté la société de conseil Tactis en appui au groupe de travail afin d'accompagner le projet lors de la phase initiale d'examen de la faisabilité d'un outil et recensement des besoins des autorités.

Lors de la réunion annuelle 2020, les orientations proposées par le comité de coordination sur la base du rapport du groupe de travail et des deux livrables de Tactis ont été approuvées.

Travaux en 2022

Dans le cadre du programme européen « Programme UE-ACP de réponse numérique à la crise Covid-19 », l'AFD s'est proposée pour accompagner Fratel dans le projet. Ce soutien vient dans la continuité de la collaboration entre Fratel et l'AFD ces dernières années au sujet des données de couverture et de qualité de service (voir publication et site…).

L'Agence a lancé un appel d'offre le 17 août 2022 pour sélectionner le prestataire. Cet appel d'offre incluait les termes de référence élaborés par le groupe de travail de Fratel. Le prestataire a été sélectionné fin 2022. La solution doit permettre la mise à disposition d'informations et de consultation des données sur la couverture et les

données de qualité de services pour le grand public à travers un portail web. Elle doit également prévoir une base de données hébergeant les données de qualité de service et de couverture mobiles aisément exploitable, accessible et consultable par les membres du réseau habilités. L'outil devrait être ouvert à tout membre du réseau.

Le prestataire choisi va mener les travaux préparatoires avec les autorités qui se sont portées volontaires pour une mise en ligne de l'outil prévue en 2023.

4. Promotion de la formation des membres du réseau

Le mastère spécialisé (MS) en régulation de l'économie numérique (RegNum) est organisé et délivré par Telecom Paris (https://regnum-ms.com).

Au sein de ce diplôme de niveau supérieur RegNum, deux Badge (Brevet d'aptitude délivré par les grandes écoles) font partie de la formation, et existent indépendamment :

- le Badge RegTel consacré à la régulation du secteur des communications électroniques, notamment aux instruments de la régulation (interconnexion, service universel, gestion du spectre…) ;
- le Badge RegFep spécifique à la régulation de la finance électronique et des postes.

Le Badge RegInt a été supprimé en 2021.

Sur les 7 sessions organisées sur 3 thèmes différents (régulation des communications électroniques, régulation de l'internet et des contenus, régulation des activités financières et postales), les participants au Mastère doivent en choisir 6.

Prenant la suite du Badge ouvert en 2005, ce Mastère a démarré en janvier 2014 avec 32 participants. En 2022, la cinquième promotion du Mastère avait admis 24 participants et les soutenances ont été organisées en mars 2022 à Abidjan tandis que la 6e promotion comptait 31 élèves.

Le Mastère s'appuie sur sept partenaires essentiels :

- l'Autorité de régulation des communications électroniques et des postes du Burkina Faso ;
- l'Autorité française de régulation des communications électroniques, des postes et de la distribution de la presse ;
- l'Autorité de régulation des télécommunications de Côte d'Ivoire ;
- la Commission nationale de l'informatique et des libertés de France ;
- L'Association francophone des autorités de protection des données personnelles ;
- l'École Multinationale Supérieure des Postes d'Abidjan ;
- et Telecom Paris.

La formation se déroule sur deux ans et compte 390 heures de cours réparties sur six sessions de deux semaines chacune, et une semaine de soutenance des thèses professionnelles. Chaque semaine comporte 30 heures partagées entre des cours magistraux, des études de cas et des débats. En temps normal, sur les deux ans que

dure le Mastère, trois sessions se déroulent à Ouagadougou, trois à Paris et une à Abidjan. Cependant, cette année, en raison de la situation sanitaire mondiale, sur les 4 sessions du Mastère prévues, la moitié s'est tenue en visio-conférence. En 2022, la session A initialement prévue à Ouagadougou (Burkina Faso) a été déplacée à Abidjan avec le concours de l'EMSP en raison de la situation politique burkinabé.

Le mastère est destiné aux cadres en charge des activités liées à la régulation de l'économie numérique, notamment dans les pays de l'Afrique francophone subsaharienne :

- cadres des instances de régulation dans le numérique ;
- cadres des opérateurs de réseaux ou de prestataires de services de communications électroniques, de diffuseurs audiovisuels ;
- cadres des directions centrales des ministères en charge des sujets du numérique ;
- cadres des prestataires de services (cabinets de conseil, d'avocats, …).

Les candidats au Mastère doivent avoir au minimum un niveau Bac+5, ou Bac+4 et 3 ans d'expérience de la régulation dans le secteur du numérique, alors que pour les Badges, un niveau de Bac+4 ou Bac+3 et 3 ans d'expérience est exigé.

Des mémoires d'étudiants sélectionnés par Télécom Paris sont disponibles sur le site de Fratel à cette adresse : https://www.fratel.org/mastere-regnum/

Plusieurs régulateurs de Fratel contribuent également à la formation des professionnels dans le secteur des télécommunications en français. Par exemple, L'ANRT du Maroc a ouvert, depuis quelques années, l'accès au cycle Ingénieur de l'Institut National des Postes des Télécommunications (INPT) aux fonctionnaires et cadres africains exerçant au sein des administrations et établissements publics de leurs pays.

L'Union internationale des télécommunications a présenté l'Initiative de politique et de régulation pour l'Afrique numérique (PRIDA), initiative conjointe de l'Union africaine (UA), de l'Union européenne (UE) et de (UIT) lors du séminaire et PTS, le régulateur suédois l'initiative de Team Europe pour le renforcement des capacités réglementaires en Afrique subsaharienne lors de la réunion annuelle.

5. Autres activités du réseau

Réunion des membres de Fratel en marge du Mobile World Congress de Barcelone

A l'occasion du Mobile World Congress de Barcelone qui s'est tenu du 28 février au 3 mars, les membres de Fratel, présents sur place, ont été invités à une visite commentée sur la sécurité et résilience des réseaux, thème des travaux de Fratel de cette année.

Réunion des membres de Fratel en marge de la Conférence de Plénipotentiaires de l'UIT

Une réunion entre les autorités présentes lors de la Conférence de Plénipotentiaires de l'UIT et d'autres en ligne a été organisée le 28 septembre à Bucarest. Le Secrétariat a pu faire le point sur le plan d'action 2022.

Réunion entre membres des réseaux Fratel et de Refram organisée par le CRTC dans le cadre de l'IRF de l'IIC

Le 2 novembre 2022, en marge du Forum international des régulateurs qui s'est tenu à Ottawa, les pays membres de Fratel et de Refram ont participé à un atelier sur le développement de compétences en matière de données pour les régulateurs. L'atelier était modéré par Mme Alicia Barin, membre du CRTC avec la participation de l'ILR du Luxembourg et l'ARPT de Guinée d'une part, et l'Arcom de France et l'HACA du Maroc d'autre part. Les participants ont pu échanger entre eux et avec la salle sur les défis et opportunités liées à la collecte, analyse et publication des données. Il a aussi été question du développement des compétences ainsi que de la collaboration avec de nouveaux acteurs et régulateurs d'autres secteurs.